**IP-адресация**

**Введение**

Адресация — это основная функция протоколов сетевого уровня, которая позволяет узлам обмениваться данными вне зависимости от того, находятся ли узлы в одной или нескольких сетях. IP-протокол версии 4 (IPv4) и IP-протокол версии 6 (IPv6) обеспечивают иерархическую адресацию пакетов, которые служат для передачи данных.

Проектирование, внедрение и управление эффективным планом IP-адресации обеспечивают надёжность и эффективность работы сетей.

В этой главе подробно рассматривается структура IP-адресов и их применение при создании и тестировании сетей и подсетей, работающих с IP-сетями.

**IP-адресация**

**Введение**

**Всеобъемлющий Интернет (IoE)**

Если изучение природы, дорожного движения, транспортного сообщения, сетевых технологий и космоса зависят от обмена цифровой информацией, каким образом пункт назначения будет определять информацию, передаваемую источником?

В этом задании вам необходимо подумать не только о содержании информации, которая определяется в мире Всеобъемлющего Интернета, но и о способах её адресации!

* Ознакомьтесь с информацией о Всеобъемлющем Интернете (IoE) в блоге или на новостном ресурсе Джона Чемберса: <http://blogs.cisco.com/news/internet-of-everything-2>. Просмотрите видеоролик, расположенный в центре страницы.
* После этого посетите главную страницу Всеобъемлющего Интернета: <http://www.cisco.com/web/tomorrow-starts-here/index.html>. Нажмите на интересующую категорию.
* Просмотрите видео, блог или документ в формате .pdf, которые относятся к выбранной вами категории IoE.
* Напишите 5 комментариев или вопросов о том, что вы увидели или прочитали и поделитесь ими с классом.

[Работа в аудитории: Всеобъемлющий Интернет (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.0.1.2%20Activity%20-%20Modeling%20the%20Internet%20of%20Everything%20_IoE.pdf)

# Сетевые IPv4-адреса

## Структура IPv4-адресов

Чтобы понять, как работают устройства в сети, необходимо взглянуть на адреса и другие данные так, как это делают устройства — то есть в двоичном представлении. Двоичное представление информации осуществляется с помощью только единиц и нулей. Компьютеры взаимодействуют с использованием двоичных данных. Двоичные данные можно использовать для представления разных видов информации. Например, когда пользователь набирает символы на клавиатуре, они отображаются на экране в удобном для чтения и понимания виде. Однако компьютер преобразует каждый символ в серии двоичных цифр для удобства хранения и передачи. Для преобразования этих символов компьютер использует Американский стандартный код для обмена информацией (ASCII).

Например, буква «А» в коде ASCII представлена в виде бита 01000001. В свою очередь, буква нижнего регистра «a» представлена в виде бита 01100001. Используйте преобразователь ASCII на рисунке 1 для преобразования символов в двоичную форму.

Хотя в целом людям не нужно углубляться в преобразование символов, необходимо понимать, как двоичные числа используются в IP-адресации. Каждое устройство в сети должно быть уникально представлено с помощью двоичного адреса. В IPv4-сетях этот адрес представлен с помощью серии из 32 бит (единиц и нулей). Затем на сетевом уровне пакеты включают в себя эту уникальную идентификационную информацию для систем источника и назначения. Таким образом, в IPv4-сети каждый пакет включает в себя 32-битный адрес источника и 32-битный адрес назначения в заголовке уровня 3.

Большинству людей сложно понять строку из 32 бит и тем более сложно её запомнить. Поэтому вместо двоичной системы для представления IPv4-адресов мы используем десятичный формат с разделительными точками. Это означает, что мы рассматриваем каждый байт (октет) в виде десятичного числа от 0 до 255. Чтобы понять этот принцип работы, необходимо уметь преобразовывать двоичные представления в десятичный формат.

**Позиционное представление чисел**

Чтобы научиться преобразовывать двоичные представления в десятичные, нужно понимать математические основы позиционной системы исчисления. В позиционном представлении цифра представляет разные значения в зависимости от своего расположения. Основанием системы позиционного представления является корень. В десятичной системе корнем является 10. Корень для двоичной системы — 2. Термины «основание» и «корень» можно использовать как синонимы. Если точнее, то значение, представленное цифрой, умножается на основание, или корень, который представлен позицией, занимаемой цифрой. Несколько примеров помогут вам лучше понять, как работает эта система.

Для десятичного числа 192 единица (1) представляет значение 1\*10^2 (1 раз 10 на 2). Единица находится на позиции сотни (100). Позиционное представление передаёт эту позицию, как основание^2, поскольку основание, или корень, — это 10, а степень — это 2. Цифра 9 представлена как 9\*10^1 (9 раз 10 на 1). Позиционное представление десятичного числа 192 показано на рисунке 2.

С помощью позиционного представления в системе исчисления с корнем 10 число 192 представлено следующим образом:

192 = (1 \* 10^2) + (9 \* 10^1) + (2 \* 10^0)

или

192 = (1 \* 100) + (9 \* 10) + (2 \* 1)

# Сетевые IPv4-адреса

## Структура IPv4-адресов

В протоколе IPv4-адреса представлены 32-битными числами. Однако для упрощения использования двоичные схемы, представляющие IPv4-адреса, выражаются десятичными представлениями с разделительными точками. Сначала каждый байт (8 бит) 32-битной комбинации (октета) отделяется точкой. Он называется октетом потому, что каждое десятичное число представляет один байт или 8 бит.

Двоичный адрес:

11000000 10101000 00001010 00001010

выражается в виде разделённых точками десятичных чисел:

192.168.10.10

На рисунке 1 нажимайте каждую кнопку, чтобы увидеть, как 32-битный двоичный адрес представлен десятичными октетами с разделительными точками.

Но как определяются их фактические десятичные эквиваленты?

**Двоичная система исчисления**

Корнем для двоичной системы исчисления является 2. Таким образом, каждое расположение представляет значение в степени 2. В 8-битных двоичных числах расположения представляют следующие суммы:

2^7 2^6 2^5 2^4 2^3 2^2 2^1 2^0

128 64 32 16 8 4 2 1

Система с основанием 2 располагает только двумя цифрами: 0 и 1.

Когда мы представляем байт в виде десятичного числа, то единица означает, что расположение представляет сумму. Если же у нас цифра ноль, то суммы нет, как показано на рисунке 1.

Рисунок 2 демонстрирует представление десятичного числа 192 в двоичном формате. Единица (1) в определённой позиции означает, что мы прибавляем это значение к общей сумме. Ноль (0) означает, что мы не добавляем это значение. Двоичное число 11000000 имеет 1 в позиции 2^7 (десятичное значение 128) и 1 в позиции 2^6 (десятичное значение 64). Оставшиеся биты — это нули, поэтому не нужно добавлять соответствующие десятичные значения. При сложении 128 + 64 получаем сумму 192, десятичный эквивалент которой 11000000.

Рассмотрим другие два примера.

**Пример 1. Октет, содержащий все единицы: 11111111**

Единица в каждой позиции означает, что мы прибавляем значение к этой позиции до общей суммы. Если в сумме все единицы, то значения каждой позиции включены в общую сумму; таким образом, значение всех единиц равняется 255.

128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255

**Пример 2. Октет, содержащий все нули: 00000000**

Ноль в каждой позиции указывает на то, что значение для данной позиции не включено в сумму. Если в каждой позиции стоит ноль, то вся сумма равняется 0.

0 + 0 + 0 + 0 + 0 + 0 + 0 + 0 = 0

Разные комбинации единиц и нулей создают различные десятичные значения.

**Сетевые IPv4-адреса**

**Структура IPv4-адресов**

Каждый октет состоит из 8 бит, каждый бит имеет значение 0 или 1. Четыре группы из 8 бит имеют одну серию допустимых значений от 0 до 255 включительно. Значения каждого размещения бита справа налево: 1, 2, 4, 8, 16, 32, 64 и 128.

Чтобы определить значение октета, нужно сложить значения позиций, в которых присутствует двоичная единица.

* Нулевые позиции в сложении не участвуют.
* Если все 8 бит имеют значение 0, 00000000, значение октета равно 0.
* Если все 8 бит имеют значение 1, 11111111, значение октета равно 255 (128+64+32+16+8+4+2+1).
* Если среди 8 бит есть и единицы, и нули, то значения прибавляются вместе. Например, значение октета 00100111 составляет 39 (32+4+2+1).

Таким образом, значение каждого из четырёх октетов находится в диапазоне от 0 до 255.

Используя 32-битный IPv4-адрес, 11000000101010000000101000001010, преобразуйте двоичное представление в десятичное с разделительными точками, с помощью следующих действий.

**Шаг 1.** Разделите 32 бита на 4 октета.

**Шаг 2.** Преобразуйте каждый октет в десятичное число.

**Шаг 3.** Добавьте «точку» между десятичными числами.

На рисунке нажмите кнопку «Воспроизведение», чтобы увидеть, как двоичный адрес преобразуется в десятичный с разделительными точками.

# Сетевые IPv4-адреса

## Структура IPv4-адресов

Необходимо уметь преобразовывать числа не только из двоичной системы в десятичную, но и наоборот.

Поскольку мы представляем IPv4-адреса в десятичном формате с разделительными точками, нам необходимо изучить только процесс преобразования 8-битного двоичного значения в десятичное от 0 до 255 для каждого октета в IPv4-адресе.

Чтобы начать процесс преобразования, мы определяем, является ли десятичное число равным или больше, чем наибольшее десятичное значение, представленное самым старшим разрядом. В наивысшей позиции мы определяем, является ли октет равным или больше числа 128. Если октет меньше 128, то мы ставим 0 в позиции бита для десятичного значения 128 и переходим к позиции бита десятичного значения 64.

Если октет в позиции бита десятичного значения 128 больше или равен 128, то мы ставим 1 в позиции бита для десятичного значения 128 и вычитаем 128 из значения преобразуемого октета. Затем мы сравниваем остаток данной операции со следующим по меньшинству значением — 64. Аналогичное действие мы применим ко всем оставшимся позициям бита.

Нажимайте на рисунки от 1 до 6, чтобы увидеть процесс преобразования числа 168 в двоичный эквивалент 10101000.

# Сетевые IPv4-адреса

## Структура IPv4-адресов

Следуйте инструкциям по преобразованию, представленным на рисунках, чтобы понять, как IP-адрес преобразуется в двоичную форму.

Рисунок 1. Преобразование 192 в двоичный формат.

Рисунок 2. Преобразование 168 в двоичный формат.

Рисунок 3. Преобразование 10 в двоичный формат.

Рисунок 4. Преобразование 10 в двоичный формат.

Рисунок 5. Объединение преобразованных октетов, начиная с первого.

# Сетевые IPv4-адреса

## Маска подсети IPv4

Понимание двоичной системы исчисления особенно важно, чтобы установить, находятся ли два узла в одной и той же сети. Как вы помните, IP-адрес является иерархическим адресом, который состоит из двух частей: сетевой и узловой. Определяя ту или иную часть, необходимо обращать внимание не на десятичное значение, а на 32-битный поток. В 32-битном потоке одна часть битов составляет сеть, а другая — узел.

Биты в сетевой части адреса должны быть одинаковыми для всех устройств, которые находятся в одной и той же сети. Биты в узловой части адреса должны быть уникальными, чтобы можно было определить конкретный узел в сети. Независимо от того, совпадают ли десятичные числа в двух IPv4-адресах, если два узла имеют одну битовую комбинацию в определённой сетевой части 32-битного потока, то эти два узла находятся в одной и той же сети.

Но как узлы определяют, какая из частей 32-битного потока является сетевой, а какая — узловой? Для этого используется маска подсети.

При настройке IP-узла ему присваивается не только IP-адрес, но и маска подсети. Как и IP-адрес, маска состоит из 32 бит. Она определяет, какая часть IP-адреса относится к сети, а какая — к узлу.

Маска сравнивается с IP-адресом побитно, слева направо. В маске подсети единицы соответствуют сетевой части, а нули — адресу узла. Как показано на рисунке 1, маска подсети создаётся путём размещения единицы (1) в каждой позиции бита, представляющей сетевую часть, и размещения нуля (0) в каждой позиции бита, которая представляет узловую часть. Обратите внимание, что маска подсети не содержит сетевую или узловую часть IPv4-адреса; она только сообщает компьютеру, в каком месте искать эти части в данном IPv4-адресе.

Как и IPv4-адреса, маска подсети для простоты использования представлена в десятичном формате с разделительными точками. Маска подсети настроена на узловом устройстве в сочетании с IPv4-адресом и необходима для того, чтобы узел мог определить, к какой сети он принадлежит. На рис. 2 показаны допустимые маски подсети для IPv4-октета.

# Сетевые IPv4-адреса

## Маска подсети IPv4

**Сетевые префиксы**

Длина префикса — это ещё один способ представления маски подсети. Длина префикса означает количество бит, установленных на единицу (1) в маске подсети. Она обозначается наклонной чертой вправо («/»), после которой идёт набор единиц. Например, если маска подсети 255.255.255.0, то в двоичной версии маски подсети на единицу настроены 24 бита, поэтому длина префикса составляет 24 бита или /24. Префикс и маска подсети — это разные способы представления одного и того же — сетевой части адреса.

Сетям не всегда назначается префикс /24. В зависимости от количества узлов в сети префикс может отличаться. Различный префикс приводит к изменению диапазона узлов и широковещательного адреса для каждой сети.

На рисунках ниже показано, как различные префиксы используют один и тот же адрес 10.1.1.0. На рис. 1 показаны префиксы от /24 до /26. На рис. 2 показаны префиксы от /27 до /28.

Обратите внимание, что сетевой адрес может не меняться, но диапазон узлов и широковещательный адрес отличаются в зависимости от длины префикса. На рисунках видно, что количество узлов, к которым можно адресоваться, также меняется.

**Сетевые IPv4-адреса**

**Маска подсети IPv4**

В диапазоне адресов каждой сети IPv4 существуют три типа адресов:

* Сетевой адрес
* Узловые адреса
* Широковещательный адрес

**Сетевой адрес**

Сетевой адрес — это стандартный способ обозначения сети. Маска подсети или длина префикса могут использоваться при обозначении сетевого адреса. Например, сеть, показанную на рисунке 1, можно обозначить как 10.1.1.0, 10.1.1.0 255.255.255.0 или 10.1.1.0/24. Все узлы в сети 10.1.1.0/24 будут иметь одинаковую сетевую часть.

