Глава 2

2 Базовые концепции сетевых технологий

Базовые концепции? Но ведь в главе 1 отмечалось, что в данной книге не рассматриваются все вопросы сетевого администрирования, поскольку основное внимание уделяет диагностике работы сети и решению возникающих проблем. Однако разобраться с той или иной проблемой невозможно без знания базовых концепций. Читатели, хорошо знакомые с основными характеристиками технологий TCP/IP, DNS, DHCP и WINS, могут переходить к главе 3; всем остальным рекомендуется потратить некоторое время и повторно ознакомиться с фундаментальными сетевыми концепциями.

Эта глава посвящена рассмотрению центральных компонентов сетей Microsoft на базе стека протоколов TCP/IP и некоторых других, все еще встречающихся в современных сетях. Поскольку многие сетевые инфраструктуры основаны на различных протоколах, начнем их рассмотрение с самых распространенных протоколов в гетерогенных сетях Microsoft.

Сетевые протоколы

Недостаток знаний о популярных сетевых протоколах очень легко может превратить простую проблему в сложную. В этом разделе кратко рассматриваются сетевые протоколы, используемые в сетях на базе систем компании Microsoft. Перед описанием сетевых протоколов посмотрим, где можно найти необходимую информацию.

Для получения доступа к параметрам сетевой конфигурации в Windows Server 2003 выполните приведенную ниже последовательность действий.

1. Выберите команду Пуск⇨Панель управления⇨Сетевые соединения (Start⇨Control Panel⇨Network Connections).
2. Щелкните правой кнопкой мыши на пиктограмме сетевого интерфейса, который необходимо настроить, и выберите опцию Свойства (Properties). Как

показано на рис. 2.1, будет отображен список установленных сетевых служб и список протоколов.

3. Щелкните на кнопке Установить (Install) для установки дополнительных служб и протоколов.

Разумеется, желательно, чтобы в сетях использовался только протокол TCP/IP, однако одного желания слишком мало. Далее в этом разделе представлена базовая информация о следующих протоколах:

- NetBEUI;
- NWLink (IPX/SPX);
- TCP/IP.

Протокол NetBEUI

Этот протокол широко использовался на компьютерах под управлением операционных систем Windows 95/98, подключенных к небольшим локальным сетям для малых или домашних офисов. Применение протокола NetBEUI (NetBIOS Enhanced User Interface) заключается в настройке сетевого адаптера и подключении компьютера к сети. Таким образом, протокол был идеальным вариантом для обеспечения взаимодействия компьютеров в рабочей группе небольшого офиса. Однако NetBEUI не поддерживает маршрутизацию данных; в этом основной недостаток данного протокола, ограничивающий его применение до одной подсети. С выпуском операционных систем Windows XP и Windows Server 2003 компания Microsoft отказалась от поддержки NetBEUI, следовательно, при доступе к ресурсам сервера под управлением Microsoft Windows использовать данный протокол нельзя.

Протокол NWLink (IPX/SPX)

Это реализация протокола Novell IPX/SPX (Internet Packet Exchange/ Sequenced Packed Exchange) компании Microsoft. Хотя операционная система NetWare 5.0 и более поздние ее версии теоретически используют исключительно протокол TCP/IP, службы MCSN (Microsoft Client Services for NetWare) и GSNW (Gateway Services for NetWare) для своей работы требуют поддержки протокола NWLink IPX/SPX.

В контексте решения возникающих проблем необходимо представлять базовые характеристики протокола IPX/SPX и понимать значение следующих терминов:

- тип кадра;
- номер внутренней сети;
- номер внешней сети.

Доступ к этим параметрам сервера Windows можно получить с помощью окна свойств протокола NWLink (рис. 2.2).

Рис. 2.1. Просмотр установленных параметров сети

Рис. 2.2. Параметры конфигурации NWLink для операционной системы Windows Server 2003

Тип кадра

Тип кадра в сетях IPX указывает методы инкапсуляции данных в пакетах протокола IPX. Вот основные типы кадров:

- Ethernet II;
- 802.3;
- 803.2;
- SNAP;
- Arcnet.

Когда протокол NWLink настраивается в операционной системе Windows, тип кадра в сети IPX определяется автоматически. Система при этом использует тип первого полученного кадра. С автоматическим определением связана проблема, при которой система под управлением Windows может взаимодействовать только с сетью с одним типом кадра, но не с сетью, где применяется два типа кадра. Например, если компьютеры под управлением операционных систем NetWare 3.11 (тип кадра 802.3) и NetWare 5.0 (тип кадра 802.2) находятся в одной физической подсети с компьютером под управлением Windows, в которой настроен протокол NWLink, то Windows по умолчанию сможет взаимодействовать только с NetWare 3.11 или NetWare 5, поскольку пакеты IPX этих систем используют различные типы кадров. При автоматическом определении первый же тип кадра, обнаруженный в сети, будет использоваться операционной системой Windows. В связи с этим нельзя делать предположения об использовании самой последней версии типа кадра (в данном случае это 802.2). Придется вручную уста-

навливать тип кадра, который будет использоваться в каждой системе Windows с установленным протоколом NWLink.

Кроме проблем, связанных с некорректным определением типа кадра, существуют вопросы использования номеров сетей IPX, рассматриваемые далее.

Замечание

Процедура ручной настройки типов кадров NWLink для клиентов и серверов Windows описывается в главе 11, "Сетевые и прикладные службы".

Номер внутренней сети

Номера внутренних сетей являются уникальными идентификаторами, которые назначаются всем серверам NetWare и требуются серверам Windows в следующих ситуациях:

- в сервере под управлением Windows установлено два или больше сетевых адаптера (NIC);
- в сервере под управлением Windows установлен один сетевой адаптер, для которого настроено два разных типа кадра IPX;
- планируется использование служб файлов и печати для NetWare (File and Print Services for NetWare) на сервере Windows;
- на компьютере под управлением Windows установлено приложение, использующее протокол IPX.

Номер внутренней сети состоит из восьми шестнадцатеричных символов и может принимать значения в диапазоне от **00000001** до **FFFFFFFE**.

