**Проблема автоматизации распределения IP-адресов**

Одной из основных задач системного администратора является настройка стека протоколов TCP/IP на всех компьютерах сети. Есть несколько необходимых параметров, которые следует настроить на каждом компьютере, – это IP-адрес, маска подсети, шлюз по умолчанию, IP-адреса DNS-серверов. Назначенные IP-адреса должны быть уникальны. В случае каких-либо изменений (например, изменился IP-адрес DNS сервера или шлюза по умолчанию) их нужно отразить на всех компьютерах. Если какие- либо параметры не указаны или не верны, сеть не будет работать стабильно.

Если в сети менее десяти компьютеров, администратор может успешно справляться с задачей настройки стека TCP/IP вручную, т. е. на каждом компьютере отдельно вводить параметры. IP-адрес, назначенный таким образом, называется статическим. При числе узлов сети более десяти (а многие сети включают десятки и сотни хостов) задача распределения параметров вручную становится трудной или вовсе не выполнимой. В стеке TCP/IP существует протокол, позволяющий автоматизировать процесс назначения IP-адресов и других сетевых параметров, который называется DHCP – Dynamic Host Configuration Protocol (протокол динамической конфигурации хоста). Использование этого протокола значительно облегчает труд системного администратора по настройке сетей средних и больших размеров. Описание протокола DHCP приводится в документе RFC 2131.

**Реализация DHCP в Windows**

Протокол DHCP реализуется по модели «клиент-сервер», т. е. в сети должны присутствовать DHCP-сервер (роль которого может исполнять компьютер с операционной системой Windows Server) и DHCP-клиент.

На компьютере-сервере хранится база данных с сетевыми параметрами и работает служба DHCP сервера. Компьютер-клиент (точнее, служба клиента DHCP) осуществляет запросы на автоматическую конфигурацию, и DHCP-сервер при наличии свободных IP-адресов выдает требуемые параметры.

Набор IP-адресов, выделяемых для компьютеров одной физической подсети, называется областью действия (scope). На одном сервере можно создать несколько областей действия. Важно только отслеживать, чтобы области действия не пересекались.

При запросе клиента DHCP-сервер выделяет ему произвольный свободный IP-адрес из области действия совместно с набором дополнительных сетевых параметров. При необходимости некоторые адреса из области действия можно зарезервировать (reserve) за определенным МАС-адресом. В этом случае только компьютеру с этим МАС-адресом (например, DNS-серверу, адрес которого не должен меняться) будет выделяться зарезервированный IP-адрес.

Адреса выделяются клиентам на определенное время, поэтому предоставление адреса называется арендой (lease). Время аренды в Windows Server может быть от 1 минуты до 999 дней (или неограниченно) и устанавливается администратором.

**Параметры DHCP**

Основная функция протокола DHCP – предоставление в аренду IP-адреса. Однако для правильной работы в сети TCP/IP хосту необходим ещё ряд параметров, которые также можно распространять посредством

DHCP. Набор параметров указан в RFC 2132.

Перечислим только основные параметры:

• Subnet mask – маска подсети;

• Router – список IP-адресов маршрутизаторов;

• Domain Name Servers – список адресов DNS-серверов;

• DNS Domain Name – DNS-суффикс клиента;

• WINS Server Names – список адресов WINS-серверов;

• Lease Time – срок аренды (в секундах);

• Renewal Time (T1) – период времени, через который клиент начинает продлевать аренду;

• Rebinding Time (T2) – период времени, через который клиент начинает осуществлять широковещательные запросы на продление аренды.

Параметры могут применяться на следующих уровнях:

• уровень сервера;

• уровень области действия;

• уровень класса;

• уровень клиента (для зарезервированных адресов).

Параметры, определенные на нижележащем уровне, перекрывают параметры вышележащего уровня, например параметры клиента имеют больший приоритет, чем параметры сервера. Самый высокий приоритет имеют параметры, настроенные вручную на клиентском компьютере.

Уровень класса используется для объединения клиентов в группы и применения для этой группы отдельных параметров. Отнести клиента к определенному классу можно, применив утилиту IPconfig с ключом /setclassid.

**Адреса для динамической конфигурации**

При настройке областей действия перед администратором встает вопрос, какой диапазон адресов выбрать для сети своей организации? Ответ зависит от того, подключена ли сеть к Интернету.

