Designed for Microsoft® Windows NT®

CD-ROM

Гарантия квалификации

# MCSE

# Учебный курс

Microsoft®

# TCP/IP

**Третье издание исправленное**

**Сертификационный экзамен 70-059**


**Официальное учебное пособие для самостоятельной подготовки**

РУССКАЯ РЕДАКЦИЯ

Microsoft® Press

# Microsoft®
# TCP/IP

*Hands-On, Self-Paced Training for Supporting TCP/IP*

Microsoft® Press

# Microsoft® TCP/IP

## *Учебный курс*

*Официальное пособие Microsoft®*
*для самостоятельной подготовки*

**Издание третье, исправленное**

РУССКАЯ РЕДАКЦИЯ

**УДК 004**
**ББК 32.973.26–018.2**

**М59**

**Microsoft Corporation**

М59 Microsoft TCP/IP. Учебный курс: Официальное пособие Microsoft для самостоятельной подготовки: Пер. с англ. — 3-е изд., испр. — М.: Издательско-торговый дом «Русская Редакция», 2001. — 400 с.: ил.

**ISBN 5–7502–0171–6**

Этот учебный курс рекомендован корпорацией Microsoft для подготовки к экзаменам на звание сертифицированного системного инженера Microsoft – Microsoft Certified Systems Engineer (MCSE). В нем подробно излагается материал, составляющий основу экзамена № 70-059 «Internetworking with Microsoft TCP/IP on Microsoft Windows NT 4.0».

Книга адресована сетевым администраторам, специалистам по программным продуктам Microsoft и всем, кто хочет ближе познакомиться с основными технологиями Интернета. Она содержит подробные сведения об архитектуре семейства протоколов TCP/IP, их установке и конфигурации, возможных проблемах и путях решения.

Богато иллюстрированный учебный курс состоит из 16 глав и списка вопросов и ответов для закрепления материала. На прилагаемом к книге компакт-диске находятся учебные материалы и файлы, необходимые для выполнения упражнений.

УДК 004
ББК 32.973.26–018.2

Подготовлено к печати по лицензионному договору с Microsoft Corporation, Редмонд, Вашингтон, США.

При работе над этой книгой использованы технологии и оборудование для построения информационных радиосетей, предоставленные **Компанией ArtCommunications Ltd.**, тел.: **943-8446, 212-0696, http://www.artcoms.ru/.**



**ISBN 1–57231–623–3 (англ.)**
**ISBN 5–7502–0171–6**

# Оглавление

# Об этой книге

Перед Вами учебный курс по Microsoft® TCP/IP (Internetworking with Microsoft TCP/IP on Microsoft® Windows NT 4.0). В этой книге системные администраторы найдут множество полезной информации по установке, конфигурации, использованию и поддержке протокола TCP/IP (Transmission Control Protocol/Internet Protocol) операционной системы Microsoft Windows NT версии 4.0 в компьютерных сетях. Изучив курс, Вы подготовитесь к экзамену на получение звания сертифицированного специалиста Microsoft по системам Интернета (Microsoft Internet Systems Certified Professional).

---

Примечание Подробнее о том, как стать сертифицированным специалистом Microsoft — в разделе «Программа сертификации специалистов Microsoft».

---

Каждая глава курса состоит из нескольких занятий, большинство которых содержат упражнения, позволяющие на практике отработать полученные навыки. Все занятия заканчиваются разделом «Резюме», а главы — списком вопросов для закрепления материала. Кроме того, некоторые главы завершаются перечнем источников дополнительной информации.

В раздел «С чего начать» включены инструкции по установке, аппаратные и программные требования для выполнения заданий курса и, если требуется, — описание сетевой конфигурации двух компьютеров, необходимых для выполнения упражнений. Непременно прочитайте его перед тем, как приступить к занятиям.

## Содержание прилагаемого к курсу компакт-диска

На компакт-диске Вы найдете видеоролики, дополняющие материал книги. Просмотрите их при выполнении упражнений (там, где предлагается это сделать), а затем используйте в качестве наглядного пособия при работе с материалом курса.

Компакт-диск также содержит файлы, необходимые для выполнения упражнений, дополнительную информацию по теме занятий, и, кроме того, другие полезные материалы — на Web-странице *Course Materials*. Для ее просмотра Вам придется установить Microsoft Internet Explorer™ 3.0. Об этом читайте в разделе «С чего начать».

## Справочные материалы

Возможно, Вам пригодятся следующие справочные материалы:

- документация по Windows NT Server версии 4.0;
- описание Microsoft Windows NT Server Resource Kit.

## Кому адресована книга

Книга написана для сетевых интеграторов, системных инженеров и специалистов, занимающихся реализацией и поддержкой протокола TCP/IP в локальных и глобальных сетях. Книга рассчитана также на тех, кто планирует сдать экзамен 70-059, «Internetworking with TCP/IP on Microsoft Windows NT 4.0».

### Требования к читателю

- Знание принципов работы и использования аппаратного обеспечения *локальной вычислительной сети* (Local Area Network, LAN), включая сетевые платы, соединения, мосты и маршрутизаторы.
- Успешная сдача экзамена 70-067, «Implementing and Supporting Microsoft Windows NT Server 4.0»

  или
- Знание курса #687, «Supporting Microsoft Windows NT Server 4.0 Core Technologies»*.

## Назначение книги

Курс предназначен для индивидуальной работы, поэтому Вы можете выбрать удобный порядок чтения, например, пропустить некоторые занятия и вернуться к ним позднее. Помните, что Вам необходимо выполнить приведенные в главе 2 инструкции для работы с упражнениями остальных глав. Используйте таблицу, чтобы выбрать оптимальный порядок работы с книгой.

| Ваша цель | Необходимые материалы |
|---|---|
| Подготовка к сдаче экзамена 70-59 на получение звания сертифицированного специалиста Microsoft, «Internetworking with TCP/IP on Microsoft Windows NT 4.0» | Изучите раздел «С чего начать», главы 1–3, а затем — оставшиеся главы в любом порядке. Чтение глав всегда начинайте с раздела «Прежде всего»: в нем определены необходимые требования |
| Установка и конфигурирование протокола TCP/IP | Прочитайте раздел «С чего начать». Изучите главу 2, затем — главы 1 и 3. Далее проработайте остальные главы в любом порядке |

* Теперь этот курс имеет номер #922. Появился и его русский вариант — #1030. — *Прим. перев.*

*(продолжение)*

| Ваша цель | Необходимые материалы |
|---|---|
| Установка TCP/IP и конфигурирование нескольких рабочих групп или компьютеров | Прочитайте раздел «С чего начать». Затем — главу, описывающую Вашу конфигурацию. Например, если Вы собираетесь создать несколько подсетей, то Вам стоит начать с главы 5: из нее Вы узнаете о создании диапазона IP-адресов. Затем проработайте главу 2 и остальные главы в любом порядке |
| Получение специальной информации о протоколе TCP/IP | Просмотрите оглавление настоящего курса |

## Соглашения, принятые в учебном курсе

Прежде всего Вам необходимо усвоить термины и понятия, принятые в книге.

### Структура книги

- Каждая глава начинается с раздела «Прежде всего», где перечислены материалы, необходимые для изучения занятий этой главы.
- Многие занятия содержат упражнения, которые позволят Вам применить полученные навыки на практике или исследовать описанную часть протокола TCP/IP. Все упражнения обозначены соответствующим значком на полях (▶).
- Раздел «Закрепление материала» в конце каждой главы — для проверки и закрепления полученных знаний. Отвечая на вопросы, Вы лучше подготовитесь к экзаменам на звание сертифицированного специалиста Microsoft.
- Раздел «Дополнительная информация» содержит список дополнительных материалов по теме занятий — ссылки на документацию по программным продуктам и интерактивным службам.
- В статье «Вопросы и ответы» перечислены вопросы из всех глав книги и ответы на них. Там же приведены ссылки на номера страниц, содержащих вопросы.

### Упражнения

- Упражнения оформлены в виде списка последовательных действий. На начало упражнения указывает треугольник на полях (▶).

## Обозначения

- Символы или команды, которые Вы должны ввести сами, выделены *курсивом*.
- Кроме того, *курсивом* в синтаксисе команд обозначены переменные параметры, а также в тексте — новые важные термины и учетные записи, под которыми Вы регистрируетесь в системе.
- Имена файлов и каталогов начинаются с заглавных букв. Однако это соглашение не жесткое — Вы вправе задавать имена файлов в диалоговом окне или командной строке прописными буквами.
- Аббревиатуры набраны заглавными буквами.
- `Шрифтом`, отличным от основного, набраны примеры кода, экранного текста, записи, которые Вам надо набрать в командной строке, или содержимое файлов.
- В квадратные скобки в синтаксических выражениях заключена функциональная информация. Например [*имя файла*] в синтаксисе команды показывает, что Вы можете сами задать его. Набирать следует только содержимое скобок, но НЕ сами скобки.
- В фигурные скобки ( { } ) в синтаксических выражениях заключены обязательные параметры. Набирайте только содержимое скобок, но НЕ сами скобки.
- **Полужирным** начертанием выделены элементы интерфейса.

## Клавиатура

- Названия клавиш набраны прописными буквами, например TAB и SHIFT.
- Знак плюс (+) между названиями клавиш означает, что Вы должны нажать их одновременно. Например, «Нажмите ALT+TAB» означает, что нужно нажать TAB, удерживая клавишу ALT.
- Запятая (,) между названиями клавиш показывает, что требуется нажать каждую клавишу по отдельности, а не одновременно. Например, «Нажмите ALT+W, L» означает, что сначала Вам надо одновременно нажать клавиши ALT и W, а затем отпустить их и нажать клавишу L.
- Команды меню можно выбирать с клавиатуры. Нажмите клавишу ALT, чтобы сделать активной строку меню, затем последовательно нажимайте клавиши, соответствующие подчеркнутой букве в пункте меню и имени команды. Для выполнения некоторых команд Вы также вправе использовать комбинацию клавиш, указанную в меню.
- С помощью клавиатуры можно выбрать или отменить флажки или опции в диалоговых окнах. Нажмите клавишу ALT, затем — клавишу, соответствующую подчеркнутой букве в имени функции. Или же на-

жимайте клавишу TAB, пока нужная зона не станет активной, а затем нажмите клавишу ПРОБЕЛ для выбора или отмены.
- Нажатием клавиши ESC Вы можете отменить отображение диалогового окна.

### Справочная информация

В курсе Вам встретится краткая информация справочного характера.
- **Совет** — поясняет возможный результат или предлагает альтернативные методы решения задачи.
- **Примечание** — содержит дополнительную информацию.
- **Внимание!** — предупреждает о возможной потере данных.

## С чего начать

### Аппаратное обеспечение

Курс содержит упражнения, выполнив которые Вы на практике изучите протокол Microsoft TCP/IP в Microsoft Windows NT 4.0. Для выполнения большинства упражнений Вам потребуются два объединенных в сеть или подключенных к большой сети компьютера.

Оба они должны работать под управлением ОС Microsoft Windows NT Server 4.0. Минимальные требования к конфигурации:
- процессор 486/33 (на базе Intel) или выше;
- 16 Мб ОЗУ (рекомендуется 32 Мб);
- 450 Мб свободного места на жестком диске каждого компьютера;
- видеоадаптер SVGA и монитор с возможностью отображения 256 цветов;
- мышь Microsoft или совместимое с ней устройство;
- плата сетевого адаптера и соответствующие кабели;
- один дисковод для дискет размером 3.5 дюйма;
- дисковод CD-ROM;
- звуковая плата с наушниками или динамиками на одном из компьютеров.

