Лабораторная работа № 3

## Администрирование сетевых и коммуникационных служб информационных систем

# ЦЕЛЬ РАБОТЫ

Изучение принципов управления информационной сетью с помощью служб протокола TCP/IP. Освоение структур и принципов назначения IP-адресов и DNS-имен компьютеров. Исследование механизма разрешения DNS-имен в IP-адреса.

# ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

**Управление сетью при помощи сетевых протоколов и служб**

### Протоколы сетевого уровня

Протокол IP – краеугольный камень набора TCP/IP, названного по двум составляющим его протоколам (Transmission Control Protocol/Internet Protocol), которые вместе обеспечивают популярный сетевой транспортный сервис. Протокол транспортного уровня TCP передает данные на сетевой уровень, где IP инкапсулирует их в кадр (пакет), добавляя свой заголовок и получая в результате *дейтаграмму* (datagram) – элемент данных, созданный протоколом сетевого уровня и состоящий из данных транспортного уровня и заголовка сетевого уровня. По существу протокол IP выполняет роль конверта, в котором данные TCP/IP доставляются по назначению. Протокол IP отвечает за передачу данных от исходной системы до целевой. Он не ориентирован на соединение, т.е. передает сообщения целевой системе, не устанавливая предварительно связи с ней. Протокол IP выполняет несколько важных функций:

- инкапсуляцию – упаковку пакета данных транспортного уровня в дейтаграмму;

- адресацию – идентификацию систем в сети по их IP-адресам (адрес IP имеет длину 32 бита и состоит из идентификатора сети и идентификатора хоста (*хостом* (host) в TCP/IP называется сетевой адаптер компьютера или другого устройства));

- маршрутизацию – определение наиболее эффективного пути к целевой системе;

- фрагментацию – разбиение данных на фрагменты, по размеру подходящие для передачи по сети;

- идентификацию протокола транспортного уровня, который сгенерировал данные в дейтаграмме.

IP-адресация существенно облегчает компьютерам распознавание друг друга и обмен информацией, но с точки зрения пользователя удобством не отличается. Запоминать IP-адреса всех компьютеров локальной сети, принтеров и дисков, к которым необходимо обратиться, достаточно сложно. Чтобы сделать TCP/IP более "дружественным", его разработчики придумали систему имен хостов, то есть понятных имен, которые администратор присваивает компьютерам в сети и которые, по мере необходимости, преобразуются в IP-адреса.

*Имя хоста* (host name) – это имя, символизирующее компьютер. Существует несколько систем именования объектов сети, одной из которых является с *истема именования доменных имен* (Domain Name System, DNS). Когда происходит обращение к другому компьютеру сети по DNS-имени, инициирующий обращение компьютер должен сначала преобразовать это имя в IP-адрес. Процесс преобразования имени в адрес называется *разрешением имени* (name resolution).

***Служба доменных имен***

**Структура доменных имен**

В основе доменных имен лежит иерархическое пространство имен. При этом все пространство имен DNS представлено в виде отдельных фрагментов, называемых *доме нами* (domains). Домены, связываясь между собой с помощью отношений родитель-потомок, образуют определенную иерархию. В зависимости от того, какое положение занимает домен в иерархии, принято говорить об уровне домена. На любом уровне домен может включать в свой состав домены более низкого уровня. Начиная со второго уровня домены могут также включать в свой состав хосты.

Домен, лежащий в основании иерархического пространства имен DNS, получил название *корневого домена* (root domain). Корневой домен выполняет функцию родоначальника всех доменов первого уровня. Фактически он является формальным элементом, символизирующим иерархичность пространства доменных имен. Для ссылки на корневой домен используются пустые кавычки (« »). При записи доменного имени корневой домен обозначается как пустое место после точки, которой оканчивается любое доменное имя.

Самое большое пространство имен DNS образует пространство имен Интернет, которое организовано следующим образом. Домены первого уровня используются для группировки других доменов по организационному или географическому признакам. В случае группировки по организационному принципу имена доменов первого уровня содержат три символа: edu (образовательные учреждения), com (коммерческие организации), org (некоммерческие организации), gov (правительственные организации), mil (военные учреждения) и др. При группировке по географическому признаку используются имена, состоящие из двух символов, например: ru (Россия), ie (Ирландия), au (Австралия) и т.п. Помимо перечисленных принципов формирования для организации доменов первого уровня используется группировка по принципу обратных запросов (reverse domains – обратных доменов). Обратные домены применяются для поиска доменного имени хоста по его IP-адресу. Обратный домен первого уровня получил название arpa. Он является единственным доменом первого уровня, имеющим имя из четырех символов. Домен содержит только один домен второго уровня: in-addr.arpa.

Вопросами создания доменов первого и второго уровней занимается специальная организация – *Сетевой информационный центр* (Network Information Center, NIC). Чтобы зарегистрировать домен второго уровня заинтересованная организация или физическое лицо должны обратиться в NIC с соответствующей заявкой. Доменное имя домена второго уровня выдается на срок на платной основе. В России регистрацией доменов второго уровня занимается *Росс ийский НИИ развития общественных сетей* (Russian Institute for Public Network, RIPN). Зарегистрировав доменное имя второго уровня, организация или физическое лицо может создавать в его приделах любое количество хостов и доменов нижних уровней.

В пространстве имен DNS домены выступают в роли контейнеров или узлов дерева. Листьями дерева являются хосты, принадлежащие тому или иному домену. Каждый хост имеет собственное имя, уникальное в пределах того домена, к которому он принадлежит. Чтобы иметь возможность ссылаться на хост из любой произвольной

точки сети, необходимо использовать его *полное доменное имя* (Fully Qualified Domain Name, FQDN). Полное доменное имя хоста образуется из имени хоста и имен всех доменов, находящихся между хостом и корневым доменом, разделенных точками. Например, для хоста w
ww
полное доменное имя записывается в виде
www.microsoft.com
. Такое имя уникально в пределах всего пространства DNS.