Как показано на рисунке 2, в пределах диапазона IPv4-адресов первый из них зарезервирован для сетевого адреса. В каждом узловом бите узловой части этого адреса указан ноль. Все узлы в этой сети используют одну сеть.

**Адрес узла**

Для обмена данными по сети каждому оконечному устройству необходим уникальный адрес. В IPv4-адресах значения между сетевым и широковещательным адресами могут быть назначены оконечным устройствам в сети. Как показано на рисунке 3, в узловой части этот адрес может иметь любую комбинацию нулей и единиц, но при этом не может состоять только из нулей или только из единиц.

**Широковещательный адрес**

Широковещательный IPv4-адрес — это особый адрес для каждой сети, который осуществляет связь для всех узлов, расположенных в этой сети. Для единовременной отправки данных на все узлы в сети узел может отправить один пакет, назначенный широковещательному адресу сети, а каждый узел в этой сети, который получит этот пакет, обработает его содержимое.

Для широковещательной рассылки используется наивысший адрес диапазона сети. В этом адресе все части узла представлены единицами (1). Сумма единиц октета в двоичной форме равняется значению 255 в десятичном формате. Таким образом, как показано на рисунке 4, для сети 10.1.1.0/24, в которой последний октет используется для узловой части, широковещательный адрес будет равен 10.1.1.255. Обратите внимание, что узловая часть не всегда представлена всем октетом целиком. Также этот адрес называют прямой широковещательной рассылкой.

# Сетевые IPv4-адреса

## Маска подсети IPv4

Чтобы удостовериться, что всем узлам в сети присвоен уникальный IP-адрес внутри диапазона сети, сначала нужно определить адреса первого и последнего узлов. В этом диапазоне узлам внутри сети могут быть присвоены IP-адреса.

**Адрес первого узла**

Как видно на рисунке 1, узловая часть первого адреса узла будет содержать все нулевые биты с единицей в крайнем справа бите. Значение этого адреса всегда на единицу больше сетевого адреса. В этом примере первым адресом узла в сети 10.1.1.0/24 является 10.1.1.1. Часто во многих схемах адресации первый адрес узла используется для маршрутизатора или шлюза по умолчанию.

**Адрес последнего узла**

Узловая часть последнего адреса узла будет содержать все единицы с нулём в крайнем справа бите. Значение этого адреса всегда на единицу меньше, чем значение широковещательного адреса. Как видно на рисунке 2, последним адресом узла в сети 10.1.1.0/24 является 10.1.1.254.

# Сетевые IPv4-адреса

## Маска подсети IPv4

Если устройству назначен IPv4-адрес, то это устройство использует маску подсети, чтобы определить, к какому сетевому адресу оно принадлежит. Сетевой адрес представляет все устройства в одной и той же сети.

При отправке данных по сети устройство использует эту информацию, чтобы определить, может ли оно пересылать пакеты локально, либо оно должно отправлять пакеты на шлюз по умолчанию для удалённой отправки. Когда узел отправляет пакет, он сравнивает сетевые части собственного IP-адреса и IP-адреса назначения, который зависит от маски подсети. Если биты сетевой части совпадают, значит, узлы источника и назначения находятся в одной и той же сети, и пакет доставляется локально. Если биты не совпадают, отправляющий узел передаёт пакет на шлюз по умолчанию для отправки в другую сеть.

**Операция И**

Операция И — одна из трёх основных двоичных операций, используемых в дискретной логике. Кроме того, существуют операции ИЛИ и НЕТ. Хотя все они используются в сетях передачи данных, операция И используется для определения сетевого адреса. Поэтому в данном случае мы рассмотрим только логическую операцию И. Логическая операция И — это сравнение двух битов со следующими результатами:

1 И 1 = 1 (см. рис. 1)

0 И 1 = 0 (см. рис. 2)

0 И 0 = 0 (см. рис. 3)

1 И 0 = 0 (см. рис. 4)

IPv4-адрес узла постепенно, бит за битом, прошел операцию И, и его маска подсети определила сетевой адрес, с которым связан узел. В результате выполнения побитовой операции И между адресом и маской подсети создаётся сетевой адрес.

# Сетевые IPv4-адреса

## Маска подсети IPv4

Любой бит адреса, прошедший операцию И со значением бита 1 из маски подсети, выводит исходное значение бита из адреса. Таким образом, 0 (из IPv4-адреса) И 1 (из маска подсети) равняется 0. 1 (из адреса IPv4) И 1 (из маски подсети) равняется 1. Таким образом, всё, что проходит операцию И со значением 0, выводит 0. Эти свойства операции И используются с маской подсети, чтобы «замаскировать» узловые биты IPv4-адреса. Каждый бит адреса проходит операцию И с соответствующим битом маски подсети.

Поскольку все биты маски подсети, представляющие узловые биты, являются нулями, узловая часть выведенного сетевого адреса состоит только из нулей. Как вы помните, IPv4-адрес со всеми нулями в узловой части представляет сетевой адрес.

И наоборот, все биты маски подсети, которые представляют сетевую часть, являются единицами. Когда каждая из этих единиц проходит операцию И с соответствующим битом адреса, полученные в результате операции биты идентичны исходным битам адреса.

Как показано на рисунке, биты 1 в маске подсети будут выведены в сетевую часть сетевого адреса с теми же битами, что и в сетевой части узла. Узловая часть сетевого адреса будет состоять из всех нулей.

Для данного IP-адреса и его подсети операцию И можно использовать для определения того, к какой подсети принадлежит этот адрес, а также того, какие другие адреса относятся к той же подсети. Помните, что если два адреса находятся в одной и той же сети или подсети, то друг для друга они являются локальными и, следовательно, могут взаимодействовать между собой напрямую. Адреса, находящиеся в разных сетях или подсетях, являются друг для друга удалёнными, поэтому для их коммуникации необходимо устройство уровня 3 (например маршрутизатор или коммутатор уровня 3).

При проверке или диагностике сети нам часто приходится определять два узла из одной локальной сети. Это определение необходимо делать с точки зрения сетевых устройств. Из-за неправильной конфигурации узел может видеть себя не в той сети. Если не провести проверку операций И, применяемых узлом, могут потребоваться лишние действия.

**Сетевые IPv4-адреса**

**Маска подсети IPv4**

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

* Часть 1: откройте калькулятор Windows
* Часть 2: преобразуйте числа из одной системы исчисления в другую
* Часть 3: преобразуйте IPv4-адреса узлов и маски подсети в двоичные значения
* Часть 4: определите количество узлов в сети с помощью двух цифр
* Часть 5: преобразуйте MAC- и IPv6-адреса в двоичную форму

[Лабораторная работа: использование калькулятора Windows с помощью сетевых адресов](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.1.2.7%20Lab%20-%20Using%20the%20Windows%20Calculator%20with%20Network%20Addresses.pdf)

**Сетевые IPv4-адреса**

**Маска подсети IPv4**

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

* Часть 1: преобразуйте IPv4-адреса из разделённых точками десятичных чисел в двоичную форму
* Часть 2: используйте побитовые операции И для определения сетевых адресов
* Часть 3: примените расчёты сетевого адреса

[Лабораторная работа: преобразование IPv4-адресов в двоичное значение](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.1.2.8%20Lab%20-%20Converting%20IPv4%20Addresses%20to%20Binary.pdf)

# Сетевые IPv4-адреса

## Одноадресная, широковещательная и многоадресная рассылка IPv4

**Адреса для устройств конечных пользователей**

В большинстве сетей передачи данных многие узлы представлены оконечными устройствами, такими как компьютеры, смартфоны, планшетные ПК, принтеры и IP-телефоны. Поскольку это основная часть устройств в сети, наибольшее количество адресов должно быть присвоено именно этим узлам. Таким узлам присваиваются IP-адреса из диапазона доступных адресов в сети. IP-адреса можно присваивать статически или динамически.

**Статическое присвоение**

Используя статический адрес, сетевой администратор может вручную настраивать сетевые данные узла. На рис. 1 показано диалоговое окно со свойствами сетевого адаптера. Чтобы настроить статический IPv4-адрес, выберите IPv4 на экране сетевого адаптера, затем ключ в статическом адресе, маску подсети и шлюз по умолчанию. На рис. 2 показана минимальная статическая конфигурация: IP-адрес, маска подсети и шлюз по умолчанию.

Статическая адресация обладает несколькими преимуществами. Например, её можно использовать для принтеров, серверов и других сетевых устройств, которые редко меняют местоположение и должны быть доступны для клиентов сети, основанной на фиксированном IP-адресе. Если обычно узлы получают доступ к серверу через конкретный IP-адрес, то изменение IP-адреса повлечёт за собой некоторые проблемы. Кроме того, статическое присвоение адресов усиливает контроль над сетевыми ресурсами. Например, можно создать фильтры доступа в зависимости от трафика по направлению к определённому IP-адресу и от него. Однако ввод статической адресации на каждом узле требует много времени.

При использовании статической IP-адресации необходимо ввести точный список IP-адресов, присвоенных каждому устройству. Эти адреса постоянны и обычно не используются повторно.

# Сетевые IPv4-адреса

## Одноадресная, широковещательная и многоадресная рассылка IPv4

**Динамическое присвоение**

Список пользователей локальной сети часто меняется. Появляются новые пользователи с ноутбуками, которые нужно подключить. У других пользователей появляются новые рабочие станции или сетевые устройства, требующие подключения, например смартфоны. Чтобы каждой станции не приходилось вручную присваивать IP-адреса, проще всего это сделать автоматически. Для этого используется протокол динамической конфигурации сетевого узла (DHCP), как показано на рисунке 1.

DHCP обеспечивает автоматическое присвоение информации об адресе, например IP-адреса, маски подсети, шлюза по умолчанию и других параметров. При настройке DHCP-сервера для присвоения клиентам DHCP этой информации необходимо использовать блок адресов, который называется пулом адресов. Присвоение адресов к этому пулу необходимо планировать таким образом, чтобы любые статические адреса, используемые другими устройствами, были исключены.

DHCP — это наиболее предпочтительный способ присвоения IPv4-адресов узлам в большой 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 узел выключается или уходит из сети, его адрес возвращается в пул для повторного использования. Это особенно полезно для мобильных пользователей, которые используют сеть не постоянно.

Если на узловом устройстве включён DHCP, команду **ipconfig** можно использовать для просмотра информации об IP-адресе, присвоенном DHCP-серверу, как показано на рисунке 2.

**Сетевые IPv4-адреса**

**Одноадресная, широковещательная и многоадресная рассылка IPv4**

В IPv4-сети узлы могут взаимодействовать одним из трёх следующих способов.

* **Одноадресная рассылка** — процесс отправки пакета с одного узла на индивидуальный
* **Широковещательная рассылка** — процесс отправки пакета с одного узла на все узлы в сети
* **Многоадресная рассылка** — процесс отправки пакета с одного узла выбранной группе узлов, возможно, в различных сетях

Эти три типа связи используются в сетях передачи данных для различных целей. Во всех трёх типах IPv4-адрес исходного узла размещён в заголовке пакета в качестве адреса источника.

**Одноадресный трафик**

Одноадресная передача используется для обычного обмена данными между узлами как в сети типа «клиент/сервер», так и в одноранговой сети. Для одноадресной рассылки пакетов в качестве адреса назначения используются адреса целевого устройства. Пакеты могут быть направлены через объединённую сеть.

Чтобы увидеть пример одноадресной передачи, включите анимационное представление.

В IPv4-сети индивидуальные адреса, применяемые к оконечному устройству, называются узловыми адресами. Для одноадресной передачи адреса, присвоенные двум оконечным устройствам, используются в качестве IPv4-адресов источника и назначения. Во время процесса инкапсуляции исходный узел размещает свой IPv4-адрес в заголовке пакета одноадресной рассылки в качестве адреса источника, а IPv4-адрес узла назначения — в заголовке пакета в качестве адреса назначения. Независимо от того, является ли пункт назначения, определивший пакет, одноадресным, широковещательным или многоадресным, источник всегда является индивидуальным адресом исходного узла.

**Примечание**. В этом курсе любая связь между устройствами является одноадресной, если не указано иное.

Узловые IPv4-адреса являются одноадресными и входят в диапазон адресов от 0.0.0.0 до 223.255.255.255. Однако в этом диапазоне есть множество адресов, зарезервированных для специальных целей. Такие адреса будут рассмотрены позже.

**Сетевые IPv4-адреса**

**Одноадресная, широковещательная и многоадресная рассылка IPv4**

**Широковещательная передача**

Трафик широковещательной рассылки используется для отправки пакетов по всем узлам в сети с помощью группового адреса сети. В пакете широковещательной рассылки содержится IP-адрес назначения, в узловой части которого присутствуют только единицы (1). Это означает, что пакеты получат и обработают все узлы в локальной сети (домене широковещательной рассылки). Широковещательные рассылки предусмотрены во многих сетевых протоколах, например в протоколе DHCP. Когда узел получает пакет, отправленный на сетевой широковещательный адрес, узел обрабатывает этот пакет так же, как обрабатывает пакет, отправленный по одноадресной рассылке.

Использование широковещательной рассылки включает в себя:

* Проведение маршрута от адресов верхнего уровня до адресов нижнего уровня
* Запрос адреса
* В отличие от одноадресной рассылки, в случае которой пакеты могут быть отправлены по объединённой сети, широковещательным пакетам запрещено проходить по локальной сети. Это ограничение зависит от конфигурации маршрутизатора шлюза и типа широковещательной рассылки. Есть два типа широковещательной рассылки: прямая и ограниченная.

**Прямая широковещательная рассылка**

Прямая широковещательная рассылка отправляется всем узлам в конкретной сети. Этот тип широковещательной рассылки полезен для отправки широковещательных пакетов на все узлы нелокальной сети. Например, для связи какого-либо узла за пределами сети 172.16.4.0/24 со всеми узлами внутри этой сети адресом назначения пакета будет являться 172.16.4.255. Несмотря на то, что маршрутизаторы не пересылают широковещательные пакеты по умолчанию, их можно для этого настроить.

**Ограниченная широковещательная рассылка**

Ограниченная широковещательная рассылка используется для обмена сообщениями между узлами в локальной сети. Эти пакеты всегда используют следующий IPv4-адрес назначения: 255.255.255.255. Маршрутизаторы не пересылают ограниченную широковещательную рассылку. Поэтому IPv4-сеть иначе называется доменом широковещательной рассылки. Маршрутизаторы формируют границы для домена широковещательной рассылки.