Номер внешней сети

В то время как номера внутренней сети используются для нумерации и идентификации каждого сервера Windows в определенном сетевом сегменте, номера внешних сетей применяются в качестве уникального логического идентификатора для целых логических сегментов сети. В контексте стека протоколов TCP/IP (рассматривается ниже) номер внешней сети соответствует идентификатору сети, а номер внутренней сети — идентификатору узла.

Базовые характеристики TCP/IP

В следующих главах этой книги представлено немало информации относительно стека протоколов TCP/IP, посвященной решению разнообразных проблем, связанных с TCP/IP. На данном этапе рассматриваются только базовые сведения о протоколе TCP/IP.

Начиная с операционной системы Windows 2000, протокол TCP/IP (Transmission Control Protocol/Internet Protocol) принят в Windows в качестве основного сетевого протокола. В этом разделе описываются основные концепции TCP/IP, а в после-

дующих разделах рассматриваются остальные компоненты сетевой инфраструктуры TCP/IP, а именно:

- служба DNS;
- служба DHCP;
- служба WINS.

Начнем рассмотрение протокола TCP/IP со структуры адреса. IP-адрес состоит из четырех фрагментов, которые называются *октетами*, поскольку каждый фрагмент состоит из 8 бит данных. Следовательно, весь IP-адрес имеет длину 32 бит. Вот пример IP-адреса: 10.8.32.6. Этот адрес состоит из четырех десятичных чисел, разделенных точками. Каждое число представляет один из октетов. Поскольку длина октет содержит 8 бит, каждый октет может принимать значения в диапазоне от **0** до **255** (**11111111**). Адрес 10.8.32.6, выраженный в десятичной форме, на самом деле представляет собой последовательность двоичных символов 00001010.00001000.00100000.00000110. Как можно осуществить такой переход? Рассмотрим метод двоичного преобразования.

Двоичное преобразование

В двоичной системе счисления используется только две цифры: **0** и **1**. Поскольку это система счисления с основанием 2, каждая позиция в двоичной последовательности представляет степень двойки. Сравним это со стандартной десятичной системой счисления, которая используется каждый день. Возьмем, например, число 201. При рассмотрении этого трехзначного числа можно заметить, что в нем присутствует разряд единиц, разряд десятков и разряд сотен. Поэтому число 201 равно 1×1+0×10+2×100. Цифра в каждом разряде умножается на степень 10 с показателем, соответствующим положению разряда. Поскольку двоичная система счисления имеет основание 2, цифра каждого разряда умножается на степень двойки, соответствующую положению разряда. Для преобразования десятичных чисел в двоичное представление, можно просто начать с единицы и продолжать удваивать числа, пока не будет достигнуто значение **128**. После этого необходимо использовать последовательность нумерации из табл. 2.1 (в этой таблице IP-адрес 10.8.32.6 преобразуется в двоичную форму).

Таблица 2.1. Таблица преобразования десятичных чисел в двоичные

Столбцы двоичных разрядов (с основанием 2)								
Десятичное число	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
10	0	0	0	0	1	0	1	0
8	0	0	0	0	1	0	0	0
32	0	0	1	0	0	0	0	0
6	0	0	0	0	0	1	1	0

Далее представлен алгоритм преобразования десятичного числа в двоичное.

1. Найдите наибольшее число в табл. 2.1, которое меньше или равно преобразуемому числу (128, 64, 32 и т.д.), и укажите в его столбце значение 1.

2. Вычтите из числа, преобразование которого выполняется, число из выбранной колонки.
3. Найдите наибольшее число в таблице преобразования, которое меньше или равно числу, оставшемуся после первого шага, и поместите значение 1 в столбец этого числа.
4. Вычтите из числа, полученного при выполнении п. 2, число из выбранного столбца.
5. Повторяйте пп. 3 и 4, пока разность не станет равна 0; после этого поместите 0 во все столбцы, которые не содержат 1. Вот это и будет двоичное число.

Для преобразования числа 10 необходимо найти в табл. 2.1 самое большое число, не превышающее 10. Это будет 8, поэтому в столбец числа 8 необходимо поместить 1. Теперь необходимо из 10 вычесть 8. В результате получится число 2. В столбце, соответствующем числу 2, необходимо разместить 1. Результатом последней операции будет 2, поэтому для завершения преобразования во все остальные столбцы необходимо поместить 0.

Использовать эту таблицу для преобразования двоичного числа в десятичное еще проще, чем для преобразования десятичного числа в двоичное. Просто запишите 8-разрядное число в таблице, указывая каждый разряд в одном столбце. После этого сложите значения столбцов таблицы, которые содержат 1. Например, двоичное число 10100001 будет равно 128+32+1, т.е. 161.

В главе 4 рассматривается бесплатная утилита (она находится на прилагаемом к книге компакт-диске), которая используется для преобразования IP-адресов в различные числовые представления. Поэтому не будем тратить время на двоичную арифметику, а сразу перейдем к структуре адреса TCP/IP.

Структура адреса TCP/IP

IP-адрес делится на две логические части:

- *идентификатор узла*, который указывает на отдельную систему в сети;
- *идентификатор сети*, указывающий на сегмент сети, в котором расположено несколько систем.

Для извлечения из IP-адреса информации об идентификаторе узла и идентификаторе сети используется *маска подсети* (*subnet mask*). Как и IP-адрес, она состоит из 32 разрядов, разделенных на четыре октета. Маска подсети отличается от IP-адреса тем, что всегда содержит непрерывную последовательность единиц (1). Например, первый октет маски подсети может выглядеть как 11110000, но не как 11100110.

Чтобы продемонстрировать, как посредством маски подсети определяются идентификаторы сети и узла, предположим, что использованный ранее IP-адрес (10.8.32.6) имеет маску подсети 255.0.0.0. Преобразование каждого октета в двоичную форму позволяет разобраться, как маска подсети определяет границу между идентификатором узла и идентификатором сети (рис. 2.3).