Все аппаратное обеспечение выбирается из *списка совместимого с ОС Windows NT 4.0 оборудования* (Microsoft Windows NT 4.0 Hardware Compatibility List, HCL).

### Программное обеспечение

Для выполнения упражнений курса требуется:
- ОС Windows NT Server 4.0;
- ОС Microsoft MS-DOS® версии 5.0 или более поздней;
- Windows NT Server 4.0 с Service Pack 2 или более поздней версией (Service Pack 2 Вы найдете на прилагаемом к курсу компакт-диске).

## Инструкции по установке

Для выполнения многих упражнений настоятельно рекомендуется использовать два сетевых или работающих в большой сети компьютера.

1. Настройте оба компьютера в соответствии с инструкциями производителя.
2. Соедините их непосредственно или при помощи концентратора, чтобы связь была, как в большой сети.
3. Обеспечьте около 450 Мб свободного места на жестком диске каждого компьютера.
4. Установите ОС Windows NT Server на каждом компьютере.

Первый компьютер настройте как *главный контроллер домена* (Primary Domain Controller, PDC). Присвойте ему имя Server1 и имя домена Domain1. Этот компьютер будет работать в качестве контроллера домена, сервера файлов, печати и приложений в домене Domain1.

Второй компьютер сконфигурируйте как сервер и рабочую станцию: в этом качестве он потребуется для большинства упражнений данного курса. Он будет частью домена Domain1 с именем Server2.

---

Внимание! Если ваши компьютеры — часть большой сети, обязательно вместе со своим сетевым администратором проверьте, не конфликтуют ли с сетью имена компьютеров, имя домена и информация об IP-адресах, взятые из таблицы. Если да, попросите сетевого администратора предоставить альтернативные данные и используйте их во всех упражнениях книги.

---

| Параметры | Используемые в курсе значения |
|---|---|
| Имя первого компьютера (PDC) | Server1 |
| IP-адрес первого компьютера | 131.107.2.200 |
| Имя второго компьютера | Server2 |
| IP-адрес второго компьютера | 131.107.2.211 |
| Диапазон IP-адресов | 131.107.2.200 — 131.107.2.211 |
| Маска подсети | 255.255.255.0 |
| Имя домена | Domain1 |
| Шлюз по умолчанию | 131.107.2.1 |

### Microsoft Internet Explorer

Для использования Web-страницы с прилагаемого к курсу компакт-диска Вы должны установить Microsoft Internet Explorer 3.0.

► **Установка Microsoft Internet Explorer 3.0**

1. Откройте каталог Ie_setup с компакт-диска и запустите Msie30.exe.

   Появится диалоговое окно **Microsoft Internet Explorer 3.0**.
2. Ответьте **Yes** на предложение установить Microsoft Internet Explorer 3.0.

   Появится диалоговое окно **Microsoft Internet Explorer 3.0** с информацией о копировании файлов во временный каталог жесткого диска.
3. Прочтите лицензионное соглашение пользователя для Microsoft Internet Explorer 3.0, а затем щелкните **I Agree**.

   Появится диалоговое окно **Microsoft Internet Explorer** с информацией о копировании файлов и установке Microsoft Internet Explorer.
4. При предложения перезагрузить компьютер щелкните **Yes**.

### Windows NT 4.0 Service Pack

Если Вы еще не установили Windows NT 4.0 Service Pack 2*, сделайте это сейчас, воспользовавшись прилагаемым к курсу компакт-диском.

► **Установка Windows NT 4.0 Service Pack**

1. Зарегистрируйтесь в системе как *Administrator*.
2. Вставьте прилагаемый к курсу компакт-диск в дисковод CD-ROM — запустится Internet Explorer и откроется начальная страница *Internetworking with Microsoft TCP/IP on Windows NT 4.0*,

   или

   запустите Windows NT Explorer, раскройте список файлов на CD-ROM, а затем дважды щелкните Open.htm.
3. Щелкните пиктограмму запуска.
4. Щелкните **Course Materials**.
5. Щелкните **Windows NT 4.0 Service Pack 2**.
6. Щелкните **Service Pack.**
7. Прокрутите и щелкните ссылку **Install Service Pack**.

   Появится диалоговое окно Internet Explorer с вопросом об открытии файла или записи его на диск.
8. Выберите **Open it**, затем щелкните **OK**.

   Запустится файл Spsetup.bat, и начнется обновление.
9. В окне **Welcome** щелкните **Next**.
10. В диалоговом окне **Service Pack Setup** выберите **Install the Service Pack**, затем щелкните **Next**.

---

* На компакт-диске также записан Service Pack 3, однако в настоящее время уже доступен Service Pack 4. — *Прим. перев.*

11. Решите, хотите ли Вы создать директорию **Uninstall**, затем щелкните **Next**.
12. Щелкните **Finish** для завершения установки Service Pack.

    Программа установки проверит Ваш компьютер, а затем начнет копирование файлов Service Pack.

    По завершении копирования появится диалоговое окно, информирующее Вас об обновлении ОС Windows NT 4.0.
13. Щелкните **ОК**, чтобы перезапустить компьютер.

## Обзор глав и приложений

Этот учебный курс включает занятия, упражнения, видеоролики и вопросы для закрепления материала, которые помогут Вам изучить работу протокола TCP/IP в ОС Microsoft Windows NT 4.0. Вы можете читать книгу как по порядку, так и изучать только интересующие Вас фрагменты. Однако, все упражнения требуют предварительной подготовки (чаще всего она проводится в предыдущей главе), поэтому сначала обязательно читайте раздел «Прежде всего», начинающий каждую главу.

Книга состоит из следующих глав и разделов.

- Статья «Об этой книге» содержит общие сведения о структуре курса, принятых в нем терминах и обозначениях. Кроме того, здесь Вы найдете информацию о том, как наиболее эффективно организовать работу с книгой при индивидуальном обучении.
- В главе 1, «Основные сведения о TCP/IP», приведены общие сведения о протоколе TCP/IP и процессе стандартизации Интернета.
- В главе 2, «Установка и конфигурация TCP/IP», описаны установка и ручное конфигурирование IP-адреса, маски подсети и шлюза по умолчанию, а также основные процедуры тестирования конфигурации с использованием утилит Ipconfig, PING и Microsoft Network Monitor.
- Глава 3, «Обзор архитектуры стека протоколов TCP/IP», посвящена семейству протоколов TCP/IP: здесь объясняется внутренняя работа протоколов каждого уровня и их взаимодействие с остальными протоколами.
- В главе 4, «IP-адресация», объясняются различия между классами IP-адресов, направлениями IP-адресации, сетевыми компонентами, требующими IP-адресации, и перечислены общие проблемы адресации.
- Глава 5, «Подсети», посвящена фундаментальным подсетям, сетевым концепциям и процедурам, в том числе необходимости применения подсети, использования сетевой маски по умолчанию, задания индивидуальной маски подсети и создания диапазона IP-адресов для каждой подсети в объединенной сети с одного IP-адреса.
- Глава 6, «Реализация IP-маршрутизации» содержит обзор концепций и терминов, применяемых в IP-маршрутизации, а также подробную информацию о ее реализации в сетевом окружении Microsoft.

- Из главы 7, «Протокол DHCP» Вы узнаете о работе протокола DHCP — централизации и управлении информацией о конфигурации путем автоматического назначения IP-адресов компьютерам, настроенным для использования протокола DHCP.
- Глава 8, «NetBIOS поверх TCP/IP», содержит обзор концепций и методов разрешения имен NetBIOS.
- В главе 9, «Windows Internet Name Service (WINS)», объясняется, как WINS уменьшает трафик широковещания при помощи NetBIOS в TCP/IP и адресует сообщения между серверами WINS. Выполнив упражнения этой главы, Вы приобретете навыки, необходимые для поддержки WINS в объединенной сети.
- В главе 10, «Просмотр сетевых ресурсов и функции доменов», описано, как просмотреть NetBIOS в объединенной сети протокола TCP/IP.
- Глава 11, «Разрешение имен узлов», посвящена концепциям и методам разрешения имени хоста.
- Глава 12, «Доменная система имен», содержит обзор структуры и компонентов DNS. Вы изучите файлы базы данных DNS и то, как определяются адреса протокола TCP/IP.
- Глава 13, «Внедрение DNS», посвящена установке и конфигурации DNS и WINS.
- В главе 14, «Взаимодействие в гетерогенных средах», рассмотрены функции использования протокола TCP/IP для работы в неоднородном окружении.
- В главе 15, «Использование SNMP-сервисов», рассказывается о протоколе SNMP (Simple Network Management Protocol), в том числе о функциях, предоставляемых станцией управления протоколом SNMP и службой Microsoft SNMP (агент протокола SNMP).
- В главе 16, «Поиск и устранение неисправностей Microsoft TCP/IP», рассматриваются проблемы при работе с протоколом TCP/IP, симптомы, возможные причины неисправностей, а также утилиты Windows NT и протокола TCP/IP, используемые при поиске неисправностей.

## Программа сертификации специалистов Microsoft

Программа *сертификации специалистов Microsoft* (Microsoft Certified Professional, MCP) предоставляет отличный способ подтвердить Ваши знания современных технологий программных продуктов этой фирмы. В программе использованы передовые методы тестирования, разработанные Microsoft. Экзамены и соответствующие сертификации убедительно подтвердят Вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft.

Программа предлагает четыре типа сертификации специалистов Microsoft.

- *Сертифицированные специалисты по продуктам Microsoft* (Microsoft Certified Product Specialists) должны глубоко знать хотя бы одну из операционных систем Microsoft. Кандидаты могут сдать дополнительные сертификационные экзамены для повышения квалификации по Microsoft BackOffice, средствам разработки или прикладным программам.
- *Сертифицированные системные инженеры Microsoft* (Microsoft Certified Systems Engineers) должны уметь эффективно планировать, реализовать и поддерживать информационные системы Microsoft Windows 95, Microsoft Windows NT, а также семейства программного обеспечения серверов Microsoft BackOffice.
- *Сертифицированные разработчики программных решений на основе продуктов Microsoft* (Microsoft Certified Solution Developers) готовятся для разработки и создания индивидуальных решений с использованием средств разработки Microsoft, технологий и платформ, включая Microsoft Office и Microsoft BackOffice.
- *Сертифицированные преподаватели по продуктам Microsoft* (Microsoft Certified Trainers). Квалифицируются для преподавания в *Авторизованном учебном центре* Microsoft (Authorized Technical Education Center, ATEC).

## Требования к соискателям

К кандидатам предъявляются различные требования, которые зависят от выбранной специальности или программного продукта.

Чтобы стать сертифицированным специалистом, необходимо сдать сложные экзамены, на которых будут объективно оценены Ваше профессиональное мастерство и навыки работы. Вам придется подтвердить свою квалификацию и продемонстрировать умение выполнять задачи, связанные с конкретными программными продуктами. Экзаменационные вопросы учитывают реальные ситуации.

- На звание сертифицированного специалиста по продуктам Microsoft надо выдержать один экзамен по ОС. Кроме того, желающие оценить свои знания могут выбрать и сдать дополнительный экзамен.
- На звание сертифицированного системного инженера Microsoft необходимо сдать базовые экзамены по ОС и экзамены на выбор.
- На звание сертифицированного разработчика Microsoft надо сдать два экзамена по базовым технологиям и два экзамена — на выбор.
- На звание сертифицированного инструктора Microsoft придется выдержать экзамены по предметам из *Официальной учебной программы Microsoft* (Microsoft Official Curriculum), которые Вы собираетесь преподавать. За дополнительной информацией о получении сертификата инструктора Microsoft, в США и Канаде обращайтесь по тел. (800) 636-7544, в других странах — в региональные отделения Microsoft.