Например, узел в пределах сети 172.16.4.0/24 отправляет широковещательную рассылку всем узлам внутри своей сети, используя пакет с адресом назначения 255.255.255.255.

Чтобы увидеть пример ограниченной широковещательной передачи, включите анимационное представление.

Широковещательный пакет использует ресурсы в сети и заставляет каждый принимающий узел в сети обрабатывать этот пакет. Таким образом, трафик широковещательной рассылки должен быть ограниченным, чтобы не влиять на производительность сети и других устройств. Поскольку маршрутизаторы отделяют домены широковещательной рассылки, разделение сети с чрезмерным трафиком широковещательной рассылки может повысить производительность сети.

**Сетевые IPv4-адреса**

**Одноадресная, широковещательная и многоадресная рассылка IPv4**

**Многоадресная передача**

Многоадресная передача предназначена для сохранения пропускной способности IPv4-сети. Такая передача сокращает трафик, позволяя узлу отправлять один пакет выбранной группе узлов, которые являются частью подписной группы мультивещания. Чтобы достичь множества целевых узлов с помощью одноадресной связи, узел-источник должен отправлять отдельный пакет на каждый адрес. В случае с многоадресной рассылкой узел-источник может отправлять один пакет, который достигает нескольких тысяч узлов назначения. Сетевое взаимодействие дублирует многоадресные потоки, чтобы они достигали только указанных получателей.

Многоадресная передача включает в себя:

* Широковещательную передачу видео и аудио
* Обмен данными маршрутизации протоколами маршрутизации
* Распространение программного обеспечения
* Игру удалённым способом

**Групповые адреса**

Протокол IPv4 имеет блок адресов, зарезервированных для групп мультивещания. Это диапазон адресов составляет от 224.0.0.0 до 239.255.255.255. Диапазон групповых адресов разделён на различные типы адресов: зарезервированные канальные и глобальные адреса. Дополнительный тип групповых адресов — это административно определяемые адреса, которые также называются ограниченными адресами.

Групповые адреса IPv4 от 224.0.0.0 до 224.0.0.255 являются зарезервированными локальными адресами. Эти адреса используются группами мультивещания в локальной сети. Маршрутизатор, подключённый к локальной сети, распознаёт, что эти пакеты адресованы локальной группе мультивещания, и не пересылает их дальше. Обычно зарезервированные локальные адреса применяются в протоколах маршрутизации с использованием многоадресной передачи для обмена данными маршрутизации.

Глобальные адреса включают в себя от 224.0.1.0 до 238.255.255.255. Их можно использовать для многоадресной передачи данных через Интернет. Например, адрес 224.0.1.1 зарезервирован для протокола сетевого времени (NTP) с целью синхронизации часов истинного времени в сетевых устройствах.

**Клиенты многоадресной рассылки**

Узлы, которые получают конкретные многоадресные данные, называются клиентами многоадресной рассылки. Клиенты многоадресной рассылки используют сервисы, запрошенные программой клиента для подписки в группу мультивещания.

Каждая группа мультивещания представлена одним групповым IPv4-адресом назначения. Когда IPv4-узел подписывается в группу мультивещания, он обрабатывает пакеты, адресованные на этот групповой адрес, а также пакеты, адресованные на его уникальный индивидуальный адрес.

На анимационном представлении показано, как клиенты получают многоадресную рассылку.

# Сетевые IPv4-адреса

## Одноадресная, широковещательная и многоадресная рассылка IPv4

Это задание позволит проанализировать свойства одноадресной, широковещательной и многоадресной рассылки. Трафик в сети чаще всего является одноадресным. Когда компьютер отправляет эхо-запрос ICMP на удалённый маршрутизатор, адрес источника в заголовке IP-пакета представляет собой IP-адрес отправляющего компьютера. Адрес назначения в заголовке IP-пакета — это IP-адрес интерфейса на удалённом маршрутизаторе. Пакет отправляется только к нужному месту назначения.

С помощью команды **ping** или функции Add Complex PDU программы Packet Tracer можно напрямую проверить широковещательные адреса для просмотра широковещательного трафика.

Для многоадресного трафика будет отображён трафик усовершенствованного протокола внутренней маршрутизации между шлюзами, EIGRP. EIGRP используется маршрутизаторами Cisco для обмена данными маршрутизации. Маршрутизаторы, использующие EIGRP, отправляют пакеты на групповой адрес 224.0.0.10, который представляет группу маршрутизаторов EIGRP. Несмотря на то, что эти пакеты получены другими устройствами, они сбрасываются на 3-м уровне всеми устройствами, кроме маршрутизаторов EIGRP, и при этом другая обработка не требуется.

[Packet Tracer: рассмотрение одноадресного, широковещательного и многоадресного трафика (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.1.3.8%20Packet%20Tracer%20-%20Investigate%20Unicast,%20Broadcast,%20and%20Multicast%20Traffic%20Instructions.pdf)

[Packet Tracer: рассмотрение одноадресного, широковещательного и многоадресного трафика (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.1.3.8%20Packet%20Tracer%20-%20Investigate%20Unicast,%20Broadcast,%20and%20Multicast%20Traffic.pka)

# Сетевые IPv4-адреса

## Типы IPv4-адресов

Хотя большая часть узловых IPv4-адресов являются публичными, т. е. предназначенными для использования в сетях, доступных через Интернет, существуют блоки адресов, которые используются в сетях, требующих ограниченного доступа в Интернет или не требующих его совсем. Эти адреса называются частными.

**Частные адреса**

Блоки частных адресов включают в себя:

10.0.0.0–10.255.255.255 (10.0.0.0/8)

172.16.0.0–172.31.255.255 (172.16.0.0/12)

192.168.0.0–192.168.255.255 (192.168.0.0/16)

Частные адреса определены в документе RFC 1918 «Присвоение адресов для частного Интернета». Иногда эти адреса называют адресами RFC 1918. Как показано на рисунке, блоки адресов частного пространства используются в частных сетях. Узлы, которые не требуют доступа в Интернет, могут использовать частные адреса. Однако в рамках частной сети узлы по-прежнему должны иметь уникальные IP-адреса внутри частного пространства.

Узлы в различных сетях могут использовать одни и те же адреса частного пространства. Пакеты, использующие эти адреса в качестве источника или назначения, не должны появляться в публичном Интернете. Маршрутизатор или устройство межсетевого экрана по периметру этих частных сетей должны блокировать или преобразовывать эти адреса. Даже если бы пакеты сами прокладывали свой путь через Интернет, у маршрутизаторов в любом случае не появилось бы маршрутов для пересылки их в соответствующую частную сеть.

В документе RFC 6598 IANA (Администрация адресного пространства Интернет) зарезервировала другую группу адресов, которая называется общим адресным пространством. Так же, как и в пространстве частных адресов RFC 1918, адреса общего адресного пространства недоступны глобально. Однако эти адреса предназначены только для использования в сетях операторов связи. Блок общих адресов — 100.64.0.0/10.

**Публичные адреса**

Подавляющее большинство адресов в диапазоне узлов одноадресной IPv4-рассылки являются публичными адресами. Эти адреса предназначены для использования в узлах с открытым доступом из Интернета. Даже в диапазоне этих блоков IPv4-адресов существует множество адресов, предназначенных для других особых целей.

# Сетевые IPv4-адреса

## Типы IPv4-адресов

Некоторые адреса невозможно назначить узлам. Также существуют особые адреса, которые могут быть назначены узлам, но с ограничениями того, как эти узлы могут взаимодействовать в сети.

**Адреса сети и широковещательной рассылки**

Как было указано выше, в каждой сети первый и последний адреса не могут быть назначены узлам. Это сетевой и широковещательный адреса соответственно.

**Логический интерфейс loopback**

Один из таких зарезервированных адресов — IPv4-адрес логического интерфейса loopback 127.0.0.1. Loopback — это особый адрес, который используют узлы, чтобы направлять трафик самим себе. Адрес обратной связи позволяет создавать ускоренный метод взаимодействия для приложений и сервисов TCP/IP, которые работают на одном и том же устройстве. С использованием loopback-адреса вместо назначенного IPv4-адреса узла два сервиса на одном узле могут обойти нижние уровни стека протоколов TCP/IP. Для проверки настройки TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес.

Хотя используется только адрес 127.0.0.1, резервируются адреса с 127.0.0.0 до 127.255.255.255. Любой адрес из этого блока даст обратную связь с локальным узлом. Ни один адрес из этого блока не должен появляться в какой-либо сети.

**Локальные адреса каналов**

В качестве локальных адресов канала используются IPv4-адреса в блоке адресов от 169.254.0.0 до 169.254.255.255 (169.254.0.0 /16). Эти адреса могут быть автоматически присвоены операционной системой локальному узлу в средах, где настройка IP-сети недоступна. Они могут использоваться в небольшой одноранговой сети или для узла, который не может автоматически получить адрес от DHCP-сервера.

Коммуникация с помощью локальных IPv4-адресов подходит только для обмена данными с другими устройствами, подключёнными к той же сети, как показано на рисунке. Узел не должен отправлять пакет с локальным IPv4-адресом назначения какому-либо маршрутизатору для пересылки, а должен задать время жизни (TTL) IPv4 для этих пакетов в значении 1.

Локальные адреса не предоставляют сервисы за пределами локальной сети. Однако многие приложения типа клиент-сервер и одноранговые приложения будут работать надлежащим образом с локальными IPv4-адресами.

**Адреса TEST-NET**

Блок адресов от 192.0.2.0 до 192.0.2.255 (192.0.2.0/24) отложен для обучающих и учебных целей. Эти адреса могут использоваться в документации и сети. В отличие от экспериментальных адресов сетевые устройства принимают эти адреса в свои конфигурации. Эти адреса часто используются в сочетании с такими доменными именами, как example.com или example.net в серии документов, имеющих статус стандартов (RFC), в документации поставщиков и протоколов. Адреса из этого блока не должны появляться в сети Интернет.

**Экспериментальные адреса**

Адреса в блоке от 240.0.0.0 до 255.255.255.254 указаны в качестве зарезервированных для использования в будущем (RFC 3330). В настоящее время эти адреса могут использоваться только в исследовательских или экспериментальных целях, но не могут использоваться в IPv4-сети. Тем не менее, в соответствии с документом RFC 3330, в будущем технически они могут быть преобразованы в доступные адреса.

# Сетевые IPv4-адреса

## Типы IPv4-адресов

Исторически сложилось так, что назначенные адреса (RFC1700) сгруппировали одноадресные диапазоны в адреса с особыми размерами, которые называются адресами класса А, класса B и класса С. Кроме того, были определены адреса класса D (групповые) и класса Е (экспериментальные), как было показано ранее. Согласно индивидуальным адресам классов A, B и C определены сети особого размера и блоки особых адресов для этих сетей. Компании или организации назначается целая сеть из блоков адресов класса A, B или C. Такое использование адресного пространства называется классовой адресацией.

**Блоки класса А**

Блок адресов класса А разработан для поддержки очень крупных сетей, содержащих более чем 16 миллионов адресов узлов. Для обозначения сетевого адреса IPv4-адреса класса А использовали фиксированный префикс /8 с первым октетом. Остальные три октета использовались для адресов узлов. Все адреса класса А требуют, чтобы самый старший разряд старшего октета был равен нулю. Это означает, что существовало только 128 возможных сетей класса А, от 0.0.0.0/8 до 127.0.0.0 /8. Даже если адреса класса А зарезервировали половину адресного пространства, в связи с их ограничением до 128 сетей они могут быть назначены только приблизительно 120 компаниям или организациям.

**Блоки класса B**

Адресное пространство класса B разработано для поддержки потребностей небольших и крупных сетей, содержащих приблизительно 65 000 узлов. IP-адрес класса B использовал два старших октета для обозначения сетевого адреса. Оставшиеся два октета определяли адреса узлов. Как и в случае с классом А, адресное пространство для оставшихся классов адресов должно быть зарезервированным. Для адресов класса B два самых старших разряда старшего октета равны 10. Это ограничивает блок адресов для класса B от 128.0.0.0/16 до 191.255.0.0/16. Назначение адресов класса B немного более эффективно по сравнению с классом А, поскольку 25% его общего пространства IPv4-адресов было разделено среди примерно 16 000 сетей.

**Блоки класса С**

Адресное пространство класса С было доступно чаще всех остальных классов адресов. Это адресное пространство предназначено для предоставления адресов небольшим сетям с максимальным количеством узлов не более 254. Блоки адресов класса С использовали префикс /24. Это означает, что сеть класса С использовала только последний октет в качестве адресов узлов с тремя старшими октетами, используемыми для обозначения сетевых адресов. Блоки адресов класса С отделяли адресное пространство с помощью фиксированного значения 110 самых старших разрядов старшего октета. Это ограничило блок адресов класса С от 192.0.0.0/24 до 223.255.255.0/24. Хотя этот блок занял только 12,5 % от общего объёма адресного IPv4-пространства, он предоставил адреса 2 миллионам сетей.

На рис. 1 показано, как разделяются эти классы адресов.

**Ограничения в системе классов**

Не все требования организаций соответствуют этим классам. Классовое распределение адресного пространства часто приводит к потере множества адресов, что отрицательным образом сказывается на доступности IPv4-адресов. Например, компании, в сети которой находится 260 узлов, необходимы адреса класса B с более 65 000 адресами.

Хотя эта классовая система была практически забыта в конце 1990-х гг., в настоящее время по-прежнему наблюдается её влияние. Например, при назначении компьютеру IPv4-адреса операционная система проверяет присваиваемый адрес, чтобы определить, к какому классу принадлежит этот адрес: A, B или C. Затем операционная система принимает префикс, используемый этим классом, и назначает маску подсети по умолчанию.

**Бесклассовая адресация**

Сегодня используется система, которая называется бесклассовой адресацией, официальное название которой — бесклассовая междоменная маршрутизация (CIDR, произносится как «сайдэ»). Классовое назначение IPv4-адресов с длинами префиксов /8, /16 и /24, каждый из которых принадлежал разному классу, было очень неэффективным. В 1993 г. организация IETF (Инженерная группа по развитию Интернета) создала новые стандарты, которые позволили операторам связи назначать IPv4-адреса в любых битовых границах (имеется в виду длина префикса) вместо адресов класса А, B или C.