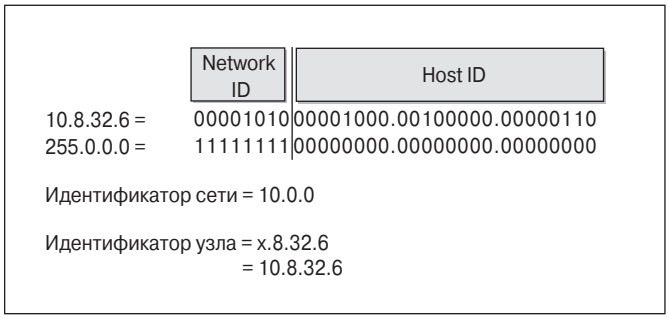

Рис. 2.3. Маска подсети разделяет IP-адрес на идентификаторы сети и узла

На рис. 2.3 единичные разряды маски подсети занимают весь первый октет. Это означает, что весь первый октет IP-адреса представляет собой идентификатор сети, а оставшаяся часть IP-адреса — идентификатор узла. Когда подсети разделены на уровне октетов, это деление называется *адресацией по классам*. Классы IP-адресов обозначаются буквами, представленными в табл. 2.2.

Таблица 2.2. Классы сетей IP-адресов: A, B и C

Класс	Число в первом октете	Маска подсети	Количество сетей	Количество узлов в сети
A	1–126	255.0.0.0 или /8	126	16 777 214
B	128–191	255.255.0.0 или /16	16 384	65 536
C	192–233	255.255.255.0 или /24	2 097 152	254

Несложно заметить, что при увеличении значения маски подсети уменьшается максимальное количество компьютеров в подсети; при этом увеличивается количество возможных подсетей. Обратите внимание на другое обозначение в столбце маски подсети. Поскольку маска подсети всегда состоит из непрерывной последовательности 1, ее можно указать в виде /8. Это означает, что маска подсети состоит из восьми единиц. Такое обозначение будет эквивалентом 255.0.0.0. Если в качестве IP-адреса предлагается запись 139.42.4.25/16, это означает, что маска подсети адреса имеет вид 255.255.0.0.

Некоторые IP-адреса нельзя маршрутизировать с помощью Internet-маршрутизаторов. Эти адреса применяются исключительно в частных сетях. Для внутренней сети организации можно использовать любой из приведенных диапазонов IP-адресов:

- 10.0.0.0–10.255.255.255;
- 169.254.0.0–169.254.255.255;
- 172.16.0.0–172.31.255.255;
- 192.168.0.0–192.168.255.255.

Не забывайте, что эти адреса не подлежат маршрутизации и доступ к ним из Internet невозможен.

Теперь перейдем к решению проблем, возникающих при использовании протокола TCP/IP. Взаимодействие компьютеров в одной физической подсети требует наличия одинакового идентификатора сети. Когда один компьютер не в состоянии связаться с остальными, возможно, был неправильно введен его IP-адрес или была настроена неправильная маска подсети.

Замечание

Системы в различных логических подсетях не могут связываться друг с другом без использования маршрутизатора.

Если одна система имеет IP-адрес 10.0.14.20, а вторая — 11.0.18.6, при этом для каждого компьютера настроена маска подсети 255.0.0.0, то системы не смогут связаться друг с другом. Дело в том, что одна система находится в подсети 10.0.0.0, а вторая — в подсети 11.0.0.0.

При несовпадении идентификаторов сети и масок подсети компьютеры в одной физической подсети не смогут взаимодействовать друг с другом посредством протокола TCP/IP. Имея некоторый опыт работы с сетями TCP/IP, можно, мельком взглянув на два адреса TCP/IP, определить их принадлежность к одной логической подсети. При использовании масок подсети, соответствующих определенным классам (/8, /16, /24), идентификатор сети выделить несложно, однако ситуация кардинально меняется, когда задействована маска подсети, не соответствующая классу, например /19. Приведение адреса в двоичную форму и сравнение его с другим адресом для определения идентификатора сети остается единственным методом определения принадлежности IP-адресов к одной логической подсети. К счастью, существуют инструменты, которые помогут выполнить эту работу за человека. Для тех, кто еще не стал волшебником в мире подсетей, определение идентификатора подсети при использовании бесклассовой маски подсети может занять от 30 минут до часа. Сократить мучительный процесс ручного подсчета поможет программа Wildpacket IP Subnet Calculator (она находится на прилагаемом к книге компакт-диске), методы использования которой для решения различных проблем с IP-подсетями представлены в главе 4.

Замечание

На Web-узле по адресу `www.learntosubnet.com` расположено отличное интерактивное обучающее пособие по IP-подсетям.

Протокол TCP/IP в маршрутизируемой среде

Для большинства сетей масштаба предприятия или даже малых домашних/офисных сетей с подключением к Internet необходимо знать основы маршрутизации протокола TCP/IP. На рис. 2.4 показан небольшой офис, в котором для подключения к Internet применяется маршрутизатор.

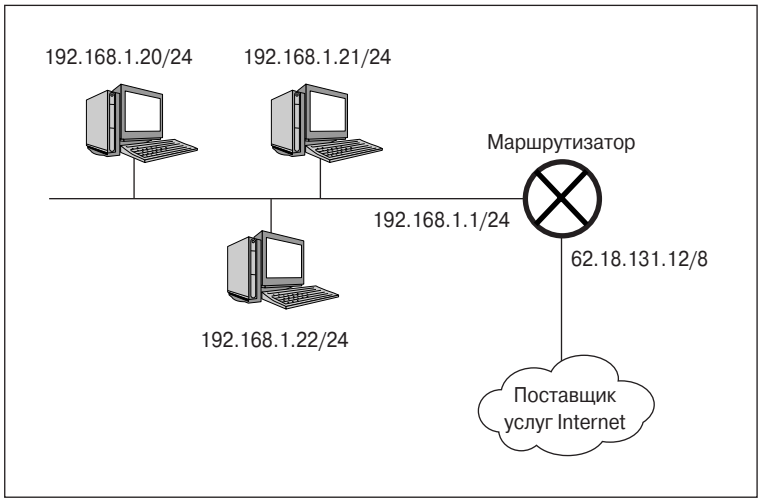

Рис. 2.4. Маршрутизатор, соединяющий небольшой офис с Internet

Каждый сетевой интерфейс маршрутизатора, который подключен к сети, имеет собственный IP-адрес и маску подсети. Маршрутизатор необходим для прямой или маршрутизируемой передачи IP-пакетов в удаленную сеть. Он имеет собственную таблицу маршрутизации для определения маршрута отправки каждого пакета данных. В качестве критерия при выборе маршрута используется IP-адрес назначения пакета. Таблица маршрутизации — это таблица перекрестных ссылок, которая содержит информацию о том, как достичь той или иной IP-сети.

