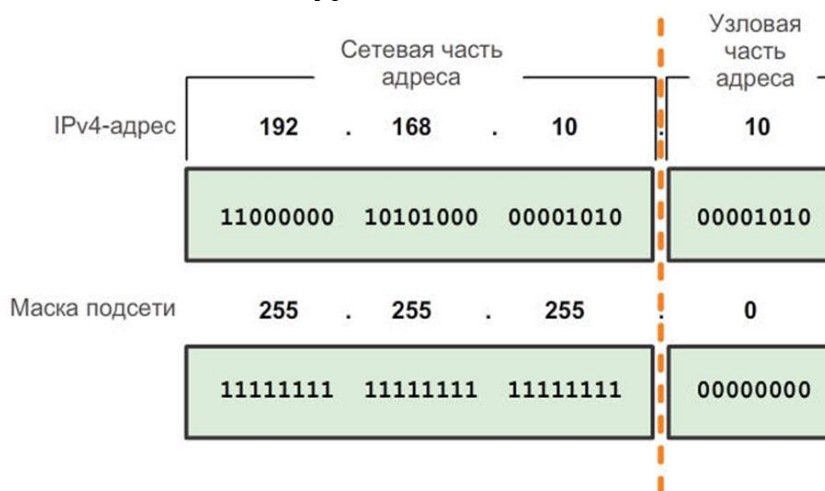


Тема 2 IP - адресация

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.

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

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 префиксы

	Десятичное представление с разделительными точками	Значимые биты, отображаемые в двоичном формате
Сетевой адрес	10.1.1.0/24	10.1.1.00000000
Адрес первого узла	10.1.1.1	10.1.1.00000001
Адрес последнего узла	10.1.1.254	10.1.1.11111110
Широковещательный адрес	10.1.1.255	10.1.1.11111111
Количество узлов: $2^8 - 2 = 254$ узлов		
Сетевой адрес	10.1.1.0/25	10.1.1.00000000
Адрес первого узла	10.1.1.1	10.1.1.00000001
Адрес последнего узла	10.1.1.126	10.1.1.0.11111110
Широковещательный адрес	10.1.1.127	10.1.1.01111111
Количество узлов: $2^7 - 2 = 126$ узлов		
Сетевой адрес	10.1.1.0/26	10.1.1.00000000
Адрес первого узла	10.1.1.1	10.1.1.00000001
Адрес последнего узла	10.1.1.62	10.1.1.00111110
Широковещательный адрес	10.1.1.63	10.1.1.00111111
Количество узлов: $2^6 - 2 = 62$ узлов		

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.

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.

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. 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. 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.

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

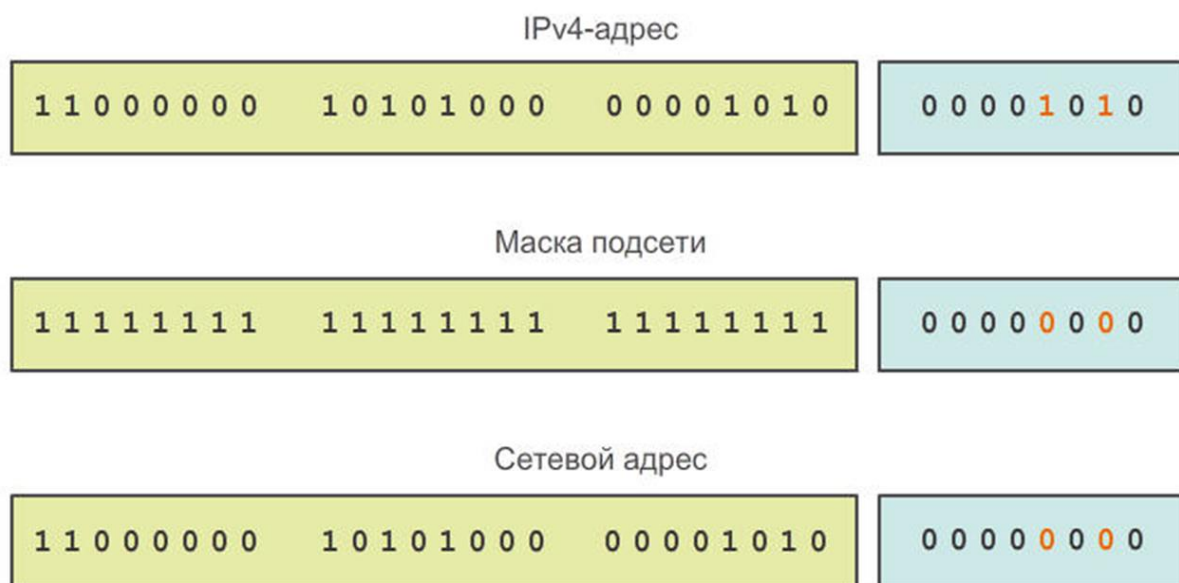
Как видно на рисунке 1, узловая часть первого адреса узла будет содержать все нулевые биты с единицей в крайнем справа бите. Значение этого адреса всегда на единицу больше сетевого адреса. В этом примере первым адресом узла в сети 10.1.1.0/24 является 10.1.1.1. Часто во многих схемах адресации первый 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. Последним адресом узла в сети 10.1.1.0/24 является 10.1.1.254.