## Microsoft Roadmap to Education and Certification

Дорогу в успешное будущее Вам укажет *Microsoft Roadmap to Education and Certification*. Там Вы найдете все необходимое для того, чтобы воспользоваться преимуществами обучения и сертификации от Microsoft. Она включает подробное описание курсов самой последней *Официальной учебной программы Microsoft*, полную информацию о программе сертификации специалистов Microsoft, пробные экзамены (MCP Assesment exams) и программу *Planning wizard*, которая поможет Вам быстро найти путь к достижению намеченных целей. *Roadmap* можно получить одним из следующих способов:

- с Web-страницы *ftp://ftp.microsoft.com/services/msedcert/e&cmap.zip;*
- через CompuServe: Go MECFORUM, Library #2, e&cmap.zip;
- из TechNet: введите ключевое слово «Roadmap» и воспользуйтесь встроенной ссылкой для установки;
- непосредственно в Microsoft: позвоните в США (800) 636-7544 и задайте вопрос о *Roadmap*; за пределами США и Канады обратитесь в региональные отделения Microsoft.

## Microsotf Online Institute

*Microsoft Online Institute* — это интерактивное обучение и информационные ресурсы, доступные через WWW и Microsoft Network (MSN™). *Microsoft Online Institute* хранит отчеты инструкторов, статьи разработчиков, форумы пользователей и другие материалы, касающиеся продуктов и технологий Microsoft.

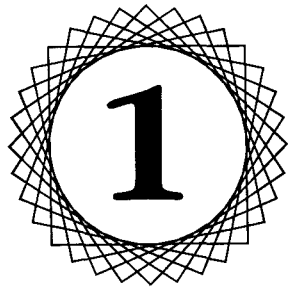
Любой, кто имеет доступ к WWW или MSN, может через Microsoft Online Institute посетить занятие, присоединиться к форуму, заказать учебные материалы или исследовать другие ресурсы *Microsoft Online Institute*.

*Microsoft Online Institute* на WWW Вы найдете по адресу: *http://moli.microsoft.com*. Дополнительную информацию о занятиях и ресурсах Вы можете получить по электронной почте — ***moli_quest@msn.com***.

## Авторизованные учебные центры

В *Авторизованном учебном центре* (Authorized Technical Education Center, ATEC) Вы пройдете обучение под руководством инструктора и подготовитесь к сдаче экзаменов на звание сертифицированного специалиста. Компания Microsoft создала всемирную сеть учебных центров, в которой сертифицированные инструкторы Microsoft преподают на основе *Официальной учебной программы Microsoft*.

В США и Канаде список *Авторизованных учебных центров* можно получить по факсу (800) 727-3351. В других странах — по факсу (206) 635-2233.



# Основные сведения о TCP/IP



## В этой главе

Эта глава содержит обзор протоколов TCP/IP. На занятиях рассматривается краткая история создания TCP/IP, обсуждается процесс стандартизации Интернета и предлагается обзор утилит TCP/IP.

## Прежде всего

Для выполнения заданий этой главы Вам необходим прилагаемый к курсу компакт-диск для получения дополнительной информации технического характера.

# Занятие 1. Знакомство с TCP/IP

Семейство протоколов Transmission Control Protocol/Internet Protocol (TCP/IP) — стандартный промышленный набор протоколов, разработанный для *глобальных вычислительных сетей* (Wide Area Networks, WAN). Здесь приведены основные сведения о концепциях TCP/IP, терминологии и о создании стандартов Сообществом Интернета (Internet Society).

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать протокол TCP/IP и его преимущества в Microsoft Windows NT 4.0;
- ✓ описать процесс стандартизации Интернета;
- ✓ объяснить назначение документов RFC (Request for Comments).

**Продолжительность занятия — 15 минут**

## История создания TCP/IP

Протокол TCP/IP был создан в результате исследований *сетей с коммутацией пакетов* (packet-switching networks), проводимых агентством DARPA Министерства Обороны США (U.S. Department of Defense Advanced Research Projects Agency) в конце 60-х — начале 70-х гг. В эволюции протокола TCP/IP можно отметить несколько важных этапов.

| | |
|---|---|
| 1970 г. | Узлы сети ARPANET начали использовать протокол NCP (Network Control Protocol). |
| 1972 г. | Первая спецификация Telnet оформлена как RFC 318. |
| 1973 г. | Введен протокол File Transfer Protocol, RFC 454. |
| 1974 г. | Представлена программа Transmission Control Program (TCP). |
| 1981 г. | В RFC 791 опубликован стандарт протокола IP. |
| 1982 г. | Агентства DCA (Defense Communications Agency) и ARPA (Advanced Research Projects Agency) объединили протокол TCP (Transmission Control Protocol) и протокол IP (Internet Protocol) в набор TCP/IP. |
| 1983 г. | Сеть ARPANET переключилась с протокола NCP на протокол TCP/IP. |
| 1984 г. | Введена *доменная система имен* (Domain Name System, DNS). |

### Протокол Microsoft TCP/IP

Протокол Microsoft TCP/IP в Windows NT 4.0 обеспечивает сетевое взаимодействие компьютеров, работающих под управлением ОС Windows NT, и возможность подключения к ним сетевых устройств и компьютеров под

управлением других ОС. Добавление протокола TCP/IP в конфигурацию Windows NT обеспечивает ряд преимуществ. Основное — TCP/IP оправданно считается наиболее совершенным и распространенным протоколом из всех доступных на сегодняшний день. Все современные ОС поддерживают протокол TCP/IP, и почти все крупные сети используют его для обеспечения большей части своего трафика. Также протокол TCP/IP является стандартным для Интернета.

Другое преимущество технологии TCP/IP — возможность объединения неоднородных систем. Сегодня существует множество утилит доступа и передачи данных, позволяющих взаимодействовать самым различным системам. Некоторые из них, например FTP (File Transfer Protocol) и Telnet, поставляются с ОС Windows NT Server.

Протокол TCP/IP, кроме того, — масштабируемый каркас для разработки приложений, использующих архитектуру клиент/сервер. Применяя протокол TCP/IP, компания Microsoft обеспечивает интерфейс *Сокетов Windows* (Windows Sockets) — стандартный сетевой интерфейс прикладного программирования для приложений Windows. Вы можете применять его для разработки приложений клиент/сервер, действующих на совместимых с Windows Sockets стеках протоколов. Приложения Windows Sockets пользуются всеми преимуществами других сетевых протоколов, например Microsoft NWLink, используемого в сетях Nowell NetWare.

## Процесс стандартизации Интернета

Международная общественная организация, именуемая *Сообществом Интернета* (Internet Society, ISOC), управляет развитием семейства протоколов TCP/IP. Стандарты для TCP/IP публикуются в сериях документов RFC (Request for Comments). Хотя Интернет не является собственностью ни одной организации, некоторые из них отвечают за управление им.

### Сообщество Интернета (ISOC)

Сообщество Интернета образовано в 1992 году и отвечает за технологии межсетевого взаимодействия и использование сети. Поскольку основная цель сообщества — развитие и доступность Интернета, оно регулирует выработку стандартов и протоколов, позволяющих ему функционировать.

### Архитектурная Группа Интернета (IAB)

*Архитектурная Группа Интернета* (Internet Architecture Board, IAB) входит в состав ISOC. Эта консалтинговая техническая группа отвечает за установку стандартов Интернета, публикацию RFC и наблюдение за процессом стандартизации сети.

Группа IAB руководит группами IETF (Internet Engineering Task Force), IANA (Internet Assigned Numbers Authority) и IRTF (Internet Research Task Force). Группа технической поддержки Интернета (IETF) разрабатывает стандарты и протоколы Интернета и решает технические проблемы по мере их возникновения в сети. IANA наблюдает и координирует назначение каждого уникального идентификатора протокола, применяемого в Интернете. Группа IRTF координирует все исследовательские проекты в области TCP/IP.

## Серия документов RFC

Стандарты для протокола TCP/IP публикуются в виде серии документов «Запрос комментариев» (Request for Comments, RFC). Они описывают устройство Интернета. Стандарты TCP/IP всегда публикуются в RFC, но не все RFC описывают стандарты.

Стандарты протоколов TCP/IP разрабатываются не специальной группой, а, скорее, всем сообществом. Любой член ISOC может представить на рассмотрение документ для его публикации в серии RFC. После этого документы просматриваются техническим экспертом, группой разработчиков или редактором RFC, а затем *классифицируются* (assigned a classification). В классификации указывают, обсуждается ли документ в настоящее время, или он уже принят в качестве стандарта. Существует пять типов RFC.

| Классификация | Описание |
|---|---|
| Required (Требуется) | Стандарт должен быть реализован на всех основанных на TCP/IP узлах и шлюзах |
| Recommended (Рекомендуется) | Предлагается реализовать спецификации RFC на всех основанных на TCP/IP-узлах и шлюзах. Рекомендуемые RFC обычно реализуются |
| Elective (Избирательно) | Реализация не обязательна. Применение согласовано, но используется нешироко |
| Limited use (Ограниченное использование) | Не рекомендуется для всеобщего применения |
| Not recommended (Не рекомендуется) | Реализация не рекомендуется |

Если документ рассматривается в качестве потенциального стандарта, то он проходит все стадии разработки, тестирования и утверждения. В процессе стандартизации Интернета они формально именуются *уровнями готовности* (maturity levels). Есть три уровня готовности стандартов Интернета.

| Уровень готовности | Описание |
|---|---|
| Proposed Standard (Предлагаемый стандарт) | Устоявшаяся спецификация, в которой разрешены спорные моменты. Она уже оценена сообществом и считается достаточно перспективной |
| Draft Standard (Черновой стандарт) | Должен быть хорошо понятен и устойчив в качестве основы для последующей реализации |
| Internet Standard (Стандарт Интернета, или просто стандарт) | Характеризуется высокой степенью технической завершенности. Предполагается, что описанный протокол или сервис предоставляет существенные преимущества всем в Интернете |

При публикации документ получает номер RFC. Первоначальный вариант RFC никогда не обновляется. Если RFC нуждается в изменениях, то обновленная версия публикуется под текущим номером. Поэтому важно убедиться в том, что у Вас находится самый «свежий» RFC на интересующую Вас тему. Группа IAB публикует *официальный стандарт протоколов IAB* (IAB Protocol Standard) — ежеквартальную заметку с перечнем самых последних RFC для каждого протокола на текущий момент.

Примечание Ссылки на некоторые RFC Вы встретите в данном курсе. Копии RFC находятся на Web-странице Course Materials прилагаемого к курсу компакт-диска.

## Резюме

TCP/IP — стандартный промышленный набор протоколов, разработанный для глобальных сетей. Добавление протокола TCP/IP в конфигурацию Windows NT обеспечивает ряд преимуществ. Стандарты для TCP/IP публикуются в сериях документов RFC.

# Занятие 2. Утилиты TCP/IP

Windows NT поддерживает ряд утилит, облегчающих использование протоколов нижних уровней. На этом занятии Вы только ознакомитесь с ними. Далее в курсе Вы узнаете больше об этих утилитах и научитесь использовать некоторые из них.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать утилиты TCP/IP, поставляемые вместе с Windows NT.

