DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных (и не очень) сетей TCP/IP.

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

Стандарт протокола DHCP был принят в октябре 1993 года. Действующая версия протокола (март 1997 года) описана в RFC 2131. Новая версия DHCP, предназначенная для использования в среде IPv6, носит название DHCPv6 и определена в RFC 3315 (июль 2003 года).

DHCP появился не на пустом месте - различные схемы управления IP-адресами в сетевой среде предлагались и раньше (см. врезку <Распределение IP-адресов...>). Однако эти схемы имеют по крайней мере один из двух недостатков - не допускают динамического назначения IP-адресов либо позволяют передавать от сервера на станцию-клиент лишь небольшое число параметров конфигурации.

При разработке протокола DHCP преследовалась цель устранить оба ограничения. Требовался механизм, который позволил бы ликвидировать стадию ручного конфигурирования компьютеров, поддерживал многосегментные сети, не требуя наличия DHCP-сервера в каждой подсети, не конфликтовал с существующими сетевыми протоколами и компьютерами, имеющими статичную конфигурацию, был способен взаимодействовать с ретранслирующими агентами протокола BOOTP и обслуживать BOOTP-клиентов, наконец, допускал управление передаваемыми параметрами конфигурации. BOOTP протокол, позволяющий бездисковым клиентам во время старта конфигурировать установки TCP/IP. Что касается более узких задач, то DHCP должен был обеспечивать уникальность сетевых адресов, используемых разными компьютерами сети в данный момент, сохранение прежней конфигурации клиентской станции после перезагрузки клиента или сервера, автоматическое присвоение параметров конфигурации вновь подключенным машинам.

Упомянутое выше требование поддержки базовых элементов протокола BOOTP возникло не случайно. DHCP разрабатывался как непосредственное расширение BOOTP и именно в таком качестве воспринимается BOOTP-клиентами. Этому обстоятельству в первую очередь способствует формат сообщений DHCP, во многом совпадающий с форматом, который применяется протоколом-предшественником и определен в документе RFC 951.

Сравнивая протоколы BOOTP и DHCP, нельзя не отметить появления в DHCP новых услуг. Во-первых, в этом протоколе предусмотрен механизм автоматической выдачи IP-адресов во временное пользование с возможностью их последующего присвоения новым клиентам. Во-вторых, клиент может получить от сервера все параметры конфигурации, которые ему необходимы для успешного функционирования в IP-сети.

Указанные отличия потребовали частичного расширения формата сообщений. Так, в нем появилось отдельное поле идентификатора клиента, сделана более прозрачной интерпретация адреса сервера (поле siaddr), переменный размер получило поле options, используемое, в частности, для передачи параметров конфигурации (его длина обычно находится в диапазоне 312-576 байт, хотя возможно и дополнительное расширение этого поля за счет полей sname и file).

В роли транспортного протокола для обмена DHCP-сообщениями выступает UDP. При отправке сообщения с клиента на сервер используется 67-й порт DHCP-сервера, при передаче в обратном направлении - 68-й. Эти номера портов, как и схожая структура сообщений, обеспечивают обратную совместимость DHCP с BOOTP. Конкретные процедуры взаимодействия клиентов и серверов BOOTP и DHCP регламентирует документ RFC 1542.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

**Устройство протокола**

Протокол DHCP является клиент-серверным, то есть в его работе участвуют клиент DHCP и сервер DHCP. Передача данных производится при помощи протокола UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68.

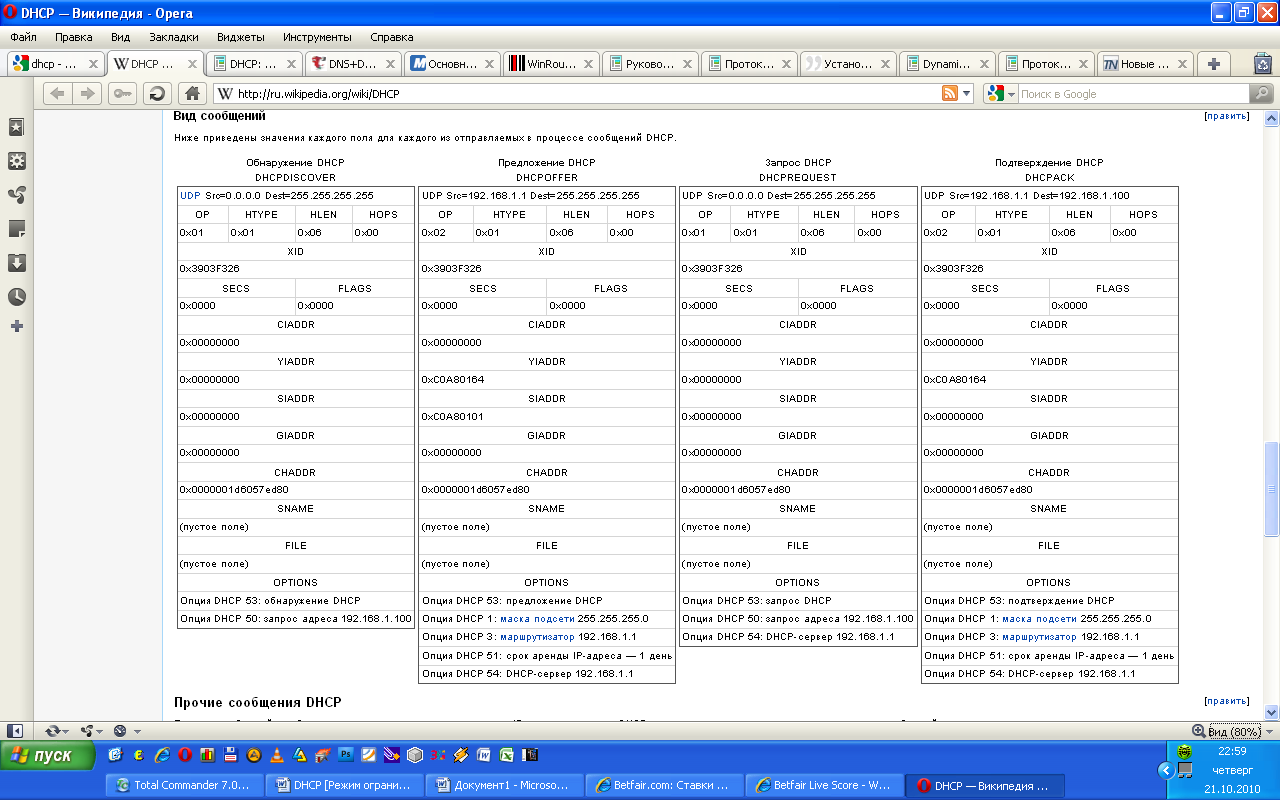
**Структура сообщений DHCP**

Все сообщения протокола DHCP разбиваются на поля, каждое из которых содержит определённую информацию. Все поля, кроме последнего (поля опций DHCP), имеют фиксированную длину.