***Процедура разрешения DNS-имени***

Главная идея построения системы доменных имен заключается в создании альтернативного метода адресации объектов сети. Соединение же между хостами может быть организовано только на уровне IP-адресов. Поэтому необходимо предусмотреть механизм трансляции имен в соответствующие IP-адреса. В качестве такого механизма традиционно используется специальная служба, получившая название с*лужбы доменных имен* (Domain Name Service, DNS). Служба DNS представляет собой распределенную базу данных, содержащую информацию об IP-адресах и соответствующих им доменных именах. Данные о доменах и принадлежащих им хостах, образующие пространство имен DNS, не концентрируются в одном месте, а хранятся в виде фрагментов на отдельных серверах. Компьютер, на котором функционирует служба DNS, принято называть сервером DNS. База данных каждого сервера DNS представляет собой фрагмент общего пространства имен, распределенного между множеством серверов. В терминологии DNS такие фрагменты пространства имен принято называть *зонами* (zone).

Служба DNS позволяет администраторам присваивать компьютерам сети имена с иерархической структурой и при необходимости разрешать их в IP-адреса. Взаимоотношения доменов различных уровней легче понять, разобравшись в том, как DNS-сервер находит IP-адрес по DNS-имени.

Распределенная природа пространства DNS-имен предполагает, что ни на одном сервере нет полного списка имен доменов Интернета и всех хостов в этих доменах. Поэтому, получив от клиентской системы запрос на разрешение имени, DNS-сервер прежде всего должен определить, где находится нужная ему информация. Он запрашивает у одного из корневых серверов адрес управляющего сервера для домена первого уровня разрешаемого имени. Например, чтобы определить IP-адрес для имени www.microsoft.com

, DNS-сервер посылает корневому серверу запрос об адресе управляющего сервера для домена com. Если инициирующий соединение компьютер размещен в зоне домена com, то DNS-серверу направляется адрес управляющего сервера для домена microsoft.com. Для других доменов корневой сервер подобрал бы адрес соответствующего сервера домена первого уровня, куда DNS-сервер отправил бы новый запрос об адресе управляющего сервера для домена второго уровня. Так при запросе компьютера, являющегося элементом другой зоны (не com), на разрешение имени www.microsoft.com
DNS-сервер сначала узнает IP-адреса доменов com и micrisoft.com, а затем направляет запрос домену micrisoft.com о разрешении IP-адреса хоста www. Сервер micrisoft.com возвращает запрашиваемый IP-адрес, а DNS-сервер перенаправляет его клиенту.

**Обратное разрешение имени**

Система DNS предназначена для поиска IP-адреса по имени, но иногда TCP/IP-компьютеру необходимо совершить обратное преобразование – определить имя по IP-адресу. Поскольку пространство DNS-имен распределено по различным доменам, выполнить эту задачу путем опроса всех управляющих DNS-серверов практически невозможно. Для решения этой проблемы в пространство DNS-имен включен специальный домен in-addr.arpa. В нем обратное преобразование (адреса в имя) осуществляется с помощью разделения на домены, в качестве имен которых используются IP-адреса. Домен  in-addr.arpa разделен на 256 доменов третьего уровня, именами которых являются числа от 0 до 255, символизирующие первый байт IP-адреса. Каждый домен третьего уровня разбит на 256 доменов четвертого уровня, представляющих второй байт IP-адреса. Также устроены домены пятого и шестого уровней. С их помощью можно найти DNS-имя для любого возможного IP-адреса. Например, IP-адресу 192.168.2.6 соответствует домен с именем 6.2.168.192.in-addr.arpa. В записи ресурса этого домена содержится DNS-имя компьютера с заданным IP-адресом. В имени домена байты IP-адреса расположены в обратном порядке.

*Службы удаленного терминального доступа Telnet и Rlogin*

Приложения, позволяющие осуществить удаленный терминальный доступ, очень популярны в Internet, так как при их применении отпадает необходимость иметь аппаратный терминал на каждом из хостов. Можно осуществить терминальное подключение к одному из хостов, а затем посредством сети подключиться к любому другому хосту (в том случае, если на этом хосте существует открытый бюджет).

В сетях TCP/IP существуют два приложения, использующие стандарт клиент-сервер,

позволяющие осуществить терминальный заход.

1. Telnet - стандартное приложение, которое присутствует практически в каждой реализации TCP/IP. Оно может быть применено для связи между хостами, работающими под управлением различных операционных систем. Telnet использует согласование опций клиента и сервера, чтобы определить, какие характеристики имеют клиенты на обеих сторонах.
2. Программа Rlogin первоначально была разработана для осуществления связи между Unix системами, однако впоследствии была перенесена и на другие операционные системы.

Рассмотрим пример, который описывает процедуры службы DNS, реализуемые посредством Rlogin. Обмен пакетами показан на рисунке.

В процессе реализации соединения осуществляются 11 шагов, при этом заранее никакой информации на сторонах клиента или сервера кэшировано (сохранено) не было.

1. Клиент 1 начинает процедуру связи. Он вводит DNS-имя компьютера (клиента 2), с которым надлежит осуществить связь, и вызывает разборщик (приложение, реализующее функцию разрешения введенного DNS-имени хоста в IP-адрес). Запрос типа A отправляется на DNS-сервер зоны клиента 1. Ресурсная запись A представляет собой запрос простого преобразования доменного имени хоста в некоторый IP-адрес.

2. Ответ от DNS-сервера зоны клиента 1 содержит имя DNS-сервера для домена, в котором находится Rlogin сервер.

3. Разборщик клиента повторно отправляет запрос типа A на DNS-сервер корневого домена. Этот запрос обычно имеет установленный флаг "рекурсия необходима".

4. В результате выполнения рекурсивных запросов клиенту 1 передается отклик с IP-адресом клиента 2.

5. Клиент Rlogin (клиент 1) устанавливает TCP соединение с сервером Rlogin. TCP модули клиента и сервера обмениваются друг с другом тремя пакетами.

6. Сервер Rlogin принимает сообщение от клиента 1 и вызывает свой разборщик, чтобы получить имя хоста (клиента 2) по его IP-адресу. Это реализуется посредством PTR запроса на DNS-сервер зоны клиента 2. Ресурсная запись типа PTR используется для организации процесса обратного разрешения IP-адреса в соответствующее доменное имя. Сервер Rlogin проверяет тот ли это сервер зоны, к которому обратился клиент 1 на шаге 1.