Подробная информация по диагностике и решению проблем, связанных с маршрутизаторами, рассматривается в главе 12, а на данном этапе наиболее важной является концепция *основного шлюза* (*default gateway*). Как уже отмечалось, компьютеры с одинаковыми идентификаторами подсети и маской подсети могут связываться друг с другом. А как же компьютер связывается с компьютерами из другой подсети? Именно в этом случае необходим основной шлюз. Для того чтобы компьютеры могли отправлять данные за пределы локальной сети, им требуется адрес основного (базового) шлюза. Для любого компьютера базовый шлюз используется как место назначения пакетов, которые имеют идентификатор сети, отличающийся от идентификатора локальной подсети. Базовый шлюз отвечает на вопрос: если не известно, куда отправлять пакет, то что же с ним делать?

На рис. 2.4 адресом шлюза, принятого по умолчанию для офисных компьютеров, является значение 192.168.1.1. Обратите внимание на то, что маршрутизатор имеет два адреса: один для локальной сети и второй для подключения офисной сети к сети поставщика услуг Internet. Поскольку маршрутизатор служит для передачи пакетов в сеть и из нее, его конфигурация крайне важна для обеспечения нормальной работы сети. Более подробно вопросы маршрутизации рассматриваются в главе 12, “Служба RRAS”.

Имена NetBIOS и FQDN

Еще одним из аспектов TCP/IP являются имена NetBIOS и полностью определенные имена доменов (Fully Qualified Domain Names — FQDN). Пользователям намного удобнее запоминать понятные имена, а не числовые IP-адреса. Имена NetBIOS и FQDN позволяют наделить сетевой объект удобным для запоминания именем, однако основным различием между этими двумя именами является их формат. FQDN обычно имеет вид *<имя компьютера>.<имя домена>.<имя домена высокого уровня>*, например `www.awl.com`, в то время как NetBIOS является буквенным обозначением системы, правда, ограниченным 15 символами. Эквивалентом FQDN `www.awl.com` в системе именования NetBIOS будет `www`.

Теперь представьте, сколько компьютеров с именем `www` подключено в данный момент к сети. Если использовать систему именования NetBIOS в Internet, будет невозможно отличить один компьютер от другого, именно поэтому система именования для распределенной сетевой среды использует FQDN.

Разобравшись с фундаментальными различиями между именованием NetBIOS и FQDN, рассмотрим их конкретные особенности.

Представим правила для имен NetBIOS:

- имена не могут начинаться с цифры;
- максимальная длина имени — 15 символов;
- в именах могут использоваться символы A–Z, a–z, 0–9 и дефисы; имена не чувствительны к регистру;
- допускается наличие пробелов (пробел считается одним из символов).

Правила для FQDN:

- имена могут начинаться с цифры;
- максимальная длина имени — 255 символов (для имен контроллеров доменов —155 символов);
- в именах могут использоваться символы A–Z, a–z, 0–9 и дефисы; имена не чувствительны к регистру;
- *не* допускается наличие пробелов;
- компоненты имени разделяются точками (`www.microsoft.com`).

Методы преобразования имен

В предыдущих разделах описано, как использовать имена NetBIOS и FQDN в качестве удобных для запоминания системных идентификаторов. Существует несколько способов преобразования имени компьютера в его IP-адрес. Далее представлены самые распространенные из них.

- *Служба имен доменов (Domain Name Service — DNS)*. Сервер, преобразующий имена FQDN в IP-адреса и обратно.
- *Служба WINS (Windows Internet Naming Service)*. Сервер, преобразующий имена NetBIOS в IP-адреса.

- *Файл* `Hosts`. Хранится локально на каждом компьютере и обеспечивает соответствие между IP-адресами и FQDN.
- *Файл* `LMHosts`. Хранится локально на каждом компьютере и используется для преобразования IP-адресов в имена NetBIOS.
- *Широковещательный запрос*. Способ, с помощью которого компьютер может "крикнуть" в сеть: "Эй, кто-нибудь знает, как найти компьютер `X`?" (Маршрутизаторы удаляют полученные широковещательные пакеты, поэтому использование широковещания ограничивается исключительно физической подсетью, к которой подключен компьютер, выполняющий запрос. Кроме того, широковещание существенно загружает полосу пропускания сети.)

В двух следующих разделах, посвященных DNS и WINS, более подробно рассматриваются методы преобразования обычных имен в IP-адреса.

Замечание

Для более детального ознакомления со стеком протоколов TCP/IP обратите внимание на книгу Дугласа Камера *Сети TCP/IP. Том 1. Принципы, протоколы и структура*, выпущенную Издательским домом "Вильямс" (ISBN 5-8459-0419-6).

Преобразование имен с помощью DNS

Служба имен доменов (DNS) является службой TCP/IP, которая используется для преобразования IP-адресов в FQDN. Кроме того, служба предназначена для обратного преобразования имен в IP-адреса. Представьте сервер DNS как большую телефонную книгу TCP/IP. Когда необходимо кому-то позвонить, требуется получить соответствующий телефонный номер. Когда один компьютер должен связаться с другим, необходимо знать IP-адрес второго компьютера. Например, при работе на домашнем компьютере необходимо просмотреть книгу на Web-узле `www.awl.com`. Домашний компьютер осуществит запрос к серверу DNS, чтобы выяснить, какой IP-адрес соответствует адресу `www.awl.com`. Сервер DNS ответит, передав домашнему компьютеру IP-адрес 165.193.123.224. Домашний компьютер будет использовать этот адрес для связи с компьютером, на котором установлен Web-сервер `www.awl.com`. В терминах DNS эта операция определяется как *прямое преобразование* (*forward lookup*). Если выполнить обратный процесс и при наличии IP-адреса потребовать от сервера DNS предоставить имя FQDN, то получится *обратное преобразование* (*reverse lookup*).