|  |  |  |
| --- | --- | --- |
| Поле | Описание | Длина (в байтах) |
| op | Тип сообщения. Может принимать два значения: BOOTREQUEST (1, запрос от клиента к серверу) и BOOTREPLY (2, ответ от сервера к клиенту). | 1 |
| htype | Тип аппаратного адреса. Допустимые значения этого поля определены в RFC «Assigned Numbers». Например, для MAC-адреса Ethernet 10 Мбит/с это поле принимает значение 1. | 1 |
| hlen | Длина аппаратного адреса в байтах. Для MAC-адреса Ethernet — 6. | 1 |
| hops | Количество промежуточных маршрутизаторов (так называемых агентов ретрансляции DHCP), через которые прошло сообщение. Клиент устанавливает это поле в 0. | 1 |
| xid | Уникальный идентификатор транзакции, генерируемый клиентом в начале процесса получения адреса. | 4 |
| secs | Время в секундах с момента начала процесса получения адреса. Может не использоваться (в этом случае оно устанавливается в 0). | 2 |
| flags | Поле для флагов — специальных параметров протокола DHCP. | 2 |
| ciaddr | IP-адрес клиента. Заполняется только в том случае, если клиент уже имеет собственный IP-адрес и способен отвечать на запросы ARP (это возможно, если клиент выполняет процедуру обновления адреса по истечении срока аренды). | 4 |
| yiaddr | 'your' (client) IP address (RFC 2131) | 4 |
| siaddr | IP-адрес сервера. Возвращается в предложении DHCP (см. ниже). | 4 |
| giaddr | IP-адрес агента ретрансляции, если таковой участвовал в процессе доставки сообщения DHCP до сервера. | 4 |
| chaddr | Аппаратный адрес (обычно MAC-адрес) клиента. | 16 |
| sname | Необязательное имя сервера в виде нуль-терминированной строки. | 64 |
| file | Необязательное имя файла на сервере, используемое бездисковыми рабочими станциями при удалённой загрузке. Как и sname, представлено в виде нуль-терминированной строки. | 128 |
| options | Поле опций DHCP. Здесь указываются различные дополнительные параметры конфигурации. В начале этого поля указываются четыре особых байта со значениями 99, 130, 83, 99 («волшебные числа»), позволяющие серверу определить наличие этого поля. | переменная |

**Вид сообщений**

Отправляемых в процессе сообщений DHCP.Обнаружение DHCP



**Распределение IP-адресов**

Протокол DHCP поддерживает три механизма выделения адресов: автоматический, динамический и ручной.

Ручное распределение. При этом способе сетевой администратор сопоставляет аппаратному адресу (обычно MAC-адресу) каждого клиентского компьютера определённый IP-адрес. Фактически, данный способ распределения адресов отличается от ручной настройки каждого компьютера лишь тем, что сведения об адресах хранятся централизованно (на сервере DHCP), и потому их проще изменять при необходимости.

Автоматическое распределение. При данном способе каждому компьютеру на постоянное использование выделяется произвольный свободный IP-адрес из определённого администратором диапазона.

Динамическое распределение. Этот способ аналогичен автоматическому распределению, за исключением того, что адрес выдаётся компьютеру не на постоянное пользование, а на определённый срок. Это называется арендой адреса. По истечении срока аренды IP-адрес вновь считается свободным, и клиент обязан запросить новый (он, впрочем, может оказаться тем же самым).

Некоторые реализации службы DHCP способны автоматически обновлять записи DNS, соответствующие клиентским компьютерам, при выделении им новых адресов. Это производится при помощи протокола обновления DNS, описанного в RFC 2136.

Выдача адреса в аренду производится по запросу клиента. DHCP-сервер (или группа серверов) гарантирует, что выделенный адрес до истечения срока его аренды не будет выдан другому клиенту; при повторных обращениях сервер старается предложить клиенту адрес, которым тот пользовался ранее. Со своей стороны, клиент может запросить пролонгацию срока аренды адреса либо, наоборот, досрочно отказаться от него. Протоколом предусмотрена также выдача IP-адреса в неограниченное пользование. При острой нехватке адресов сервер может сократить срок аренды адреса по сравнению с запрошенным.

Выдача нового адреса. Последовательность событий в этом случае такова (рис. 2).

Рассмотрим пример процесса получения IP-адреса клиентом от сервера DHCP. Предположим, клиент ещё не имеет собственного IP-адреса, но ему известен его предыдущий адрес — 192.168.1.100.

1. Клиент посылает в собственную физическую подсеть широковещательное сообщение DHCPDISCOVER, в котором могут указываться устраивающие клиента IP-адрес и срок его аренды.

при этом в качестве IP-адреса источника указывается 0.0.0.0 (так как компьютер ещё не имеет собственного IP-адреса), а в качестве адреса назначения — широковещательный адрес 255.255.255.255.

Если в данной подсети DHCP-сервер отсутствует, сообщение будет передано в другие подсети ретранслирующими агентами протокола BOOTP (они же вернут клиенту ответные сообщения сервера).

Клиент заполняет несколько полей сообщения начальными значениями:

В поле xid помещается уникальный идентификатор транзакции, который позволяет отличать данный процесс получения IP-адреса от других, протекающих в то же время.

В поле chaddr помещается аппаратный адрес (MAC-адрес) клиента.

В поле опций указывается последний известный клиенту IP-адрес. В данном примере это 192.168.1.100. Это необязательно и может быть проигнорировано сервером.

2. Любой из DHCP-серверов может ответить на поступившее сообщение DHCPDISCOVER сообщением DHCPOFFER, включив в него доступный IP-адрес (yiaddr) и, если требуется, параметры конфигурации клиента. На этой стадии сервер не обязан резервировать указанный адрес. В принципе, он имеет право предложить его другому клиенту, также отправившему запрос DHCPDISCOVER. Тем не менее спецификации RFC 2131 рекомендуют серверу без необходимости не применять подобную тактику, а кроме того, убедиться (например, выдав эхо-запрос ICMP) в том, что предложенный адрес в текущий момент не используется каким-либо из компьютеров сети.

3. Клиент не обязан реагировать на первое же поступившее предложение. Допускается, чтобы он дождался откликов от нескольких серверов и, остановившись на одном из предложений, отправил в сеть широковещательное сообщение DHCPREQUEST. В нем содержатся идентификатор выбранного сервера и, возможно, желательные значения запрашиваемых параметров конфигурации.

Не исключено, что клиента не устроит ни одно из серверных предложений. Тогда вместо DHCPREQUEST он снова выдаст в сеть запрос DHCPDISCOVER, а серверы так и не узнают, что их предложения отклонены. Именно по этой причине сервер не обязан резервировать помещенный в DHCPOFFER адрес.

Если в процессе ожидания серверных откликов на DHCPDISCOVER достигнут тайм-аут, клиент выдает данное сообщение повторно.

