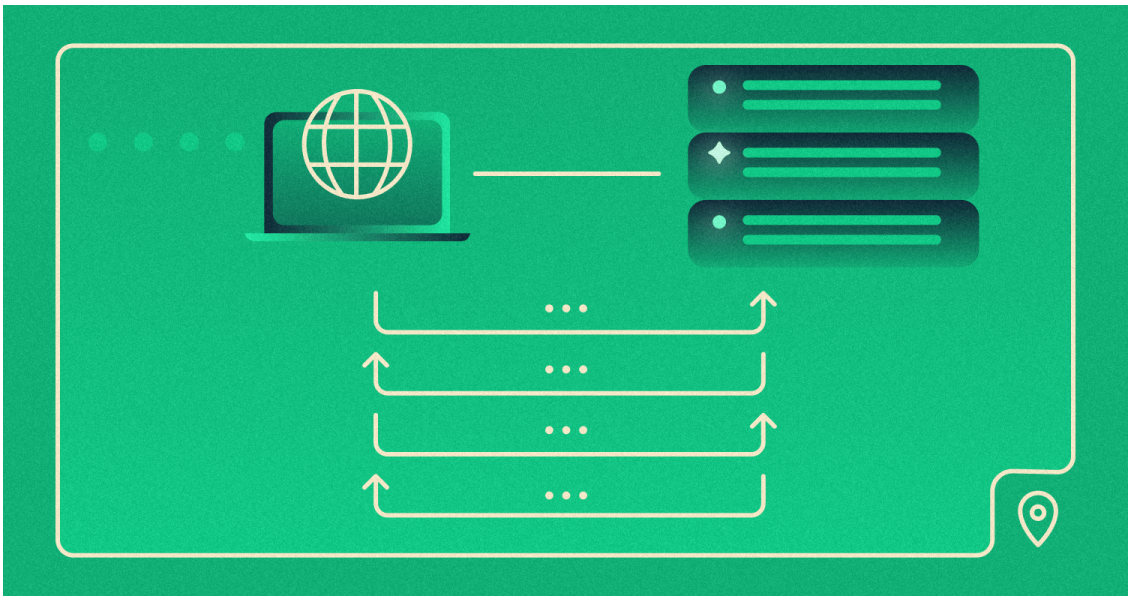
Принципы работы протокола DHCP

В статье рассказываем о принципах работы DHCP-протокола, процессе DORA, основных опциях и других его аспектах.

Эта инструкция — часть курса «Как работают сетевые протоколы».

Смотреть весь курс



Для чего нужен протокол DHCP

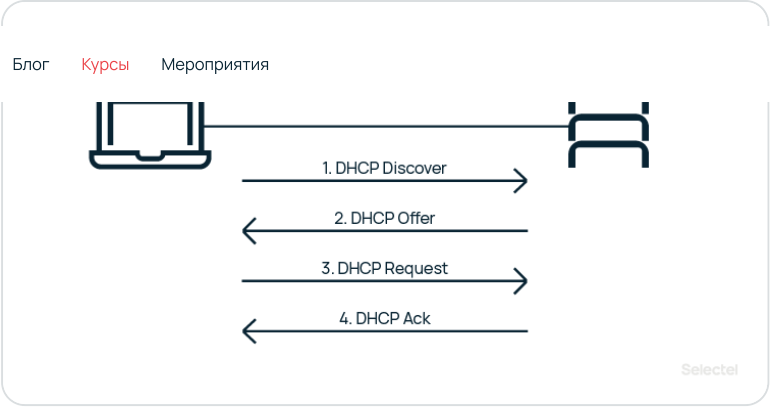
DHCP — протокол прикладного уровня модели TCP/IP, служит для назначения IP-адреса клиенту. Это следует из его названия — Dynamic Host Configuration Protocol. IP-адрес можно назначать вручную каждому клиенту, то есть компьютеру в локальной сети. Но в больших сетях это очень трудозатратно, к тому же, чем больше локальная сеть, тем выше возрастает вероятность ошибки при настройке. Поэтому для автоматизации назначения IP был создан протокол DHCP.

Впервые протокол был описан в 1993 году в документе RFC 1531, но с тех пор в описание вносились правки. На сегодняшний день основным документом, регламентирующим протокол, является RFC 2131. Помимо автоматизации процесса настройки IP, DHCP позволяет упростить диагностику подключения и переход из одной подсети в другую, оставляя уведомления для системного администратора в логах.