В IETF понимали, что бесклассовая междоменная маршрутизация (CIDR) была только временным решением и для поддержки быстрого развития количества пользователей Интернета необходим новый IP-протокол. В 1994 г. в IETF начались поиски преемника IPv4. Им стал протокол IPv6.

На рис. 2 показаны классовые диапазоны адресов.

**Сетевые IPv4-адреса**

**Типы IPv4-адресов**

Чтобы располагать сетевыми узлами, например веб-серверами, компании или организации необходим блок назначенных публичных адресов. Как вы помните, публичные адреса должны быть уникальными, а использование этих публичных адресов контролируется и назначается отдельно для каждой организации. Это утверждение является верным в отношении IPv4- и IPv6-адресов.

**IANA (Администрация адресного пространства Интернет) и RIR (региональные интернет-регистраторы)**

Администрация адресного пространства Интернет IANA ([http://www.iana.org](http://www.iana.org/)) регулирует назначение IPv4- и IPv6-адресов. До середины 1990-х гг. управление всем адресным IPv4-пространством осуществлялось напрямую организацией IANA. В то время оставшееся адресное IPv4-пространство было распространено среди различных регистраторов для облегчённого управления конкретными целями и регионами. Такие регистрационные компании называются региональными интернет-регистраторами (RIR), как показано на рисунке.

Основные реестры:

* AfriNIC (Африканский сетевой информационный центр) — Африканский регион [http://www.afrinic.net](http://www.afrinic.net/)
* APNIC (Азиатско-Тихоокеанский сетевой информационный центр) — Азиатско-Тихоокеанский регион [http://www.apnic.net](http://www.apnic.net/)
* ARIN (Американский реестр интернет-адресов) — Североамериканский регион [http://www.arin.net](http://www.arin.net/)
* LACNIC (Латиноамериканский и Карибский сетевой информационный центр) — Латинская Америка и некоторые острова Карибского моря [http://www.lacnic.net](http://www.lacnic.net/)
* RIPE NCC (Координационный центр европейской континентальной сети) — Европа, Ближний Восток и Азия [http://www.ripe.net](http://www.ripe.net/)

**Интернет-провайдеры**

Региональные интернет-регистраторы отвечают за выделение IP-адресов интернет-провайдерам (ISP). Большинство компаний или организаций получают блоки IPv4-адресов от интернет-провайдеров. Обычно, помимо всех остальных услуг, провайдер предоставляет своим заказчикам небольшое количество доступных IPv4-адресов (6 или 14). Большие блоки адресов можно получить в соответствии с потребностями и за дополнительную плату.

По сути, провайдеры одалживают своим клиентам эти адреса. При смене интернет-провайдера новый поставщик услуг предоставляет адреса из своих адресных блоков, а предыдущий получает обратно свои адреса и одалживает их другому заказчику.

IPv6-адреса можно получить от интернет-провайдера или, в некоторых случаях, напрямую от интернет-регистраторов. IPv6-адреса и блоки адресов стандартных размеров будут рассмотрены в этой главе далее.

# Сетевые IPv4-адреса

## Типы IPv4-адресов

**Сервисы интернет-провайдера**

Для получения доступа к услугам сети Интернет нам необходимо подключить нашу сеть для передачи данных в Интернет с помощью интернет-провайдера (ISP).

У интернет-провайдеров есть свои сети передачи данных для управления подключением к Интернету и предоставления связанных с ним услуг. Среди прочих услуг, которые интернет-провайдеры обычно предоставляют своим заказчикам, существуют сервис DNS, сервис электронной почты и веб-сайты. В зависимости от уровня требуемых и доступных услуг заказчики обращаются к различным уровням интернет-провайдеров.

**Уровни интернет-провайдеров**

Интернет-провайдеры классифицируются по иерархии в соответствии с уровнем подключения к магистральному каналу Интернет. Каждый низший уровень получает подключение к магистрали через соединение к провайдеру высшего уровня, как показано на рисунках.

**Уровень 1**

Как показано на рис. 1, в верхней части иерархии интернет-провайдеров находятся провайдеры уровня 1. Эти провайдеры, подключённые напрямую к магистральному каналу Интернет, работают в национальных и международных масштабах. Заказчики провайдеров уровня 1 — это либо интернет-провайдеры более низших уровней, либо крупные компании и организации. Поскольку они располагаются в верхней части иерархии подключения к Интернету, они предоставляют надёжное подключение и услуги высокого уровня. Для обеспечения такой надёжности используются множественные подключения к магистральному каналу Интернет.

Основные преимущества интернет-провайдеров уровня 1 для заказчиков — надёжность и скорость. Поскольку эти заказчики находятся только в одном шаге от магистрали, они испытывают меньше неполадок с соединением и проблем с пропускной способностью. Высокая стоимость услуг — единственный недостаток для заказчиков интернет-провайдеров уровня 1.

**Уровень 2**

Как показано на рисунке 2, провайдеры уровня 2 получают подключение к Интернету от интернет-провайдеров уровня 1. Как правило, интернет-провайдеры уровня 2 основное внимание уделяют бизнес-клиентам. Интернет-провайдеры уровня 2 обычно предлагают больше услуг, чем провайдеры остальных двух уровней. В компаниях интернет-провайдеров уровня 2 работают ИТ-специалисты, которые регулируют работу таких сервисов, как DNS, сервисов электронной почты и веб-серверов. Кроме того, провайдеры уровня 2 могут предлагать услуги по разработке и обслуживанию веб-сайтов, обеспечению электронной торговли и онлайн-бизнеса, а также голосовой передачи по протоколу VoIP.

Основной недостаток провайдеров уровня 2 по сравнению с уровнем 1 — более медленный доступ к сети Интернет. Поскольку поставщики уровня 2 находятся как минимум в одном шаге от магистрального канала Интернет, они предлагают меньшую надёжность, чем поставщики уровня 1.

**Уровень 3**

Как показано на рисунке 3, провайдеры уровня 3 получают подключение к Интернету от провайдеров уровня 2. Эти провайдеры нацелены на розничные и домашние рынки в конкретном регионе. Обычно заказчикам уровня 3 не требуется такое количество услуг, как клиентам уровня 2. Прежде всего, им необходимы подключение к Интернету и техническая поддержка.

Зачастую эти заказчики не обладают обширными знаниями в компьютерных и сетевых технологиях. Интернет-провайдеры уровня 3 часто предлагают подключение к сети Интернет, входящей в часть договора на обслуживание сетей и компьютеров. Хотя поставщики уровня 3 предоставляют небольшую пропускную способность и менее надёжны по сравнению с провайдерами уровней 1 и 2, они оптимально подходят для средних и малых компаний.

**Сетевые IPv4-адреса**

**Типы IPv4-адресов**

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

* Часть 1: определите IPv4-адреса
* Часть 2: классифицируйте IPv4-адреса

[Лабораторная работа: определение IPv4-адресов](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.1.4.8%20Lab%20-%20Identifying%20IPv4%20Addresses.pdf)

# Сетевые IPv6-адреса

## Проблемы с IPv4

Протокол IPv6 разработан как преемник протокола IPv4. В протоколе IPv6 больше 128-битного адресного пространства, что достаточно для 340 ундециллионов адресов. (Это число 340, за которым следует 36 нолей.) Однако IPv6 — не просто большие адреса. Когда специалисты IETF начали разработку преемника IPv4, они использовали эту возможность для устранения ограничений протокола IPv4 и внесения дополнительных улучшений. Среди таких улучшений — протокол управляющих сообщений версии 6 (ICMPv6), который включает в себя разрешение адресов и автонастройку адресов, что отсутствовало в протоколе ICMP для IPv4 (ICMPv4). Протоколы ICMPv4 и ICMPv6 будут рассмотрены далее в этой главе.

**Потребность в IPv6**

Сокращение адресного пространства протокола IPv4 — основной стимулирующий фактор для перехода к использованию IPv6. По мере того как Африка, Азия и другие регионы планеты всё больше нуждаются в подключении к сети Интернет, остается всё меньше IPv4-адресов для поддержки таких темпов развития. 31 января 2011 г. Администрация адресного пространства Интернет IANA назначила последние 2 блока IPv4-адресов /8 региональным интернет-регистраторам (RIR). Согласно различным прогнозам в период между 2015 и 2020 годами у всех пяти интернет-регистраторов закончатся IPv4-адреса. Оставшиеся IPv4-адреса будут распределены среди интернет-провайдеров.

Теоретическое максимальное количество IPv4-адресов — 4,3 миллиарда. Частные адреса RFC 1918 в сочетании с преобразованием сетевых адресов (NAT) служат для замедления истощения адресного пространства IPv4. Преобразование сетевых адресов (NAT) имеет ограничения, которые препятствуют одноранговой связи.

**Интернет вещей**

Современная сеть Интернет значительно отличается от Интернета последних десятилетий. Сегодня это не просто электронная почта, веб-страницы и передача файлов между компьютерами. Интернет развивается и становится неотъемлемой частью нашей жизни. Скоро можно будет получить доступ к Интернету не только через компьютеры, планшеты и смартфоны. В будущем Интернет станет неотделим от многих устройств и технического оборудования, в том числе автомобилей и биомедицинских аппаратов, домашней техники и экосистемы. Представьте себе встречу с заказчиком на его территории, которая автоматически запланирована вашим календарным приложением за час до начала обычного рабочего дня. Однако перед встречей вы можете забыть проверить свой календарь или поставить будильник, чтобы встать вовремя, и это повлечёт за собой серьёзные проблемы. Теперь представьте, что календарное приложение напрямую передаёт эту информацию в будильник и автомобиль. Ваша машина автоматически прогреется, чтобы лёд на лобовом стекле растаял прямо перед тем, как вы сядете в машину, а после этого создаст верный маршрут до места встречи.

В связи с распространением Интернета ограниченным адресным пространством IPv4, проблемами с преобразованием сетевых адресов и проникновением Интернета в нашу жизнь пришло время для перехода на протокол IPv6.

**Сетевые IPv6-адреса**

**Проблемы с IPv4**

Точно неизвестно, когда мы перейдем на протокол IPv6. В ближайшем будущем протоколы IPv4 и IPv6 будут существовать совместно. Полный переход может занять многие годы. Специалисты IETF создали различные протоколы и инструменты, которые позволяют сетевым администраторам постепенно переводить свои сети на протокол IPv6. Методы перехода можно разделить на 3 категории:

* **Двойной стек**: как показано на рис. 1, двойной стек позволяет протоколам IPv4 и IPv6 сосуществовать в одной сети. Устройства с двойным стеком одновременно работают с протокольными стеками IPv4 и IPv6.
* **Туннелирование**: как показано на рисунке 2, туннелирование — это способ транспортировки IPv6-пакетов через IPv4-сеть. IPv6-пакет инкапсулируется внутри IPv4-пакета, как и другие типы данных.
* **Преобразование**: как показано на рис. 3, преобразование сетевых адресов 64 (NAT64) позволяет устройствам под управлением IPv6 обмениваться данными с устройствами под управлением IPv4 с помощью метода преобразования, похожего на метод преобразования из NAT для IPv4. IPv6-пакет преобразовывается в пакет IPv4-пакет и наоборот.

# Сетевые IPv6-адреса

## Адресация IPv6

В отличие от IPv4-адресов, которые выражены в десятичном формате с разделительными точками, IPv6-адреса представлены с помощью шестнадцатеричных значений. Вы уже видели использование шестнадцатеричного кода в панели Packets Byte программы Wireshark. В программе Wireshark шестнадцатеричная система используется для представления двоичных значений в кадрах и пакетах. Также шестнадцатеричная система исчисления используется для представления адреса управления доступом к среде передачи данных Ethernet (MAC).

**Шестнадцатеричная нумерация**

Шестнадцатеричная система исчисления («Hex») — это удобный способ представления двоичных значений. Так же, как в десятичной системе основанием является 10, в двоичной системе основанием является 2, основание шестнадцатеричной системы исчисления — 16.

Система с основанием 16 использует цифры от 0 до 9 и буквы от A до F. На рис. 1 показаны эквиваленты значений десятичной, двоичной и шестнадцатеричной систем. Это 16 уникальных комбинаций из четырёх битов, от 0000 до 1111. Шестнадцатеричная система исчисления очень удобна в использовании, поскольку любые четыре бита могут быть представлены одним шестнадцатеричным значением.

**Общие сведения о байтах**

Если 8 бит (байт) — это общепринятая бинарная группа, двоичный код 00000000—11111111 может быть представлен в шестнадцатеричной системе исчисления в качестве диапазона 00–FF. Для завершения 8-битного представления можно просмотреть ведущие нули. Например, двоичное значение 0000 1010 показано в шестнадцатеричной системе как 0A.

**Представление шестнадцатеричных значений**

**Примечание**. Важно отличать шестнадцатеричные значения от десятичных в отношении символов от 0 до 9.

Шестнадцатеричное значение обычно представлено в тексте значением, которое располагается после 0x (например, 0x73) или подстрочного индекса 16. В остальных, более редких случаях, за ним может располагаться H (например, 73H). Однако, поскольку подстрочный текст не распознаётся в командной строке или средах программирования, перед техническим представлением шестнадцатеричных значений стоит «0x» (нулевой Х). Так, приведённые выше примеры будут отображаться как 0x0A и 0x73 соответственно.

**Шестнадцатеричные преобразования**

Числовые преобразования между десятичными и шестнадцатеричными значениями не вызывают затруднений, однако быстрое деление или умножение на 16 не всегда удобно.

Обладая определённым опытом, можно распознать шаблоны двоичных разрядов, совпадающих с десятичными и шестнадцатеричными значениями. На рис. 2 такие шаблоны показаны для выбранных 8-битных значений.

# Сетевые IPv6-адреса

## Адресация IPv6

Длина IPv6-адресов составляет 128 бит, написанных в виде строки шестнадцатеричных значений. Каждые 4 бита представлены одной шестнадцатеричной цифрой, причём общее количество шестнадцатеричных значений равно 32. IPv6-адреса не чувствительны к регистру, их можно записывать как строчными, так и прописными буквами.

**Предпочтительный формат**

Как показано на рис. 1, предпочтительный формат для записи IPv6-адреса: x: x: x: x: x: x: x: x, где каждый «x» состоит из четырёх шестнадцатеричных значений. Октеты — это термин, который используется для обозначения 8 бит IPv4-адреса. В IPv6 шестнадцатеричное число — это термин, используемый для обозначения сегмента из 16 бит или четырёх шестнадцатеричных значений. Каждый «x» — это одно шестнадцатеричное число, 16 бит или 4 шестнадцатеричных цифр.