4. Присутствующий в сообщении DHCPREQUEST идентификатор позволяет соответствующему DHCP-серверу убедиться в том, что клиент принял именно его предложение. В ответ сервер отправляет подтверждение DHCPACK, содержащее значения требуемых параметров конфигурации, и производит соответствующую запись в базу данных.

Если к моменту поступления сообщения DHCPREQUEST предложенный адрес уже <ушел> к другому клиенту (например, первая станция слишком долго <размышляла> над поступившими предложениями), сервер отвечает сообщением DHCPNACK.

5. Получив сообщение DHCPACK, клиент обязан убедиться в уникальности IP-адреса (средствами протокола ARP) и зафиксировать суммарный срок его аренды. Последний рассчитывается как время, прошедшее между отправкой сообщения DHCPREQUEST и приемом ответного сообщения DHCPACK, плюс срок аренды, указанный в DHCPACK.

Обнаружив, что адрес уже используется другой станцией, клиент обязан отправить серверу сообщение DHCPDECLINE и не ранее чем через 10 с начать всю процедуру снова. Процесс конфигурирования возобновляется и при получении серверного сообщения DHCPNACK.

При достижении тайм-аута в процессе ожидания серверных откликов на сообщение DHCPREQUEST клиент выдает его повторно.

6. Для досрочного прекращения аренды адреса клиент отправляет серверу сообщение DHCPRELEASE.

Приведенная последовательность действий заметно упрощается, если станция-клиент желает повторно работать с IP-адресом, который когда-то уже был ей выделен. В этом случае первым отправляемым сообщением является DHCPREQUEST, в котором клиент указывает прежде использовавшийся адрес. В ответ он может получить сообщение DHCPACK или DHCPNACK (если адрес занят либо клиентский запрос является некорректным, например из-за перемещения клиента в другую подсеть). Обязанность проверить уникальность IP-адреса опять-таки возлагается на клиента.

Выбор адреса DHCP-сервером. 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.

Заметим, что исходя из определенной сетевым администратором политики 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.

**Истечение срока аренды.** По мере того как срок аренды подходит к концу, клиент может завершить работу с данным адресом, отправив на DHCP-сервер сообщение DHCPRELEASE, либо заблаговременно запросить продление срока аренды. В первом случае возвращение в сеть потребует выполнения всей процедуры инициализации заново. Во втором - станция продолжит функционировать в сети без видимого замедления работы пользовательских приложений.

При пролонгировании 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.

**Параметры конфигурации**

Хранение параметров сетевой конфигурации станций-клиентов является второй услугой, предоставляемой DHCP-сервером. В создаваемой базе данных на каждого клиента заводится отдельная запись с уникальным ключом-идентификатором и строкой конфигурационных параметров.

Роль идентификатора может играть пара <номер подсети IP, аппаратный адрес>, которая позволит использовать аппаратный адрес сразу в нескольких подсетях, либо пара <номер подсети IP, имя хост-компьютера>, позволяющая серверу взаимодействовать с клиентом, перемещенным в другую подсеть.

Что касается собственно параметров конфигурации, то их набор, поддерживаемый протоколом DHCP, определен в спецификациях RFC 1122, 1123, 1196 и 1256. В него входят выданный адрес, срок его аренды, назначавшиеся ранее адреса, а также максимальный размер реассемблируемого пакета, перечень фильтров для нелокальной маршрутизации от источника, адрес, используемый в широковещательных пакетах, параметры статических маршрутов и т.д. Впрочем, из всей совокупности допустимых параметров (а их более 30) в процессе инициализации могут передаваться только те, которые действительно необходимы для работы клиента либо определяются спецификой конкретной подсети.

Редукция объема передаваемых сведений о конфигурации достигается двумя способами. Во-первых, для большей части параметров в упомянутых выше документах RFC определены значения, принимаемые по умолчанию. Клиент будет использовать их, если в сообщении, поступившем от сервера, какие-то параметры опущены. Во-вторых, отправляя сообщение DHCPDISCOVER или DHCPREQUEST, клиентская станция может явно указать в нем параметры, значения которых она хотела бы получить.

Очевидно, что в обоих случаях передача параметров конфигурации осуществляется в ходе основной процедуры выделения IP-адреса. Возможен, однако, случай, когда клиент уже имеет IP-адрес (например, он был задан вручную). Тогда он может выдать сообщение DHCPINFORM\*, содержащее уже имеющийся адрес и запрос об отдельных параметрах конфигурации. Получив это сообщение, DHCP-сервер проверяет правильность адреса клиента (но не наличие аренды) и направляет ему сообщение DHCPACK с требуемыми параметрами конфигурации.

Отметим одно логическое противоречие, с которым связано применение протокола DHCP. Алгоритм выделения IP-адреса компьютеру сети предполагает, что установленное на нем программное обеспечение TCP/IP в состоянии воспринимать адресованные ему посредством <аппаратного> адреса IP-пакеты и транслировать их на IP-уровень еще до того, как станция получит свой IP-адрес, а сами средства TCP/IP будут полностью сконфигурированы. Такая возможность, очевидно, существует не всегда. Для работы с клиентами, не способными корректно обрабатывать одноадресные IP-дейтаграммы, используется поле flags. Такие клиенты должны установить первый бит данного поля в единичное значение, тем самым указав серверу на необходимость отправки в соответствующую подсеть только широковещательных сообщений.

**Недостатки DHCP**

Освобождая сетевых администраторов от множества рутинных операций, DHCP оставляет нерешенными ряд проблем, которые рано или поздно могут возникнуть в реальной сетевой среде.

К недостаткам этого протокола прежде всего следует отнести крайне низкий уровень информационной безопасности, что обусловлено непосредственным использованием протоколов UDP и IP. В настоящее время не существует практически никакой защиты от появления в сети несанкционированных DHCP-серверов, способных рассылать клиентам ошибочную или потенциально опасную информацию - некорректные или уже задействованные IP-адреса, неверные сведения о маршрутизации и т.д. И наоборот, клиенты, запущенные с неблаговидными целями, могут извлекать конфигурационные сведения, предназначенные для <законных> компьютеров сети, и тем самым оттягивать на себя значительную часть имеющихся ресурсов. Понятно, что возможности административного ограничения доступа, о которых говорилось выше, не способны закрыть эту брешь в системе информационной безопасности.

По мнению некоторых экспертов, в настоящее время DHCP недостаточно отказоустойчив. Протоколу явно недостает механизма активного уведомления клиентов об экстремальных ситуациях (например, о систематической нехватке адресов) и серверного подтверждения об освобождении адреса, иногда в сети наблюдаются всплески числа запросов на повторное использование адресов и т.д. Впрочем, работа над протоколом еще не завершена, и не исключено, что некоторые недостатки будут устранены в последующих редакциях.

**Опции DHCP**

Помимо IP-адреса, DHCP также может сообщать клиенту дополнительные параметры, необходимые для нормальной работы в сети. Эти параметры называются опциями DHCP. Список стандартных опций можно найти в RFC 2132.