Принцип работы DHCP

Из вступления ясно, какие функции предоставляет DHCP, но по какому принципу он работает? Получение адреса проходит в четыре шага. Этот процесс называют DORA по первым буквам каждого шага: Discovery, Offer, Request, Acknowledgement.

Давайте подробнее рассмотрим DORA — принцип работы DHCP.



Протокол DHCP, получение адреса IP — DORA

Discovery, или поиск

Изначально клиент находится в состоянии инициализации (INIT) и не имеет своего IP-адреса. Поэтому он отправляет широковещательное (broadcast) сообщение DHCPDISCOVER на все устройства в локальной сети. В той же локальной сети находится DHCP-сервер. DHCP-сервер — это, например, маршрутизатор или коммутатор, существуют также выделенные DHCP-серверы.

Не всегда одну сеть обслуживает один DHCP-сервер, нередко организации устанавливают сразу несколько. Какие порты использует DHCP? Сервер всегда слушает 67 порт, ожидает широковещательное сообщение от клиента, а после его получения отправляет ответное предложение — DHCPOFFER. Клиент принимает сообщение на 68 порту.

Offer, или предложение

DHCP-сервер отвечает на поиск предложением, он сообщает IP, который может подойти клиенту. IP выделяются из области (SCOPE) доступных адресов, которая задается администратором.

Если имеются адреса, которые не должны быть назначены DHCP-сервером, область можно ограничить, указав только разрешенные адреса. Например, администратор может задать диапазон используемых IP-адресов от 192.0.0.10 до 192.0.0.254.

Бывает и так, что не все доступные адреса должны быть назначены клиентам. Например, администратор может исключить (exclude) диапазон 192.0.0.100 — 192.0.0.200 из используемой области. Такое ограничение называется исключением.

DHCP выделяет доступные IP-адреса из области только временно (об этом позже), поэтому нет гарантии, что при следующем подключении у данного клиента останется прежний IP. Но есть возможность назначить какому-либо клиенту определенный IP навсегда. К примеру, забронировать 192.0.0.10 за компьютером системного администратора. Такое сохранение IP для отдельных клиентов называют резервацией (reservation).

DHCPOFFER содержит IP из доступной области, который предлагается клиенту отправкой широковещательного (broadcast, «если вы тот, кто запрашивал IP-адрес, то доступен вот такой») или прямого (unicast, «вы запрашивали IP, предлагаю вот такой») сообщения. При этом, поскольку нужный клиент пока не имеет IP, для отправки прямого сообщения он идентифицируется по MAC-адресу.

Request, или запрос

Клиент получает DHCPOFFER, а затем отправляет на сервер сообщение DHCPREQUEST. Этим сообщением он принимает предлагаемый адрес и уведомляет DHCP-сервер об этом. Широковещательное сообщение почти полностью дублирует DHCPDISCOVER, но содержит в себе уникальный IP, выделенный сервером. Таким образом, клиент сообщает всем доступным DHCP-серверам «да, я беру этот адрес», а сервера помечают IP как занятый.

Сервер получает от клиента DHCPREQUEST и окончательно подтверждает передачу IP-адреса клиенту сообщением DHCPACK. Это широковещательное или прямое сообщение утверждает не только владельца IP, но и срок, в течение которого клиент может использовать этот адрес.

Со схемой отправки сообщений разобрались, но, если в сети несколько DHCP-серверов, пославших предложение, какое из них выберет клиент? Хороший вопрос. В состоянии INIT, если клиент получает адрес впервые, он будет принимать только первое предложение IP. Однако, если клиент уже общался ранее с определенным DHCP-сервером, он отдаст предпочтение этому серверу и, наоборот, сервер выберет знакомого клиента.

Срок аренды

Когда DHCP-сервер выделяет IP из области, он оставляет запись о том, что этот адрес зарезервирован за клиентом с указанием срока действия IP. Этот срок действия называется срок аренды (lease time). Срок аренды по умолчанию выставлен на 24 часа, но может доходить до нескольких дней, недель или даже месяцев. Период задается в настройках самого сервера.

Предоставление адреса в аренду, а не на постоянной основе необходимо по нескольким причинам. Во-первых, это разумное использование IP-адресов — отключенные или вышедшие из строя клиенты не резервируют за собой адрес. Во-вторых, это гарантия того, что новые клиенты при необходимости смогут получить уникальный адрес.

После получения адреса из области, клиент берет его в аренду на время, называемое T. Клиент переходит в связанное (BOUND) состояние и продолжает нормальную работу, пока не наступит время половины срока аренды — T1.

