**Практическая работа № 1**

**Тема:** Настройка DHCP-сервер.

**Цель:** Научиться разворачивать DHCP-сервер и производить начальные настройки сервера.

**Оборудование** ПК, Virtual Box, ОС Windows Server 2012

**Основные сведения**

Служба DHCP (Dynamic Host Configuration Protocol ) — это одна из служб поддержки протокола TCP/IP, разработанная для упрощения администрирования IP-сети за счет использования специально настроенного сервера для централизованного управления IP-адресами и другими параметрами протокола TCP/IP, необходимыми сетевым узлам.

Работа протокола DHCP базируется на классической схеме клиент-сервер. В роли клиентов выступают компьютеры сети, стремящиеся получить IP-адреса в так называемую аренду (lease), а DHCP-серверы выполняют функции диспетчеров, которые выдают адреса, контролируют их использование и сообщают клиентам требуемые параметры конфигурации. Параметры выделяются клиенту на определенный срок, после чего считается свободным и может быть выдан другому клиенту.

Сервер поддерживает пул свободных адресов и, кроме того, ведет собственную регистрационную базу данных. Взаимодействие DHCP-серверов со станциями-клиентами осуществляется путем обмена сообщениями.

Для взаимодействия DHCP-сервера и DHCP-клиента используется специальный протокол DHCP, который является расширением протокола BOOTP (Bootstrap Protocol). DHCP устраняет определенные ограничения, которые BOOTP имел в качестве службы настройки узла.

Сервер DHCP избавляет сетевого администратора от необходимости ручного выполнения таких операций, как:

* автоматическое назначение сетевым узлам IP-адресов и прочих параметров протокола TCP/IP (например, маска подсети, адрес основного шлюза подсети, адреса серверов DNS и WINS);
* недопущение дублирования IP-адресов, назначаемых различным узлам сети;
* освобождение IP-адресов узлов, удаленных из сети;
* ведение централизованной БД выданных IP-адресов.

Во взаимодействии по протоколу DHCP принимают участие две или три стороны:

1. DHCP-клиент — тот, кто хочет получить параметры настройки TCP/IP;
2. DHCP-сервер — тот, кто выдаёт эти параметры;
3. DHCP-ретранслятор (relay agent) — вспомогательный участник, который может играть роль посредника между клиентом и сервером. Он используется в тех случаях, когда у клиента нет возможности обратиться к серверу напрямую, в частности, в том случае, если они находятся в разных широковещательных доменах. DHCP-ретранслятор обрабатывает стандартный широковещательный DHCP-запрос и перенаправляет его на DHCP-сервер в виде целенаправленного (unicast) пакета, а полученный от DHCP-сервера ответ, в свою очередь, перенаправляет DHCP-клиенту.

Как правило, DHCP-сервер выделяет IP-адреса (и прочие параметры TCP/IP) одним из двух способов:

1. Случайным образом из предопределённого пула (в том случае, если клиенту ранее уже выдавался какой-то адрес, он может попробовать получить его вновь);
2. Жёстко зафиксированным образом, исходя из MAC-адреса клиента.

В роли DHCP сервера может выступать сервер под управлением серверной ОС семейства Linux или Windows, некоторые модели коммутаторов и даже обычные компьютеры с клиентскими операционными системами, в случае если на них установлено специализированное программное обеспечение.

Клиент DHCP и автоматическая настройка параметров сети

Протокол DHCP поддерживает три механизма выделения адресов: автоматический, динамический и ручной. В первом случае клиент получает постоянный IP-адрес, в последнем DHCP используется только для уведомления клиента об адресе, который администратор присвоил ему вручную.

Механизм получения динамического IP адреса клиентом DHCP клиентом достаточно прост, но требует более детального рассмотрения.