Некоторыми из наиболее часто используемых опций являются:

IP-адрес маршрутизатора по умолчанию;

маска подсети;

адреса серверов DNS;

имя домена DNS.

Некоторые поставщики программного обеспечения могут определять собственные, дополнительные опции DHCP.

**Информация DHCP**

Сообщение информации DHCP (DHCPINFORM) предназначено для определения дополнительных параметров TCP/IP (например, адреса маршрутизатора по умолчанию, DNS-серверов и т. п.) теми клиентами, которым не нужен динамический IP-адрес (то есть адрес которых настроен вручную). Серверы отвечают на такой запрос сообщением подтверждения (DHCPACK) без выделения IP-адреса.

**Реализации**

Компания Microsoft впервые включила сервер DHCP в поставку серверной версии Windows NT 3.5, выпущенной в 1994 году. Начиная с Windows 2000 Server реализация DHCP-сервера от Microsoft позволяет динамически обновлять записи DNS, что используется в Active Directory.

Internet Systems Consortium выпустил первую версию ISC DHCP Server (для Unix-подобных систем) 6 декабря 1997 года. 22 июня 1999 года вышла версия 2.0, более точно соответствующая стандарту.

Компания Cisco включила сервер DHCP в Cisco IOS 12.0 в феврале 1999 года. Sun добавила DHCP-сервер в Solaris 8 в июле 2001 года.

Тем не менее, как частенько бывает в сетевой индустрии, механизмы DHCP уже реализованы в продуктах ряда производителей. К счастью, любые изменения в алгоритмах его работы легко учесть на программном уровне, так что, приобретая серверное или клиентское программное обеспечение определенной компании, можно не опасаться заточения в неприступную крепость патентованных решений. Скорее, следует обратить внимание на то, насколько удачно конкретная реализация DHCP вписывается в имеющуюся вычислительную среду и взаимодействует с другими сетевыми службами, в частности с DNS. Публикуемые в этом номере результаты сравнительных испытаний DNS- и DHCP-серверов (см. статью <Игра в имена>) способны стать неплохим подспорьем для пользователя.

**Распределение IP-адресов: возможны варианты**

BOOTP, DRARP, TFTP, ICMP, NIP - вероятно, это еще не полный перечень протоколов, в той или иной мере претендующих на решение задачи управления IP-адресами и конфигурацией в сетевой среде. Не исключено, что после стандартизации DHCP довольно быстро вытеснит их со сцены, однако на сегодняшний день многие из названных протоколов нередко упоминаются в литературе и используются в готовых продуктах.

Подобно DHCP, протокол Bootstrap Protocol (BOOTP) сегодня также имеет статус предварительного стандарта и рекомендован к применению консорциумом IETF. Именно его следует считать непосредственным предшественником DHCP. Появившиеся в 1993 г. дополнения расширили перечень конфигурационных параметров, охватываемых протоколом BOOTP. Более того, к настоящему времени даже предложена модификация BOOTP, поддерживающая динамическое назначение IP-адресов.

Протокол Reverse Address Resolution Protocol (RARP), впервые описанный в июне 1984 г. (RFC 903), используется компанией Sun Microsystems и рядом других производителей, в частности, для запуска бездисковых рабочих станций. Основной принцип его работы сводится к тому, что клиент должен самостоятельно отыскать свой IP-адрес, а не принять адрес, выделенный сервером. Сравнительно недавно появился динамический вариант этого протокола (Dynamic RARP, DRARP), реализующий алгоритм автоматического присвоения IP-адресов. Стоит отметить, что изначальный вариант RARP не поддерживает передачу клиенту каких-либо параметров конфигурации (кроме IP-адреса), в том числе применяемых при маршрутизации. В результате один сервер RARP способен обслуживать только одну локальную сеть.

Упрощенный вариант FTP - протокол Trivial File Transfer Protocol (TFTP) - увидел свет около 20 лет назад, его вторая версия описана в документе RFC 783. Фактически TFTP предоставляет транспортный механизм для передачи с сервера загрузочного образа клиентской системы.

Протокол Internet Control Message Protocol (ICMP) сегодня также можно отнести к поколению ветеранов Всемирной сети. Он позволяет информировать компьютеры о наличии в сети дополнительных маршрутизаторов (имеется специальный механизм для обнаружения этих устройств), предусматривает специальные типы сообщений для передачи маски подсети и других служебных сведений.

Наконец, протокол Network Information Protocol (NIP) был разработан в конце 80-х гг. сотрудниками Массачусетского технологического института в качестве распределенного механизма для динамического присвоения IP-адресов в сетях Ethernet.

Отметим еще спецификации RFC 1122 и 1123, которые используются рядом протоколов (в том числе DHCP). Они содержат требования к процедуре изменения конфигурации компьютеров сети и, кроме того, предлагают сценарий первоначального конфигурирования бездисковых станций.

**Использование DNS-серверов с DHCP**

При установке службы DHCP в Windows Server 2003 можно настроить сервер на выполнение от имени DHCP-клиентов обновлений любых серверов DNS (Domain Name System), поддерживающих динамическое обновление.

Порядок выполнения обновлений DHCP/DNS

DHCP-сервер может использоваться для регистрации и обновления записей ресурсов указателя (PTR) и адреса (A) от имени своих DHCP-клиентов.

Этот процесс требует использования дополнительного параметра DHCP — «Полное имя клиента» (код 81). Этот параметр позволяет клиенту предоставлять для DHCP-сервера свое полное доменное имя, а также инструкции по обработке динамических обновлений DNS от своего имени.

При получении параметра 81 от квалифицированного DHCP-клиента, например от компьютера, работающего под управлением Windows 2000, Windows XP; или операционной системы семейства Windows Server 2003, DHCP-серверы Windows Server 2003 обрабатывают его, определяя порядок инициирования сервером обновлений от имени данного клиента. Если сервер настроен на выполнение динамических обновлений DNS, он выполняет одно из следующих действий:

DHCP-сервер обновляет в DNS записи A и PTR при наличии соответствующего запроса клиента в параметре 81;

DHCP-сервер обновляет в DNS записи A и PTR независимо от того, запрошено это действие клиентом или нет.

Кроме того, DHCP-сервер может динамически обновлять в DNS записи A и PTR от имени устаревших клиентов, которые не могут отправить параметр 81 на сервер. DHCP-сервер можно также настроить на уничтожение записей A и PTR клиента при удалении его аренды.

DHCP-сервер может быть настроен одним из следующих способов.

DHCP-сервер регистрирует и обновляет сведения о клиенте на официальном DNS-севере зоны, в которой расположен DHCP-сервер, в соответствии с запросом DHCP-клиента.