**Продолжительность занятия — 5 минут**

Утилиты Microsoft TCP/IP работают с протоколами TCP/IP, обеспечивая доступ к другим узлам и Интернету. В ОС Windows NT все утилиты реализованы только как клиентское программное обеспечение, за исключением протокола FTP, реализованного в качестве программного обеспечения и клиента, и сервера.

## Утилиты передачи данных

В ОС Windows NT имеются утилиты для соединения с другими узлами, использующими TCP/IP. Наиболее распространенная утилита передачи данных — FTP. Протокол FTP обеспечивает двустороннюю передачу файлов между узлами TCP/IP, на одном из которых исполняется программное обеспечение FTP-сервера.

Остальные утилиты, используемые для передачи данных, реализуют протоколы Trivial File Transfer Protocol (TFTP) и Remote Copy Protocol (RCP). Первый, подобно FTP, обеспечивает двустороннюю передачу файлов между узлами протокола TCP/IP, один из которых работает под управлением программного обеспечения сервера TFTP. Второй копирует файлы между компьютером, работающим под управлением ОС Window NT и хостом ОС UNIX.

## Утилиты удаленного выполнения

Windows NT также имеет утилиты для соединения и удаленной работы с другими узлами TCP/IP. Наиболее часто используемая утилита удаленного выполнения — Telnet. Она обеспечивает эмуляцию терминала узла TCP/IP, на котором исполняется программное обеспечение сервера Telnet. Кроме того, применяется утилита RSH (Remote Shell), выполняющая команды на хосте ОС UNIX, и REXEC (Remote Execution), запускающая процесс на удаленном компьютере.

## Утилиты печати

Две утилиты TCP/IP отвечают за печать и получение данных о состоянии принтера, поддерживающего TCP/IP. Утилита LPR (Line Printer Remote)

печатает файл, передавая его на узел, где работает сервис LPD (Line Printing Daemon). Утилита LPQ (Line Printer Queue) предоставляет сведения об очереди на печать на узле, где работает сервис LPD.

---

Примечание Эти утилиты требуют наличия специального программного обеспечения на компьютерах клиента и сервера. Microsoft предоставляет ПО серверов FTP и LPD. Более подробно о них — см. главу 14.

---

## Диагностические утилиты

Windows NT 4.0 предоставляет несколько утилит для диагностики неисправностей, характерных для протокола TCP/IP. Изучая этот курс, Вы будете использовать некоторые из них.

| Утилита | Описание |
|---|---|
| Ping (Packet InterNet Groper) | Проверяет корректность конфигурации протокола TCP/IP и доступность другого узла |
| Ipconfig | Проверяет конфигурацию протокола TCP/IP, включая адреса серверов DHCP, DNS и WINS |
| Finger | Получает системную информацию с удаленного компьютера, поддерживающего сервис Finger |
| Nslookup | Позволяет просматривать записи в базе данных сервера DNS, относящиеся к тому или иному узлу или домену |
| Hostname | Возвращает имя локального компьютера для аутентификации |
| Netstat | Отображает статистику протокола и текущее состояние соединений TCP/IP |
| Route | Просматривает или изменяет локальную таблицу маршрутизации |
| Tracert | Прослеживает маршрут от локального до удаленного узла |
| Arp | Отображает локальный кэш соответствий IP-адресов адресам сетевых адаптеров |

## Резюме

ОС Windows NT предоставляет набор утилит, позволяющих соединиться с другим узлами TCP/IP или обнаружить неисправности TCP/IP-соединения.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Что такое TCP/IP?

2. Публикуются ли стандарты протокола TCP/IP в RFC? Все ли RFC описывают стандарты?

# Дополнительная информация

- На Web-странице *Course Materials* прилагаемого к курсу компакт-диска содержится информация технического характера о протоколах TCP/IP.
- Прочитайте обзорную статью, озаглавленную *Microsoft Windows NT 3.5/ 3.51/4.0: Подробности реализации стека протоколов TCP/IP и его сервисов* (Microsoft Windows NT 3.5/3.51/4.0: TCP/IP Implementation Details, TCP/IP Protocol Stack and Services, Version 2.0).
- Прочитайте книгу «Межсетевое взаимодействие с использованием TCP/IP», том I, Дуглас Е. Комер (Internetworking with TCP/IP Volume I, by Douglas E. Comer).

# Установка и конфигурация TCP/IP



## В этой главе

В этой главе Вам предложен обзор процедур для установки и ручной конфигурации IP-адреса, маски подсети и шлюза по умолчанию. Вы установите и настроите вручную протокол Microsoft TCP/IP. Кроме того, Вы узнаете об основных процедурах тестирования конфигурации с использованием утилит Ipconfig, Ping и Microsoft Network Monitor.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- настроить Ваш(и) компьютер(ы), как это описано в разделе «Инструкции по установке» статьи «Об этой книге».

# Занятие 1. Установка и настройка Microsoft TCP/IP

Занятие посвящено установке Microsoft TCP/IP. Если Вы ранее не устанавливали сетевой протокол TCP/IP на компьютер(ы), используемые Вами для выполнения упражнений курса, то попрактикуйтесь здесь.

**Изучив материал этого занятия, Вы сможете:**

- ✓ установить и настроить протокол Microsoft TCP/IP.

**Продолжительность занятия — 20 минут**

При установке TCP/IP создается несколько системных файлов и файлов разрешения имен в каталогах System32\Drivers и System32\Drivers\Etc Вашей ОС Windows NT. TCP/IP использует файлы разрешения имени, перечисленные ниже. О них — см. далее.

| Файл конфигурации | Описание |
|---|---|
| HOSTS | Обеспечивает разрешение имен узлов в IP-адреса |
| LMHOSTS | Обеспечивает разрешение имен NetBIOS в IP-адреса |
| NETWORKS | Обеспечивает разрешение имен сетей в идентификаторы сетей |
| PROTOCOL | Преобразует имя протокола в идентификатор протокола, заданный в RFC. Номер протокола — поле в заголовке IP-пакета, идентифицирующее, какому протоколу верхнего уровня (например, TCP или UDP) будут переданы данные протокола IP |
| SERVICES | Обеспечивает преобразование имени сервиса в номер порта и имя протокола. Номер порта — это поле в заголовке TCP или UDP-пакета, идентифицирующее процесс, использующий TCP или UDP |

## Параметры конфигурации

Протокол TCP/IP использует IP-адрес, маску подсети и шлюз по умолчанию для соединения с узлами. Узлы TCP/IP, работающие в глобальной сети, требуют задания всех трех параметров в конфигурации. Каждая

плата сетевого адаптера в компьютере, использующем TCP/IP, нуждается в этих параметрах.

### IP-адрес

IP-адрес — это логический 32-разрядный адрес, однозначно определяющий узел TCP/IP. Каждый IP-адрес состоит из двух частей: идентификатора сети и идентификатора узла. Первый служит для обозначения всех узлов в одной физической сети. Второй обозначает конкретный узел сети. Каждому компьютеру, использующему TCP/IP, требуется уникальный IP-адрес, например 131.107.2.200.

О назначении IP-адресов — см. главу 4.

### Маска подсети

Маска подсети выделяет часть IP-адреса и позволяет TCP/IP отличить идентификатор сети от идентификатора узла. Пытаясь связаться, узлы TCP/IP используют маску подсети (например, 255.255.255.0), чтобы определить, находится узел-получатель в локальной или удаленной сети. В главе 5 объясняется, как правильно назначать маску подсети.

### Шлюз по умолчанию

Для того чтобы установить соединение с узлом из другой сети, Вы должны сконфигурировать IP-адрес шлюза по умолчанию. TCP/IP посылает пакеты, предназначенные для удаленных сетей, на шлюз по умолчанию только в том случае, если на локальном узле не сконфигурирован другой маршрут к сети получателя. Если Вы не сконфигурируете шлюз по умолчанию, то связь может быть ограничена локальной сетью. Например, адрес шлюза по умолчанию — 131.107.2.1.

## Упражнения

Вы установите и сконфигурируете протокол TCP/IP при помощи программы **Network**, в **Control Panel**. В первую очередь просмотрите установленные на Ваш компьютер сетевые протоколы. Если протокола TCP/IP среди них нет, установите его.

---

Примечание Если у Вас два сетевых компьютера, эту операцию придется выполнить на каждом из них.

---

▶ **Просмотр сетевых протоколов на Вашем компьютере**

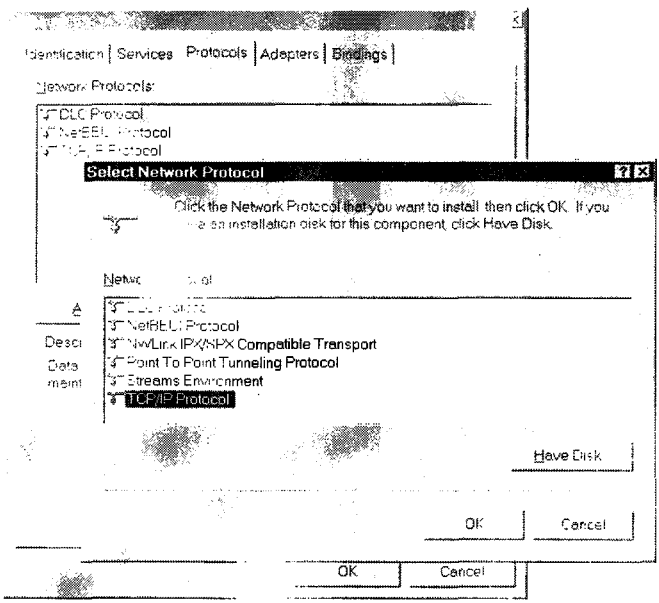
1. Зарегистрируйтесь в системе как *Administrator*.
2. Щелкните кнопку **Start**, подведите указатель к пункту **Settings**, затем щелкните строку **Control Panel**.

   Появится окно **Control Panel**.

3. Дважды щелкните пиктограмму **Network**.
   Появится диалоговое окно **Network**.
4. Щелкните вкладку **Protocols**.
   Если протокола TCP/IP нет в списке установленных сетевых протоколов, выполните следующую инструкцию.

▶ **Установка протокола Microsoft TCP/IP в ОС Windows NT 4.0**

1. Щелкните кнопку **Add** во вкладке **Protocols**.
   Появится диалоговое окно **Select Network Protocol**.
2. Выберите **TCP/IP Protocol**, затем щелкните **OK**.
   Появится диалоговое окно **DHCP Server**.




Примечание Далее, выполняя инструкцию, Вы вручную сконфигурируете параметры протокола TCP/IP. Подробнее о сервисе DHCP — см. главу 7.

3. Щелкните кнопку **No**.
   Появится диалоговое окно **Windows NT Setup**, запрашивающее полный путь к установочным файлам ОС Windows NT.
4. Наберите полный путь к установочным файлам ОС Windows NT Server.

5. Щелкните кнопку **Continue**.

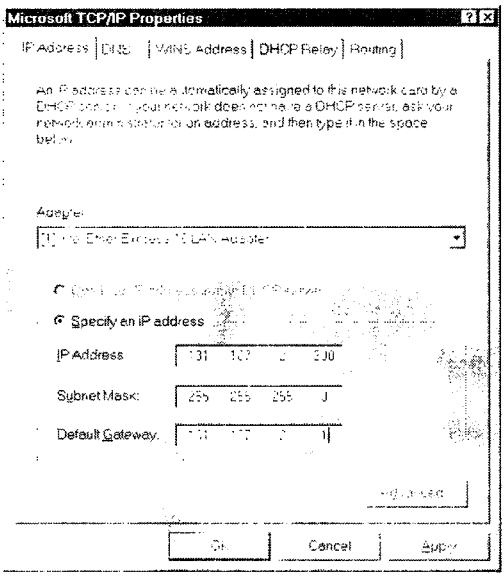
   Программа Setup установит файлы, найденные по указанному пути.
6. Щелкните кнопку **Close**.