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.



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.

$$1 \text{ И } 1 = 1 \quad 1 \text{ И } 0 = 0 \quad 0 \text{ И } 1 = 0 \quad 0 \text{ И } 0 = 0$$

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.

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. 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.

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.

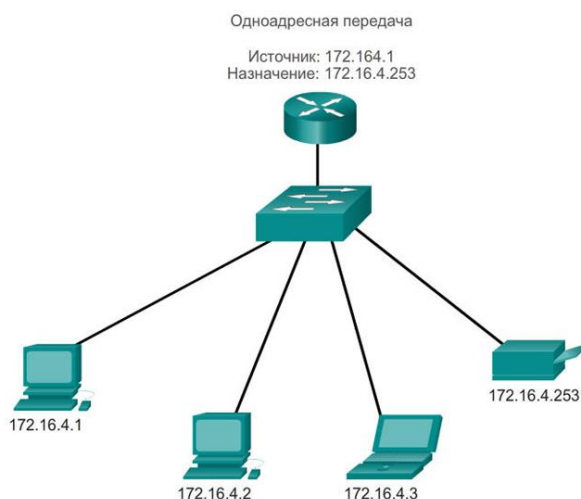
Если на узловом устройстве включён DHCP, команду **ipconfig** можно использовать для просмотра информации об IP-адресе, присвоенном DHCP-серверу.

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.

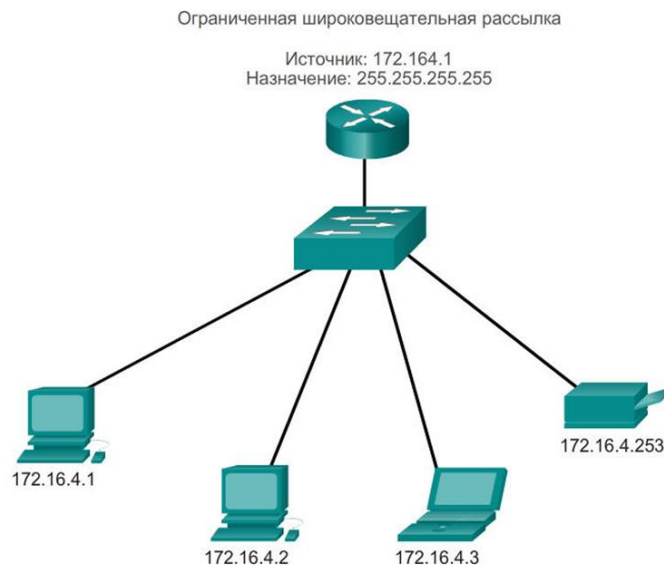
Одноадресный трафик



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.

В IPv4-сети индивидуальные адреса, применяемые к конечному устройству, называются узловыми адресами. Для одноадресной передачи адреса, присвоенные двум конечным 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.

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 получают и обрабатывают 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.

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 мультитещения. Это диапазон адресов составляет от 224.0.0.0 до 239.255.255.255.

Групповые адреса IPv4 от 224.0.0.0 до 224.0.0.255 являются зарезервированными локальными адресами. Эти адреса используются группами мультитещения в локальной сети. Маршрутизатор, подключённый к локальной сети, распознаёт, что эти пакеты адресованы локальной группе мультитещения, 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.

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. 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, 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.

Классы IPv4-адресов

Классы IP-адресов					
Класс адреса	Диапазон 1-го октета (десятичное представление)	Биты 1-го октета (зелёные биты не меняются)	Сетевая (C) и узловая (Y) части адреса	Маска подсети по умолчанию (в двоичном и десятичном форматах)	Число возможных сетей и узлов для каждой сети
A	1-127**	00000000- 01111111	N.N.N.N	255.0.0.0	128 сетей (2^7) 16 777 214 узлов для каждой сети (2^{24-2})
B	128-191	10 000000- 10111111	N.N.N.N	255.255.0.0	16 384 сети (2^{14}) 65 534 узла для каждой сети (2^{16-2})
C	192-223	110 00000- 11011111	N.N.N.N	255.255.255.0	2 097 150 сетей (2^{21}) 254 узла для каждой сети (2^{8-2})
D	224-239	11100000- 11101111	Многоадресная передача NA		
E	240-255	11110000- 11111111	NA (экспериментальное)		

Примечание. Все адреса узлов, состоящие только из нулей (0) или единиц (1), являются недействительными.

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 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 В

Адресное пространство класса В разработано для поддержки потребностей небольших и крупных сетей, содержащих приблизительно 65 000 узлов. IP-адрес класса В 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 В два самых старших разряда старшего октета равны 10. Это ограничивает блок адресов для класса В от 128.0.0.0/16 до 191.255.0.0/16. Назначение адресов класса В 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 объема 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 В 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: А, В или С. Затем

операционная система принимает префикс, используемый этим классом, и назначает маску подсети по умолчанию.