Это стандартная конфигурация для DHCP-серверов, работающих под управлением Windows Server 2003, и DHCP-клиентов под управлением Windows 2000, Windows XP; или операционной системы Windows Server 2003. В этом режиме DHCP-клиент может запрашивать способ обновления DHCP-сервером записей ресурсов адреса (A) и указателя (PTR). Если это возможно, DHCP-сервер удовлетворяет запрос клиента на обновление сведений о его имени и IP-адресе в DNS.

Чтобы изменить этот режим, установите флажок Динамически обновлять DNS A- и PTR-записи только по запросу DHCP-клиента, расположенный на вкладке Служба DNS диалогового окна свойств соответствующего DHCP-сервера или одной из его областей.

DHCP-сервер всегда регистрирует и обновляет сведения о клиенте в DNS.

Это модифицированная конфигурация, поддерживаемая для DHCP-серверов, работающих под управлением Windows Server 2003, и DHCP-клиентов под управлением Windows 2000, Windows XP; или операционной системы Windows Server 2003. В данном режиме DHCP-сервер всегда выполняет обновление сведений о полном имени клиента и предоставленном ему в аренду IP-адресе, а также записей ресурсов адреса (A) и указателя (PTR), независимо от того, запрашивал ли клиент выполнение обновлений.

Чтобы изменить этот режим, установите флажок Включить динамическое обновление DNS в соответствии с настройкой и установите параметр Всегда динамически обновлять DNS A- и PTR-записи, расположенный на вкладке Служба DNS диалогового окна свойств соответствующего DHCP-сервера или одной из его областей.

DHCP-сервер никогда не регистрирует и не обновляет сведения о клиенте в DNS.

Для перехода в этот режим необходимо отключить на DHCP-сервере выполнение обновлений DHCP/DNS от имени клиентов. После отключения этой возможности обновление записей ресурсов адресов (A) и указателей (PTR) для DHCP-клиентов в DNS не выполняется.

При необходимости выполнить это изменение настроек на DHCP-серверах, работающих под управлением Windows Server 2003, можно снять флажок Включить динамическое обновление DNS в соответствии с настройкой, расположенный на вкладке Служба DNS диалогового окна свойств соответствующего DHCP-сервера или одной из его областей. По умолчанию обновления для устанавливаемых новых DHCP-серверов, работающих под управлением Windows Server 2003, и создаваемых для них областей выполняются всегда.

Дополнительные параметры конфигурации сервера DHCP/DNS

Помимо описанного стандартного взаимодействия DHCP/DNS, можно настроить DHCP-сервер на выполнение следующих дополнительных задач по обновлению.

Сервер можно настроить таким образом, чтобы он не отправлял обновления для удаления записей ресурсов адресов (A) клиентов, для которых истек срок аренды.

Когда на DHCP-сервере включено выполнение обновлений DNS, он всегда отправляет обновления для удаления записей ресурсов указателей (PTR) клиентов по окончании срока аренды. Аналогичный режим для записей ресурсов адресов (A) клиентов можно включать и отключать (по умолчанию данный режим включен).

Для этого используется флажок Удалять просроченные записи зоны прямого просмотра на вкладке Служба DNS в окнесвойств DHCP-сервера.

Сервер можно настроить таким образом, чтобы он не отправлял обновления для клиентов, неспособных использовать параметр «Полное имя клиента» (код 81) для запроса способа обработки обновлений.

По умолчанию DHCP-сервер не отправляет обновления для клиентов, не поддерживающих параметр 81.

Чтобы изменить этот режим, установите флажок Динамически обновлять DNS A- и PTR-записи для DHCP-клиентов, не требующих обновления (например, клиенты с Windows NT 4.0), расположенный на вкладке Служба DNS диалогового окна свойств соответствующего DHCP-сервера или одной из его областей.

DHCP-клиенты Windows и протокол динамического обновления DNS

DHCP-клиенты, работающие под управлением Windows 2000, Windows XP; или операционной системы Windows Server 2003, выполняют описанные выше обновления DHCP/DNS не так, как более ранние версии Windows. Примеры и рисунки, иллюстрирующие отличия в различных случаях, приведены ниже.

Пример 1. Обновление DHCP/DNS для DHCP-клиентов, работающих под управлением Windows 2000, Windows XP или операционной системы семейства Windows Server 2003

DHCP-клиенты, работающие под управлением Windows 2000, Windows XP; или операционной системы Windows Server 2003, взаимодействуют с протоколом динамического обновления DNS следующим образом.

Клиент отправляет на сервер сообщение-запрос DHCP (DHCPREQUEST) с включением DHCP-параметра 81. По умолчанию клиент запрашивает выполнение DHCP-сервером регистрации DNS-записи PTR, а DNS-запись A клиент регистрирует самостоятельно.

Сервер возвращает клиенту сообщение подтверждения DHCP (DHCPACK), предоставляющее ему в аренду IP-адрес и включающее DHCP-параметр 81. Если DHCP-сервер использует настройки по умолчанию (динамически обновляет в DNS записи A и PTR только по запросу DHCP-клиентов), то параметр 81 указывает клиенту, что DHCP-сервер зарегистрирует в DNS запись PTR, а клиент — запись A.

Регистрация в DNS собственной записи A клиентом и регистрация записи PTR клиента DHCP-сервером выполняются асинхронно.

Пример 2. Обновление DHCP/DNS для DHCP-клиентов, работающих под управлением более ранних версий Windows (до Windows 2000)

DHCP-клиенты, работающие под управлением более ранних версий Windows, не поддерживают процесс динамического обновления DNS непосредственно, поэтому не могут непосредственно взаимодействовать с DNS-сервером. Для этих клиентов DHCP обновления обычно выполняются следующим образом.

Клиент отправляет на сервер сообщение-запрос DHCP (DHCPREQUEST). DHCP-параметр 81 в запрос не включается.

Сервер возвращает клиенту сообщение подтверждения DHCP (DHCPACK), предоставляющее ему в аренду IP-адрес, без DHCP-параметра 81.

Затем сервер отправляет серверу DNS обновления записи прямого просмотра клиента, которая представляет собой запись ресурса адреса (A). Сервер также отправляет обновления записи обратного просмотра клиента, которая представляет собой запись ресурса указателя (PTR).

Владение записью DNS и группа DnsUpdateProxy

Как было описано выше, DHCP-сервер можно настроить таким образом, чтобы он динамически регистрировал записи ресурсов адреса (A) и указателя (PTR) от имени DHCP-клиентов. В этом режиме использование безопасного динамического обновления с DNS-серверами может привести к устареванию записей ресурсов.

Предположим, что происходит следующая последовательность событий.

DHCP-сервер Windows Server 2003 (DHCP1) выполняет от имени одного из клиентов безопасное динамическое обновление конкретного имени домена DNS.

Поскольку DHCP-сервер успешно создает имя, он становится владельцем этого имени.

Когда DHCP-сервер становится владельцем имени, обновлять записи DNS для этого имени может только данный DHCP-сервер.