В предпочтительном формате IPv6-адрес записан с помощью 32 шестнадцатеричных цифр. Тем не менее, это не самый оптимальный способ представления IPv6-адреса. Ниже мы увидим два правила, которые помогут сократить количество цифр, необходимых для представления IPv6-адреса.

На рис. 2 показаны примеры IPv6-адресов в предпочтительном формате.

**Сетевые IPv6-адреса**

**Адресация IPv6**

Первое правило для сокращения записи IPv6-адресов — пропуск всех ведущих 0 (нулей) в шестнадцатеричной записи. Например:

* 01AB можно представить как 1AB
* 09F0 можно представить как 9F0
* 0A00 можно представить как A00
* 00AB можно представить как AB

Это правило применяется только к ведущим нулям, а НЕ к последующим, иначе адрес будет записан неясно. Например, шестнадцатеричное число «ABC» может быть представлено как «0ABC» или «ABC0».

На рис. с 1 по 8 показаны примеры того, как пропуск ведущих нулей способствует сокращению размера IPv6-адреса. Для каждого примера показан предпочтительный формат. Обратите внимание, как во многих примерах пропуск ведущих нулей приводит к уменьшенному представлению адреса.

**Сетевые IPv6-адреса**

**Адресация IPv6**

Второе правило для сокращения записи адресов IPv6 заключается в том, что двойное двоеточие (::) может заменить любую единую, смежную строку одного или нескольких 16-битных сегментов (хекстетов), состоящих из нулей.

Двойное двоеточие (::) может использоваться в адресе только один раз, в противном случае в результате может возникнуть несколько адресов. Сочетание этого правила с методом пропуска нулей помогает значительно сократить запись IPv6-адреса. Это называется сжатым форматом.

Неверный адрес:

* 2001:0DB8::ABCD::1234

Возможные расширения неоднозначно записанных сжатых адресов:

* 2001:0DB8::ABCD:0000:0000:1234
* 2001:0DB8::ABCD:0000:0000:0000:1234
* 2001:0DB8:0000:ABCD::1234
* 2001:0DB8:0000:0000:ABCD::1234

На рис. с 1 по 7 показаны примеры того, как использование двойного двоеточия способствует сокращению размера IPv6-адреса.

**Сетевые IPv6-адреса**

**Типы IPv6-адресов**

Существует три типа IPv6-адресов.

* **Индивидуальный**: служит для определения интерфейса на устройстве под управлением протокола IPv6. Как показано на рисунке, IPv6-адрес источника должен быть индивидуальным.
* **Групповой**: используется для отправки IPv6-пакетов по нескольким адресам назначения.
* **Произвольный**: любой индивидуальный IPv6-адрес, который может быть назначен нескольким устройствам. Пакет, отправляемый на адрес произвольной рассылки, направляется к ближайшему устройству с этим адресом. Произвольные адреса не рассматриваются в данном курсе.

В отличие от протокола IPv4, IPv6 не использует адрес широковещательной рассылки. Однако есть групповой IPv6-адрес для всех узлов, который даёт аналогичный результат.

# Сетевые IPv6-адреса

## Типы IPv6-адресов

Как вы помните, префикс, или сетевая часть адреса IPv4, может быть обозначен маской подсети в десятичном формате с разделительными точками или длиной префикса (запись с наклонной чертой). Например, IP-адрес 192.168.1.10 с маской подсети в десятичном формате с разделительными точками 255.255.255.0 эквивалентен записи 192.168.1.10/24.

Протокол IPv6 использует длину префикса для обозначения части префикса адреса. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Длина префикса обозначает сетевую часть IPv6-адреса с помощью адреса или длины IPv6-префикса.

Диапазон длины префикса может составлять от 0 до 128. Традиционная длина IPv6-префикса для локальных и других типов сетей — /64. Это означает, что длина префикса, или сетевая часть адреса, составляет 64 бита, а оставшиеся 64 бита остаются для идентификатора интерфейса (узловой части) адреса.

# Сетевые IPv6-адреса

## Типы IPv6-адресов

Индивидуальный адрес служит для определения интерфейса устройства под управлением протокола IPv6. Пакет, который отправляется на индивидуальный адрес, будет получен интерфейсом, присвоенным для этого адреса. Как и в случае с протоколом IPv4, IPv6-адрес должен быть индивидуальным. IPv6-адрес назначения может быть как индивидуальным, так и групповым.

Существует шесть типов индивидуальных IPv6-адресов:

**Глобальный индивидуальный адрес**

Глобальный индивидуальный адрес мало чем отличается от публичного IPv4-адреса. Эти адреса, к которым можно проложить маршрут по Интернету, являются уникальными по всему миру. Глобальные индивидуальные адреса могут быть настроены статически или присвоены динамически. В динамическом назначении IPv6-адреса устройством имеются некоторые важные отличия по сравнению с динамическим назначением IPv4-адреса.

**Локальный адрес канала**

Локальные адреса канала используются для обмена данными с другими устройствами по одному локальному каналу. В протоколе IPv6 термин «канал» означает подсеть. Локальные адреса каналов ограничены одним каналом. Они должны быть уникальны только в рамках этого канала, поскольку вне канала к ним нельзя проложить маршрут. Другими словами, маршрутизаторы не смогут пересылать пакеты, имея локальный адрес канала источника или назначения.

**Логический интерфейс loopback**

Loopback-адрес используется узлом для отправки пакета самому себе и не может быть назначен физическому интерфейсу. Как и на loopback-адрес IPv4, для проверки настроек TCP/IP на локальном узле можно послать эхо-запрос на loopback-адрес IPv6. Loopback-адрес IPv6 состоит из нулей, за исключением последнего бита, который выглядит как ::1/128 или просто ::1 в сжатом формате.

**Неопределённый адрес**

Неопределённый адрес состоит из нулей и в сжатом формате представлен как ::/128 или просто :: Он не может быть назначен интерфейсу и используется только в качестве адреса источника в IPv6-пакете. Неопределённый адрес используется в качестве адреса источника, когда устройству еще не назначен постоянный IPv6-адрес или когда источник пакета не относится к месту назначения.

**Уникальный локальный адрес**

Уникальные локальные IPv6-адреса имеют некоторые общие особенности с частными адресами RFC 1918 для IPv4, но при этом между ними имеются и значительные различия. Уникальные локальные адреса используются для локальной адресации в пределах узла или между ограниченным количеством узлов. Эти адреса не следует маршрутизировать в глобальном протоколе IPv6. Уникальные локальные адреса находятся в диапазоне от FC00::/7 до FDFF::/7.

В случае с IPv4 частные адреса объединены с преобразованием сетевых портов и адресов (NAT/PAT) для обеспечения преобразования адресов из частных в публичные. Это делается из-за недостатка адресного пространства IPv4. На многих сайтах также используют частный характер адресов RFC 1918, чтобы обеспечить безопасность или защитить сеть от потенциальных угроз. Однако такая мера никогда не была целью использования данных технологий, и организация IETF всегда рекомендовала предпринимать правильные меры предосторожности при работе маршрутизатора в Интернете. Хотя протокол IPv6 обеспечивает особую адресацию для сайтов, он не предназначен для того, чтобы скрывать внутренние устройства под управлением IPv6 от Интернета IPv6. IETF рекомендует ограничивать доступ к устройствам с помощью наилучших мер безопасности.

**Примечание**. Исходная спецификация IPv6 определяет локальные адреса для тех же целей с помощью диапазона префикса FEC0:: /10. В спецификации были обнаружены некоторые неточности, и локальные адреса сайтов были запрещены IETF в пользу уникальных локальных адресов.

**Встроенный IPv4**

Последними из рассматриваемых типов индивидуальных адресов являются встроенные IPv4-адреса. Использование этих адресов способствует переходу с протокола IPv4 на IPv6. Встроенные IPv4-адреса не рассматриваются в этом курсе.

# Сетевые IPv6-адреса

## Типы IPv6-адресов

Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Пакеты с локальным адресом канала источника или назначения не могут быть направлены за пределы того канала, в котором пакет создаётся.

В отличие от локальных IPv4-адресов канала, локальные адреса канала IPv6 играют важную роль в различных аспектах сети. Глобальный индивидуальный адрес не обязателен. Однако для содержания локального адреса канала необходим сетевой интерфейс под управлением протокола IPv6.

Если локальный адрес канала не настроен вручную на интерфейсе, устройство автоматически создаёт собственный адрес, не обращаясь к DHCP-серверу. Узлы под управлением IPv6 создают локальный IPv6-адрес канала даже в том случае, если устройству не был назначен глобальный IPv6-адрес. Это позволяет устройствам под управлением IPv6 обмениваться данными с другими устройствами под управлением IPv6 в одной подсети, в том числе со шлюзом по умолчанию (маршрутизатором).

Локальные IPv6-адреса канала находятся в диапазоне FE80::/10. /10 указывает на то, что первые 10 бит — 1111 1110 10xx xxxx. Первый хекстет имеет диапазон от 1111 1110 10**00 0000** (FE80) до 1111 1110 10**11 1111** (FEBF).

На рис. 1 показан пример коммуникации с помощью локальных IPv6-адресов.

На рис. 2 показан формат локального IPv6-адреса.

Локальные IPv6-адреса также используются IPv6-протоколами маршрутизации для обмена сообщениями, а также в качестве следующего адреса пересылки в IPv6-таблице маршрутизации. Локальные адреса каналов будут рассмотрены подробнее в следующем курсе.

**Примечание**. Как правило, в качестве шлюза по умолчанию для других устройств в канале используется локальный адрес маршрутизатора, а не глобальный индивидуальный адрес.

**Сетевые IPv6-адреса**

**Индивидуальные IPv6-адреса**

Глобальные индивидуальные IPv6-адреса уникальны по всему миру и доступны для маршрутизации через Интернет IPv6. Эти адреса эквивалентны публичным IPv4-адресам. Ассоциация по присвоению имен и номеров Интернета (ICANN), оператор Администрации адресного пространства Интернет (IANA), выделяет блоки IPv6-адресов пяти региональным интернет-регистраторам (RIR). В настоящее время назначаются только глобальные индивидуальные адреса с первыми тремя битами 001 или 2000::/3. Это лишь 1/8 от всего доступного адресного пространства IPv6, за исключением очень незначительного количества других типов адресов индивидуальных и групповых адресов.

**Примечание**. Адрес 2001:0DB8::/32 был зарезервирован для документации, в том числе для использования в примерах.

На рис. 1 показаны структура и диапазон глобальных индивидуальных адресов.

Глобальный индивидуальный адрес состоит из трёх частей:

* Префикс глобальной маршрутизации
* Идентификатор подсети
* Идентификатор интерфейса

**Префикс глобальной маршрутизации**

Префикс глобальной маршрутизации — это префиксальная или сетевая часть адреса, назначаемая интернет-провайдером заказчику или узлу. В настоящее время /48 является префиксом глобальной маршрутизации, который в настоящее время интернет-регистраторы назначают своим заказчикам — корпоративным сетям и индивидуальным пользователям. Этого адресного пространства более чем достаточно для большинства заказчиков.

На рис. 2 показана структура глобальных индивидуальных адресов, использующих префикс глобальной маршрутизации /48. Префиксы /48 — наиболее распространённые назначаемые префиксы глобальной маршрутизации, которые будут использоваться в большинстве примеров в рамках данного курса.

Например, IPv6-адрес 2001:0DB8:ACAD::/48 обладает префиксом, который обозначает, что первые 48 бит (3 хекстета) (2001:0DB8:ACAD) — это префиксальная или сетевая часть адреса. Двойное двоеточие (::) перед длиной префикса /48 означает, что остальные адреса состоят из нулей.

**Идентификатор подсети**

Идентификатор подсети используется организациями для обозначения подсетей в каждом узле.

**Идентификатор интерфейса**

Идентификатор IPv6-интерфейса эквивалентен узловой части адреса IPv4-адреса. Термин «идентификатор интерфейса» используется в том случае, когда один узел может иметь несколько интерфейсов, каждый из которых обладает одним или более IPv6-адресами.

**Примечание**. В отличие от IPv4, при использовании протокола IPv6 устройству можно назначить адрес узла, состоящий из одних 0 или из одних 1. Адрес из одних 1 можно использовать по той причине, что в протоколе IPv6 не используются широковещательные адреса. Можно также использовать адрес из одних 0, но он зарезервирован в качестве адреса произвольной рассылки Subnet-Router, и его следует назначать только маршрутизаторам.

Чтобы без труда прочитать большинство IPv6-адресов, нужно подсчитать количество хекстетов. Как показано на рис. 3, в глобальном индивидуальном адресе первые четыре хекстета отображают сетевую часть адреса, причём четвертый хекстет обозначает идентификатор подсети. Остальные четыре хекстета используются для идентификатора интерфейса.

**Сетевые IPv6-адреса**

**Индивидуальные IPv6-адреса**

**Конфигурация маршрутизатора**

Большинство команд конфигурации и проверки IPv6 в Cisco IOS похожи на свои IPv4-аналоги. В большинстве случаев единственная разница между ними — использование в командах **ipv6** вместо **ip**.

Для настройки глобального индивидуального IPv6-адреса в интерфейсе используется команда из группы **interface**, которая выглядит следующим образом: **ipv6 address** *ipv6-address/prefix-length*.

Обратите внимание, что между *ipv6-address* и *prefix-length* отсутствует пробел.

Для примера настройки используется топология, показанная на рис. 1, и следующие IPv6-подсети:

* 2001:0DB8:ACAD:0001:/64 (*или* 2001:DB8:ACAD:1:: /64)
* 2001:0DB8:ACAD:0002:/64 (*или* 2001:DB8:ACAD:2:: /64)
* 2001:0DB8:ACAD:0003:/64 (*или* 2001:DB8:ACAD:3:: /64)

Как показано на рис. 2, для настройки индивидуального глобального IPv6-адреса в интерфейсе GigabitEthernet 0/0 маршрутизатора R1 используются следующие команды:

**Router(config)#interface GigabitEthernet 0/0**

**Router(config-if)#ipv6 address 2001:db8:acad:1::1/64**

**Router(config-if)#no shutdown**

**Конфигурация узла**

Ручная настройка IPv6-адреса на узле мало чем отличается от настройки IPv4-адреса.

Как показано на рис. 3, для ПК1 настраивается следующий адрес шлюза по умолчанию: 2001:DB8:ACAD:1::1, который является глобальным индивидуальным адресом маршрутизатора R1 интерфейса GigabitEthernet в той же сети.