Прежде чем перейти к обсуждению терминологии службы DNS, рассмотрим сам процесс преобразования имен. Вместо сервера DNS в процессе преобразования могут участвовать и другие логические компоненты. Ниже приведен порядок применения системой Windows 2000 и более новыми версиями методов преобразования имени FQDN в IP-адрес.

1. Кэш преобразователя имен и файл `Hosts`.
2. Служба DNS.

3. Кэш NetBIOS.
4. Служба WINS.
5. Широковещательный запрос.
6. Файл `LMHosts`.

Кэш преобразователя имен

Когда для определенного имени FQDN необходимо получить IP-адрес, система ищет информацию о нем прежде всего в кэше преобразователя имен. *Кэш преобразователя имен* (resolver cache) — это место, в котором компьютер хранит информацию о предыдущих запросах на преобразование имен FQDN в IP-адрес. Кэш предназначен для повышения производительности системы. Например, если посещать Web-узел `www.microsoft.com` 20 раз в день, нет необходимости "заставлять" компьютер каждый раз заново находить адрес сервера, содержащего этот Web-узел. Вместо этого компьютер проводит поиск в кэше преобразователя имен. Преобразование выполняется быстрее, если информация о преобразовании имен в IP-адрес хранится на локальном жестком диске компьютера. Кроме того, Windows кэширует негативные ответы для несуществующих имен FQDN. Например, если попытаться отправить диагностический эхо-пакет на любимый Web-узел Барри Кауфмана (Barry Kauffman) `freesoftware.microsoft.com`, будет получен ответ, что Web-узла не существует (сервер DNS компании Microsoft ответит: "Такого зверя нет в природе."). Локальная система сохранит информацию о негативном ответе для этого имени в локальном кэше преобразователя имен. Таким образом, при следующей попытке доступа к Web-узлу `freesoftware.microsoft.com` компьютер сообщит, что такого Web-узла или Web-страницы не существует.

Если необходимо просмотреть содержимое кэша преобразователя имен в системе, в приглашении командной строки введите команду `ipconfig /displaydns`. С другой стороны, чтобы очистить содержимое кэша локального преобразователя, введите в командной строке команду `ipconfig /flushdns` (возможности программы `ipconfig` подробно рассматриваются в главе 4).

Операционная система Windows по умолчанию кэширует положительные ответы в течение периода TTL (Time To Live — время жизни), которое предоставляется сервером DNS, ответившим ранее на запрос о преобразовании имен, однако запись никогда не кэшируется дольше, чем на 86 400 секунд (24 часа). Значение TTL представляет собой период истечения работоспособности записи, измеряемый в секундах. Для того чтобы это доказать, можно последовательно запустить команду `ipconfig /displaydns` несколько раз и обратить внимание, как значения параметра TTL для кэшированных записей постоянно уменьшаются. Негативные результаты кэшируются в течение 300 секунд (5 минут). Оба этих значения могут быть изменены при редактировании записи системного реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNSCache\Parameters`. Чтобы изменить максимальное время кэширования для позитивных ответов, создайте запись типа `DWORD`, которая называется `MaxCacheEntryTtlLimit`, и присвойте ей необходимое значение в секундах.

Для изменения времени кэширования отрицательных ответов создайте запись типа DWORD, которая называется NegativeCacheTime, и присвойте ей значение в виде количества секунд, в течение которых система будет хранить в кэше результат преобразования. Если необходимо запретить хранение отрицательных результатов запросов, присвойте записи значение **0**.

Файл hosts

При загрузке системы содержимое файла Hosts автоматически загружается в кэш преобразователя имен, поэтому содержимое файла Hosts и кэш преобразователя проверяются одновременно. Кроме того, при каждом изменении и сохранении файла Hosts его содержимое автоматически загружается в кэш преобразователя имен.

Файл Hosts можно представить в виде локального "мини-сервера DNS" для клиентской системы. Как и сервер DNS, файл Hosts содержит информацию для преобразования имен FQDN в IP-адреса. Но одним из главных отличий файла Hosts от сервера DNS является то, что статический текстовый файл Hosts хранится на локальном компьютере. Это означает, что для использования файла Hosts в масштабе предприятия придется копировать или устанавливать файл Hosts на каждом компьютере, которому требуются данные относительно соответствия FQDN и IP-адресов.

Если необходимо просмотреть содержимое файла Hosts (рис. 2.5), в любой системе достаточно запустить программу Проводник (Windows Explorer) и перейти в каталог %systemroot%\system32\drivers\etc (c:\Windows\system32\drivers\etc при настройках, принятых по умолчанию). В папке etc можно воспользоваться редактором Блокнот (Notepad) для просмотра и редактирования файла Hosts.

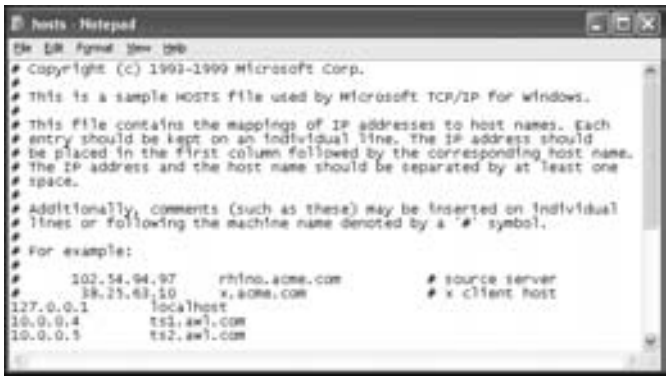

Рис. 2.5. Содержимое файла Hosts

Замечание

Если у одной клиентской системы возникают проблемы при доступе к какому-либо компьютеру по его имени FQDN, а все остальные системы работают нормально, проверьте, не содержит ли файл Hosts на проблемной системе некорректной статической записи.