Если сеть имеет доступ в Интернет, диапазон адресов назначается провайдером (ISP – Internet Service Provider, поставщик интернет-услуг) таким образом, чтобы обеспечить уникальность адресов в Интернете. Чаще всего бывает так, что провайдер выделяет один или несколько адресов для прямого доступа в Интернет и они присваиваются прокси-серверам, почтовым серверам и другим хостам, которые являются буферными узлами между сетью организации и Интернетом. Большинство остальных хостов получают доступ к интернет-трафику через эти буферные узлы. В этом случае диапазон внутренних адресов организации должен выбираться из множества частных адресов.

Частные адреса(Private addresses), описанные в RFC 1918, специально выделены для применения во внутренних сетях и не могут быть присвоены хостам в Интернете. Существует три диапазона частных адресов:

• ID подсети – 10.0.0.0, маска подсети: 255.0.0.0;

• ID подсети – 172.16.0.0, маска подсети: 255.240.0.0;

• ID подсети – 192.168.0.0, маска подсети: 255.255.0.0.

Внутри этих диапазонов адресов можно организовывать любые возможные подсети.

Если сеть не имеет доступа в Интернет, то теоретически можно выбрать любой диапазон IP-адресов, не учитывая наличия хостов с такими же адресами в Интернете. Однако на практике все равно лучше выбирать адреса из диапазона частных адресов, так как для сети, не имеющей выхода в

Интернет, в ближайшем будущем подключение к глобальной сети может оказаться необходимым, и тогда возникнет проблема изменения схемы адресации.

Также следует отметить, что помимо описанных частных адресов существует диапазон автоматических частных адресов APIPA (Automatic Private IP Address): ID подсети – 169.254.0.0, маска подсети: 255.255.0.0. Адрес из этого диапазона выбирается хостом TCP/IP случайно, если отсутствует статический IP-адрес, DHCP-сервер не отвечает, и не указан альтернативный статический адрес. После выбора IP-адреса, хост продолжает посылать запросы DHCP-серверу каждые пять минут.

**Принцип работы DHCP**



Диаграмма переходов, иллюстрирующая принципы работы протокола DHCP, приведена на. На схеме овалами обозначены состояния, в которых может находиться DHCP-клиент. Из одного состояния в другое клиент может переходить только по дугам. Каждая дуга помечена дробью, числитель которой обозначает событие (чаще всего это сообщение от DHCP-сервера), после которого клиент переходит в соответствующее состояние, а знаменатель описывает действия DHCP-клиента при переходе. Черточка в числителе означает безусловный переход. Начальное состояние, в котором оказывается служба DHCP-клиента при запуске, – это «Инициализация». Из этого состояния происходит безусловный переход в состояние «Выбор» с рассылкой широковещательного сообщения DHCPDISCOVER. DHCP-серверы (в одной сети их может быть несколько), принимая сообщение, анализируют свою базу данных на предмет наличия свободных IP-адресов. В случае успеха, серверы отправляют сообщение DHCPOFFER, которое помимо IP-адреса содержит дополнительные параметры, призванные помочь клиенту выбрать лучшее предложение.

Сделав выбор, клиент посылает широковещательное сообщение DHCPREQUEST, запрашивая предложенный IP-адрес и требуемые параметры (например, маска подсети, шлюз по умолчанию, IP-адреса DNS-серверов и др.) и переходит в состояние «Запрос». Данное сообщение требуется посылать широковещательно (т. е. оно должно доставляться всем компьютерам подсети), так как DHCP-серверы, предложения которых клиент отклонил, должны знать об отказе.

В состоянии «Запрос» клиент ожидает подтверждение сервера о возможности использования предложенных сетевых параметров. В случае прихода такого подтверждения (сообщение DHCPACK) клиент переходит в состояние «Аренда», одновременно начиная отсчет интервалов времени Т1 и Т2. Если сервер по каким-либо причинам не готов предоставить клиенту предложенный IP-адрес, он посылает сообщение DHCPNAK. Клиент реагирует на это сообщение переходом в исходное состояние «Инициализация», чтобы снова начать процесс получения IP-адреса. Состояние «Аренда» является основным рабочим состоянием – у клиента присутствуют все необходимые сетевые параметры, и сеть может успешно функционировать.