7. Отклик корневого сервера содержит имя DNS-сервера домена in-addr.arpa хоста.

8. Разборщик сервера повторно отправляет PTR запрос к DNS-серверу клиента 2.

9. PTR отклик содержит FQDN клиента 2.

10. Разборщик сервера отправляет запрос типа A к DNS серверу клиента 2, спрашивая IP-адрес, соответствующий имени, возвращенному в предыдущем шаге.

11. Отклик от DNS-сервера содержит запись A клиента 1 для хоста (клиента 2). Сервер Rlogin сравнивает запись A с IP-адресом клиента 1, потребовавшего открыть TCP соединение.

Кэширование может уменьшить количество пакетов, которыми производится обмен в рассмотренном примере.

**Защита сетевых сообщений**

Механизмы защиты передаваемых сообщений действуют в основном в пределах одной сети (или подсети), т.е. ограничивают доступ пользователей только файлами и ресурсами, которые нужны им для работы. Большое количество опасностей сосредоточено вне частной сети, а входят они в нее через главный канал связи с внешним миром – подключение к Интернету. *Брандмауэром* (firewall) называется устройство или программа, защищающая сеть от несанкционированного доступа извне. Обычно брандмауэры применяют для защиты частной сети или интерсети от несанкционированного доступа через Интернет. Однако ничто не мешает использовать брандмауэры и для внутреннего употребления, чтобы защитить части сети от неавторизованного доступа из других ее частей. Брандмауэр, по сути, является границей между двумя сетями, которой весь входящий трафик (поток обмена информацией) оценивается на предмет возможности передачи в другую сеть.

Для проверки сетевого трафика и обнаружения потенциальных угроз разработано множество методов.

***Фильтрование пакетов.*** Фильтр принимает пакеты, поступающие в его интерфейсы, анализирует информацию, которую оставили в заголовке пакета различные протоколы, использовавшиеся при его создании, и принимает решение о возможности передачи пакета в другую сеть.

***Аппаратные адреса.*** Передавать данные в другую сеть разрешается только определенным компьютерам. С помощью такого подхода можно, например, ограничить круг компьютеров, допущенных в определенную локальную информационную сеть.

***IP-адреса.*** Передавать данные в другую сеть разрешается только на заданные IP-адреса и/или пришедшие только с заданных IP-адресов.

***Идентификаторы протоколов.*** Через фильтр пропускаются только те пакеты, IP-дейтаграммы в которых созданы заданными протоколами, например TCP.

***Номера портов.*** Брандмауэр пропускает или задерживает пакеты, опираясь на номер целевого порта или порта-источника, указанный в заголовке транспортного уровня.

***Технология трансляции сетевых адресов*** (Network Address Translation, NAT). Она действует на сетевом уровне и защищает компьютеры от вторжения из Интернета, маскируя их IP-адреса. Если сеть подключена к Интернету, но не защищена брандмауэром, каждому компьютеру в ней должен быть назначен зарегистрированный IP-адрес, чтобы компьютер мог обмениваться информацией с другими компьютерами. Зарегистрированный адрес для определения из Интернета "виден", а это значит, что любой пользователь, проявив немного изобретательности, может получить доступ к компьютерам сети и ее ресурсам. Благодаря NAT появляется возможность назначить компьютерам незарегистрированные IP-адреса, после чего доступ к ним из Интернета получить уже не удастся.

***Прокси-сервер*** (proxy server) – это программный продукт, подобный NAT, но действует он на прикладном уровне. Как и NAT-маршрутизатор, прокси-сервер действует как посредник между клиентами частной сети и ресурсами Интернета, к которому они хотят получить доступ. Клиент посылает запрос прокси-серверу, а тот отправляет дубликат запроса целевому серверу Интернета. Сервер Интернета отвечает прокси-серверу, а тот переадресует ответ клиенту. По сути, это означает, что сама сеть из Интернета не видна.

## ПРАКТИЧЕСКАЯ ЧАСТЬ

### Инструкция пользования оболочкой «Имитатор компьютерной сети на основе Windows 2000 Server» и порядок выполнения работы

1. Для эффективной работы с программой необходимо установить разрешение экрана 1024x768.
2. Перед запуском программы каждой из бригад студентов необходимо создать индивидуальный каталог, в который скопировать программные модули лабораторной работы, размещенные в каталоге преподавателя.

3. Открытие оболочки производится запуском на выполнение файла Imitation.exe. В результате выводится окно имитатора управления сетевыми службами. Активация работы оболочки производится кнопкой «Запуск».

4. Оболочка имеет четыре независимых модуля:

- тест,
- администрирование сети,
- рекурсивный запрос,
- удаленный доступ к сети.

1. Программа «Тест» позволяет производить проверку знаний студентов в области администрирования сетей. В окне «Тест» следует отметить правильный ответ на поставленный вопрос. Реакция системы на ответы отображается в нижней части окна. Здесь же подсчитывается общий рейтинг тестирования. Смена вопроса производится нажатием на кнопку «Ответить». Результат тестирования, выводимый после анализа всех ответов на ряд поставленных вопросов, показать преподавателю.

2. Для вызова оболочки имитатора сети необходимо нажать кнопку «Администрирование сети». В результате на экране появится схема, состоящая из двух сетей, содержащих серверы DNS первого, второго и третьего уровней. Сети включают зоны администрирования, управляемые серверами с определенными DNS-именами и соответствующими им IP-адресами. В каждую из сетей включены четыре рабочих станции под управлением сервера третьего уровня. Параметры любого хоста можно посмотреть, наведя курсор на его изображение и кликнув правой кнопкой мыши (ПКМ).

3. Для обеих сетей следует задать DNS-имена и соответствующие им IP-адреса (их значения приведены ниже в скобках). Левая сеть должна содержать хосты, обладающие следующими параметрами:

- edu. (205.0.0.0),

- gb.edu. (205.100.0.0),
- garv.gb.edu. (205.100.15.0),
- elektr.garv.gb.edu. (205.100.15.1),
- progr.garv.gb.edu. (205.100.15.2),
- matem.garv.gb.edu. (205.100.15.3),
- lingv.garv.gb.edu. (205.100.15.4).