   Появится диалоговое окно **Microsoft TCP/IP Properties**.
7. Если сервер DHCP недоступен, то Вы можете сконфигурировать IP-адрес, маску подсети и шлюз по умолчанию вручную. Если Вам необходимо связываться с узлами вне локальной сети, назначьте шлюз по умолчанию. Задайте параметры конфигурации протокола TCP/IP, как описано в таблице.

Внимание! Если Ваш(и) компьютер(ы) включены в большую сеть, Вы должны вместе с сетевым администратором убедиться, что имена компьютеров, имя домена и информация об IP-адресе не конфликтуют с сетью. В случае конфликта попросите Вашего сетевого администратора предоставить другие параметры для выполнения практических упражнений данного курса.

| Параметр | Описание |
|---|---|
| IP address (IP-адрес) | IP-адрес является обязательным параметром. Если Вы конфигурируете два сетевых компьютера для выполнения упражнений, укажите IP-адрес для Server1 — 131.107.2.200, а для Server2 — 131.107.2.211 |
| Subnet mask (Маска подсети) | Обязательный параметр. Если Вы конфигурируете свои компьютеры для выполнения упражнений, то укажите маску подсети — 255.255.255.0 |
| Default gateway (Шлюз по умолчанию) | Шлюз по умолчанию — необязательный параметр. Его можно опустить при условии, что Вы не связываетесь с узлами в удаленной сети. Если Вы конфигурируете Ваши компьютеры для выполнения упражнений, то этот параметр должен быть 131.107.2.1 |

Примечание Соединения протокола IP могут не работать, если несколько устройств используют один IP-адрес.




8. Щелкните **OK**.

   Появится диалоговое окно **Network Settings Change** с предложением перезапустить компьютер.

9. Щелкните **Yes**.

   Компьютер перезапустится с новыми параметрами.

## Резюме

Во время установки TCP/IP некоторые системные файлы и файлы разрешения имен копируются в подкаталоги основного каталога Вашей ОС Windows NT. Если Вы настраиваете параметры протокола TCP/IP вручную, то должны задать IP-адрес и маску подсети.

# Занятие 2. Тестирование TCP/IP при помощи утилит Ipconfig и Ping

После того как Вы установите протокол TCP/IP, полезно проверить и протестировать конфигурацию и все соединения с другими узлами TCP/IP и сетями. На этом занятии объясняются основы тестирования конфигурации TCP/IP с использованием утилит Ipconfig и Ping.

**Изучив материал этого занятия, Вы сможете:**

- ✓ проверить параметры конфигурации TCP/IP при помощи утилиты Ipconfig;
- ✓ протестировать конфигурацию TCP/IP и соединения протокола IP при помощи утилиты Ping.

**Продолжительность занятия — 10 минут**

## Утилита Ipconfig

Используйте утилиту Ipconfig для проверки параметров конфигурации узла, включая IP-адрес, маску подсети и шлюз по умолчанию. Это полезно при выяснении, успешно ли прошла инициализация TCP/IP и не дублируется ли IP-адрес, указанный в конфигурации. Синтаксис команды:

```
ipconfig
```

Если протокол инициализировался успешно с заданной конфигурацией, то на экране отобразится IP-адрес, маска подсети и шлюз по умолчанию. Если адрес, заданный в конфигурации уже используется другим узлом в сети на том же сегменте, то отобразится заданный IP-адрес, но маска подсети будет равна 0.0.0.0*.

---

Примечание Утилита Winipcfg, входящая в состав ОС Windows 95, также проверяет конфигурацию протокола TCP/IP.

---

## Утилита Ping

После проверки конфигурации утилитой Ipconfig Вы можете запустить утилиту Ping (Packet InterNet Groper) для тестирования соединений. Это диагностическое средство тестирует конфигурации TCP/IP и позволяет опре-

---

* Если при загрузке операционной системы обнаруживается, что заданный IP-адрес уже используется, то даже после его изменения в конфигурации протокол не инициализируется, пока система не будет перезагружена. — *Прим. перев.*

делить неисправности соединения. Утилита Ping использует пакеты *эхо-запроса* (echo request) и *эхо-ответа* (echo reply) протокола ICMP (Internet Control Message Protocol) для проверки доступности и работоспособности определенного узла TCP/IP. Синтаксис команды:

```
ping IP_адрес
```

Если проверка прошла успешно, то отобразится сообщение типа:

```
Pinging IP_адрес with 32 bytes of data:
Reply from IP_адрес: bytes= x time<10ms TTL= x
Reply from IP_адрес: bytes= x time<10ms TTL= x
Reply from IP_адрес: bytes= x time<10ms TTL= x
Reply from IP_адрес: bytes= x time<10ms TTL= x
```

## Упражнение

Вы используете Ipconfig для просмотра конфигурации протокола IP и утилиту Ping для тестирования конфигурации Вашей рабочей станции и соединений с другим узлом протокола TCP/IP.

---

Примечание Для выполнения части упражнений Вам необходим второй сетевой компьютер. Предварительно просмотрите раздел «Инструкции по установке» статьи «Об этой книге». Выполняйте задание на компьютере, сконфигурированном как Server1.

---

▶ **Проверка конфигурации компьютера и тестирование соединений маршрутизатора**

1. Используйте утилиту Ipconfig для проверки инициализации Вашей конфигурации протокола TCP/IP. Наберите в командной строке:

   ```
   ipconfig
   ```

   Если конфигурация инициализирована корректно, то отобразятся IP-адрес, маска подсети и шлюз по умолчанию (если сконфигурирован).
2. Выполните Ping для адреса локальной заглушки, чтобы проверить корректность установки и загрузки протокола TCP/IP. Наберите в командной строке:

   ```
   ping 127.0.0.1
   ```

   Затем нажмите ENTER.

Примечание Адрес локальной заглушки (127.0.0.1) использует драйверы локальной заглушки для маршрутизации исходящих пакетов обратно на компьютер-отправитель. Эти драйверы полностью обходят плату сетевого адаптера. Если Вы работаете на компьютере, не подключенном к сети, можно использовать адрес локальной заглушки для большинства упражнений данного курса.

3. Выполните Ping на IP-адрес Вашего компьютера, чтобы проверить его корректность. Наберите:

   ```
   ping 131.107.2.200
   ```

4. Выполните Ping на IP-адрес *второго* Вашего компьютера для проверки возможности связи с узлом в локальной сети. Наберите:

   ```
   ping 131.107.2.211
   ```

5. При наличии удаленного узла выполните Ping на его IP-адрес для проверки возможности связи через маршрутизатор. Наберите:

   ```
   ping IP_адрес_удаленного_узла
   ```

Совет Если вызов утилиты Ipconfig покажет, что протокол TCP/IP установлен правильно и использует корректный IP-адрес, то Вам не надо выполнять пункты 2 и 3.

Если Вы начали с пункта 5 и Ping осуществлен успешно, то пункты 2–4 выполнять не надо, так как результат будет положительным в любом случае.

Если адрес некорректен, или протокол TCP/IP сконфигурирован неправильно, утилита Ping прекратит работу по истечении определенного времени.

## Резюме

Утилиты Ipconfig и Ping помогут Вам протестировать Вашу конфигурацию после установки протокола TCP/IP. Утилита Ipconfig проверяет IP-адрес, маску подсети и шлюз по умолчанию. Утилита Ping тестирует соединения и диагностирует их неисправности.

# Занятие 3. Microsoft Network Monitor

Microsoft Network Monitor упрощает поиск сложных сетевых неисправностей. На этом занятии Вам предлагается обзор данных средств, а используете Вы их в главе 3.

**Изучив материал этого занятия, Вы сможете:**

- ✓ установить и сконфигурировать Microsoft Network Monitor.

**Продолжительность занятия – 15 минут**

Microsoft Network Monitor производит поиск сетевых неисправностей, отслеживая и анализируя сетевой трафик, и при этом конфигурирует плату сетевого адаптера для перехвата всех входящих и исходящих пакетов.

Вы можете задать фильтры перехвата, чтобы сохранить только определенные кадры для анализа. Или же задать фильтры на основе адресов сетевых адаптеров отправителя и получателя, адресов протокола отправителя и получателя и образцов для сравнения. Фильтрование перехваченных пакетов повышает эффективность поиска неисправностей. Перехватывая и фильтруя пакеты, Network Monitor интерпретирует захваченные данные и предоставляет отчет в реальном времени.

---

Примечание Версия Network Monitor, входящая в состав ОС Windows NT, предназначена для перехвата данных только на локальном компьютере. Полная версия доступна вместе с Microsoft Systems Management Server, позволяющим централизованно управлять распределенными системами.

---

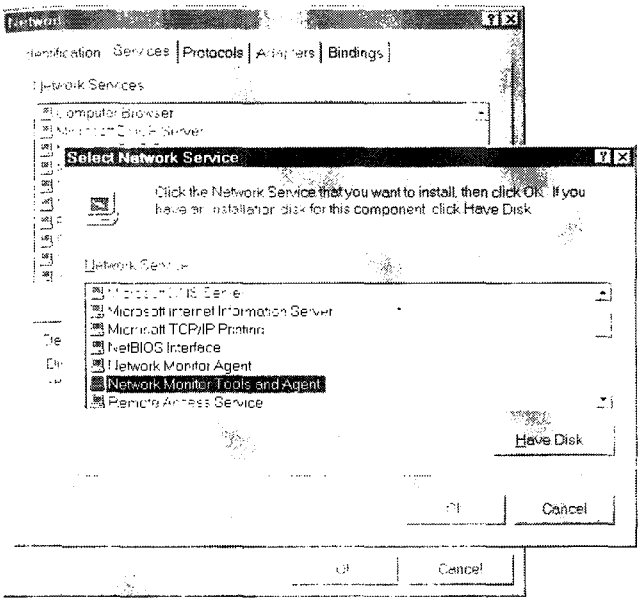
## Упражнение

Вы установите Network Monitor, используя вкладку **Services** программы **Network**. Это подготовит Ваш(и) компьютер(ы) для просмотра пакетов в упражнении главы 3.

▶ **Установка Network Monitor**

1. Зарегистрируйтесь в системе как *Administrator*.
2. Дважды щелкните пиктограмму **Network** в **Control Panel**, затем — вкладку **Services**.
3. Щелкните кнопку **Add**.

   Появится диалоговое окно **Select Network Service**.




4. Щелкните строку **Network Monitor Tools and Agent** в списке **Network Service**, затем — кнопку **OK**.

   Windows NT Setup отобразит диалоговое окно с запросом полного пути к установочным файлам ОС Windows NT.
5. Наберите путь к установочным файлам, затем щелкните **Continue**.
6. В диалоговом окне **Network** щелкните кнопку **Close**.
7. Щелкните **Yes** в ответ на приглашение перезапустить компьютер.