При включении компьютера, настроенного на автоматическое получение параметров сети, он выполняет широковещательный запрос на IP адрес 255.255.255.255, а в качестве своего IP адреса указывает 0.0.0.0 (так как у него еще нет IP адреса). В ходе данного широковещательного запроса рассылается сообщение DHCPDISCOVER, данное сообщение содержит в себе информацию позволяющую отличить его от других типов запросов/сообщений (то-есть указывает на то, что это сообщение предназначено для DHCP сервера, для получения IP адреса), MAC адрес устройства сформировавшего запрос, а также предыдущий IP адрес устройства (если он у него был).

Так как сообщение DHCPDISCOVER рассылается широковещательным способом, оно попадает не только на DHCP сервер, но и на другие устройства данного сегмента сети, но так как в сообщение DHCPDISCOVER указывается, что оно предназначено только для DHCP сервера, остальные устройства сети отвергают данное сообщение.

При получении сообщения DHCPDISCOVER DHCP сервером, он анализирует его содержание и в соответствии со своими настройками выбирает подходящую конфигурацию для запросившего компьютера и отправляет ее обратно в сообщении DHCPOFFER. Обычно сообщение DHCPOFFER отсылается только на MAC адрес компьютера, который был указан в сообщении DHCPDISCOVER, но иногда оно может рассылаться и методом широковещательной рассылки.

В случае если в сети существует несколько DHCP серверов компьютер может получить в ответ на сообщение DHCPDISCOVER несколько сообщений DHCPOFFER от разных DHCP серверов. Из них компьютер выбирает одно, обычно полученное первым. И отвечает на него сообщением DHCPREQUEST, которое содержит в себе всю туже информацию, что и сообщение DHCPDISCOVER + IP адрес выбранного DHCP сервера. Сообщение DHCPREQUEST рассылается широковещательным методом, для того чтобы его могли получить все DHCP сервера сети, если их несколько.

Все устройства сети, не являющиеся DHCP серверами игнорируют сообщение DHCPREQUEST. DHCP сервера, IP адрес которых не содержится в сообщении DHCPREQUEST понимают, что их не выбрали в качестве DHCP сервера. DHCP сервер IP адрес которого указан в сообщении DHCPREQUEST получает его и понимает, что именного его выбрали в качестве DHCP сервера для нового компьютера, на что он отвечает сообщением DHCPACK, которое как бы подтверждает данный выбор. Сообщение DHCPACK отправляется на MAC адрес компьютера указанного в сообщении DHCPREQUEST.

Компьютер, запрашивающий конфигурацию, получает сообщения DHCPACK. И применяет конфигурацию, которая была получена в сообщении DHCPOFFER. Вот так путем несложного обмена сообщениями функционирует протокол DHCP.

DHCP сервер может быть настроен по разному, и в зависимости от его конфигурации он будет выдавать IP адреса, запрашивающим компьютерам разными способами. Если на момент получения запроса DHCPDISCOVER сервер не располагает свободными IP-адресами, он может направить уведомление о возникшей проблеме администратору. В противном случае при выборе адреса обычно применяется следующий алгоритм. Клиенту выделяется адрес, записанный за ним в данный момент. Если это невозможно, сервер предложит адрес, которым пользовался клиент до окончания срока последней аренды (при условии, что данный адрес свободен), либо адрес, запрошенный самим клиентом при помощи соответствующей опции (опять же, если адрес не занят). Наконец, в том случае, когда все предыдущие варианты не проходят, новый адрес выбирается из пула доступных адресов с учетом подсети, из которой поступил клиентский запрос.

Исходя из определенной сетевым администратором политики и, соответственно, настроек сервер может выдать клиенту адрес, отличающийся от запрошенного (даже при доступности последнего), вообще отказать в предоставлении адреса или предложить адрес, относящийся к другой подсети. Более того, DHCP-сервер вообще не обязан реагировать на каждый поступивший запрос DHCPDISCOVER. Это предоставляет администратору возможность контролировать доступ к сети, например разрешив серверу отвечать только тем клиентам, которые предварительно зарегистрировались с помощью специальной процедуры.