**Правая сеть должна включать хосты**

- ru. (192.0.0.0),
- ryazan.ru. (192.186.0.0),
- rgrta.ryazan.ru. (195.186.1.0),
- asu.rgrta.ryazan.ru. (192.186.1.1),
- aitp.rgrta.ryazan.ru. (192.186.1.2),
- aimm.rgrta.ryazan.ru. (192.186.1.3),

- vpm.rgrta.ryazan.ru. (192.186.1.4).

1. Методика изменения DNS-имени компьютера состоит в следующем. Необходимо курсор мыши навести на пиктограмму хоста и щелкнуть ПКМ. В раскрывающемся окне кликнуть на надписи «Свойства» и в поле наименование компьютера (сервера или рабочей станции) ввести его доменное имя. Для рабочих станций необходимо также задать уровень приоритета доступа к серверу и время, в течение которого доступ к серверу разрешен (приоритет доступа следует назначить соответственно номеру подключаемой рабочей станции, а время доступа указать произвольным, по усмотрению студентов). Далее для сохранения изменения параметров необходимо нажать кнопку «Применить». Выход из окна «Свойства станции» производится нажатием на кнопку «Выход».
2. Внесение записей в общую базу данных распределенной системы DNS производится с помощью оболочки управления сервером первого уровня левой сети. Для вызова базы данных необходимо в окне управления сервером кликнуть левой кнопкой мыши (ЛКМ) на надписи «Соединить». В открывающемся окне «Организация соединения» нажать кнопку «Работа с БД». В открывающейся оболочке «База данных сервера» в полях «Доменное имя» и «IP-адрес» ввести соответствующие данные хостов. Нумерация элементов сетей начинается с рабочих станций левой сети и заканчивается рабочими станциями правой сети. Хосты одного уровня обозначаются одинаковыми номерами.

10. В окне редактора записей базы данных необходимо изменить имена и IP-адреса, соответствующие хостам. Любое изменение в базе сохраняется после нажатия (клика ЛКМ) на значке «Ö». Если требуется отменить неправильно введенное изменение, то непосредственно после набора или сохранения данных необходимо нажать значок «х». Выход из оболочки редактора базы данных производится кликом ЛКМ на кнопке «Выход».

11. Для рабочих станций с приоритетами 3 и 4 в поле «Маскирование» следует вместо флага «True» установить флаг «False». Это соответствует тому, что данные об этих компьютерах в файлы зоны, используемые публично, не вносятся. При обзоре структуры сети со стороны сервера высшего приоритета указанные рабочие станции подключенными к сети не отображаются.

12. Следует учитывать, что изменения можно вносить только в базу данных сервера первого уровня левой сети. Они реплицируются в базы данных всех серверов

(изменяются значения их файлов зон) после вызова и закрытия редактора базы данных (без внесения изменений в базу данных) соответствующего сервера.

13. Для реализации процедуры связи между компьютерами необходимо вызвать окно организации соединений, кликнуть ЛКМ на кнопках серого цвета (в результате в это окно перемещается треугольник, закрашенный черным цветом), расположенных напротив доменных имен хостов, с которыми возможно соединение, и нажать кнопку «Соединение». Связь между хостами отображается линиями красного цвета. Отмена соединения производится аналогично, но в этом случае необходимо нажать на кнопку «Отключить». Структура базы данных DNS открытой сети отображается совокупностью баз данных, вызываемых на серверах нажатием в выпадающем меню кнопки «Соединить». Подключение отключенных рабочих станций (формирование закрытой локальной сети), которое невозможно осуществить со стороны сервера, можно выполнить со стороны рабочей станции, кликнув ЛКМ в его окне на надписи «Соединить с сервером». Структура закрытой сети отображается совокупностью подключений рабочих станций к серверу третьего уровня.

14. Осуществить разрешение IP-адресов vpm.rgrta.ryazan.ru. и electr.garv.gb.edu., к которым обращается локальная станция asu.rgrta.ryazan.ru. Весь процесс поиска разрешения IP-адресов запротоколировать в виде файла кэширующего сервера DNS.

15. Рассмотреть процедуры разрешения IP-адресов prog.garv.gb.edu. и lingv.garv.gb.edu. инициированные той же локальной станцией. Результаты разрешений запротоколировать.

16. Ознакомиться с процедурой работы протокола Rlogin и, вызвав программу оболочки «Рекурсивный запрос», правильно отметить последовательность действий, выполняемых в данном связном протоколе. Результаты ответов показать преподавателю. Для указания последовательности обращений к элементам сети в процессе установления соединения необходимо сначала кликнуть на вопросе, а затем на номере ответа. Если ответ дан правильно, то данная кнопка будет подсвечена зеленым цветом, если неправильно – красным цветом.

17. С помощью оболочки «Удаленный доступ к сети» освоить процедуры подключения к локальной и глобальной (через Интернет) сетям с удаленного компьютера, выполняемые мастером сетевого подключения. Для вызова мастера необходимо кликнуть на

пиктограмме «Создание нового подключения». Проанализировать последовательность выполняемых подключений.

## Содержание отчета

Итоговый отчет по лабораторной работе должен содержать:

1) краткие теоретические сведения о службах, используемых в клиент-серверных сетях для разрешения DNS-имени в IP-адрес,

2) графическое изображение администрируемых сетей с указанием параметров каждого хоста, зон DNS и структур файлов каждой из зон,

3) описание последовательности запросов при разрешении IP-адресов,

4) алгоритм работы службы удаленного терминального доступа Rlogin.

## Контрольные вопросы

1. Какую структуру имеют IP-адрес хоста и маска подсети?

2. В какой из записей файла зоны содержится информация о соответствии DNS-имен и IP-адресов?

3. Каким образом реализуется процедура разрешения IP-адреса на основе доменного имени хоста?

4. Каким образом реализуется защита ресурсов элементов сети?

5. По какому принципу строится система доменных имен Интернета?

**Библиографический список**

1. Шапиро Дж., Бойс Дж. Windows 2000 Server. Библия пользователя.: Пер. с англ. М.: Издательский дом «Вильямс», 2002. 912 с.