По наступлении T1 клиент инициализирует процедуру получения нового IP или обновления адреса — состояние RENEWING. Процесс повторного получения происходит по упрощенной схеме: клиент прямым сообщением запрашивает (DHCPREQUEST), а сервер подтверждает (DHCPACK) запрос. Время аренды начинает отсчитываться заново.

Если подтверждение (DHCPACK) от сервера не поступает, клиент снова запрашивает адрес, но только когда истекает половина T1. Если запрос адреса остается без ответа второй раз, клиент отправляет еще одно сообщение, когда истекает половина от T1/2 (25% от полного срока аренды). Следующий запрос будет отправлен после истечения еще половины оставшегося времени, потом еще половины. И так далее, пока не наступит T2, которое равняется 87,5%, или 7/8 от всего времени аренды. После T2 все попытки продлить аренду IP будут широковещательными. Это значит, что, если первый сервер по какой-то причине недоступен, на запрос адреса сможет ответить любой другой, и работа не будет прервана.

Три подхода к распределению адресов

Сервер назначает IP одним из трех основных способов.

Статическое распределение (static allocation). Почти как ввод адреса на каждом компьютере вручную. Отличие в том, что системный администратор задает нужные соответствия IP для MAC-адресов клиентов на самом DHCP-сервере. IP останется за клиентом, даже если тот выйдет из сети, отключится, перейдет в новую сеть и т.п.

Автоматическое распределение (automatic allocation). Сервер закрепляет IP из области за каждым клиентом навсегда. Срок аренды не ограничен.

Динамическое распределение (dynamic allocation). DHCP-сервер назначает адрес из области на определенное время, называемое сроком аренды. Такой подход полезен, если число доступных IP ограничено. IP назначается каждому клиенту при подключении к сети и возвращается в область, как только клиент его освобождает. В таком случае IP может отличаться при каждом подключении, но обычно назначается прежний.

Особые DHCP сообщения

Кроме DORA — четырех сообщений для получения адреса — DHCP использует и является неправильным, так как RFC 2131 регламентирует именно NAK. DHCPNAK отправляется сервером вместо окончательного подтверждения. Такой отказ может быть отправлен клиенту, если аренда запрашиваемого IP истекла или клиент перешел в новую подсеть.

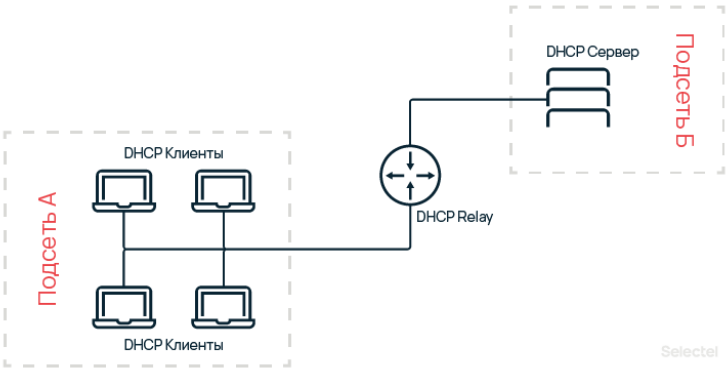
DHCPRELEASE. Клиент отправляет это сообщение, чтобы уведомить сервер об освобождении занимаемого IP. Иными словами, это досрочное окончание аренды.

DHCPINFORM. Этим сообщением клиент запрашивает у сервера локальные настройки. Отправляется, когда клиент уже получил IP, но для правильной работы ему требуется конфигурация сети. Сервер информирует клиента ответным сообщением с указанием всех запрошенных опций.

Опции DHCP

Для работы в сети клиенту требуется не только IP, но и другие параметры DHCP — например, маска подсети, шлюз по умолчанию и адрес сервера. Опции представляют собой пронумерованные пункты, строки данных, которые содержат необходимые клиенту сервера параметры конфигурации. Дадим описания некоторым опциям:

- Option 1 — маска подсети IP;
- Option 3 — основной шлюз;
- Option 6 — адрес сервера DNS (основной и резервный);
- Option 51 определяет, на какой срок IP-адрес предоставляется в аренду клиенту;
- Option 55 — список запрашиваемых опций. Клиент всегда запрашивает опции для правильной конфигурации. Отправляя сообщение с Option 55, клиент выставляет список запрашиваемых числовых кодов опций в порядке предпочтения. DHCP-сервер старается отправить ответ с опциями в том же порядке.