Спустя примерно половину этого срока клиент пытается возобновить его. Если клиент не может обновить аренду, он будет пытаться сделать это снова до окончания срока аренды. Если эти попытки не принесут успеха, клиент будет пытаться обратиться к другому DHCP-серверу.
При обновлении аренды клиент проходит два состояния — обновления адреса (RENEWING) и обновления конфигурации (REBINDING). Первое наступает примерно на половине срока аренды адреса (так называемый момент T1), второе — по истечении приблизительно 7/8 полного времени аренды (момент T2); для рассинхронизации процессов реконфигурирования разных клиентов значения этих временных меток рандомизируются с помощью случайной добавки.

В момент T1 клиент оправляет DHCP-серверу, выдавшему адрес, сообщение DHCPREQUEST с просьбой продлить срок аренды. Получив положительный ответ (DHCPACK), клиент пересчитывает срок аренды и продолжает работу в обычном режиме. Клиент ожидает прихода ответа от сервера в течение (T2 — t)/2 с (при условии, что это значение не меньше 60 с), где t — время отсылки последнего сообщения DHCPREQUEST, после чего отправляет данное сообщение повторно.

Если ответ от сервера не поступил к моменту T2, клиент переходит в состояние REBINDING и передает уже широковещательное сообщение DHCPREQUEST со своим текущим сетевым адресом. В этом случае моменты повторных выдач запросов DHCPREQUEST рассчитываются аналогично предыдущему случаю, только вместо T2 фигурирует время окончания срока аренды.

Не исключено, однако, что ответ DHCPACK не придет до окончания срока аренды. Тогда клиент обязан немедленно прекратить выполнение любых сетевых операций и заново начать процесс инициализации. Если запоздавший ответ DHCPACK все-таки поступит, клиенту рекомендуется сразу же возобновить работу под прежним адресом.

Невозобновленный IP-адрес возвращается в пул адресов. Если клиент связался с сервером, но текущий IP-адрес не может быть возобновлен, DHCP-сервер присваивает клиенту новый IP-адрес.

DHCP-сервер обычно не влияет на процедуру загрузки или входа в есть. Загрузка клиентов и регистрация пользователей возможна даже при нефункционирующем сервере DHCP.

Возможности сервера DHCP

Но самый главный плюс DHCP вовсе не в том, что с его помощью можно автоматически раздавать IP-адреса. На этом функционал протокола не заканчивается. Основная его ценность в другом: с его помощью вы можете назначать хостам и другие, не менее важные настройки. Например:

* Шлюзы по умолчанию. Если в вашей сети имеется несколько Интернет-каналов (для обеспечения бесперебойной работы), вы можете назначить хостам несколько шлюзов и порядок их предпочтения. В случае выхода одного из каналов из строя, переключение на резервный канал произойдет автоматически, без вашего вмешательства. Это же дает возможность организовать простейшую балансировку нагрузки между каналами, назначив по DHCP одной группе хостов один маршрутизатор в качестве шлюза, а другой группе – второй.
* Статические маршруты. Если в вашей сети есть несколько подсетей, соединенных маршрутизаторами, то при помощи DHCP можно автоматически оповещать хосты о наличии маршрутов в другие подсети. Причем это, по желанию, можно сделать только для избранных – например, используя привязку к MAC. Эта же опция полезна при организации VPN-доступа к корпоративной сети – VPN-клиентам можно сообщить маршруты лишь к нужным им подсетям, оставив другие подсети недоступными для подключающихся по VPN пользователей.
* Смещение времени. Если ваши пользователи часто бывают в различных временных поясах (например, мотаются из Питера во Владивосток и обратно), то можно заставить системные часы их ноутбука адаптироваться к вашему местному времени при помощи DHCP.
* Сервер синхронизации времени. Поскольку часы компьютеров славятся своей неточностью, их желательно синхронизировать с какими-то эталонными часами. Для этого используется служба NTP. Информацию о сервере NTP можно раздавать хостам при помощи DHCP.
* DNS-серверы. С помощью этой опции вы можете назначать вашим клиентам DNS-серверы как внутри сети, так и за ее пределами. Причем, в отличие ручной настройки интерфейса, вы можете передать хосту обширный список доступных DNS-серверов.
* Настройки сервера загрузки – настройки протокола TFTP/BOOTP, необходимые для бездисковой загрузки хостов. Эта возможность востребована при наличии в сети бездисковых терминалов, загружающихся по сети, и при организации дистанционной автоматической установки ОС на компьютеры пользователей (об этом поговорим отдельно)
* Списки доступных SMTP и POP серверов.
* Настройки WINS и Netbios
* Размер MTU, время жизни кэша ARP, размер TTL и др.