2. Поляк-Брагинский А.В. Сеть своими руками. 2-е изд., перераб. и доп. СПб.: БХВ-Петербург, 2004. 432 с.

# Лабораторная работа  4

**Администрирование служб DHCP и DNS**

ЦЕЛЬ РАБОТЫ

Изучение методов администрирования служб DHCP и DNS сетевой операционной системы Windows 2000 Server. Приобретение навыков работы с оболочками указанных служб.

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

## Служба DHCP

Протокол DHCP обеспечивает динамическое назначение IP-адресов из доступного набора и отбор не дублирующихся адресов. Это гарантирует, что IP-адреса в сети не будут дублироваться, а также позволяет администратору перемещать компьютеры из одной подсети в другую, не заботясь об их перенастройке.

В стандарте DHCP определены три способа назначения IP-адреса.

- ***Назначение вручную*** – администратор сам назначает компьютеру конкретный IP-адрес в настройках DHCP-сервера, а сервер по запросу выдает этот адрес компьютеру.

- ***Автоматическое назначение*** – DHCP-сервер назначает клиенту постоянный IP-адрес, выбирая его из базы доступных адресов.

- ***Динамическое назначение*** – DHCP-сервер выделяет временные IP-адреса из базы доступных адресов на правах аренды. Клиент должен периодически обновлять аренду, иначе адрес возвращается в базу и становится доступным для следующего назначения.

Ручной способ назначения адресов необходим для настройки систем, которым присваиваются постоянные IP-адреса, например, различного рода серверам. Автоматическим назначением удобно пользоваться в сетях, в которых компьютеры редко перемещаются из одной подсети в другую. Назначение IP-адресов из пула (контейнера) или диапазона (scope) доступных адресов избавляет администратора от необходимости придумывать их и следить за их уникальностью.

При использовании динамического назначения конфигурация клиентов TCP/IP происходит автоматически. Администратор может добавлять компьютеры в сеть, удалять или перемещать их. При запуске компьютера сервер на определенное время выдает ему адрес, а по окончании этого времени обновляет аренду, если компьютер активен, или отбирает адрес и возвращает его в пул, если адрес не используется. Причем возвращенный в пул адрес размещается в конце пула и может быть назначен вновь только после того, как были выданы все IP-адреса, предшествующие ему.

### *Создание области действия DHCP*

Понятие области действия тесным образом связано с понятием физической подсети. Создавая область действия, администратор предписывает серверу использовать некоторый пул адресов для обслуживания клиентов, принадлежащих данной физической подсети. Область DHCP обладает свойствами, определяющими срок аренды принадлежащих ей адресов, а также конфигурации параметров IP, передаваемых клиентами.

Прежде чем приступить к созданию области, необходимо определить следующие параметры:

1) начальный и конечный адреса используемого диапазона IP-адресов;

2) маску, используемую в подсети, для которой назначается область;

3) клиентов, имеющих статические IP-адреса в выбранным диапазоне;

4) срок аренды IP-адресов;

5) дополнительную конфигурационную информацию IP, которую следует передавать клиентам помимо IP-адреса и маски подсети.

### *Настройка конфигурационных параметров службы DHCP*

Значения параметров конфигурации IP могут быть настроены на уровне сервера, области, класса или индивидуального клиента.

1. *Уровень сервера*. Параметры, назначенные на уровне сервера, действуют в отношении всех областей, существующих на данном сервере.
2. *Уровень области*. Стандартный уровень, на котором следует настраивать конфигурационные параметры IP. Значения параметров действуют в отношении всех адресов, принадлежащих области.
3. *Уровень класса*. На этом уровне администратор может настроить параметры для клиентов, принадлежащих к различным областям DHCP, но являющихся членами одного класса.
4. *Уровень клиента*. Параметры, настроенные на данном уровне, как правило, комбинируются с *резервациями*. Резервации используются в случае, если требуется, чтобы клиент использовал службу DHCP для обновления своей IP-конфигурации и при этом сохранял неизменным свой IP-адрес.

Если возникает конфликт значений параметров, присвоенных на разных уровнях, в силу вступают значения, настроенные на более низком уровне. Значения параметров IP на уровне клиента отменяют все значения, предлагаемые службой DHCP.

### *Активация и деактивация DHCP*

После того как область создана, её следует активизировать. Только после активации области клиенты DHCP смогут получить адреса, принадлежащие данной области.

В крупной корпоративной сети в целях обеспечения отказоустойчивости может быть установлено несколько серверов DHCP. При этом достаточно часто администратор не имеет возможности проследить за тем, как клиенты получают свои адреса. Возможна ситуация, когда при существовании в сети нескольких серверов DHCP реализуется выделение одинаковых IP-адресов различным хостам, что в итоге приводит к

неправильной конфигурации клиентов. Для того чтобы разрешить эту проблему, любой сервер DHCP должен быть авторизирован. То есть работа службы DHCP может быть разрешена только на компьютерах с определенными администратором IP-адресами. Список IP-адресов компьютеров, на которых может быть выполнена авторизация службы DHCP, создаётся администратором для Windows 2000 с помощью службы каталога Active Directory (глобального каталога, хранящего всю информации о сети).

Удаление (деактивацию) области следует выполнять с особой осторожностью. Если удалить область, то клиенты, пользующиеся IP-адресами, принадлежащими данной области, могут использовать их до тех пор, пока не истечёт полный срок аренды адреса. Клиенты могут использовать полученные ими ранее IP-адреса даже в том случае, если будет создана новая область, включающая эти IP-адреса. Чтобы заставить клиентов получить адреса из новой области, администратор должен в консоли каждого из клиентов отдать команду «освободить старый адрес» и «получить новый адрес».

Задачу можно решить  другим способом. Не следует удалять старую область сразу же после создания новой. Если необходимо, чтобы все клиенты перестали использовать адреса из одной области и начали использовать адреса из другой области, следует создать новую область, активизировать её, а затем деактивировать старую область. По мере того, как клиенты будут пытаться обновить свои IP-адреса, принадлежащие старой области, используя пакеты DHCPREQUEST, сервер будет возвращать сообщения DHCPNACK. При этом клиенты будут вынуждены прекратить использование своих IP-адресов и обратиться к службе DHCP за получением новых.