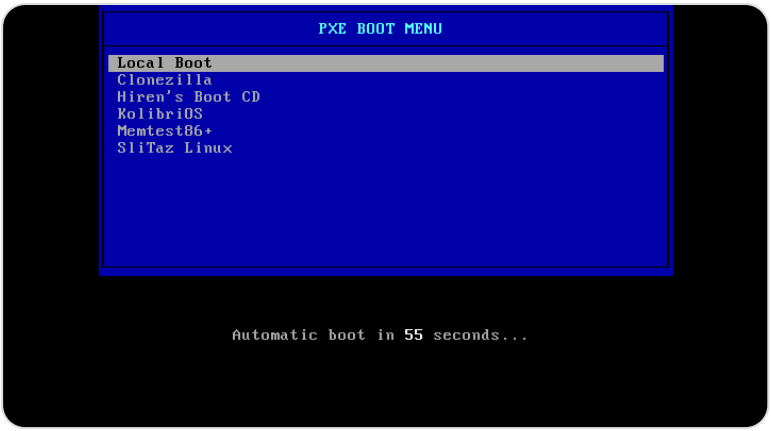
Option 82 — ретрансляция DHCP-сервера

Option 82 — информация об агенте ретрансляции (relay agent information). Благодаря ретранслятору клиент и сервер могут общаться, находясь в разных подсетях. По умолчанию широковещательные сообщения не могут выходить за пределы текущего широковещательного домена (подсети). Внимательный читатель скажет, что выше мы писали, как клиент отправляет широковещательное сообщение DHCPDISCOVER всем доступным DHCP-серверам. А что если в сети нет DHCP?

Предположим, широковещательные сообщения не выходят за пределы подсети компании, которая не установила DHCP-сервер. В таком случае сообщение DHCPDISCOVER должно будет пропасть, и ни один компьютер компании не сможет выйти в интернет. Однако в реальности отсутствие DHCP-сервера не мешает выходу в сеть.

Значит ли это, что широковещательные сообщения каким-то образом выходят за пределы подсети? Не совсем. За пределы подсети выходят только широковещательные DHCP-сообщения. Это становится возможным благодаря агенту ретрансляции. Обычно в его роли выступает маршрутизатор или сервер. Ретранслятор получает сообщения от клиента в своей подсети, направляют его

на DHCP-сервер, который тем же образом — через ретранслятор — отправляет



Опции DHCP для загрузки PXE

Протокол DHCP позволяет загрузку компьютера без использования носителя данных. Такая загрузка происходит с сетевой карты и называется PXE (Preboot eXecution Environment). Для конфигурации сетевой загрузки LEGACY BIOS PXE используются DHCP-опции 43, 60, 66 и 67.

— Option 43 зарезервирована для обмена информацией производителей;
— Option 60 — классовый идентификатор; здесь указывается, например, PXE клиент;
— Option 66 и 67 необходимы для указания имени сервера PXE и имени файла загрузки соответственно.

Взаимодействие DHCP и DNS

Как мы упоминали выше, Option 6 — это сервер DNS. Давайте рассмотрим подробнее взаимодействие двух протоколов.

DNS (система доменных имен) отвечает за соответствие доменных имен и IP-адресов. Доменное имя — это не только адрес в интернете, например, selectel.ru, но также имя компьютера в локальной сети, например, Director PC. DNS проводит соединительную линию между IP и буквенно-числовым доменным именем компьютера или веб-сайта. DHCP занимается выделением и назначением IP из области. Очевидно, что два протокола должны тесно взаимодействовать между собой.

В статье мы уже говорили, что DHCP-сервер имеет область IP-адресов, которые допускается распределять между клиентами в сети. DNS-сервер занимается тем, что сопоставляет IP-адреса и доменные имена. Это не только имена сайтов, но и имена компьютеров в сети, (например, NetworkServer PC).

Если вы хотите создать свою локальную сеть на базе Linux, потому что это бесплатно и вы не хотите связываться Windows, то вы можете столкнуться с проблемой взаимодействия DNS и DHCP. Linux не имеет Active Directory, как в Windows, позволяющей тесно связать DHCP и DNS, избегая необходимости обращаться к клиенту каждый раз по IP. Однако способы организовать такую связь существуют и для свободной системы.

Первый вариант — настроить DHCP-сервер так, чтобы фиксировал адрес за [illegible] метод будет расточительным, то необходимо дать двум серверам работать вместе.

Взаимодействие DHCP и DNS необходимо для того, чтобы DNS-сервер вовремя получал информацию о новом IP клиента и мог сопоставить его с именем клиента в сети. Если сервера не будет взаимодействовать, это чревато ошибками и недоступностью клиентов.