Если у вас сеть разбита на несколько подсетей, разделенных маршрутизаторами, то одним DHCP-сервером вам ограничиться не получится. DHCP-запросы и ответы не маршрутизируются между подсетями и распространяются в пределах лишь одного сегмента. Это связано в первую очередь с тем, что протокол DHCP не использует для передачи данных IP- адресацию, а работают на более низком уровне. Следовательно, в каждом из сегментов сети, имеющем свой диапазон IP-адресов вам потребуется отдельная DHCP- служба.

**Порядок выполнения работы**

У нас простая сетка 192.168.1.0/24. Роутер во внешний мир пусть будет по адресу 192.168.1.1, на нем же DNS сервер.

DHCP сервер будет 192.168.1.2. Устанавливаем на нем Windows 2012 R2, добавляем роль DHCP Server. **Серверу надо дать статический IP-адрес!**

Сервер терминалов будет 192.168.1.3, на нем установлены WTware 5.4.16, все настройки по умолчанию. WTware DHCP отключен, TFTP включен.

Логинимся в DHCP сервер администратором, запускаем консоль управления DHCP.



Создаем новый диапазон адресов (scope).



Назовем наш диапазон LAN.





Исключим первые 15 адресов из раздачи (в принципе можно это не делать, потом внести все статические адреса в резервации).



Длительность аренды адреса оставим по умолчанию.



Конфигурируем опции.



Роутер (шлюз по умолчанию).



Адрес сервера DNS и имя локального домена (если нужно).



WINS — укажите, если используете этот анахронизм.



Активируем диапазон.



Жмем Finish.



Диапазон адресов создан.



На этом этапе рабочие станции будут получать адреса и базовые настройки от DHCP сервера. Теперь приступим к конфигурированию загрузки по сети (network boot).

Загружать по сети будем два типа клиентов:

1. x86 — BIOS
2. x86 — UEFI 64-bit

Для выбора нужных файлов загрузки воспользуемся политиками DHCP. Политики DHCP — это правила, которые позволяют назначать IP-адреса и/или опции DHCP для клиентов, которые соответствуют условиям политики.

При получении запроса от клиента DHCP сервер назначает адреса и опции в следующем порядке:

1. Политики, назначенные для диапазона (Scope Policies) в порядке приоритета.
2. Опции, назначенные для диапазона (Scope Options)
3. Политики, назначенные для сервера (Server Policies) в порядке приоритета.
4. Опции, назначенные для сервера (Server Options)



У каждой политики есть приоритет. Приоритеты нумеруются начиная с 1. Чем меньше номер, тем приоритетнее политика. Если в двух политиках определены одинаковые опции, клиенту отправляется та, которая определена в политике с более высоким приоритетом. Приоритет политики можно менять через GUI, кликнув правой кнопкой мыши по названию политики и выбрать "Up" или "Down".

**На MAC-адреса, прописанные в резервациях (Reservations) действие политик не распространяется!**

Условия применения политик могут быть следующие:

1. Vendor Class
2. User Class
3. MAC-адрес
4. PXE GUID клиента
5. Доменное имя клиента (опция 12)
6. DHCP Relay, обслуживающий запрос клиента.