Типы запросов DNS

Если запрошенный адрес имени FQDN не найден в кэше преобразователя или в файле `Hosts`, клиент выполняет рекурсивный запрос к первичному серверу DNS. *Рекурсивный запрос* — это запрос на выполнение полного преобразования имени FQDN в IP-адрес. Если сервер DNS содержит информацию об искомой записи, он передаст клиенту соответствующий ответ, а если не содержит — может выполнить несколько итеративных запросов к корневым серверам системы DNS. *Итеративный запрос* является запросом на преобразование только части имени FQDN. Например, если система запрашивает сервер DNS для получения IP-адреса имени `freesoftware.microsoft.com` и сервер не имеет информации об адресе этого узла, то сначала система выполнит итеративный запрос к серверу домена `com`, чтобы узнать адрес сервера DNS для домена `microsoft.com`. Затем будет выполнен итеративный запрос к серверу `microsoft.com` для получения IP-адреса узла, который называется `freesoftware`. Тем, кто еще не разобрался в особенностях итеративного и рекурсивного преобразования имен, стоит обратиться к главе 8, "Служба DNS".

Кэш NetBIOS

Если все запросы к указанному для клиента серверу DNS не принесут необходимого результата, клиент воспользуется кэшем имен NetBIOS для получения записей, которые соответствуют имени узла в имени FQDN, например `freesoftware`. Кэш NetBIOS является эквивалентом кэша преобразователя имен DNS и отличается только тем, что содержит информацию о преобразовании имен NetBIOS (а не FQDN) в IP-адреса. Для просмотра содержимого кэша NetBIOS введите в командной строке команду `nbtstat -c`.

Служба WINS/широковещательный запрос/файл lmhosts

В том случае, если имя NetBIOS отсутствует в кэше преобразования NetBIOS, клиент выполнит запрос к серверу WINS для преобразования имени узла в IP-адрес. Если сервер WINS не настроен или клиент не знает его адреса, будет сделан широковещательный запрос. Его можно воспринимать, как следующий запрос к сети: "Кто знает IP-адрес компьютера `freesoftware`?" Маршрутизаторы всегда блокируют широковещательные пакеты, поэтому каждый широковещательный запрос получают только клиентские системы в локальной подсети. Если широковещательный запрос не дал результатов, клиентская система будет искать ответ в файле `LMHosts`. Этот файл может содержать данные о соответствии имен NetBIOS и IP-адресов. Файл `LMHosts` по своему формату напоминает файл `Hosts`, причем оба файла расположены в одном и том же каталоге. Основное отличие заключается в том, что файл `LMHosts` обеспечивает соответствие между именами NetBIOS и IP-адресами, а файл `Hosts` — между FQDN и IP-адресами.

Несложно заметить, что преобразование имен может быть довольно длительным процессом. Именно поэтому при попытке получить доступ к Web-узлу и при вводе его неправильного имени (тогда узла просто не существует) приходится ждать несколько секунд, пока не завершится поиск адреса необходимой Web-страницы. Для окончательного заполнения белых пятен в общей картине требуется рассмотреть основные концепции служб DHCP и WINS, чему и посвящены следующие разделы.

Служба WINS

Эта служба применяется для преобразования имен NetBIOS в IP-адреса. В сети на базе Windows 2000/XP/2003 нет необходимости применять WINS. Однако по политическим мотивам или для обеспечения обратной совместимости со старыми системами служба WINS все же может быть установлена, поэтому имеет смысл остановиться подробнее на особенностях WINS.

Как уже отмечалось, одним из методов преобразования имен NetBIOS в IP-адреса является использование широковещательных запросов. Так как несколько "болтливых" компьютеров могут замедлить быстродействие локальной сети, служба WINS была предложена в качестве технологии преобразования IP-адресов в имена NetBIOS. Это позволило сократить количество широковещательных запросов в отдельных сегментах локальных сетей. Вместо отправки запроса ко всей сети клиентский компьютер отправляет запрос на преобразование имени NetBIOS в IP-адрес непосредственно серверу WINS. Если сервер не содержит записи для этого имени NetBIOS, клиент выполняет соответствующий широковещательный запрос.

Метод или порядок, используемый клиентом для преобразования имени NetBIOS в IP-адрес, зависит от типа клиента NetBIOS, в качестве которого настроена система. Клиенты NetBIOS могут быть настроены для использования одного из перечисленных ниже режимов преобразования имен NetBIOS.

- *B-Node (широковещательный узел)* — широковещательные запросы для преобразования имен NetBIOS в IP-адреса.
- *P-Node (равноправный узел)* — соединение "точка–точка" с сервером имен NetBIOS (например, с сервером WINS) для преобразования имен NetBIOS в IP-адреса.
- *M-Node (смешанный узел)* — комбинация методов *B* и *P* для преобразования имен NetBIOS в IP-адреса. Клиентская система сначала задействует широковещательный запрос, а в случае неудачи запрашивает преобразование у сервера имен NetBIOS.
- *H-Node (гибридный узел)* — комбинация методов *B* и *P* для преобразования имен NetBIOS в IP-адреса. Клиентская система сначала обращается к серверу имен NetBIOS, затем проверяется содержимое файла `LMHosts` и наконец проводится широковещательный запрос.

Обычно для уменьшения объема данных, передаваемых по сети, клиенты, использующие WINS, настраиваются как клиенты H-node. Эта конфигурация позволяет сэкономить пропускную способность локальной сети. В свою очередь, клиентские системы Windows могут получить любые IP-адреса от сервера DHCP при использовании одноименной службы (которая рассматривается ниже). Следовательно, при снижении быстродействия службы преобразования имен NetBIOS стоит обратить внимание на флажок WINS/NBT Node Type сервера DHCP.