В некоторых случаях это может вызывать затруднения. Например, в случае отказа DHCP1 резервный DHCP-сервер не сможет обновить имя клиента, поскольку не является владельцем этого имени.

В другом примере, если DHCP-сервер выполняет динамические обновления DNS для устаревших DHCP-клиентов (работающих под управлением более ранней версии Windows, чем Windows 2000), то после обновления этих клиентов до Windows 2000, Windows XP; или Windows Server 2003 обновленный клиент не сможет стать владельцем собственных записей DNS или обновлять их.

Для разрешения этого затруднения предусмотрена встроенная группа безопасности DnsUpdateProxy. Если все DHCP-серверы добавлены в группу DnsUpdateProxy, то в случае сбоя одного сервера его записи могут обновляться другим сервером. Кроме того, поскольку все объекты, создаваемые участниками группы DnsUpdateProxy, не защищены, владельцем имени DNS становится первый пользователь (не входящий в группу DnsUpdateProxy), изменяющий набор записей, связанный с именем DNS. После обновления устаревшие клиенты могут стать владельцами записей собственных имен на DNS-сервере. Обсуждавшаяся выше проблема устраняется путем включения в группу DnsUpdateProxy всех DHCP-серверов, регистрирующих записи ресурсов для клиентов устаревших версий.

Для настройки группы безопасности DnsUpdateProxy можно пользоваться оснасткой «Active Directory — пользователи и компьютеры». Дополнительные сведения см. в разделе Добавление участника группы.

Защита записей при использовании группы DnsUpdateProxy

DNS-имена, регистрируемые DHCP-сервером, входящим в группу DnsUpdateProxy, не защищены. Примером может служить запись ресурса адреса (A) для самого DHCP-сервера. Кроме того, незащищенность объектов, создаваемых участниками группы DnsUpdateProxy, делает невозможным эффективное использование этой группы в интегрированной зоне Active Directory, разрешающей только безопасные динамические обновления (если не предприняты дополнительные шаги по разрешению защиты записей, создаваемых участниками группы).

Для защиты от незащищенных записей или для предоставления участникам группы DnsUpdateProxy возможности регистрировать записи в зонах, допускающих только безопасные динамические обновления, можно создать выделенную учетную запись пользователя и настроить DHCP-серверы на выполнение динамических обновлений DNS с использованием ее учетных данных (имя пользователя, пароль и домен). Учетные данные одной выделенной учетной записи пользователя могут использоваться несколькими DHCP-серверами.

Выделенной учетной записью пользователя называют учетную запись пользователя, единственным назначением которой является предоставление DHCP-серверам учетных данных для регистрации при динамическом обновлении DNS. Когда выделенная учетная запись пользователя создана и DHCP-серверы настроены с использованием ее учетных данных, каждый DHCP-сервер предоставляет эти учетные данные при регистрации имен от имени DHCP-клиентов, использующих динамическое обновление DNS. Выделенная учетная запись пользователя должна быть создана в том же лесу, где находится основной DNS-сервер для зоны, которую требуется обновлять. Выделенная учетная запись пользователя также может быть расположена в другом лесу, если у него имеется доверие лесов с лесом, содержащим основной DNS-сервер для зоны, которую требуется обновлять. Дополнительные сведения об установлении доверия лесов см. в разделе Доверия лесов.

Если служба DHCP-сервера установлена на контроллере домена, настройка DHCP-сервера с учетными данными выделенной учетной записи пользователя приводит к прекращению наследования возможностей контроллера домена и возможного злоупотребления ими. При установке на контроллере домена служба DHCP-сервера наследует разрешения безопасности контроллера домена и обладает полномочиями обновлять или удалять любые записи DNS, зарегистрированные в безопасной зоне, интегрированной в Active Directory (включая записи, которые были безопасно зарегистрированы другими компьютерами, работающими под управлением Windows 2000 или операционной системы семейства Windows Server 2003, в том числе контроллерами домена).

В следующих ситуациях настройка выделенной учетной записи пользователя и настройка DHCP-сервера с использованием ее учетных данных необходимы:

контроллер домена настроен для выполнения функций DHCP-сервера;

DHCP-сервер настроен для выполнения динамических обновлений DNS от имени DHCP-клиентов;

зоны DNS, которые будут обновляться DHCP-сервером, допускают только безопасные динамические обновления.

После создания выделенной учетной записи пользователя можно настроить DHCP-сервер с использованием ее учетных данных при помощи консоли DHCP или команды Netsh DHCP server set dnscredentials. Дополнительные сведения о настройке учетных данных с помощью консоли DHCP см. в разделе Настройка учетных данных динамического обновления DNS. Полный справочник команд Netsh для DHCP (включая синтаксис, параметры и примеры использования команды set dnscredentials в контексте netsh dhcpserver), см. в разделе Netsh (команды для протокола DHCP).

Дополнительные сведения о группах и учетных записях см. в разделах Создание новой учетной записи пользователя и Группы по умолчанию.

Дополнительные ресурсы по вопросам взаимодействия DHCP и DNS

Ниже перечислены дополнительные разделы, с которыми можно ознакомиться при возникновении затруднений при внедрении взаимодействия DHCP и DNS.

Источники дополнительных сведений.

Сведения о протоколе динамического обновления DNS и о защите динамических обновлений при использовании Active Directory.

Сведения о настройке DNS-серверов для выполнения некоторых или всех обновлений для конкретных зон см. в разделах Разрешение динамических обновлений и Разрешение только безопасных динамических обновлений.

Сведения о включении на DHCP-серверах режима инициирования обновлений от имени клиентов для конкретных (или всех) областей см. в разделе Разрешение динамического обновления DNS для клиентов.

Сведения о возможных модификациях или настройке компьютеров для инициирования динамических обновлений от собственного имени см. в разделе Настройка TCP/IP на использование DNS.

Сведения о записях ресурсов DNS см. в разделах Служба DNS или Справочник по записям ресурсов.

**Установка и настройка DHCP-сервера в Windows Server 2008**

**Составьте план**

Перед тем, как приступить к конфигурированию DHCP-сервера, нужно тщательно подготовиться. Заранее соберите всю необходимую информацию. В частности, полезно будет знать:

• Диапазон IP-адресов, которым будет управлять сервер (например, от 192.168.1.50 до 192.168.1.200).

• Каким машинам понадобятся статические IP-адреса (например, серверы и маршрутизаторы, настраиваемые вручную, которым не нужен DHCP для получения IP-адреса).

• Какую сетевую информацию вы хотите отправлять DHCP-клиентам после того, как те получат свои IP-адреса (например, адреса для шлюза по умолчанию, DNS-серверов, WINS-серверов).

Настроить DHCP-сервер будет гораздо легче, уже имея на руках всю необходимую информацию, чем если искать её в процессе.

**Установка DHCP**

Установить DHCP в Windows 2008 проще простого. Разработчики создали удобный мастер, который проведёт вас через весь процесс.