## Анализ сетевого трафика

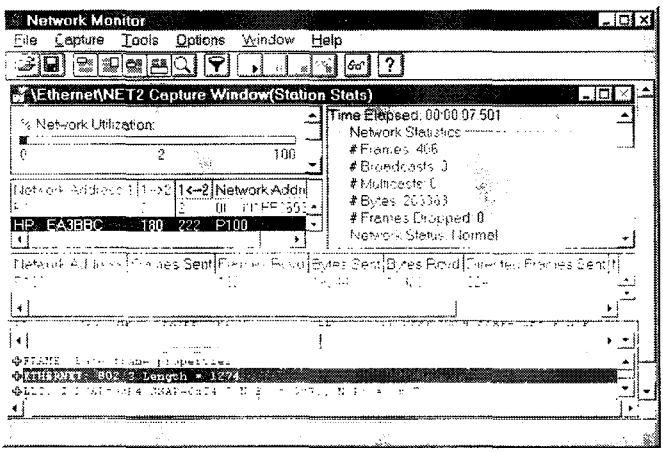
Для анализа сетевого трафика при помощи Network Monitor Вам необходимо запустить процесс захвата, сгенерировать любой сетевой трафик, затем остановить захват и просмотреть данные. Для использования Network Monitor щелкните кнопку **Start**, укажите на **Programs**, затем — на **Administrative Tools** и щелкните **Network Monitor**.

### Запуск перехвата

Network Monitor использует множество окон для отображения данных. Одно из основных — окно **Capture**. Когда оно активно, на панели инструментов доступны функции запуска, паузы, остановки или остановки с просмотром перехваченных данных. В меню **Capture** щелкните **Start** для начала перехвата. В процессе перехвата Network Monitor отображает статистическую информацию в окне **Capture**.

## Остановка перехвата

После того как Вы сгенерируете сетевой трафик, щелкните **Stop** в меню **Capture** для остановки перехвата. Вы можете организовать другой перехват или отобразить захваченные данные. Щелкните **Stop and View** в меню **Capture** для остановки перехвата и немедленного просмотра данных.




## Просмотр данных

При просмотре перехваченных данных появляется окно **Summary**, которое отображает каждый перехваченный кадр и показывает номер кадра, время приема и адреса отправителя и получателя. Оно также указывает протокол самого высокого уровня, используемый в кадре, и описание кадра*.

Для получения более подробной информации о конкретном окне щелкните кнопкой мыши **Zoom** в меню **Window**. В режиме просмотра **Zoom** появятся два дополнительных окна — **Detail** и **Hexadecimal**. Первое отображает подробную информацию о протоколе, второе — собственно байты захваченного кадра.

---

Примечание Вы воспользуетесь Network Monitor для просмотра пакетов в главе 3.

---

* Зачастую на практике порядок отображения перехваченных кадров в списке не вполне соответствует реальному. Недостатком Network Monitor является то, что кадры, следующие друг за другом с очень малым интервалом, при демонстрации часто помешаются в обратном порядке. Поэтому относитесь внимательно к перехваченным данным. — *Прим. перев.*

## Резюме

Network Monitor помогает найти серьезные сетевые неисправности. Использование Network Monitor проходит в 3 этапа: запуск процесса перехвата, генерирование сетевого трафика и остановка перехвата для просмотра данных.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие утилиты используются для проверки и тестирования конфигурации TCP/IP?

2. Какие параметры должны в обязательном порядке назначаться компьютеру с ОС Windows NT, использующему TCP/IP в глобальной сети?

# Дополнительная информация

- Прочитайте документацию программного продукта Microsoft Network Monitor.

# Обзор архитектуры стека протоколов TCP/IP



## В этой главе

В этой главе описываются уровни стека протоколов TCP/IP и подробно объясняется, как протоколы каждого уровня взаимодействуют с остальными. Два видеоролика познакомят Вас с TCP/IP. В ходе занятий Вы просмотрите и обновите кэш протокола ARP (Address Resolution Protocol) и увидите сетевые пакеты при помощи Network Monitor.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить ОС Windows NT Server 4.0 с протоколом TCP/IP;
- установить сервис Network Monitor Tools and Agent Network (см. гл. 2);
- найти прилагаемый компакт-диск с мультимедийной презентацией.

Желательно приобрести звуковую плату, а также наушники или колонки.

# Занятие 1. Стек протоколов Microsoft TCP/IP

На этом занятии описываются четыре уровня *стека протоколов TCP/IP* (TCP/IP protocol suite) и объясняется внутренняя работа протоколов каждого уровня, а также их взаимодействие с остальными протоколами. Перед началом занятия посмотрите видеоролик, описывающий TCP/IP.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать TCP/IP с помощью четырехуровневой модели;
- ✓ перечислить протоколы уровня сетевого интерфейса, поддерживаемые протоколом IP (Internet Protocol).

**Продолжительность занятия — 30 минут**

## Видеоролик: обзор семейства протоколов TCP/IP

В этом 15-минутном видеоролике представлен обзор стека протоколов TCP/IP компании Microsoft и других фирм, описано их представление в виде четырехуровневой модели, рассказано о работе протоколов каждого уровня, а также о их взаимодействии с другими протоколами.

▶ **Запуск видеоролика**

1. Вставьте прилагаемый к курсу компакт-диск в CD-ROM-дисковод — запустится Microsoft Internet Explorer и откроется страница *The Internetworking with Microsoft TCP/IP on Windows NT 4.0*,

   или

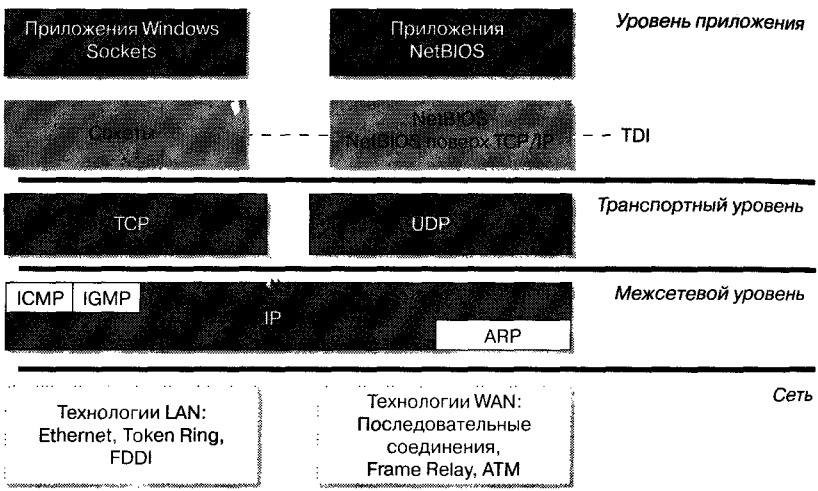
   запустите Microsoft Internet Explorer, перейдите на прилагаемый к курсу компакт-диск и дважды щелкните файл Open.htm.
2. Щелкните пиктограмму начальной страницы.
3. Щелкните **Course Materials**.
4. Щелкните **Multimedia Presentation**.
5. Щелкните **Overview of the TCP/IP Protocol Suite**.

   Появится диалоговое окно Internet Explorer с вопросом, хотите Вы открыть файл или записать его на диск.
6. Выберите **Open it**, затем щелкните **OK**.
7. Если на экране появится диалоговое окно системы безопасности, щелкните в нем кнопку **OK**.

   Начнется показ видеоролика. Если на Вашем компьютере нет звуковой платы и динамиков, то щелкните **Text On**.

## Четырехуровневая модель

Протоколы семейства TCP/IP можно представить в виде модели, состоящей из четырех уровней: *приложения* (Application layer), *транспортного* (Transport layer), *межсетевого, или уровня Интернета* (Internet layer), и *сетевого интерфейса* (Network Interface layer). Основные протоколы Microsoft TCP/IP — это набор стандартов для соединения компьютеров и межсетевого взаимодействия.




### Уровень сетевого интерфейса

В основе этой модели лежит уровень сетевого интерфейса. Соответствующие ему компоненты отвечают за отправку и прием из сети кадров, содержащих пакеты информации. Кадры передаются по сети как единое целое.

### Межсетевой уровень

Протоколы Интернета инкапсулируют пакеты данных в датаграммы Интернета* и проводят необходимую маршрутизацию. Четыре основных протокола Интернета предназначены:

- IP (Internet Protocol) — в основном для отправки и маршрутизации пакетов между сетями и узлами;
- ARP (Address Resolution Protocol) — для получения адресов сетевых адаптеров узлов в рамках одной физической сети;

* Транспортируемые независимо от других массивы данных, далее — пакеты. — *Прим. перев.*

- ICMP (Internet Control Message Protocol) — для отправки извещений и сообщений об ошибках, связанных с доставкой пакетов;
- IGMP (Internet Group Management Protocol) используется IP-узлами для сообщения поддерживающим групповую передачу маршрутизаторам о своем участии в группах.

### Транспортный уровень

Транспортный уровень обеспечивает сеансы связи между компьютерами. Существуют два транспортных протокола: TCP (Transmission Control Protocol) и UDP (User Datagram Protocol). Использование одного из них зависит от выбранного метода доставки данных.

TCP ориентирован на соединение и используется приложениями, обычно передающими большие объемы данных за одну операцию, так как обеспечивает надежное соединение, а также теми приложениями, которым необходимо подтверждение приема данных.

Протокол UDP обеспечивает не ориентированную на соединение передачу данных и не гарантирует доставку пакетов. Приложения, использующие протокол UDP, обычно передают небольшие объемы данных за одну операцию. Ответственность за надежную доставку данных несет само приложение.

### Уровень приложения

Это уровень, на котором приложения получают доступ к сетевым компонентам. Здесь работает множество стандартных утилит и сервисов протокола TCP/IP, например FTP, Telnet, SNMP и DNS.

Протокол Microsoft TCP/IP предоставляет сетевым приложениям два различных интерфейса к сервисам TCP/IP. Первый из них — *Сокеты Windows* (Windows Sockets) — обеспечивает стандартный *интерфейс прикладного программирования* (API) под Microsoft Windows для работы с такими транспортными протоколами, как TCP/IP и IPX. Второй — NetBIOS — стандартный интерфейс к протоколам, поддерживающим имена и сообщения NetBIOS, например TCP/IP и NetBEUI*.

## Технологии сетевых интерфейсов

Протокол IP использует *спецификацию интерфейса сетевого драйвера* (Network Driver Interface Specification, NDIS) для передачи кадров модулям уровня сетевого интерфейса. IP поддерживает технологии сетевых интерфейсов как для локальных (LAN), так и для глобальных (WAN) сетей.

* NWLink в Windows NT тоже поддерживает NetBIOS-интерфейс. — *Прим перев.*

Поддерживаемые протоколом TCP/IP технологии LAN включают Ethernet (Ethernet II и 802.3), Token Ring, ArcNet и технологии MAN (Metropolitan Area Network), например FDDI.

Для использования TCP/IP в глобальных сетях требуется служба удаленного доступа Windows NT RAS (Remote Access Service) или дополнительное аппаратное обеспечение. Существует две основные категории оборудования WAN, поддерживаемого протоколом TCP/IP: *последовательные линии связи* (serial lines) и *сети с коммутацией пакетов* (packet-switched networks). Последние включают технологию X.25, *сети с ретрансляцией кадров* (frame relay) и сети асинхронной передачи (ATM).

### Протоколы последовательной линии

По телефонным линиям данные TCP/IP обычно передаются при помощи SLIP (Serial Line Internet Protocol) или PPP (Point-to-Point Protocol).

Протокол SLIP — промышленный стандарт, разработанный в начале 80-х годов для поддержки TCP/IP при соединении через низкоскоростные последовательные интерфейсы. Применяя службу Windows NT RAS, компьютеры под управлением Windows NT могут использовать протоколы TCP/IP и SLIP для связи с удаленными узлами.