Во времена Windows NT 4.0 служба WINS считалась важным шагом вперед, поскольку была динамической. Это означало, что клиенты WINS могли автоматически регистрировать имена NetBIOS и IP-адреса на сервере WINS. Предполагалось, что это освободит администратора от ручного отслеживания соответствий между IP-адресами и именами NetBIOS. Более ранние версии DNS не были динамическими, поэтому, когда требовалось обеспечить динамическое преобразование имен в IP-адреса, служба WINS представляла собой единственно возможный вариант. Благодаря службе DNS в операционной системе Windows 2000 клиенты под управлением этой и более поздних версий могут автоматически регистрировать имена FQDN и IP-адреса посредством сервера DNS. Для клиентов под управлением более ранних версий операционной системы Windows (до версии 2000) сервер DHCP операционной системы Windows 2000 позволяет самостоятельно регистрировать имя и IP-адрес на сервере DNS. Учитывая эти факты, службе WINS более не место в сетевой инфраструктуре на базе Windows 2000.

Замечание

Главы 8 и 9 содержат немало полезных сведений о вопросах интеграции служб DNS и DHCP с WINS.

Служба DHCP

Динамический протокол настройки узлов (Dynamic Host Configuration Protocol — DHCP) позволяет клиентам и серверам в сети автоматически получать IP-адреса от сервера DHCP. При работе с сотнями или даже тысячами компьютеров сервер DHCP может сэкономить немало времени и ресурсов, если в качестве альтернативы рассматривать ручное конфигурирование статических IP-адресов на клиентских компьютерах.

Чтобы понять принципы работы протокола DHCP, необходимо ознакомиться со следующими терминами:

- аренда DHCP;
- область DHCP;
- резервирование;
- параметры DHCP;
- агент ретрансляции DHCP;
- автоматическая частная IP-адресация.

Аренда DHCP

При работе в Ethernet сетевые адаптеры (NIC) идентифицируются посредством 48-разрядного адреса MAC (Media Control Access). Адреса MAC встраиваются в сетевые адаптеры производителем, поэтому каждый сетевой адаптер имеет уникальный адрес MAC. В отличие от IP-адресов в сети, адреса MAC выражаются в виде последовательности шестнадцатеричных чисел. Поскольку одна шестнадцатеричная цифра представляет собой четыре двоичных разряда, типичный адрес MAC длиной в 48 разрядов будет записываться примерно таким образом: 00-03-2F-01-D0-1B.

Адреса MAC позволяют идентифицировать сетевую карту в сети без вмешательства пользователя. Когда загружается компьютер, настроенный для автоматического получения IP-адреса, он осуществляет широковещательный запрос *DHCP Discover*. При этом система пытается получить в сети ответ на вопрос о том, есть ли здесь хоть один сервер DHCP. Сервер или серверы DHCP, которые получают этот запрос, в соответствии с адресом MAC запрашивающего компьютера предлагают ему IP-адрес. Этот этап называется *DHCP Offer*. Затем клиент отправляет пакет *DHCP Request* первому серверу DHCP, который предоставил клиенту соответствующее предложение. При этом клиент запрашивает предложенный сервером IP-адрес. Наконец, сервер DHCP отправляет клиенту пакет *DHCP Acknowledge*, подтверждая предоставление данного IP-адреса.

Сервер DHCP предоставляет IP-адрес клиентам DHCP только в аренду. Поэтому после получения IP-адреса от сервера DHCP клиент не становится автоматически его постоянным владельцем. Например, если сервер DHCP настроен на предоставление IP-адресов в аренду сроком на две недели и клиент DHCP не подключался к сети в течение двух недель с момента получения своего IP-адреса, сервер DHCP аннулирует аренду и может выдать этот IP-адрес другому компьютеру. Пока клиентская система подключена к сети, по истечении половины срока аренды она автоматически попытается связаться с сервером DHCP для продления этого срока.

Область DHCP

Адреса DHCP и их аренда настраиваются для *областей DHCP* (*scope*). Кроме диапазона IP-адресов, которые выдаются клиентам, и срока аренды IP-адресов, область определяет множество других параметров DHCP, в том числе:

- маску подсети;
- исключения из диапазона IP-адресов;
- резервирование IP-адресов;
- параметры DHCP.

Маска подсети для диапазона IP-адресов указывается в момент создания области DHCP и не может быть изменена впоследствии. Единственным способом изменения маски подсети для области является удаление и повторное создание области. Если в сети используется несколько серверов, которым присвоены фиксированные IP-адреса, можно попытаться определить *исключения адресов*. После настрой-

ки исключений IP-адреса, попавшие в диапазон исключений, не будут выдаваться клиентам сервером DHCP.

Резервирование

Если в сети присутствуют клиенты DHCP, которым необходимо получить один и тот же IP-адрес при каждом подключении, можно настроить *резервирование* DHCP. При создании резервирования необходимо знать адрес MAC сетевого адаптера, для которого необходимо зарезервировать IP-адрес. Резервирование является не чем иным, как "привязкой" сервером DHCP определенных IP-адресов к адресам MAC. Поскольку адреса MAC должны вводиться для каждого резервирования DHCP, иногда проще присвоить статические IP-адреса соответствующим компьютерам в сети, после чего создать диапазон исключений на сервере DHCP. Итак, область DHCP определяет диапазон IP-адресов и маску подсети для клиентов DHCP. Все остальные параметры сети настраиваются в разделе параметров сервера DHCP.

Параметры DHCP

Параметры DHCP позволяют автоматически предоставить клиентам намного больше информации, чем IP-адрес и маска подсети. Настроив параметры DHCP, можно выдавать клиентам DHCP следующую информацию:

- адрес базового шлюза;
- адреса серверов DNS;
- имя домена DNS;
- адреса серверов WINS;
- тип узла WINS.

При корректно настроенных серверах DHCP достаточно вставить сетевой кабель в адаптер компьютера, а всю остальную настройку параметров сетевого взаимодействия обеспечит сервер DHCP.