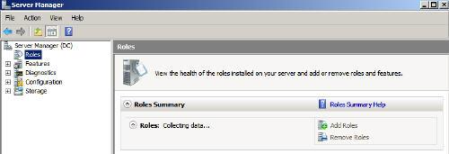
Чтобы установить DHCP-сервер из "Панели управления" (Control Panel):

1...В меню "Пуск" (Start) выберите "Панель управления" (Control Panel) | "Администрирование" (Administrative Tools) | "Управление сервером" (Server Manager).

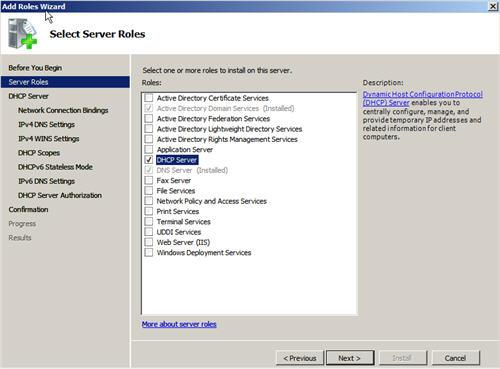
2...Раскройте вкладку и выберите объект "Роли" (Roles) (изображение A).

3...Выберите команду "Добавить роли" (Add Roles) и, щёлкнув на DHCP, следуйте указаниям мастера (изображение B).

4...На экране появится новый мастер настройки DHCP-сервера.



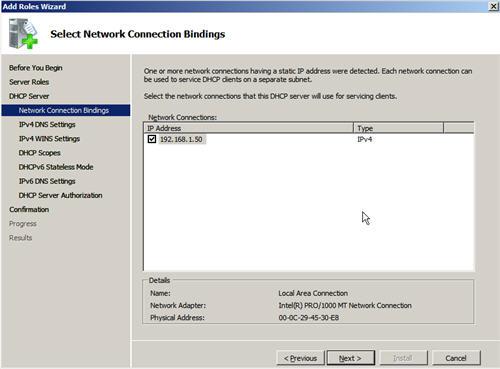
Изображение A. Управление сервером



Изображение B. Мастер добавления ролей

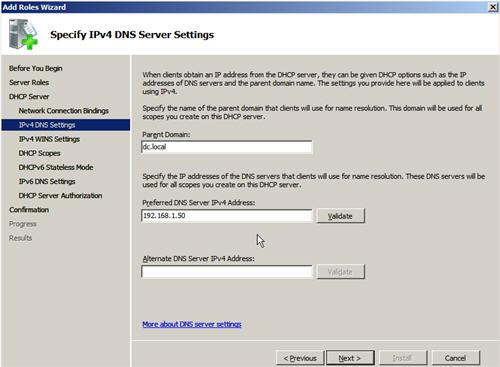
В предыдущей версии Windows мастер не помогал в настройке DHCP-сервера. В Windows Server 2008 весь процесс разбит на семь шагов. Разумеется, по-прежнему можно управлять DHCP при помощи оснастки "Консоль управления" (DHCP Microsoft Management Console, MMC), либо создавать и удалять контексты по ходу дела.

Вернемся к мастеру. Сетевые карты и статические IP-адреса будут автоматически обнаружены, можно выбрать, как DHCP будет обслуживать клиентов в различных подсетях (изображение C).

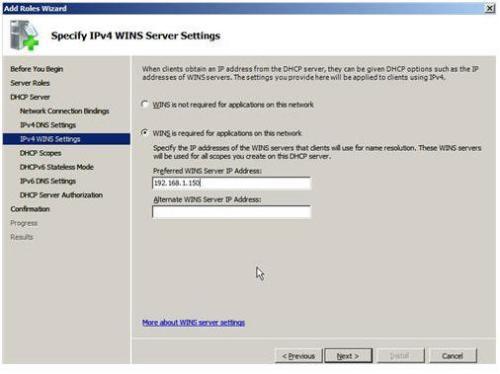


Изображение C. Выберите свои статический IP-адреса для обслуживания DHCP-клиентов

В следующем окне (изображение D) определяется подходящий DNS-сервер(ы) для использования с DHCP после утверждения адреса. На изображении E показано, где нужно указать подходящие WINS-серверы, если они используются в сети.



Изображение D. Введите IP-адрес вашего DNS-сервера



Изображение E. Введите IP-адрес вашего WINS-сервера

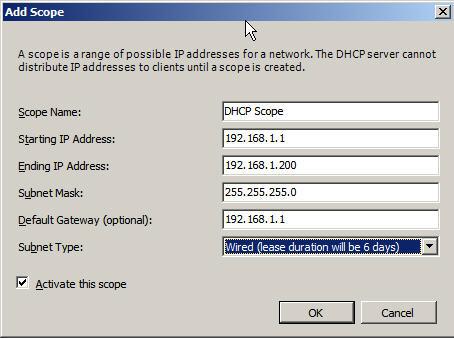
**О контекстах**

При создании контекста нужно выбрать диапазон IP-адресов и указать соответствующие опции. Эти опции уже были упомянуты выше (дополнительная сетевая информация поступающая клиентам при получении ими IP-адресов).

Опции делятся на два вида: для всех контекстов (Global) и для одного из выбранной области (Scope). Глобальные опции распространяются на все контексты, созданные в данном DHCP-сервере, контекстные опции — для отдельной области, с которой вы работаете.

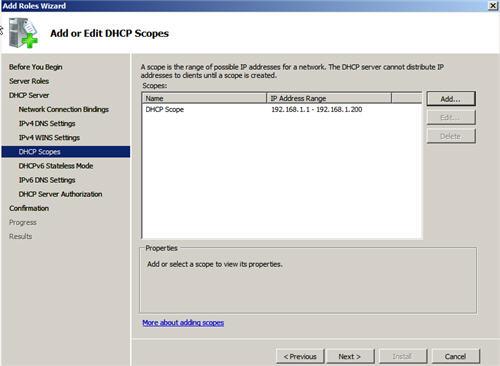
К примеру, если вы создали разные контексты для нескольких подсетей и у каждой из них будет отдельный шлюз по умолчанию, но один DNS-сервер на всех, следует активизировать DNS-сервера в качестве глобальной опции, а шлюзы — отдельно в каждой области как контекстную опцию.

Контексты создаются в соответствующем окне "Добавить область" (Add scope). Параметры настраиваются в зависимости от размера сети и количества пользователей, которым будут присвоены IP-адреса. Я создал простой контекст (изображение F).