Для настройки глобального индивидуального IPv6-адреса используйте проверку синтаксиса на рисунке 4.

Как и в случае с IPv4, настройка статических адресов для клиентов не распространяется на крупные среды. Именно поэтому большинство сетевых администраторов IPv6-сети будут назначать IPv6-адреса динамически.

Устройство может автоматически получать глобальный индивидуальный IPv6-адрес двумя способами:

* Автоконфигурация без сохранения состояния адреса (SLAAC)
* DHCPv6

**Сетевые IPv6-адреса**

**Индивидуальные IPv6-адреса**

**Автоконфигурация без сохранения состояния адреса (SLAAC)**

SLAAC — это способ, который позволяет устройству получить свой префикс, длину префикса и адрес шлюза по умолчанию от *маршрутизатора IPv6* без помощи DHCPv6-сервера. При использовании SLAAC для получения необходимой информации устройства полагаются на сообщения «Объявления маршрутизатора ICMPv6».

IPv6-маршрутизаторы периодически отправляют сообщения «Объявления маршрутизатора ICMPv6» всем устройствам в сети под управлением IPv6. По умолчанию маршрутизаторы Cisco отправляют такие сообщения каждые 200 секунд на адрес групповой передачи всем IPv6-узлам. IPv6-устройству, находящемуся в сети, не нужно ждать этих периодических сообщений. Устройство может отправить сообщение «Запрос маршрутизатора ICMPv6», который использует адрес групповой передачи всем IPv6-узлам. Когда маршрутизатор IPv6 получает такое сообщение, он сразу же отправляет в ответ объявление маршрутизатора.

Несмотря на то, что интерфейс маршрутизатора Cisco можно настроить с IPv6-адресом, это не превращает его в «IPv6-маршрутизатор». IPv6-маршрутизатор обладает следующими характеристиками.

* Пересылает IPv6-пакеты между сетями.
* Может быть настроен со статическими IPv6-маршрутами или с динамическим IPv6-протоколом маршрутизации.
* Отправляет сообщения «Объявления маршрутизатора ICMPv6».

IPv6-маршрутизация не включена по умолчанию. Чтобы маршрутизатор работал как IPv6-маршрутизатор, необходимо использовать команду глобальной конфигурации **ipv6 unicast-routing**.

**Примечание**. Маршрутизаторы Cisco по умолчанию работают как IPv4-маршрутизаторы.

Сообщение «Объявления маршрутизатора ICMPv6» содержит префикс, длину префикса и другие сведения IPv6-устройства. Кроме того, такое сообщение указывает IPv6-устройству, как ему получить информацию по адресации. Как показано на рисунке, сообщение «Объявления маршрутизатора» может выглядеть в одном из следующих 3 вариантов.

* **Вариант 1: только SLAAC**. Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». Другая информация недоступна с DHCPv6-сервера.
* **Вариант 2: SLAAC и DHCPv6**. Устройство должно использовать префикс, длину префикса и шлюз по умолчанию, которые содержатся в сообщении «Объявления маршрутизатора». На DHCPv6-сервере доступна и другая информация, например адрес DNS-сервера. Устройство получит эту дополнительную информацию в процессе поисков и запросов к DHCPv6-серверу. Этот процесс называется «DHCPv6 без запоминания состояний», поскольку DHCPv6-серверы не выделяют и не отслеживают какие-либо назначения IPv6-адресов, а предоставляют дополнительную информацию, например об адресе DNS-сервера.
* **Вариант 3: только DHCPv6**. Устройство не должно использовать информацию из сообщения «Объявления маршрутизатора» для пополнения своей информации об адресации. Вместо этого устройство будет использовать обычные процессы поисков и запросов к DHCPv6-серверам для получения всей своей информации об адресации. Такая информация включает в себя индивидуальный адрес IPv6, длину префикса, адрес шлюза по умолчанию и адреса DNS-серверов. В этом случае DHCPv6-сервер работает как DHCP-сервер, который фиксирует данные аналогично DHCP-серверу для IPv4. DHCPv6-сервер выделяет и отслеживает IPv6-адреса, чтобы не назначать один и тот же IPv6-адрес на нескольких устройствах.

Маршрутизаторы отправляют сообщения «Объявления маршрутизатора ICMPv6», используя локальный адрес канала в качестве IPv6-адреса источника. Устройства, использующие SLAAC, применяют локальные адреса маршрутизатора в качестве адреса шлюза по умолчанию.

# Сетевые IPv6-адреса

## Индивидуальные IPv6-адреса

**DHCPv6**

Протокол динамической конфигурации сетевого узла для IPv6 (DHCPv6) работает по тем же принципам, что и DHCP-протокол для IPv4. Устройство может автоматически получить свою информацию об адресации, включая глобальный индивидуальный адрес, длину префикса, адрес шлюза по умолчанию и адреса DNS-серверов, с помощью сервисов DHCPv6-сервера.

Устройство может получить всю или часть своей информации об IPv6-адресации с DHCPv6-сервера в зависимости от того, в каком из вариантов представлено объявление маршрутизатора ICMPv6: в варианте 2 (SLAAC и DHCPv6) или в варианте 3 (только DHCPv6). Кроме того, ОС узла может предпочесть проигнорировать любую информацию в сообщении «Объявления маршрутизатора» и получить IPv6-адрес и другие данные непосредственно с DHCPv6-сервера.

Перед развёртыванием IPv6-устройств в сети рекомендуется проверить, соблюдает ли узел варианты в сообщении «Объявления маршрутизатора».

Устройство может получить свой индивидуальный IPv6-адрес динамически, а также может быть настроено с несколькими статическими IPv6-адресами на аналогичном интерфейсе. IPv6-протокол разрешает на одном интерфейсе настройку нескольких IPv6-адресов, принадлежащих к одной IPv6-сети.

Также устройство может быть настроено с одним или несколькими IPv6-адресами шлюза по умолчанию. Для получения дополнительной информации о том, каким образом определяется, какой адрес используется в качестве IPv6-адреса источника или какой используется адрес шлюза по умолчанию, см. документ RFC 6724 «Выбор адреса по умолчанию для IPv6».

**Идентификатор интерфейса**

Если клиент не использует информацию, приведённую в объявлении маршрутизатора, и полагается исключительно на DHCPv6-сервер, то DHCPv6-сервер должен предоставить весь глобальный индивидуальный IPv6-адрес, включая префикс и идентификатор интерфейса.

Однако если используется вариант 1 (только SLAAC) или вариант 2 (SLAAC с DHCPv6), то клиент не получает фактическую часть идентификатора интерфейса адреса из этих процессов. Клиентское устройство должно определить собственный 64-битный идентификатор интерфейса либо с помощью расширенного уникального идентификатора EUI-64, либо путём создания случайного 64-битного числа.

**Сетевые IPv6-адреса**

**Индивидуальные IPv6-адреса**

**Процесс EUI-64**

Организация IEEE разработала расширенный уникальный идентификатор (EUI) или изменённый процесс EUI-64. Этот процесс использует 48-битный MAC-адрес Ethernet клиента и в середину этого адреса вставляет ещё 16 бит для создания 64-битного идентификатора интерфейса.

MАС-адреса Ethernet обычно представлены в шестнадцатеричном формате и состоят из двух частей:

* **Уникальный идентификатор организации (OUI)** — это 24-битный (шесть шестнадцатеричных цифр) код поставщика, назначенный IEEE.
* **Идентификатор устройства** — это уникальное 24-битное (6 шестнадцатеричных цифр) значение с общим уникальным идентификатором организации (OUI).

Идентификатор интерфейса в формате EUI-64 представлен в двоичном формате и состоит из трёх частей:

* 24-битный OUI на основе MAC-адреса клиента, в котором седьмой бит является обратным, т.е. если седьмой бит имеет значение 0, то он становится 1, и наоборот.
* В середину вставляется 16-битное значение FFFE (в шестнадцатеричной системе исчисления)
* 24-битный идентификатор устройства на основе MAC-адреса клиента

Процесс EUI-64 проиллюстрирован на рис. 1 с помощью MAC-адреса маршрутизатора R1 GigabitEthernet FC99:4775:CEE0.

**Шаг 1:** разделите MAC-адрес между OUI и идентификатором устройства.

**Шаг 2:** вставьте шестнадцатеричное значение FFFE в двоичном формате: 1111 1111 1111 1110.

**Шаг 3:** преобразуйте первые 2 шестнадцатеричных значения уникального идентификатора организации (OUI) в двоичный формат и отразите бит U/L (бит 7). В данном случае 0 в седьмом бите меняется на 1.

В результате генерируется следующий EUI-64 идентификатор интерфейса FE99: 47FF:FE75:CEE0.

**Примечание**. Использование обратного бита (U/L) и причины для отражения его значения описаны в документе RFC 5342.

Преимущество EUI-64 MAC-адреса Ethernet заключается в том, что его можно использовать для определения идентификатора интерфейса. Кроме того, сетевые администраторы могут легко отслеживать IPv6-адрес до конечных устройств с помощью уникального МАС-адреса. Однако это беспокоит других пользователей в связи с угрозой их конфиденциальности. Они обеспокоены тем, что их пакеты можно отследить до физического компьютера. Чтобы избежать таких осложнений, можно использовать случайно сгенерированный идентификатор интерфейса.

**Случайно сгенерированные идентификаторы интерфейса**

В зависимости от операционной системы устройство может использовать случайно сгенерированный идентификатор интерфейса вместо МАС-адресов и EUI-64. Например, начиная с Windows Vista в операционных системах Windows используется случайно сгенерированный идентификатор интерфейса вместо созданного через EUI-64. В ОС Windows XP и в предыдущих операционных системах Windows использовался EUI-64.

Как показано на рисунке, чтобы без труда определить, что адрес был создан с помощью EUI-64, нужно поместить FFFE в середину идентификатора интерфейса.

После установления идентификатора интерфейса либо с помощью EUI-64, либо через случайную генерацию его можно объединить с префиксом IPv6 для создания глобального индивидуального адреса или локального адреса канала.

* **Глобальный индивидуальный адрес**. При использовании SLAAC устройство получает свой префикс из объявления маршрутизатора ICMPv6 и объединяет его с идентификатором интерфейса.
* **Локальный адрес канала**. Локальный префикс начинается с FE80:: /10. Обычно в качестве префикса и длины префикса устройство использует FE80:: /64, за которым следует идентификатор интерфейса

**Сетевые IPv6-адреса**

**Индивидуальные IPv6-адреса**

При использовании варианта SLAAC (только SLAAC или SLAAC с DHCPV6) устройство получает префикс и длину префикса из объявления маршрутизатора ICMPv6. Поскольку префикс адреса был назначен объявлением маршрутизатора, устройство должно обеспечивать только часть идентификатора интерфейса своего адреса. Как было упомянуто ранее, идентификатор интерфейса может быть сгенерирован автоматически с помощью процесса EUI-64 или, в зависимости от ОС, сгенерирован произвольно. С помощью информации из объявления маршрутизатора и идентификатора интерфейса устройство может установить свой глобальный индивидуальный адрес.

После назначения интерфейсу глобального индивидуального адреса устройство под управлением IPv6 автоматически создаёт свой локальный адрес канала. Устройства под управлением IPv6 должны иметь как минимум локальный адрес канала. Как вы помните, локальный IPv6-адрес позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 в одной и той же подсети.

Локальные IPv6-адреса используются для различных целей, указанных ниже.

* Узел использует локальный адрес канала локального маршрутизатора для IPv6-адреса шлюза по умолчанию.
* Маршрутизаторы используют локальные адреса канала для обмена сообщениями протокола динамической маршрутизации.
* Таблицы маршрутизации маршрутизаторов используют локальный адрес канала для определения маршрутизатора следующего перехода при передаче IPv6-пакетов.

Локальный адрес канала можно настроить динамически или настроить вручную в качестве статического локального адреса канала.

**Динамическое назначение локального адреса канала**

Локальный адрес канала динамически создаётся с помощью префикса FE80:: /10 и идентификатора интерфейса.

По умолчанию маршрутизаторы Cisco IOS используют EUI-64 для создания идентификатора интерфейса для всех локальных адресов канала в IPv6-интерфейсах. Для последовательных интерфейсов маршрутизатор будет использовать MAC-адрес интерфейса Ethernet. Вспомните, что локальный адрес канала должен быть уникальным только в данном канале или сети. Однако недостаток использования динамически назначенного локального адреса канала — это его длина, которая затрудняет определение и запоминание назначенных адресов.

# Сетевые IPv6-адреса

## Индивидуальные IPv6-адреса

**Статические локальные адреса канала**

Ручная настройка локального адреса канала позволяет создавать адрес, который легче узнать и запомнить.

Локальные адреса каналов можно настраивать вручную с помощью аналогичной команды, которая использовалась для создания глобальных индивидуальных IPv6-адресов, но с дополнительным параметром:

**Router(config-if)#ipv6 address link-local-address link-local**

На рис. 1 показано, что локальный адрес канала имеет префикс в диапазоне от FE80 до FEBF. Если адрес начинается с этого хекстета (16-битный сегмент), то параметры локального канала должны следовать за адресом.

На рис. 2 показана конфигурация локального адреса канала с помощью команды **ipv6 address interface**. Локальный адрес канала FE80::1 используется для указания на то, что он принадлежит маршрутизатору R1. Такой же локальный адрес канала IPv6 настроен на всех интерфейсах маршрутизатора R1. FE80::1 можно настроить на каждом канале, поскольку он должен быть уникальным только на данном канале.

Как и в случае с маршрутизатором R1, маршрутизатору R2 будет настроен адрес FE80::2 в качестве локального адреса канала IPv6 на всех интерфейсах.

# Сетевые IPv6-адреса

## Индивидуальные IPv6-адреса

Как показано на рис. 1, команда для настройки IPv6-интерфейса схожа с командой, используемой для IPv4.

Команда **show interface** отображает MAC-адрес интерфейсов Ethernet. Процесс EUI-64 использует этот MAC-адрес для создания идентификатора интерфейса локального адреса канала. Кроме того, команда **show ipv6 interface** отображает сокращённые выходные данные для каждого из интерфейсов. Выходные данные [up/up] в той же строке, что и интерфейс, отображают состояние интерфейса 1-го и 2-го уровней. Аналогичные данные отображаются в столбцах «Состояние» и «Протокол» при выходных данных эквивалентной команды IPv4.