Если надо лишь временно приостановить выдачу IP-адресов из некоторой области, рекомендуется создать временные диапазоны исключений таким образом, чтобы предотвратить выделение клиентам неарендованных на данный момент адресов.

## Служба DNS

### *Зоны DNS*

В системе DNS используется распределенная модель администрирования. Отдельной административной единицей в составе домена DNS-сервера является зона. *Зона* –

файл, который хранится на DNS-сервере и содержит информацию об именах, принадлежащих домену. Такой файл называют
*файлом зоны*
(zone file). Сервер, на котором хранится главный файл зоны (master zone file), является первичным DNS-сервером домена. Любой сервер, содержащий главный файл зоны или его копию, называется авторитетным для данной зоны.

***Серверы DNS***

Наряду с первичным (primary) DNS-сервером в сети могут функционировать вторичные (secondary) серверы имен зоны. Вторичные серверы содержат копию файла зоны. Изменения можно вносить только в файл зоны, расположенный на первичном сервере имен зоны. Перемещение информации о зоне с одного DNS-сервера на другой называется *трансфертом зоны*. В ходе трансферта зоны один из серверов передает информацию о зоне, а другой принимает ее. Первый сервер называется главным (master), а второй – подчиненным (slave). Главный сервер не всегда является первичным. В некоторых случаях вторичный сервер может запросить информацию не только у главного сервера, но и другого вторичного сервера. Первый из вторичных серверов будет главным secondary master, а второй – вторичным подчиненным secondary slave. Вторичные серверы служат для распределения нагрузки и повышения надежности. Один и тот же сервер DNS может быть одновременно первичным сервером для одной зоны и вторичным для другой или нескольких других зон. С точки зрения клиента первичные и вторичные серверы имен ничем не отличаются, так как и те и другие выполняют одну и ту же функцию разрешения имен. Обслуживать запрос клиента может любой из них.

## Отказоустойчивость и распределение нагрузки

Для создания рабочий среды DNS, в которой функционирует несколько дублирующих друг друга DNS, требуется выполнить две задачи:

1) помимо первичного сервера необходимо создать, по крайней мере, один вторичный сервер DNS;

2) необходимо сообщить клиентам DNS о существовании нескольких дублирующих друг друга DNS-серверов и возможности направления запросов к любому из них.

Основная функция вторичного DNS-сервера – обслуживание клиентов, если первичный DNS-сервер вышел из строя, находится слишком далеко или перегружен. Вторичный DNS-сервер также становится бесценным источником информации, если файлы зоны, расположенные на первичном сервере, утеряны или повреждены и не поддаются восстановлению. В подобной ситуации можно просто скопировать файл зоны с вторичного сервера на первичный. Если важные записи в ресурсах были удалены и файл зоны резервного сервера изменялся относительно недавно, необходимо остановить работу службы DNS на вторичном сервере для того, чтобы предотвратить трансферт зоны. Затем его необходимо восстановить на первичный сервер, используя не модифицированный файл зоны вторичного сервера.

ПРАКТИЧЕСКАЯ ЧАСТЬ

---

**Руководство для работы с обучающей программой**

Обучающая программа условно разделена на две части. Одна из частей позволяет пользователю осуществить установку и настройку службы каталогов Active Directory, другая – настройку службы DHCP.

Запуск программы осуществляется с помощью файла NetAdmin.exe. После запуска файла откроется окно «Сетевое администрирование».

***Настройка Active Directory***

Программа настройки Active Directory предполагает выполнение пользователем задачи, состоящей из нескольких шагов (последовательность выполнения шагов описана в инструкции далее). Пользователю необходимо сделать компьютер, применяемый в работе, первым контроллером домена дерева Active Directory. В ходе установки будет настроена и сконфигурирована служба DNS (Domain Name Service), позволяющая реализовать процедуру разрешения имен. Необходимо осуществить следующие шаги.

1. Войдите в закладку **Сервис** окна «Сетевое администрирование» и выберите пункт **Эм улятор настройки Active Directory**
. На экране после выполнения имитации процесса загрузки компьютера появится рабочий стол виртуального сервера с окном регистрации. В окне регистрации на сервере необходимо зарегистрироваться под именем
**Admin**
с паролем
**password**
.

2. Кликните ЛКМ на кнопке **Пуск** рабочего окна и в выпадающем меню выберите пункт **К омандная строка.**
В появившемся окне введите имя файла
**dcpromo.exe**
и запустите его, нажав на кнопке
**Enter**
на клавиатуре. Данный файл является программой, запускающей мастер установки Active Directory. Откроется окно
«
Мастер установки «Active Directory
»
.
Щелкните ЛКМ на кнопке
**Next**
.

3. В открывшемся окне «Тип контроллера домена» после изучения служебной информации выберите пункт **Контрол лер домена в новом домене**
и щелкните
**Next**
. В результате откроется окно
«
Создания дерева или дочернего домена
»
. Для изменения зафиксированных параметров можно осуществлять возврат в предыдущие окна установки с помощью клавиши
**Back**
.

4. Ознакомьтесь с информацией, содержащейся в окне «Создание дерева или дочернего домена » и убедитесь, что выбран переключатель **Создать новое доменное дерево**. Щелкните на кнопке **Next**. Откроется окно «Создание леса или присоединение к лесу». В данном окне активна опция **Создать новый лес доменных деревьев**. После щелчка на кнопке **Next** откроется окно «Имя DNS–домена».

5. В окне «Имя DNS–домена» в поле **Полное DNS-имя нового домена** введите полное имя домена с расширением com, например **corp.com.** Щелкните **Next**.

6. Следующее открывающееся окно имеет имя «NetBIOS-имя домена». Данное окно позволяет задать имя домена для работы с компьютерами, оснащенным операционными системами ранних модификаций Windows. В нем в поле **NetBIOS-имя домена** следует указать имя, например CORP, и щелкнуть **Next**.

