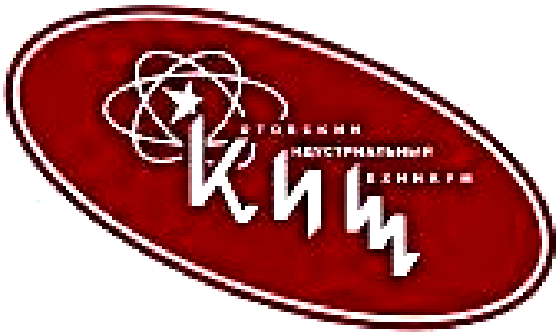
Управление образования и науки Тамбовской области
Тамбовское областное государственное бюджетное профессиональное образовательное учреждение
«Котовский индустриальный техникум»



Методическая разработка по дисциплине «ЭОСИ» IPv4-адресация

Выполнил: Мухин А.С.

Котовск, 2016

IPv4-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.

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 «A» в коде ASCII представлена в виде бита 01000001. В свою очередь, буква нижнего регистра «a» представлена в виде бита 01100001.

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).

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)

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

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.

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.

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.

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.

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. 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.

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.

Обратите внимание, что сетевой адрес может не меняться, но диапазон узлов и широковещательный адрес отличаются в зависимости от длины префикса. 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.

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. 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, 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.

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.

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.

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.

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. Чтобы настроить статический IPv4-адрес, выберите IPv4 на экране сетевого адаптера, затем ключ в статическом адресе, маску 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.

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).

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.

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.

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.

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.

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. 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.

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. 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.

Исторически сложилось так, что назначенные адреса (RFC1700) сгруппировали одноадресные диапазоны в адреса с особыми размерами, которые называются адресами класса A, класса B и класса C. Кроме того, были определены адреса класса D (групповые) и класса E (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 A

Блок адресов класса A разработан для поддержки очень крупных сетей, содержащих более чем 16 миллионов адресов узлов. Для обозначения сетевого адреса

IPv4-адреса класса A использовали фиксированный префикс /8 с первым октетом. Остальные три октета использовались для адресов узлов. Все адреса класса A требуют, чтобы самый старший разряд старшего октета был равен нулю. Это означает, что существовало только 128 возможных сетей класса A, от 0.0.0.0/8 до 127.0.0.0 /8. Даже если адреса класса A 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 A, 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 A, поскольку 25% его общего пространства IPv4-адресов было разделено среди примерно 16 000 сетей.

Блоки класса C

Адресное пространство класса C 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 C использовали префикс /24. Это означает, что сеть класса C использовала только последний октет в качестве адресов узлов с тремя старшими октетами, используемыми для обозначения сетевых адресов. Блоки адресов класса C отделяли адресное пространство с помощью фиксированного значения 110 самых старших разрядов старшего октета. Это ограничило блок адресов класса C 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.

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 A, 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.

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) 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).

Основные реестры:

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

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.

Уровень 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

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

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.