Через временной интервал Т1 от момента получения аренды (обычно Т1 равно половине общего времени аренды)1 DHCP-клиент переходит в состояние «Обновление» и начинает процесс обновления аренды IP-адреса. Сначала клиент посылает DHCP-серверу сообщение DHCPREQUEST, включающее арендованный IP-адрес. Если DHCP-сервер готов продлить аренду этого адреса, то он отвечает сообщением DHCPACK и клиент возвращается в состояние «Аренда» и заново начинает отсчитывать интервалы Т1 и Т2.

В случае, если в состоянии «Обновление» по истечении интервала времени Т2 (который обычно устанавливается равным 87,5% от общего времени аренды) все ещё не получено подтверждение DHCPACK, клиент переходит в состояние «Широковещательное обновление» с рассылкой широковещательного сообщения DHCPREQUEST. Такая рассылка делается в предположении, что DHCP-сервер поменял свой IP-адрес (или перешел в другую подсеть) и передал свою область действия другому серверу. В этом состоянии получение DHCPACK возвращает клиента в состояние «Аренда» и аренда данного IP-адреса продлевается. Если клиент получает от сервера сообщение DHCPNAK или общее время аренды истекает, то происходит переход в состояние «Инициализация» и клиент снова пытается получить IP-адрес.

В процессе работы может оказаться, что время аренды не истекло, а служба DHCP-клиента прекратила работу (например, в случае перезагрузки).

В этом случае DHCP-клиент начинает работу в состоянии «Инициализация после перезагрузки», рассылает широковещательное сообщение DHCPREQUEST и переходит в состояние «Перезагрузка». В случае подтверждения продления аренды (сообщение DHCPACK от DHCP-сервера) клиент переходит в состояние «Аренда». Иначе (сообщение DHCPNAK) клиент оказывается в состоянии «Инициализация».

**Авторизация DHCP-сервера**

Неправильное функционирование DHCP-сервера в любой сети может привести к нарушению работы всей сети. Ошибки в настройке могут быть вызваны неправильным планированием, когда в одной подсети оказываются несколько DHCP-серверов, или действиями некомпетентного лица (а возможно, и злоумышленника). Для предотвращения последствий таких действий в Windows Server предусмотрен механизм авторизации

1 Заблаговременные попытки продления аренды клиент предпринимает для того, чтобы в момент истечения времени аренды компьютер не оказался без IP-адреса. При этом работа клиента в сети была бы нарушена.

DHCP-серверов. Неавторизованный DHCP-сервер (unauthorized DHCP server) не будет работать в этой операционной системе.

Процедуру авторизации может выполнить только администратор. При этом адрес авторизованного DHCP-сервера регистрируется в каталоге Active Directory (см. лекцию 7). Затем при запуске служба DHCP-сервера проверяет наличие IP-адреса своего компьютера в списке авторизованных DHCP-серверов Active Directory и только после этого может продолжать свою работу.

**Вывод**

Существенной проблемой в компьютерных сетях является настройка сетевых параметров на всех узлах сети в условиях большого числа узлов и возможных изменений параметров. В сетях TCP/IP для решения указанной проблемы служит протокол DHCP, обеспечивающий автоматическую настройку сетевых параметров.

Протокол DHCP реализует соответствующая служба, работающая по модели «клиент-сервер». Служба DHCP по запросу клиентов выдает им IP-адреса из заданного диапазона и другие сетевые параметры в аренду на определенное время. По истечении времени аренды клиенты должны обновлять её.

Наиболее часто в локальных сетях применяются адреса из частных диапазонов, которые не используются в Интернете. В случае, если клиенту не назначен IP-адрес и он не смог получить его самостоятельно у DHCP-сервера, выбирается случайный автоматический частный адрес из подсети 169.254.0.0/16.

Для предотвращения несанкционированного использования DHCP-серверов в сетях Active Directory применяется механизм авторизации.

**ПРОЧИТАТЬ И СДЕЛАТЬ КОНСПЕКТ.**

**ФОТООТЧЕТ ОТПРАВИТЬ НА ПОЧТУ ИЛИ В ЛИЧНЫЕ СООБЩЕНИЯ ВКОНТАКТЕ ДО 17:00 05.12.2022**

**selenginskaj@mail.ru**

**https://vk.com/akatik172**