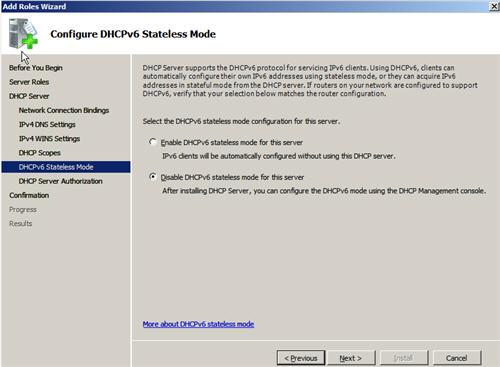
Изображение F. Создание контекста

Ниспадающее меню для выбора подсети предусматривает вариант беспроводной сети (изображение G). Срок действия по умолчанию составляет 24 часа. Если требуется активировать контекст по завершению работы мастера, отметьте параметр "Активировать эту область" (Activate this scope). Если этого не сделать, активировать область придётся посредством оснастки DHCP MMC.



Изображение G. Прежде чем продолжить, можно добавить несколько контекстов

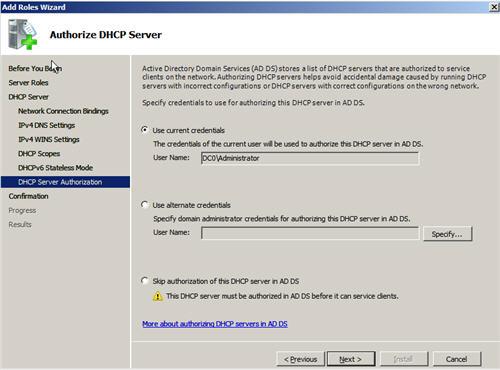
В Windows Server 2008 при наличии маршрутизатора (изображение H), поддерживающего и настроенного для работы с протоколом IPv6, можно включить соответствующую функцию.



Изображение H. Включение IPv6 в режиме без сохранения адресов (Enable IPv6 stateless mode)

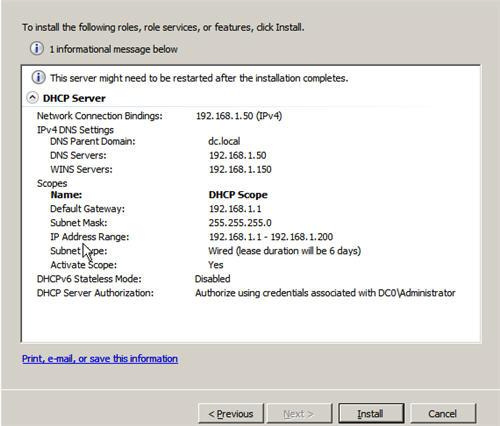
Авторизация DHCP-сервера и активация контекстов

В предыдущих версиях Windows Server требовалось установить и настроить DHCP-сервер, а уже после этого авторизировать его через оснастку DHCP MMC. Авторизация DHCP нужна для предотвращения попыток изменения конфигурации сервера хакерами. В Windows Server 2008 есть выбор: авторизировать сервер при помощи Мастера или в оснастке DHCP MMC по завершению настройки (изображение I).

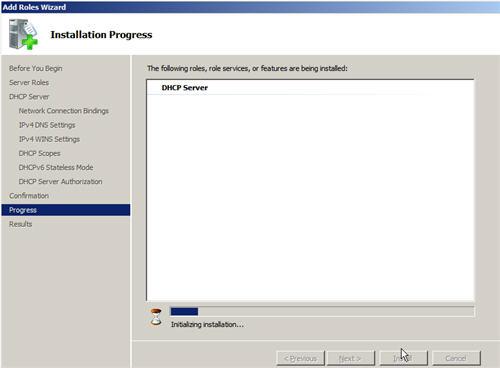


Изображение I. Авторизация DHCP-сервера

Теперь можно просмотреть (изображение J) и подтвердить настройки перед их вступлением в силу (изображение K).



Изображение J. Обзор конфигурации DHCP перед принятием настроек



Изображение K. Ход процесса установки DHCP

Управление установленным DCHP-сервером осуществляется при помощи оснастки DHCP MMC (изображение O), которую можно вызвать из меню "Администрирование" (Administrative tools). На этом экране можно указать исключения (exclusions) и резервирования (reservations).

**Добавление резервирования**

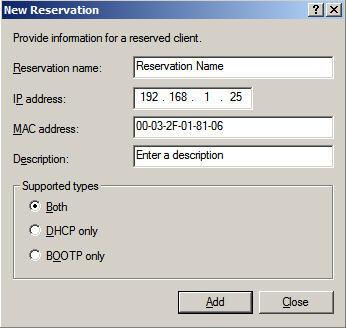
Помимо указанных диапазонов исключений, в DHCP-сервер можно добавить резервирования. Добавляя резервирование, вы гарантируете, что указанная машина может всегда использовать один и тот же IP-адрес.

1...Щёлкните правой кнопкой на "Резервированиях" (Reservations) и выберите "Создать резервирование" (New reservation).

2...Введите имя резервирования и IP-адрес для данной машины или устройства.

3...Введите MAC-адрес машины или устройства. MAC-адрес компьютера Windows можно узнать, запустив команду ipconfig/all в командной строке данной машины.

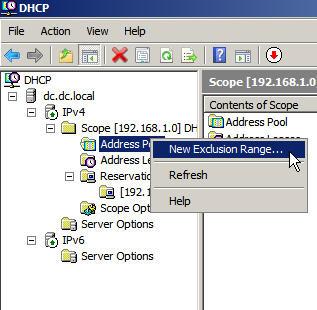
4...Введите описание и выберите тип резервирования: DHCP, BOOTP (проходит через маршрутизатор) либо оба (изображение L). Нажмите "Добавить" (Add).



Изображение L. Добавление резервирования

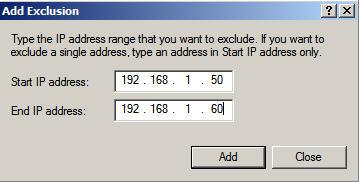
**Добавление исключений**

Помимо указанных резервирований, в DHCP-сервер можно добавить исключения (изображение M). Добавляя исключение, вы гарантируете, что данный диапазон IP-адресов не будет предоставляться службой DHCP. Чрезвычайно полезно блокировать IP-адреса серверов и маршрутизаторов.

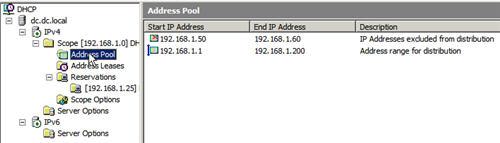


Изображение M. Добавление диапазона исключения

Для того чтобы добавить исключение, щёлкните правой кнопкой на "Пуле доступных адресов" (Address Pools) и выберите команду "Создать диапазон исключений" (New Exclusion Range) (изображения N и O).



Изображение N. Диапазон исключения IP-адресов



Изображение O. Оснастка DCHP MMC

**Устранение неполадок в работе DHCP**

После проведения всех настроек DHCP самым простым способом устранения неисправностей с сервером DHCP будет запуск команды Ipconfig из командной строки. Чтобы получить отчёт по TCP/IP для данной машины, введите ipconfig/all. Для обнуления предоставленного DHCP адреса введите ipconfig/release; для получения нового введите ipconfig/renew.