Обратите внимание, что каждый интерфейс располагает двумя IPv6-адресами. Второй адрес для каждого интерфейса — это глобальный индивидуальный адрес. Первый адрес, который начинается с FE80, это локальный индивидуальный адрес канала для интерфейса. Как вы помните, локальный адрес канала автоматически присоединяется к интерфейсу при назначении глобального индивидуального адреса.

Кроме того, обратите внимание, что последовательный локальный адрес маршрутизатора R1 0/0/0 идентичен интерфейсу GigabitEthernet 0/0. Последовательные интерфейсы не имеют МАС-адресов Ethernet, поэтому Cisco IOS использует MAC-адрес первого доступного интерфейса Ethernet. Это возможно благодаря тому, что локальные интерфейсы канала должны быть уникальными только на данном канале.

Как правило, локальный адрес канала интерфейса маршрутизатора — это адрес шлюза по умолчанию для устройств в данном канале или сети.

Как показано на рисунке 2, команду **show ipv6 route** можно использовать для проверки успешной установки IPv6-сетей и особых адресов IPv6-интерфейса в таблице IPv6-маршрутизации. Команда **show ipv6 route** отображает только сети на основе протокола IPv6, а не IPv4.

В таблице маршрутизации буква «С» напротив маршрута означает, что эта сеть подключена напрямую. Когда интерфейс маршрутизатора настраивается с глобальным индивидуальным адресом и находится в состоянии «up/up», IPv6-префикс и длина префикса добавляются в таблицу IPv6-маршрутизации в качестве подключённого маршрута.

Глобальный индивидуальный IPv6-адрес, настраиваемый на интерфейсе, также устанавливается в таблице маршрутизации в качестве локального маршрута. Локальный маршрут имеет префикс /128. Локальные маршруты используются таблицей маршрутизации для эффективной обработки пакетов с адресом назначения адреса интерфейса маршрутизатора.

В случаях, когда IPv6-адрес не используется, команда **ping** для протокола IPv6 должна быть аналогична команде, используемой с протоколом IPv4. Как показано на рис. 3, эта команда используется для проверки подключения 3-го уровня между маршрутизатором R1 и ПК1. При отправке эхо-запроса от маршрутизатора на локальный адрес канала Cisco IOS запросит у пользователя открыть выходной интерфейс. Поскольку локальный адрес канала назначения может находиться на одном или нескольких каналах или сетях, маршрутизатору необходимо уточнить, в какой интерфейс отправлять эхо-запрос.

Для проверки конфигурации IPv6-адресов используйте средство проверки синтаксиса (см. рис. 4).

**Сетевые IPv6-адреса**

**Групповые IPv6-адреса**

Групповые IPv6-адреса мало чем отличаются от групповых IPv4-адресов. Как вы помните, групповой адрес используется для отправки одного пакета по одному или нескольким назначениям (группе мультивещания). Групповые IPv6-адреса имеют префикс FF00::/8.

**Примечание**. Групповые адреса могут быть только адресами назначения, а не адресами источника.

Существует два типа групповых IPv6-адресов:

* присвоенный групповой адрес;
* групповой адрес запрошенного узла.

**Присвоенный групповой адрес**

Присвоенные групповые адреса зарезервированы для заданных групп устройств. Присвоенный групповой адрес — это один адрес, используемый для осуществления связи с группой устройств, работающих на одном протоколе или сервисе. Присвоенные групповые адреса используются вместе с конкретными протоколами, например с протоколом DHCPv6.

Рассмотрим две распространённые группы присвоенных групповых IPv6-адресов.

* **Группа мультивещания для всех узлов FF02::1**. Это группа мультивещания, к которой подключены все устройства под управлением протокола IPv6. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-интерфейсами в канале или сети. Эта группа адресов работает так же, как широковещательный адрес в протоколе IPv4. На рисунке приводится пример осуществления связи с использованием групповых адресов для всех узлов. IPv6-маршрутизатор отправляет объявления маршрутизатора протокола управляющих сообщений версии 6 (RA ICMPv6) группе мультивещания для всех узлов. Объявление маршрутизатора предоставляет всем устройствам IPv6, находящимся в сети, информацию об адресации: префикс, длину префикса и шлюз по умолчанию.
* **Группа мультивещания для всех маршрутизаторов FF02::2**. Это группа мультивещания, к которой подключены все IPv6-маршрутизаторы. Маршрутизатор становится частью этой группы, когда переходит под управление протоколом IPv6 с помощью команды глобальной конфигурации **ipv6 unicast-routing**. Пакет, отправленный этой группе, получается и обрабатывается всеми IPv6-маршрутизаторами в канале или сети.

Устройства под управлением протокола IPv6 отправляют сообщения с запросом маршрутизатора групповому адресу для всех маршрутизаторов. Такие сообщения запрашивают у IPv6-маршрутизатора объявление маршрутизатора, чтобы помочь устройству в процессе адресной конфигурации.

**Сетевые IPv6-адреса**

**Групповые IPv6-адреса**

Многоадресная рассылка запрашиваемого узла похожа на многоадресную рассылку всем узлам. Как вы помните, групповой адрес для всех узлов — это, по сути, то же самое, что и широковещательная IPv4-рассылка. Все устройства в сети должны обрабатывать трафик, отправляемый на адрес всех узлов. Для уменьшения количества устройств, которым необходимо обрабатывать трафик, используйте групповой адрес запрашиваемого узла.

Групповой адрес запрашиваемого узла — это адрес, который соответствует только 24 битам глобального индивидуального IPv6-адреса устройства. Обрабатывать эти пакеты должны только те устройства, которые имеют аналогичные 24 бита в наименее значащей, крайней правой части идентификатора интерфейса.

Групповой IPv6-адрес запрашиваемого узла создаётся автоматически при назначении глобального индивидуального адреса или локального адреса канала. Групповой IPv6-адрес запрашиваемого узла создаётся посредством объединения специального префикса FF02:0:0:0:0:1:FF00::/104 с крайними правыми 24 битами его индивидуального адреса.

Групповой адрес запрашиваемого узла состоит из 2 частей.

* **Групповой префикс FF02:0:0:0:0:1:FF00::/104**: первые 104 бита группового адреса запрашиваемого узла.
* **Наименее значимые 24 бита**: последние или крайние правые 24 бита группового адреса запрашиваемого узла. Эти биты копируются из крайних правых 24 битов глобального индивидуального адреса или локального адреса канала устройства.

Существует вероятность того, что у нескольких устройств будет один и тот же групповой адрес запрашиваемого узла. Довольно редко в идентификаторах интерфейса устройств встречаются одинаковые крайние правые 24 бита. Это не влечёт за собой никаких проблем, поскольку устройство по-прежнему будет обрабатывать инкапсулированное сообщение, в котором содержится полный IPv6-адрес запрашиваемого устройства.

# Сетевые IPv6-адреса

## Групповые IPv6-адреса

В этом задании вам предстоит отработать настройку IPv6-адресов на маршрутизаторе, серверах и клиентах. Кроме того, вы отработаете проверку внедрения IPv6-адресации.

[Packet Tracer: настройка IPv6-адресации (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.2.5.3%20Packet%20Tracer%20-%20Configuring%20IPv6%20Addressing%20Instructions.pdf)

[Packet Tracer: настройка IPv6-адресации (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.2.5.3%20Packet%20Tracer%20-%20Configuring%20IPv6%20Addressing.pka)

**Сетевые IPv6-адреса**

**Групповые IPv6-адреса**

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

* Часть 1: определите различные типы IPv6-адресов
* Часть 2: проанализируйте сетевой интерфейс и адрес IPv6-узла
* Часть 3: отработайте сокращение IPv6-адреса
* Часть 4: определите иерархию сетевого префикса глобального индивидуального IPv6-адреса

[Лабораторная работа: определение IPv6-адресов](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.2.5.4%20Lab%20-%20Identifying%20IPv6%20Addresses.pdf)

**Сетевые IPv6-адреса**

**Групповые IPv6-адреса**

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

* Часть 1: выполните настройку топологии и конфигурации основных параметров маршрутизатора и коммутатора
* Часть 2: выполните настройку IPv6-адресов вручную
* Часть 3: проверьте сквозное подключение

[Лабораторная работа: настройка IPv6-адресов на сетевых устройствах](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.2.5.5%20Lab%20-%20Configuring%20IPv6%20Addresses%20on%20Network%20Devices.pdf)

**Проверка соединения**

**ICMP**

Хотя IP не является надёжным протоколом, набор протоколов TCP/IP обеспечивает отправку сообщений даже в случае возникновения каких-либо ошибок. Эти сообщения отправляются с помощью ICMP-сервисов. Назначение таких сообщений — предоставлять отзывы о проблемах, связанных с обработкой IP-пакетов в определённых условиях, а не повышать надёжность протокола IP. Из соображений безопасности ICMP-сообщения не обязательны, а часто даже не разрешаются в рамках сети.

ICMP может использоваться как с IPv4, так и с IPv6. ICMPv4 — это протокол обмена сообщениями для IPv4. Протокол ICMPv6 предоставляет те же сервисы для IPv6, но при этом включает в себя дополнительные функциональные возможности. В рамках данного курса термин ICMP будет использоваться для обозначения как ICMPv4, так и ICMPv6.

Существует множество типов ICMP-сообщений, а также причин их отправки. Рассмотрим некоторые наиболее распространённые сообщения.

ICMP-сообщения, общие для ICMPv4 и ICMPv6, включают в себя:

* Подтверждение узла
* Назначение или услуга недоступны
* Истечение времени
* Переадресация маршрутов

**Подтверждение узла**

Эхо-запрос по протоколу ICMP можно использовать, чтобы определить, функционирует ли узел. Локальный узел отправляет узлу эхо-запрос ICMP. Если узел доступен, узел назначения отправляет эхо-ответ. На рисунке нажмите кнопку «Воспроизведение», чтобы посмотреть анимационное представление, иллюстрирующее принцип работы эхо-запроса и эхо-ответа ICMP. Такое использование эхо-запросов по протоколу ICMP заложено в основу служебной программы проверки связи.

**Назначение или услуга недоступны**

Когда узел или шлюз получает пакет, который не может доставить, он может использовать ICMP-сообщение «Назначение недоступно», чтобы сообщить источнику о том, что назначение или услуга для них недоступны. Такое сообщение содержит код, сообщающий, что пакет не может быть доставлен.

Коды о недоступном назначении для ICMPv4 включают в себя:

* 0 - сеть недоступна.
* 1 - узел недоступен.
* 2 - протокол недоступен.
* 3 - порт недоступен.

**Примечание**. За исключением некоторых различий, протокол ICMPv6 обладает схожими кодами для сообщений о недоступном назначении.

**Истечение времени**

Сообщение ICMPv4 об истечении времени используется маршрутизатором для указания на то, что пакет переслать невозможно, поскольку значение в поле «Время жизни» (TTL) пакета было изменено на 0. Если маршрутизатор получает пакет и изменяет значение в поле «Время жизни» (TTL) IPv4-пакета на ноль, он отбрасывает пакет и отправляет в узел источника сообщение об истечении времени.

Также протокол ICMPv6 отправляет сообщение об истечении времени в том случае, если маршрутизатор не может переслать пакет IPv6 ввиду того, что пакет истек. В протоколе IPv6 поле «Время жизни» (TTL) отсутствует. Для указания на то, что срок жизни пакета истёк, им используется поле «Ограничение перехода».

**Переадресация маршрутов**

Маршрутизатор может использовать сообщение переадресации ICMP, чтобы сообщить узлам в сети, что для определённого назначения доступен лучший маршрут. Это сообщение может использоваться только в том случае, если узел источника находится в той же физической сети, что и шлюзы.

Оба протокола ICMPv4 и ICMPv6 используют сообщения переадресации маршрута.

**Проверка соединения**

**ICMP**

Информационные сообщения и сообщения об ошибках, возникающие в протоколе ICMPv6, очень похожи на сообщения о контроле и ошибках, используемые протоколом ICMPv4. Однако протокол ICMPv6 располагает повышенной функциональностью и новыми возможностями, которых нет в ICMPv4.

ICMPv6 включает четыре новых протокола в составе протокола обнаружения соседних узлов (ND или NDP):

* Сообщение «Запрос к маршрутизатору»
* Сообщение «Объявление маршрутизатора»
* Сообщение «Запрос соседнего узла»
* Сообщение «Объявление соседнего узла»

**Сообщения «Запрос маршрутизатора» и «Объявление маршрутизатора»**

Устройства под управлением протокола IPv6 можно разделить на две категории - маршрутизаторы и узлы. Сообщения «Запрос маршрутизатора» и «Объявление маршрутизатора» передаются между узлами и маршрутизаторами.

* **Сообщения «Запрос маршрутизатора» (RS):** отправляются от узла маршрутизатору, когда узел настроен для автоматического получения своей информации по адресации с помощью SLAAC. Такой запрос отправляется в виде многоадресного сообщения IPv6 для всех узлов.
* **Сообщение «Объявление маршрутизатора» (RA):** отправляется маршрутизаторами для предоставления узлам информации об адресации с помощью SLAAC. Такое сообщение может включать в себя информацию об адресации для узла, например префикс и длину префикса. Маршрутизатор отправляет подобное сообщение либо периодически, либо в ответ на сообщение запроса маршрутизатора. По умолчанию маршрутизаторы Cisco отправляют подобные сообщения каждые 200 секунд. Объявления маршрутизатора отправляются на групповые IPv6-адреса для всех узлов. Узел, использующий SLAAC, выполнит настройку шлюза по умолчанию для локального адреса канала того маршрутизатора, который отправил объявление RA.

**Проверка соединения**

**ICMP**

Протокол обнаружения соседских узлов ICMPv6 включает в себя два дополнительных типа сообщений: «Запрос соседнего узла» (NS) и «Объявление соседнего узла» (NA).

Такие сообщения используются для:

* разрешения адресов;
* обнаружения адресов-дубликатов (DAD).

**Разрешение адресов**

Разрешение адресов используется в том случае, когда устройству в локальной сети известен индивидуальный IPv6-адрес назначения, но неизвестен MAC-адрес Ethernet. Чтобы определить MAC-адреса назначения, устройство отправляет запрос соседнего узла на адрес запрашиваемого узла. Сообщение будет содержать известный (целевой) IPv6-адрес. Устройство, которое располагает целевым адресом IPv6, отправляет в ответ объявление соседнего узла, которое содержит его MAC-адрес Ethernet.