7. В результате откроется окно «Местоположение базы данных и журнала». Для указания пути размещения базы данных и журнала в окнах ввода введите путь c:WinntNtds и щелкните на кнопке

**Next**
. Введение пути можно также осуществить путем использования кнопки
**Обзор**
каждого из полей ввода.

8. В появившемся окне «Общий доступ к системному тому» изучите информацию и выберите для размещения папки Sysvol путь c:WinntSysvol и щелкните кнопку
**Next**
. После нажатия кнопки
**Next**
на экране появится сообщение о том, что мастер не может связаться с DNS-сервером, обрабатывающим имя corp.com.
Для закрытия сообщения щелкните
**OK**
.

9. Поскольку мастер установки не нашел пути к DNS-серверу, откроется окно «Настройк а DNS ».
Далее пользователю будут предложены два пути установки: установка автоматическая и установка вручную. Для осуществления автоматической установки следует выбрать пункт
**Автоматически установить и настроить DNS**
и тем самым отказаться от обучающего этапа настройки DNS. Выбрав пункт
**Настроить и установить DNS вручную,**
пользователь получит возможность лично произвести настройку DNS на одном из следующих шагов прохождения обучающей программы. Второй путь является более предпочтительным, так как дает более детальное представление о настройках сетевых компонентов операционной системы.

10. Выберите пункт **Автоматически установить и настроить DNS** и щелкните **Next**. Откроется окно
«
Разрешения
»
. Первоначально контроллер домена запустится в
***смешанном режиме***
, который позволяет ему взаимодействовать с любыми контроллерами доменов под управлением Windows NT 3.51 или 4.0. Кроме того, смешанный режим нужен для входа в сеть любому клиенту, использующему аутентификацию NTML и службу каталога Windows NT 3.51 или Windows NT 4.0.

***Основной режим***
можно устанавливать в случае, когда на всех контроллерах домена установлена операционная система (ОС) Windows 2000 Server и не планируется добавление в домен контроллеров с ОС ранних версий Windows (контроллеров нижнего уровня). При изменении режима со смешанного на основной происходит следующее:

- прекращается поддержка репликации нижнего уровня, после чего в этом домене больше нельзя будет иметь контроллеры, управляемые предыдущими версиями Windows;

- запрещается добавление в данный домен новых контроллеров нижнего уровня;
- сервер, исполнявший роль основного контроллера домена, перестает быть основным; все контроллеры становятся равноправными.

Изменения режима домена носят однонаправленный характер (невозможно перейти из основного режима в смешанный).

11. Выполняемая работа предполагает использование смешанного режима, поэтому убедитесь в том, что выбран переключатель **Разрешения, совместимые с серверами пред-Windows 2000** и щелкните на кнопке **Next**. Откроется окно «Пароль администратора для режима восстановления». Изучите информацию, размещенную в этом окне, а затем наберите password в обоих полях и щелкните **Next**. В результате на экране появится окно «Сводка». Данное окно является *листингом* проделанной работы и позволяет пользователю просмотреть установленные им параметры. В окне «Сводка» указывается имя нового домена, имя нового леса доменов, имя NetBIOS-домена, размещение базы данных, размещение файла журнала, размещение папки Sysvol, выбранный режим работы. Изучив содержание окна

«
Сводка
»,
пользователь может перейти к следующему этапу установки, нажав
**Next**
, или, нажав
**Back**
,
вернуться на предыдущие шаги и изменить параметры установки.

12. После клика на кнопке **Next** подготавливается запуск процедуры настройки каталога **Active Directory**. Старт процедуры производится кликом на кнопке
**OK**
. Далее осуществляется имитация процесса перезагрузки компьютера. Для продолжения работы следует ввести в окне приглашения имя регистрации
**admin**
, пароль
**password**
и кликнуть на кнопке
**OK**
.

13. В эмуляторе настройки **Active Directory** щелкните на пиктограмме рабочего стола **Сетевое окружение**
и правой кнопкой мыши активизируйте меню, в котором выберите опцию
**Открыть**
. Далее кнопкой
**Отобразить**
высветите структуру дерева сети. Уясните место нахождения домена CORP в структуре сети. Кликом на кнопке «х» закройте окно «Сеть». Также кликом на кнопке «х» закройте окно «Эмулятор настройки Active Directory». В появляющейся вкладке «Сетевое администрирование» выберите опцию несохранения параметров настройки. В результате производится переход к отображению окна «Сетевое администрирование».

14. Повторите операции, выполняемые в п.п. 1-9, после чего в окне «Настройка DNS» выберите пункт **Настроить и установить DNS вручную** и кликните на кнопке **Next**. Далее, осуществляя последовательное нажатие кнопки
**Next**
и выполнив подтверждение пароля, перейдите в окно

«
Сводка». После того как установленные параметры, перечисленные в окне
«
Сводка», будут подтверждены нажатем кнопки
**Next**
, на экране появится вкладка запуска установки конфигурации
**Active Directory**
. На закладке «Сетевое администрирование» нажмите кнопку
**OK**
, после чего будет произведена виртуальная перезагрузка компьютера, и на экране снова появится окно регистрации пользователя.

15. Зарегистрируйтесь под именем **Admin** с паролем **password** и нажмите **OK**. Так как был выбран режим
**Настройка DNS в ручную**
, на экране появится информационное сообщение о предоставлении возможности настройки DNS в ручную. Нажмите
**OK**
. В результате появится окно диспетчера службы доменных имен DNS. Первоначально в дереве находится только сервер DNS. Чтобы добавить в сеть новый сервер, на котором будет запущена служба DNS, необходимо щелкнуть ПКМ по значку
**DNS**
и выбрать пункт
**Добавить сервер**
. В появившемся окне с помощью клавиши
**Обзор**
необходимо выбрать для добавления в сеть один из двух предлагаемых серверов (
**Admin**
или
**UserMashin**
). В сеть можно добавить оба сервера. Далее щелкните ПКМ по вновь созданному серверу и выберите пункт
**Свойства**
. Появится окно
**Пересылка данных**
, которое позволит настроить поиск IP-адресов с помощью сервера DNS. Введите для указанных серверов IP-адреса 192.168.1.1 и 192.168.2.1 соответственно и нажмите
**OK**
. В результате дерево сети пополнится зоной DNS домена, включающей ссылки на зарезервированные IP-адреса серверов DNS-субдоменов и реверсивные зоны поиска. Реверсивная зона поиска необходима для разрешения обратных запросов (DNS-имени по его IP-адресу) лишь в случаях, когда приложения для обеспечения повышенной безопасности проверяют, на каких компьютерах они запускаются. Закрытие окна настройки DNS осуществляется обычным способом оконного интерфейса.