Нас интересуют в основном Vendor Class. Перед созданием политики надо создать нужные нам Vendor Class.



Надо определить пять классов:

1. PXE Client x86
2. PXE Client UEFI x64
3. PXE Client UEFI BC
4. WTware

Жмем "Add…" чтобы добавить новый Vendor Class.



Заполняем имя класса: PXE Client x86

Заполняем ID класса: PXEClient:Arch:00000

Можно заполнять либо Binary (16-ричные значения), либо ASCII (просто набивать текст). Тут важно не ошибиться, иначе ничего не заработает.



Нажимаем OK и видим:



Аналогично добавляем следующие классы:

* Имя класса: PXE Client EFI BC
* ID класса: PXEClient:Arch:00007



Имя класса: PXE Client EFI x64

ID класса: PXEClient:Arch:00009



Имя класса: wtware

ID класса: wtware



Классы определены. Нажимаем "Close" и приступаем к созданию политик, которые будут пользоваться нашими классами.



Имя политики: pxeclient-x86

Политика будет определять загрузку BIOS клиентов.



Добавляем условие для нашей политики.



Устанавливаем так, как на картинке:



Обратите внимание на чекбокс "Append wildcard(\*)". Это означает, что любой Vendor Class, который начинается с "PXEClient:Arch:00000", будет соответствовать условию.

Нажимаем "Add".



Нажимаем OK.



Условие добавлено, жмем Next.



Нам не нужно резервировать IP-адреса, поэтому жмем No и Next.



Конфигурируем опцию 66.

192.168.1.3 — адрес нашего TFTP сервера, на котором лежат загрузочные файлы WTware.



Конфигурируем опцию 67.

Имя загрузочного файла: 5.4.16/wtware.pxe

Для загрузки по HTTP имя загрузочного файла: 5.4.16/wtware.http



Жмем Next и завершаем конфигурирование политики.



Политика добавлена.



Следующая политика будет определять загрузку UEFI x64 клиентов. Имя политики: pxeclient-uefi64



Добавляем первое условие.



Добавляем второе условие.



Условие политики будет срабатывать при совпадении с любым из двух Vendor Class.





Конфигурацию IP-адресов пропускаем, как в предыдущей политике.

Далее конфигурируем опции по аналогии с предыдущей политикой:

* опция 66: 192.168.1.3
* опция 67: 5.4.16/bootx64.efi

Для загрузки по HTTP опция 67: 5.4.16/http.efi



Завершаем конфигурирование политики.



Вторая политика готова.



Осталась последняя политика — для WTware. Она читает опции 66 и 67 для определения пути загрузки пакетов. Делаем аналогично предыдущей политике:

Имя политики: wtware

В условии политики устанавливаем Vendor Class "wtware"

* Опция 66 = 192.168.1.3
* Опция 67 = 5.4.16/wtware.pxe

Для загрузки по HTTP опция 67 = 5.4.16/http.efi (имя файла именно такое, иначе под UEFI загрузка не переключится на HTTP).

Сюда же можно добавить специфические для WTware опции 18 и 179, по желанию.



Конфигурация завершена. Все типы клиентов должны загружаться.



Здесь, конечно, рассмотрен простейший случай. В реальных сетях все намного сложнее.

**Важное дополнение:** Поскольку политики несовместимы с резервациями, если вам потребуется указать имя хоста (опция 12) или дать определенному клиенту выделенный IP-адрес, создайте новую политику по условию "MAC-address" и настройте нужные параметры для этого MAC-адреса через свойства политики

**Контрольные вопросы**

1 Назначение DHCP-сервера?

2 Назначение пула адресов?

3 Как работает клиент DHCP?

**Окончание работы**

На каждом этапе работы необходимо сделать скриншот, ответить на контрольные вопросы и оформить отчет в соответствии с требованиями нормоконтроля.