**Обнаружение адресов-дубликатов (DAD)**

Когда устройству назначен глобальный индивидуальный адрес или локальный индивидуальный адрес канала, на этом адресе рекомендуется осуществить обнаружение адресов-дубликатов, чтобы убедиться в его уникальности. Для проверки уникальности адреса устройство отправит запрос соседнего узла со своим собственным IPv6-адресом в качестве целевого. Если другое устройство в сети обладает тем же адресом, оно отвечает объявлением соседнего узла. Такое объявление соседнего узла уведомит устройство отправителя о том, что данный адрес уже используется. Если соответствующее объявление соседнего узла не возвращается по истечении определённого периода времени, индивидуальный адрес признаётся уникальным и допустимым к использованию.

**Примечание**. Обнаружение адресов-дубликатов не обязательно, однако документ RFC 4861 рекомендует применять этот процесс на индивидуальных адресах.

# Проверка соединения

## Тестирование и проверка

Эхо-запрос — это инструмент тестирования, использующий эхо-запросы и эхо-ответы ICMP для проверки соединения между узлами. Эхо-запрос работает с узлами под управлением протоколов IPv4 и IPv6.

Для проверки соединения с другим узлом в сети с помощью команды **ping** на узловой адрес отправляется эхо-запрос. Если узел с указанным адресом получает эхо-запрос, он отправляет эхо-ответ. После получения каждого эхо-ответа служба эхо-тестирования предоставляет данные о времени, прошедшем между отправкой запроса и получением ответа. Это позволяет измерить производительность сети.

Время для получения эхо-ответа ограничено. Если в течение лимита времени эхо-ответ не получен, служба тестирования сообщает, что ответа нет. Обычно это свидетельствует о наличии проблемы, но также это может указывать на то, что в сети функционируют меры безопасности, которые блокируют эхо-запросы.

После отправки всех запросов служба тестирования предоставляет сводную информацию, которая включает в себя количество успешных попыток и данные о среднем времени прохождения от источника к назначению.

**Отправка эхо-запроса на локальные loopback-адреса**

Мы используем эхо-запросы в особых случаях проверки и тестирования соединения. Один из таких случаев — тестирование внутренней конфигурации IPv4 или IPv6 на локальном узле. Для выполнения такой проверки мы отправляем эхо-запрос на локальный loopback-адрес 127.0.0.1 для IPv4 (:: 1 для IPv6). Тестирование loopback-адреса IPv4 показано на рисунке.

Ответ от адреса 127.0.0.1 для IPv4 или :: 1 для IPv6 означает, что IP-сеть настроена на узле правильно. Этот ответ поступает с сетевого уровня. Однако ответ не является признаком того, что адреса, маски или шлюзы были настроены верно. Также он не указывает на состояние нижнего уровня сетевого стека. Ответ является результатом проверки IP-сети через сетевой уровень. Если мы получаем сообщение об ошибке, это означает, что протокол управления передачей не работает на данном узле.

# Проверка соединения

## Тестирование и проверка

Кроме того, можно использовать эхо-запрос, чтобы проверить способность узла обмениваться данными в своей локальной сети. Обычно для этого отправляется эхо-запрос на IP-адрес шлюза узла. Эхо-запрос на шлюз указывает на то, что интерфейсы узла и маршрутизатора, функционирующие в качестве шлюза, работают в локальной сети.

Для этой проверки чаще всего используется адрес шлюза, поскольку, как правило, маршрутизатор всегда находится в рабочем состоянии. Если адрес шлюза не отвечает, эхо-запрос можно отправить на IP-адрес другого узла в локальной сети, который наверняка является рабочим.

Если отвечает либо шлюз, либо другой узел, то локальный узел может уверенно обмениваться данными по локальной сети. Если шлюз не отвечает, зато отвечает другой узел, это может свидетельствовать о проблеме с интерфейсом маршрутизатора, который работает в качестве шлюза.

Возможно, на узле был настроен неверный адрес шлюза. Также существует вероятность того, что интерфейс маршрутизатора работает исправно, но функционирующие на нём меры безопасности не позволяют ему обрабатывать или отвечать на эхо-запросы.

# Проверка соединения

## Тестирование и проверка

Кроме того, эхо-запрос можно использовать для проверки возможности локального узла обмениваться данными по объединённой сети. Как показано на рисунке, локальный узел может отправлять эхо-запрос на рабочий IPv4-узел удалённой сети.

Если эхо-запрос обработан успешно, то сетевое взаимодействие признаётся возможным. Успешное тестирование с помощью эхо-запроса по сетевому взаимодействию подтверждает возможность коммуникации в локальной сети, работу маршрутизатора, выступающего в качестве нашего шлюза, а также работу всех других маршрутизаторов, которые могут оказаться на пути между локальной сетью и сетью удалённого узла.

Кроме того, может быть подтверждена функциональность удалённого узла. Если удалённый узел не поддерживает коммуникацию вне локальной сети, то он не может ответить на эхо-запрос.

**Примечание**. Многие сетевые администраторы ограничивают или запрещают ввод ICMP-сообщений в корпоративную сеть; в связи с этим меры по обеспечению безопасности могут стать причиной отсутствия эхо-ответа.

# Проверка соединения

## Тестирование и проверка

Эхо-запрос используется для проверки связи между двумя узлами, но не предоставляет информацию об устройствах на пути между узлами. Трассировка маршрута (команда «tracert») создаёт список успешных переходов по заданному пути. Этот список может включать в себя важные данные о проверке и устранению неисправностей. Если узел назначения получает данные, то процесс трассировки маршрута указывает интерфейсы каждого маршрутизатора на пути между узлами. Если при каком-либо переходе возникли проблемы с передачей данных, адрес последнего ответившего маршрутизатора указывает, где возникла проблема или какие были обнаружены ограничения.

**Время прохождения сигнала в прямом и обратном направлениях (RTT)**

Процесс трассировки маршрута указывает время прохождения сигнала в прямом и обратном направлениях для каждого узла на пути передачи, а также позволяет определить неудавшиеся переходы. Время прохождения сигнала в прямом и обратном направлениях — это время, необходимое для достижения пакетом удалённого узела и для получения ответа от этого целевого узла. Звёздочка (\*) используется для обозначения потерянного пакета или пакета без ответа.

Эту информацию можно использовать для поиска проблемного маршрутизатора на пути. Если в результате трассировки выявлены потери данных или превышение допустимого времени ответа, это указывает на проблемы с ресурсами маршрутизатора или его соединениями.

**Время жизни (TTL) IPv4 и предел переходов IPv6**

Процесс трассировки маршрута использует поля «Время жизни (TTL)» в протоколе IPv4 и «Предел переходов» в IPv6 в заголовках 3-го уровня вместе с сообщением об истечении времени ICMP.

Чтобы увидеть, как трассировка маршрута использует преимущества TTL, включите анимационное представление на рисунке.

Первая последовательность сообщений, отправленных при трассировке маршрута, укажет в поле «Время жизни (TTL)» значение 1. Это приводит к истечению времени жизни (TTL) IPv4-пакета на первом маршрутизаторе. Затем этот маршрутизатор отвечает ICMPv4-сообщением. Теперь трассировка маршрута располагает адресом первого перехода.

Затем трассировка маршрута постепенно увеличивает значение в поле «Время жизни (TTL)» (2, 3, 4...) для каждой последовательности сообщений. Таким образом, трассировка маршрута получает адрес каждого перехода по мере того, как время пакетов истекает по пути. Значение в поле «Время жизни (TTL)» продолжает увеличиваться, пока не будет достигнуто место назначения или максимальное значение.

По достижении конечного назначения узел отвечает либо сообщением о недостижимом порте ICMP, либо эхо-ответом ICMP вместо сообщения об истечении времени ICMP.

# Проверка соединения

## Тестирование и проверка

Протоколы IPv4 и IPv6 могут сосуществовать в одной сети. В командной строке ПК существуют некоторые различия в том, как вводятся команды и отображаются выходные данные.

[Packet Tracer: проверка адресации IPv4 и IPv6 (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.5%20Packet%20Tracer%20-%20Verifying%20IPv4%20and%20IPv6%20Addressing%20Instructions.pdf)

[Packet Tracer: проверка адресации IPv4 и IPv6 (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.5%20Packet%20Tracer%20-%20Verifying%20IPv4%20and%20IPv6%20Addressing.pka)

# Проверка соединения

## Тестирование и проверка

В этом задании имеются проблемы подключения. Помимо сбора и документирования информации о сети, необходимо определить проблемы и использовать приемлемые решения для восстановления соединения.

[Packet Tracer: отправка эхо-запросов и выполнение трассировки маршрута для проверки пути (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.6%20Packet%20Tracer%20-%20Pinging%20and%20Tracing%20to%20Test%20the%20Path%20Instructions.pdf)

[Packet Tracer: отправка эхо-запросов и выполнение трассировки маршрута для проверки пути (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.6%20Packet%20Tracer%20-%20Pinging%20and%20Tracing%20to%20Test%20the%20Path.pka)

**Проверка соединения**

**Тестирование и проверка**

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

* Часть 1: создайте сеть и выполните её настройку
* Часть 2: используйте команду «ping» для базового тестирования сети
* Часть 3. Тестирование основной сети с помощью команд tracert и traceroute
* Часть 4. Поиск и устранение неисправностей в топологии

[Лабораторная работа: тестирование сетевого подключения с помощью команд «ping» и «traceroute»](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.7%20Lab%20-%20Testing%20Network%20Connectivity%20with%20Ping%20and%20Traceroute.pdf)

# Проверка соединения

## Тестирование и проверка

Вы — специалист по сетевым подключениям в компании, которая приняла решение отказаться от использования протокола IPv4 и перейти на протокол IPv6. Но пока необходима поддержка обоих протоколов (двойной стек). В справочную службу обратились три сотрудника, у которых возникли некоторые проблемы. Им оказали ограниченную помощь. Справочная служба переадресовала вопрос вам, специалисту 2-го уровня по техническим вопросам.

[Packet Tracer: устранение проблем во время адресации IPv4 и IPv6 (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.8%20Packet%20Tracer%20-%20Troubleshooting%20IPv4%20and%20IPv6%20Addressing%20Instructions.pdf)

[Packet Tracer: устранение проблем во время адресации IPv4 и IPv6 (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.3.2.8%20Packet%20Tracer%20-%20Troubleshooting%20IPv4%20and%20IPv6%20Addressing.pka)

**Заключение**

**Заключение**

**Настоящий Всеобъемлющий Интернет!**

В этой главе вы узнали о том, как предприятия малого и среднего бизнеса подключаются к сети группами. Также в начале упражнения по моделированию мы рассмотрели основы Всеобъемлющего Интернета

Для этого упражнения выберите одну из следующих тем:

* Совершение банковских операций онлайн
* Международные новости
* Прогноз погоды
* Условия дорожного движения

Разработайте схему IPv6-адресации для выбранной темы. Включите в эту схему план следующих операций:

* Разделение на подсети
* Одноадресные рассылки
* Многоадресные рассылки
* Широковещательные рассылки

Сохраните копию схемы, чтобы позже показать её группе или другим учащимся. Будьте готовы объяснить следующие аспекты.

* Способы совместного использования одноадресных, многоадресных и широковещательных рассылок после разделение на подсети.
* Области применения созданной вами схемы адресации.
* Последствия применения вашего плана в работе небольших и средних предприятий.

[Работа в аудитории: настоящий Всеобъемлющий Интернет! (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.4.1.1%20The%20Internet%20of%20Everything...Naturally%20Instructions.pdf)

# Заключение

## Заключение

Ваша компания получила контракт на установку небольшой сети для одного ресторатора. Ему принадлежат два ресторана, которые находятся рядом друг с другом и используют одно общее подключение. Оборудование и кабели установлены, сетевым администратором разработан план реализации. Вам необходимо применить оставшуюся часть схемы адресации в соответствии с сокращённой таблицей адресации и проверить соединение.

[Packet Tracer: отработка комплексных практических навыков (инструкции)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge%20Instructions.pdf)

[Packet Tracer: отработка комплексных практических навыков (PKA)](https://static-course-assets.s3.amazonaws.com/ITN50RU/files/8.4.1.2%20Packet%20Tracer%20-%20Skills%20Integration%20Challenge.pka)

# Заключение

## Заключение

IP-адреса представляют собой иерархическую структуру с сетевой частью, маской подсети и узловой частью. IP-адрес может представлять всю сеть, определённый узел или сетевой адрес широковещательной рассылки.

Понимание двоичной системы исчисления особенно важно, чтобы установить, находятся ли два узла в одной и той же сети. Биты в сетевой части IP-адреса должны быть идентичны для всех устройств, которые находятся в одной и той же сети. Маска подсети или префикс используется для определения сетевой части IP-адреса. IP-адреса можно присваивать статически или динамически. DHCP обеспечивает автоматическое присвоение информации об адресе, например IP-адреса, маски подсети, шлюза по умолчанию и других параметров.

IPv4-узлы могут обмениваться данными с помощью одного из трёх способов: одноадресной, широковещательной или многоадресной рассылки. Кроме того, блоки адресов, которые используются в сетях, требующих ограниченного доступа в Интернет или не требующих его совсем, называются частными адресами. Блоки частного IPv4-адреса имеют следующий вид: 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16.

Сокращение адресного пространства протокола IPv4 — основной стимулирующий фактор для перехода к использованию IPv6. Каждый IPv6-адрес имеет 128 бит вместо 32 бит, как в протоколе IPv4. IPv6 не использует для маски подсети десятичное представление с разделительными точками. Длина префикса используется для обозначения сетевой части IPv6-адреса с помощью следующего формата: IPv6-адрес/длина префикса.

Существует три типа IPv6-адресов: индивидуальные, групповые и произвольные. Локальный IPv6-адрес канала позволяет устройству обмениваться данными с другими устройствами под управлением IPv6 по одному и тому же каналу и только по данному каналу (подсети). Пакеты с локальным адресом канала источника или назначения не могут быть направлены за пределы того канала, в котором пакет создаётся. Локальные IPv6-адреса канала находятся в диапазоне FE80::/10.

ICMP может использоваться как с IPv4, так и с IPv6. ICMPv4 — это протокол обмена сообщениями для IPv4. Протокол ICMPv6 предоставляет IPv6 аналогичные сервисы, но при этом включает в себя дополнительные функциональные возможности.

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