---

Примечание Windows NT поддерживает только клиентскую часть протокола SLIP, но не SLIP-сервер. Серверы Windows NT RAS не могут устанавливать соединения со SLIP-клиентами.

---

Протокол PPP, разработанный как расширение SLIP, является *протоколом канального уровня* (data-link protocol) и обеспечивает стандартный метод передачи сетевых пакетов через *соединение типа «точка-точка»* (point-to-point link). Поскольку протокол PPP обеспечивает лучшую защиту, управление конфигурацией и обнаружение ошибок, чем протокол SLIP, на последовательных линиях рекомендуется использовать именно его.

Примечание Передача данных протокола IP по телефонным линиям описана в RFC 1055. Протокол PPP описан в RFC 1547 и 1661. Копии этих документов находятся на Web-странице Course Materials прилагаемого к курсу компакт-диска.

---

## Резюме

TCP/IP можно представить в виде четырехуровневой концептуальной модели, состоящей из следующих уровней: приложения, транспортного, Интернета (межсетевого) и сетевого интерфейса. Протокол IP можно использовать как в локальных, так и в глобальных сетях.

# Занятие 2. Протокол ARP

Для того чтобы установить соединение, узлам должны быть известны адреса сетевых адаптеров других узлов. *Разрешение адреса* (address resolution) — это процесс определения аппаратного адреса сетевого адаптера по его IP-адресу. Протокол ARP (Address Resolution Protocol) — часть уровня Интернета модели TCP/IP — позволяет определять адреса сетевых адаптеров узлов, расположенных в одной физической сети.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как протокол ARP преобразует IP-адрес в адрес сетевого адаптера;
- ✓ объяснить, как протокол ARP добавляет и удаляет записи из своего кэша;
- ✓ просмотреть и изменить кэш протокола ARP.

**Продолжительность занятия — 45 минут**

Протокол ARP нужен для получения адресов сетевых адаптеров TCP/IP-узлов в сетях, поддерживающих широковещание. Он использует широковещательные запросы, содержащие IP-адрес получателя, чтобы выяснить адрес сетевого адаптера этого узла или адрес необходимого шлюза.

Получив адрес сетевого адаптера, ARP сохраняет его вместе с соответствующим IP-адресом в своем кэше. Протокол ARP перед формированием широковещательного ARP-запроса всегда ищет в кэше адрес IP и сетевого адаптера.

*Обратное разрешение адреса* (reverse address resolution) — отображение адреса сетевого адаптера узла в его IP-адрес. Microsoft TCP/IP этот механизм не поддерживает.

Примечание Протокол ARP описан в RFC 826. Копия этого документа находится на Web-странице Course Materials прилагаемого к курсу компакт-диска.

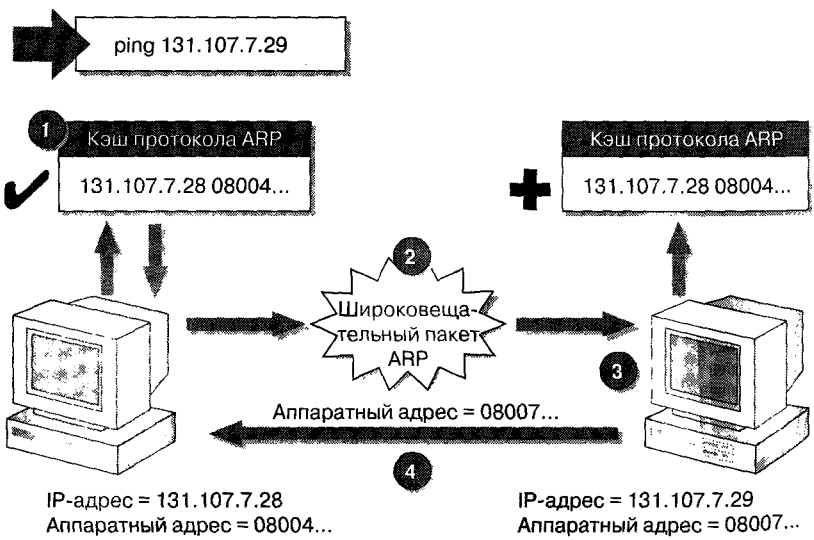
## Разрешение локального IP-адреса

Перед соединением двух узлов IP-адрес каждого из них должен быть преобразован в адрес сетевого адаптера. Этот процесс состоит из выполнения ARP-запроса и получения ARP-ответа.

1. ARP-запрос формируется каждый раз при попытке одного узла связаться с другим.

Если протокол IP определит, что IP-адрес принадлежит локальной сети, узел-отправитель ищет адрес узла-получателя в своем ARP-кэше.

2. Если он не найден, протокол ARP формирует запрос типа «Чей это IP-адрес и каков Ваш адрес сетевого адаптера?», в который также включаются адреса IP и сетевого адаптера узла-отправителя. ARP-запрос посылается в широковещательном режиме, чтобы все узлы в локальной сети могли принять и обработать его.
3. Каждый узел в локальной сети получает этот широковещательный запрос и сравнивает указанный в нем IP-адрес со своим собственным. Если они не совпадают, запрос игнорируется.
4. Узел-получатель определяет, что IP-адрес в запросе совпадает с его собственным, он посылает на узел-отправитель ARP-ответ, в котором указывает свой адрес сетевого адаптера. Затем он обновляет свой ARP-кэш, занося в него соответствие IP-адреса узла-отправителя адресу его сетевого адаптера. После того как узел-отправитель получает ARP-ответ, соединение может быть установлено.




## Разрешение удаленного IP-адреса

Протокол ARP также позволяет связываться двум узлам из различных сетей. В этом случае широковещательный ARP-запрос обеспечивает возможность выяснить адрес используемого отправителем шлюза по умолчанию, а не узла-получателя.

Если получатель находится в удаленной сети, то широковещательный ARP-запрос используется для поиска маршрутизатора, который может пересылать пакеты в эту сеть.

1. При соединении определяется, что IP-адрес узла-получателя принадлежит удаленной сети.

   Узел-отправитель ищет в локальной таблице маршрутизации путь к узлу-получателю или его сети. Если путь не найден в таблице, узел-отправитель определяет IP-адрес шлюза по умолчанию. Затем он ищет в кэше протокола ARP соответствующий ему адрес сетевого адаптера.

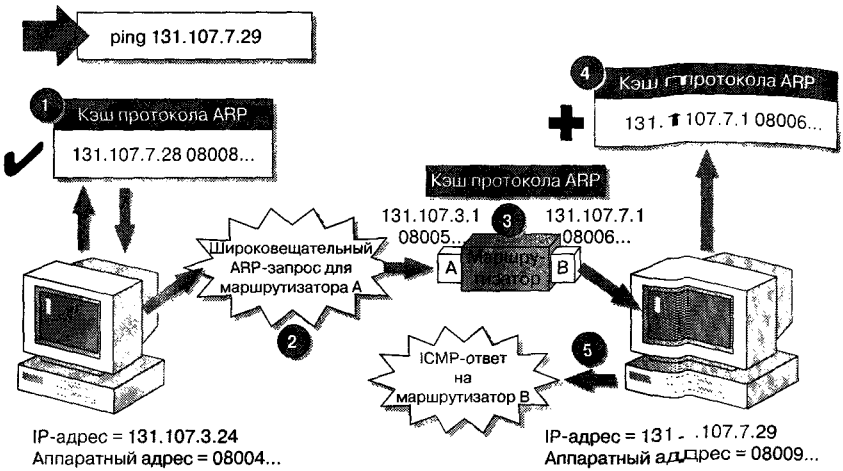
2. Если этот адрес в кэше отсутствует, то широковещательный ARP-запрос используется для получения адреса шлюза.

   Маршрутизатор (шлюз) в ответ на ARP-запрос узла-отправителя посылает адрес своего сетевого адаптера. Затем узел-отправитель адресует пакет на маршрутизатор для доставки его в сеть получателя и далее — узлу-получателю.

3. На маршрутизаторе выясняется, является ли IP-адрес получателя локальным или удаленным. Если он локальный, маршрутизатор использует протокол ARP (кэш или широковещание) для получения его адреса сетевого адаптера. Если же удаленный, маршрутизатор ищет в своей таблице маршрутизации необходимый шлюз, а затем использует протокол ARP (кэш или широковещание) для получения адреса его сетевого адаптера. Далее пакет отправляется непосредственно следующему получателю в этой цепочке.

4. Когда пакет достигнет получателя и будет обработан им, все исходящие пакеты таким же образом будут доставлены обратно. Например, при выполнении команды Ping в ответ на эхо-запрос узел-получатель пакета формирует *эхо-ответ протокола ICMP* (ICMP echo-reply). Поскольку узел-отправитель находится в удаленной сети, в локальной таблице маршрутизации ищется адрес шлюза к сети узла-отправителя. Если поиск завершается успешно, адрес сетевого адаптера шлюза выясняется с помощью ARP.

5. Если адреса сетевого адаптера указанного шлюза нет в кэше протокола ARP, то для его определения используется широковещательный ARP-запрос. Как только адрес получен, эхо-ответ протокола ICMP посылается на маршрутизатор, который перенаправляет его на исходный узел-отправитель.




## Кэш протокола ARP

Для уменьшения числа широковещательных пакетов ARP кэширует адреса для последующего использования. Применяется два типа записей в кэше ARP — динамические (добавляются и удаляются автоматически) и статические (находятся в кэше до перезагрузки компьютера).

В дополнение к этому в кэше протокола ARP всегда присутствует адрес для широковещания в локальной подсети (FFFFFFFFFFFF) в виде статической записи, которая не отображается при просмотре кэша.

По умолчанию для кэша протокола ARP установлены тайм-ауты, равные 2 минутам для невостребованных записей и 10 минутам для записей, к которым обращались. Если в реестр добавить параметр **ARPCacheLife** и задать тайм-аут в секундах, именно эта величина будет использоваться вместо упомянутых.

---

Примечание В некоторых реализациях TCP/IP при повторном использовании записи ей присваивается новая отметка о времени поступления, которая добавляет дополнительные 10 минут ко времени ее жизни. В Windows NT 4.0 эта функция не реализована.

---

### Добавление статических (постоянных) записей

Добавление статической ARP-записи уменьшает количество ARP-запросов для узлов, к которым обращаются достаточно часто. На компью-

тере, работающем под управлением Windows NT 4.0, статическая запись, добавленная в кэш ARP, доступна до:

- перезагрузки компьютера;
- удаления записи вручную при помощи команды *arp -d*;
- получения в широковещательном ARP-сообщении другого адреса сетевого адаптера (при этом тип записи меняется со статического на динамический и полученный в сообщении адрес заменяет текущий).

Примечание Если Вы вручную помещаете запись в кэш протокола ARP, адрес сетевого адаптера в команде arp следует разделять дефисами.