Агент ретрансляции DHCP

В разделе, посвященном аренде DHCP, упоминалось, что при загрузке клиентской системы последняя отправляет широковещательный запрос для поиска сервера DHCP. Проблема широковещательных запросов заключается в том, что маршрутизаторы "отбрасывают" такие пакеты данных. Широковещательные запросы DHCP могут быть исключением из правил, в зависимости от типа маршрутизатора. Если маршутизатор соответствует стандарту RFC 1542 и на нем активизирована функция запросов BOOTP, то маршрутизатор сможет передавать между сетями пакеты DHCP Discover. Если маршрутизаторы не соответствуют стандарту RFC 1542 и у сервера DCHP, расположенного в одной подсети, есть клиенты в нескольких подсетях, существует два метода решения данной проблемы:

- приобрести новый маршрутизатор, совместимый со стандартом RFC 1542;
- настроить сервер Windows, поддерживающий службу RAS (Routing and Remote Access) для работы в качестве агента ретрансляции запросов DHCP.

Вторая концепция иллюстрируется на рис. 2.6.

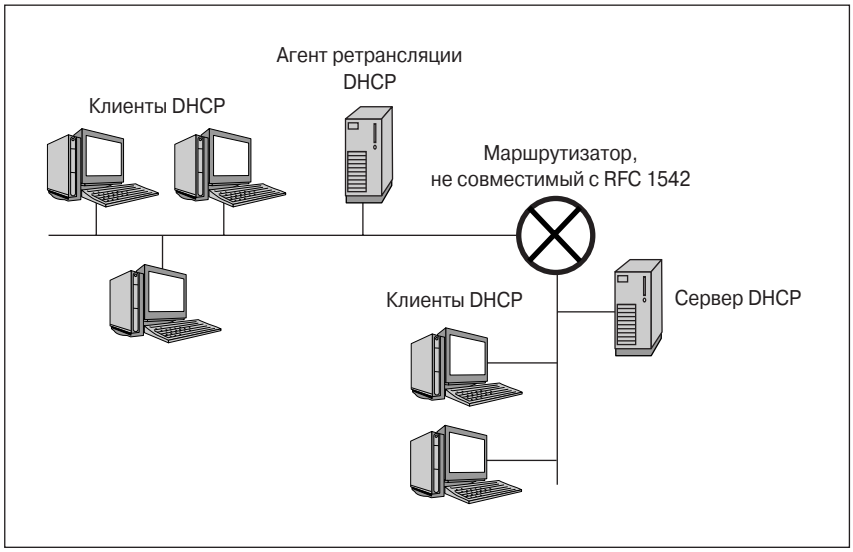

Рис. 2.6. Размещение агента ретрансляции DHCP

Обратите внимание, что на рис. 2.6 агент ретрансляции DHCP размещен не в той же подсети, где расположен сервер DHCP. Находясь в том же сегменте, что и клиент, агент ретрансляции DHCP перехватывает все широковещательные запросы DHCP Discover и передает их непосредственно серверу DHCP. Поскольку выполняется прямая передача пакетов данных между агентом ретрансляции DHCP и сервером (пакеты содержат адрес сервера DHCP), пакеты не отбрасываются маршрутизатором.

А что, если агента ретрансляции DHCP не существует? Именно для такого случая Microsoft изобрела технологию APIPA.

Автоматическая частная IP-адресация

Эта технология стала ответом на ожидания тех, кто мечтал о комфортном применении протокола TCP/IP. Операционные системы компании Microsoft поступают в продажу уже настроенными на использование протокола TCP/IP и автоматическое получение IP-адреса. При использовании автоматической частной IP-адресации (Automatic Private IP Addressing — APIPA) операционная система Windows 2000 и более поздние версии, которые не могут связаться с сервером DHCP, выбирают себе IP-адрес самостоятельно. Этот адрес предназначен для сети класса

В в диапазоне от 169.254.0.1 до 169.254.255.254 с маской подсети 255.255.0.0. Технология APIPA позволяет автоматически настроить сеть TCP/IP, не выполняя никаких действий, кроме подключения сетевого кабеля к адаптеру и коммутатору/концентратору.

Замечание

Технология APIPA — лучший помощник администратора, решающего проблемы протокола DHCP. Почему? Если в сети есть клиент или клиенты, которые в своей локальной подсети не могут общаться с другими компьютерами, запустите на них программу `ipconfig`. В том случае, если у клиента IP-адрес относится к подсети 169.254.x.x, подключение к серверу DHCP становится невозможным.

Дополнительная информация

В этой книге основное внимание уделяется решению разнообразных проблем. Читателям, которые не совсем уверены в понимании некоторых концепций или терминологии сетевого администрирования, а также интересуются дополнительной информацией по определенным темам, рекомендуется посетить перечисленные ниже Web-узлы.

- `www.webopedia.com` — простые определения для большинства аббревиатур и концепций.
- `www.whatis.com` — поисковый сервер, ориентированный на информационные технологии.
- `support.microsoft.com` — официальный Web-узел службы технической поддержки компании Microsoft. Содержит ответы на большинство вопросов. Доступ к ответам можно получить с помощью поиска в базе знаний (Knowledge Base).
- `www.mcpmag.com` — содержит возможность поиска и чтения статей из прошлых выпусков журнала *MCP Magazine*.
- `www.winnetmag.com` — содержит большое количество статьей из журналов *Windows Magazine* и *.NET Magazine*.
- `www.labmice.net` — огромное количество ресурсов, посвященных Windows NT/2000 и Windows Server 2003.
- `www.microsoft.com/technet` — база данных TechNet, поддерживающая поиск и содержащая большой объем полезной информации по решению разнообразных проблем.
- `www.techrepublic.com` — отличный источник статей, посвященных Windows и информационным технологиям, а также другим продуктам.
- `www.windows2000faq.com` — список часто задаваемых вопросов по операционной системе Windows.

Резюме

Рассмотрев некоторые базовые понятия, концепции и протоколы сетевого взаимодействия, можно переходить к главной теме книги — решению разнообразных проблем. В следующей главе описываются хорошо зарекомендовавшие себя методы выявления и диагностики возникающих проблем. Затем рассматриваются сетевые протоколы и их роль в решении актуальных системных задач.