Настроить данное взаимодействие можно в четыре шага при помощи пакета dnsmasq, доступного в стандартных репозиториях Ubuntu и Debian. Мы не будем давать детальную инструкцию по осуществлению, а лишь кратко опишем каждый шаг.

Шаг 1 — конфигурация сети

В первую очередь необходимо определиться с компьютером, который будет выполнять роль сервера. Важно выбрать тот компьютер (Ubuntu Server или Ubuntu Desktop), который вы не планируете выключать слишком часто. Если после полной настройки вы решите выключить компьютер, то вся сеть тоже выключится.

Выбранному компьютеру необходимо назначить статический IP. Делается это редактированием конфигурационного файла в директории **/etc/network/interfaces**.

Шаг 2 — установка dnsmasq

Установите пакет dnsmasq командой из терминала:

```
sudo apt-get install dnsmasq -y
```

А затем откройте файл конфигурации **/etc/dnsmasq.conf**. Файл конфигурации dnsmasq очень большой, но он содержит комментарии с объяснениями того, за что отвечает каждая настройка. Чтобы добавить требуемые настройки, откройте файл и удалите решетку (#), означающую комментарий, в начале нужных строк.

Шаг 3 — настройка фаервола

Для изменения настроек фаервола можно использовать Ubuntu Uncomplicated Firewall. Используйте следующие команды:

```
sudo ufw allow bootps
```

```
sudo ufw allow 53/udp
```

```
sudo ufw allow 53/tcp
```

Шаг 4 — изменение настроек роутера

Зайдите в настройки вашего роутера из браузера, отключите DHCP для локальной сети, измените все настройки DNS так, чтобы они указывали на ваш только что настроенный сервер. Последнее действие — перезапуск сети на

сервере. Для этого вы можете просто перезагрузить компьютер или

```
sudo service dnsmasq restart
```

```
sudo service network-manager restart
```

Недостатки протокола DHCP

DHCP имеет свои уязвимости. Основная заключается в четырех шагах, необходимых для получения IP. Процесс DORA подразумевает рассылку сообщений широковещательного типа, когда первый откликнувшийся DHCP-сервер получает возможность предложить IP из своей области. Если злоумышленник сможет использовать свой сервер, который даст самый быстрый ответ клиенту, то у него откроется возможность получить контроль над действиями пользователя в сети и нанести существенный ущерб.

Следующий недостаток — ненадежность UDP. UDP не обеспечивает гарантию доставки информации. Этот протокол допускает потери и ошибки, которые могут сказаться и на работе DHCP, в частности при PXE-загрузке.

Заключение

Мы рассмотрели основные принципы работы DHCP-серверов. Несмотря на недостатки и частые доработки, протокол DHCP широко используется в современных сетях. Также изучили процесс DORA, основные опции и другие аспекты протокола. Надеемся, эта статья оказалась вам полезна.

Сети

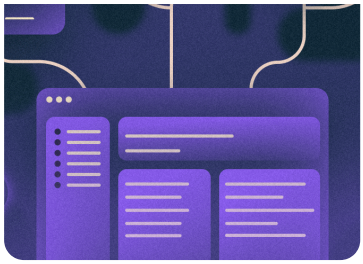
23 минуты
OSPF-протокол: основные термины и алгоритмы работы
Предыдущий материал

14 минут
OAuth 2: введение в протокол авторизации
Следующий материал

Читайте также:

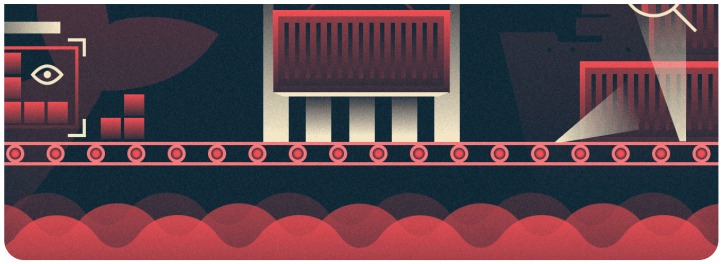
Как упавший сервер влияет на SEO

Марина Киреева
Специалист по продвижению сайтов



Обзор ISPmanager — панели управления веб-сервером и сайтами

Тирекс
Самый зубастый автор



Исчерпывающее пособие по безопасной сборке Docker-образов

Эллада Нуралиева
Специалист по ИБ

Email

Соглашаюсь на получение новостной рассылки
в соответствии с Политикой