16. Зайдите в меню **Пуск** и выберите пункт **Отчет о проделанной работе**. В случае успешного прохождения всех шагов лабораторного задания на экран будет выведено сообщение: ***«Задание 1 успешно выполнено»***
. В противном случае появится сообщение:
***«Задание 1 не выполнено»***
. Закрытие сообщения производится нажатием на кнопку
**OK**
. Для просмотра созданного домена дважды щелкните по иконке
«
Сетевое окружение
»
и с помощью клавиши
**Отобразить**
просмотрите структуру созданной сети с входящим в нее доменом.

Выход из подпрограммы настройки **Active Directory** осуществляется через меню **Пуск** кликом на надписи
**Выключить компьютер**
. Программа предложит сохранить параметры настройки. Подтвердите решение сохранить настройки нажатием на клавишу
**Да**
.

***Настройка службы DHCP***

Второй режим работы программы предназначен для обучения пользователя настройке службы DHCP. В процессе выполнения настройки службы DHCP необходимо выполнить следующие действия.

1. В окне «Сетевое администрирование» необходимо открыть закладку **Регистрация** и выбрать пункт
**Настроить DHCP**
. В открывшемся окне диспетчера службы динамического назначения IP-адресов хостов в зоне структуры сетевого дерева щелкните ПКМ по значку DHCP и в выпадающем меню выберите пункт
**Добавить сервер**

.

2. В окне **AddForm** активизируйте опцию **Этот сервер** и с помощью клавиши **Обзор** выполните просмотр доступных серверов DHCP (Admin и UserMachin) и включите их в состав сети. Для включения новых серверов в сеть необходимо последовательно кликнуть на кнопках
**OK**
в закладках
**Выбрать компьютер**
и
**AddForm**
. Для каждого из серверов указанную последовательность действий следует выполнять отдельно. В установленных серверах работа службы DHCP запрещена, о чем свидетельствует статус режима работы службы
**Остановлен**
.

3. Запуск работы службы DHCP на серверах производится ее активизацией. Для активизации службы необходимо щелкнуть ПКМ по значку **DHCP** и в выпадающем меню выбрать пункт
**Управлять авторизованными серверами**
. Выбор авторизуемого сервера производится из списка, отображаемого после нажатия кнопки
**Авторизовать**
. Включенные в листинг серверы можно авторизовать нажатием на кнопку
**OK**
в окне «Управление авторизованными серверами». Статус авторизованных серверов DHCP в окне «DHCP» изменяется на
**Работает**
и сигнализация состояния сервера меняет цвет с красного на зеленый.Отмена авторизации производится также в этом окне путем выделения имени деавторизуемого сервера и нажатия последовательно на кнопки
**Деавторизовать**
и
**OK**
.

4. Для авторизованных серверов необходимо задать новые области действия. Для этого в поле **Дерево** щелкните ПКМ по значку авторизованного сервера и выберите пункт **Новая область действия**. Появится окно «Мастер новой области действия». В этом окне необходимо указать имя области действия, задать диапазон IP-адресов зоны, маску подсети. При подведении курсора к любому из полей ввода в нижней части экрана отображается подсказка по правилам его заполнения. Можно исключить определенный набор IP-адресов из пула динамически назначаемых адресов (создать резервацию). В окне мастера настройки области действия предусмотрена возможность задания длительности аренды IP-адресов. В

области **Имя домена и DNS-серверы** указать имя домена, созданного на стадии настройки Active Directory, и имя DNS-сервера, выбранного при настройке DNS. IP-адреса DNS-сервера и WINS-сервера, выбранные из диапазона резерваций, должны соответствовать администрируемой зоне. После заполнения параметров серверов следует разрешить их работу, кликнув на кнопке **Разрешить**. Важно указать как минимум один IP-адрес маршрутизатора, в противном случае процедура пересылки пакетов информации будет запрещена. Параметры настройки окна «Мастер новой области действия» для каждого из вариантов заданий указаны в таблице, представленной в конце раздела «Настройка службы DHCP». По окончании установки всех параметров нажмите **OK**.

5. В окне DHCP, перемещаясь по структуре дерева заданной области действия, можно просматривать установленные параметры. Далее следует закрыть окно настройки DHCP и перейти на главное окно программы.

6. Пользователю предоставляется возможность арендовать IP-адреса. Для этого необходимо войти в закладку «Регистрация» и выбрать пункт «Получить IP-адрес». Откроется окно со списком пула IP-адресов. Для аренды необходимо выделить сервер, указать имя клиента и нажать **OK**. Перечень клиентов, арендовавших IP-адреса, можно просмотреть с помощью окна «Параметры хоста», выход в которое осуществляется через закладку «Обозреватель». Освободить зарезервированные адреса можно с помощью пункта «Освободить IP-адрес» в закладке «Регистрация».

7. Пользователь может осуществить виртуальную передачу пакета в сети. Для этого необходимо выбрать в закладке «Регистрация» пункт «Отправить пакет». Источником пересылки пакета будет служить один из клиентов, зарезервировавших IP-адрес, а получателем пакета - виртуальная локальная машина. Пересылка пакета будет недоступна, если ранее в параметрах области действия не был задан IP-адрес маршрутизатора. В открывающемся окне «Отправить пакет» следует выделить название компьютера, используемого в качестве источника информации, и нажать кнопку **OK**. Если имитация пересылки пакета выполняется, то выводится сообщение - **Пакет отправлен**.

8. Состояние службы каталогов **Active Directory** можно просмотреть в закладке «Обозреватель». В этой же закладке находится **Журнал событий**, в котором фиксируются действия пользователя в процессе настройки Active Directory, DNS, DHCP.

Выход из обучающей программы осуществляется с помощью пункта **Выход** закладки «Регистрация».