## Структура ARP-пакета

Хотя протокол ARP был разработан для разрешения именно IP-адресов, структура ARP-пакета может быть использована и для разрешения адресов других типов. Кадрам, содержащим ARP-пакеты, в поле EtherType соответствует значение 0x08-06. Поля пакета ARP показаны в таблице.

| Поле | Описание |
|---|---|
| Hardware Type (Тип аппаратного обеспечения) | Задается тип используемого сетевого оборудования (Network Access Layer), например Ethernet |
| Protocol Type (Тип протокола) | С помощью значений поля EtherType кадра Ethernet задается используемый при разрешении адресов протокол. Для протокола IP значение поля Protocol Type равно 0x08-00 |
| Hardware Address Length (Длина адреса сетевого адаптера) | Задается длина адреса сетевого адаптера в байтах. Для Ethernet и Token Ring длина равна 6 байтам |
| Protocol Address Length (Длина адреса протокола) | Задается длина адреса протокола в байтах. Для протокола IP длина равна 4 байтам |
| Operation (Opcode) [Операция (Код операции)] | Задается выполняемая операция |
| Sender's Hardware Address (Адрес сетевого адаптера отправителя) | Задается адрес сетевого адаптера отправителя |
| Sender's Protocol Address (Адрес протокола отправителя) | Задается адрес протокола отправителя |

(*продолжение*)

| Поле | Описание |
|---|---|
| Target's Hardware Address (Адрес сетевого адаптера получателя) | Задается адрес сетевого адаптера получателя |
| Target's Protocol Address (Адрес протокола получателя) | Задается адрес протокола получателя |

## Упражнения

Вы используете Network Monitor для захвата и просмотра пакетов протокола ARP. Затем Вы изучите ARP-запрос и ARP-ответ.

---

Примечание Для выполнения упражнения Вам потребуются два сетевых компьютера, описанных в разделе «Об этой книге». Выполняйте задание на компьютере, сконфигурированном как Server1.

---

▶ **Запуск Network Monitor**

1. Зарегистрируйтесь в системе как *Administrator*.
2. Щелкните кнопку **Start**, выберите **Programs**, укажите на **Administrative Tools**, затем щелкните **Network Monitor**.

   Появится окно **Network Monitor**.
3. Разверните окно **Network Monitor** до максимального размера.
4. Разверните окно **Capture** до максимального размера.

▶ **Перехват сетевых данных**

1. Щелкните кнопку **Start** в меню **Capture**.

   Начнется перехват данных. **Network Monitor** зарезервирует для них буфер и начнет перехват кадров.
2. В командной строке наберите:

```
ping 131.107.2.211
```

▶ **Завершение перехвата сетевых данных**

1. Переключитесь обратно в **Network Monitor**.
2. Щелкните кнопку **Stop** в меню **Capture** в **Network Monitor**.

   Network Monitor прекратит перехват кадров и отобразит четыре панели: **Graph**, **Total Stats**, **Session Stats** и **Station Stats**.

▶ **Просмотр перехваченных данных**

- Щелкните кнопку **Display Captured Data** в меню **Capture**.

  Появится окно **Network Monitor Capture Summary** с итоговыми сведениями обо всех перехваченных кадрах.

А сейчас Вы измените цвет, которым выделяются при отображении кадры протокола ARP. Это полезно при просмотре кадров конкретного протокола.

▶ **Выделение цветом перехваченных данных**

1. Щелкните кнопкой мыши **Colors** в меню **Display**.
   Появится диалоговое окно **Protocol Colors**.
2. В поле **Name** выберите **ARP_RARP**.
3. В поле **Colors** установите значение **Foreground** в **Red**, и щелкните **OK**.
   Появится окно **Network Monitor Capture Summary**: в нем все кадры протокола ARP выделены красным цветом.

▶ **Подробный просмотр кадра ARP-запроса**

1. В колонке **Description** дважды щелкните строку **ARP: Request.**
   Появятся три отдельных окна. Верхнее отображает общую информацию о кадрах, среднее — данные о выбранных кадрах, а нижнее — содержимое выбранных кадров в шестнадцатеричном представлении.
2. В окне **Detail** щелкните надпись **Frame**, которой предшествует знак плюс (+).
3. Раскройте список **Frame**, щелкнув знак (+).
   Появится подробная информация. Содержимое пакета, выделенное цветом, отобразится в шестнадцатеричном формате в нижнем окне.
   Просмотрите полный размер кадра.
4. Сверните окно свойств основного кадра.
5. В окне **Detail** разверните **ETHERNET**.
   Появятся свойства кадра **ETHERNET**.
   Каков адрес получателя?

   _____

   Соответствует ли адрес получателя какому-нибудь адресу сетевого адаптера?

   _____

   Каков адрес отправителя?

   _____

   Какой тип имеет этот кадр Ethernet?

   _____

6. Сверните свойства **ETHERNET**.
7. В окне **Detail** разверните **ARP_RARP**.
   Каков адрес сетевого адаптера отправителя?

   _____

Каков адрес сетевого адаптера получателя?

---

Каков адрес протокола получателя?

---

► **Подробный просмотр кадра ARP-ответа**

1. В поле **Description** дважды щелкните **ARP: Reply.**
2. В окне **Detail** разверните **ETHERNET:ETYPE.**

   Появятся свойства кадра **ETHERNET:ETYPE.**

   Каков адрес получателя?

---

Соответствует ли адрес получателя какому-нибудь адресу сетевого адаптера?

---

Каков адрес отправителя?

---

Каков тип кадра Ethernet?

---

3. Сверните свойства **ETHERNET.**
4. В окне **Detail** разверните **ARP_RARP.**

   Каков адрес сетевого адаптера отправителя?

---

Если Вы хотите сохранить перехваченные данные для дальнейшего анализа, выполните операцию, описанную далее.

► **Запись перехваченных данных**

1. Выберите пункт **Save As** в меню **File.**
2. В поле **File Name** наберите имя файла, затем щелкните кнопку **OK.**
3. В меню **File** выберите пункт **Close.**

   Появится окно **Network Monitor Capture**, отображающее статистическую информацию о последнем перехвате данных.
4. Выйдите из Network Monitor.

**Вы используете утилиту Arp для просмотра записей в кэше протокола ARP Вашего компьютера, а затем — для его изменения.**

Примечание Вам потребуются два сетевых компьютера, описанных в статье «Об этой книге». Если Вы закончили предыдущее упражнение несколько минут назад, необходимо обновить кэш протокола ARP. Для этого выполните Ping на адрес второго Вашего компьютера.

▶ **Просмотр кэша протокола ARP**

1. Наберите *arp -g* в командной строке и нажмите ENTER для просмотра кэша протокола ARP.
2. Запомните запись для шлюза по умолчанию (если он сконфигурирован), например:

   131.107.2.1 08-00-02-6c-28-93

▶ **Выполнение Ping на адрес локального узла**

1. Выполните Ping на IP-адрес Вашего второго компьютера.

   В результате этого в кэш добавится новая запись.
2. Просмотрите новую запись в кэше протокола ARP.

   Какая запись была добавлена?

   Какого она типа?

Примечание Адрес шлюза по умолчанию был добавлен в кэш протокола ARP при выполнении Ping на адрес удаленного узла. Это произошло потому, что Ping должен использовать шлюз по умолчанию для достижения удаленного узла.

▶ **Добавление ARP-записи**

1. Наберите следующую команду для добавления в кэш записи, полученной на первом этапе:

   `arp -s 131.107.2.1` *адрес_адаптера*

Примечание Убедитесь в том, что числа в адресе сетевого адаптера Вы разделили дефисами, как это показано раньше.

2. Просмотрите кэш протокола ARP и убедитесь, что запись добавлена. Какого она типа?

Почему тип этой записи отличается от предыдущих записей?

### Проблемы, связанные с разрешением IP-адресов

Возможны ситуации, когда протокол ARP не сумеет по заданному IP-адресу выяснить адрес сетевого адаптера. Если кэш протокола ARP содержит неправильный адрес сетевого адаптера, попытка установить связь с удаленным узлом прекращается по истечении некоторого времени.

## Резюме

Разрешение адреса — это поиск адреса сетевого адаптера, соответствующего заданному IP-адресу. Разрешение адреса состоит из ARP-запроса и ARP-ответа. Кэш протокола ARP поддерживает как статические, так и динамические записи. Первые — остаются в кэше до перезагрузки компьютера, вторые — удаляются по истечении определенного времени.

# Занятие 3. Протоколы ICMP и IGMP

В то время как протокол IP используется для маршрутизации в объединенных сетях, протокол ICMP (Internet Control Message Protocol) оповещает об ошибках и управляет сообщениями для протокола IP, который информирует маршрутизаторы о существовании в сети узлов, принадлежащих некой группе, при помощи IGMP (Internet Group Management Protocol).

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как ICMP сообщает об ошибках протокола IP;
- ✓ дать определение IGMP и понять структуру его пакета.

**Продолжительность занятия — 10 минут**

## Протокол ICMP

Протокол ICMP не используется для повышения надежности IP, а лишь сообщает об ошибках и обеспечивает в некоторых случаях обратную связь. Его сообщения передаются в виде IP-датаграмм и поэтому ненадежны.

Если узел TCP/IP посылает датаграммы другому узлу со скоростью, перегружающей маршрутизаторы или каналы между ними, то маршрутизаторы могут ответить сообщением ICMP Source Quench, содержащим предложение снизить скорость передачи. Узел TCP/IP под управлением Windows NT выполняет это требование и уменьшает скорость отправки датаграмм. Однако, если компьютер, работающий под управлением Windows NT, используется как маршрутизатор и не успевает перенаправлять датаграммы, он отвергает все датаграммы, которые нельзя буферизовать. В этом случае он не посылает ICMP-сообщений отправителям*.

### Структура ICMP-пакета

Все пакеты протокола ICMP имеют одинаковую структуру.

| Поле | Описание |
|---|---|
| Type (Тип) | 8-битное поле Type отображает тип пакета протокола ICMP (Echo Request, Echo Reply и т.д.) |
| Code (Код) | 8-битное поле Code отображает одну из нескольких возможных функций для данного типа пакета. Если в типе только одна функция, то значение в поле Code устанавливается равным 0 |

* Маршрутизатор под управлением Windows NT с установленной службой Routing And Remote Access Update эту функцию выполняет. — *Прим. перев.*

(*продолжение*)

| Поле | Описание |
|---|---|
| Checksum (Контрольная сумма) | 16-битовая контрольная сумма части пакета, относящейся к протоколу ICMP |
| Type-Specific Data (Специальные данные типа) | Дополнительные данные, различные для каждого типа пакета |

Примечание Протокол ICMP описан в RFC 792. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Протокол IGMP

Информация протокола IGMP проходит через другие маршрутизаторы таким образом, что каждый поддерживающий групповую адресацию маршрутизатор знает, какая группа узлов в какой сети находится. Пакеты IGMP передаются датаграммами протокола IP и поэтому ненадежны.

### Структура IGMP-пакета

Поля пакета протокола IGMP перечислены в таблице.

| Поле | Описание |
|---|---|
| Version (Версия) | Версия протокола ICMP. Данное поле имеет фиксированное значение 0x1 |
| Type (Тип) | Тип IGMP-сообщения. Тип 0x1 называется Host Membership Query (запрос узла о принадлежности к некоторой группе) и используется групповыми маршрутизаторами для опроса нескольких членов указанной группы. Тип 0x2 — Host Membership Report (ответ узла о принадлежности к некоторой группе) — используется для объявления членства в группе или для ответа на запрос Host Membership Query, поступивший от маршрутизатора |
| Unused (Не используется) | Не используемое поле. Обнуляется отправителем и игнорируется получателем |
| Checksum (Контрольная сумма) | 16-битная контрольная сумма на 8-байтный заголовок IGMP-пакета |

(*продолжение*)

| Поле | Описание |
|---|---|
| Group Address (Групповой адрес) | Используется узлами в сообщении Host Membership Report для хранения группового IP-адреса. В запросе Host Membership Query групповой адрес заполняется нулями, а для идентификации группы узлов используется широковещательный адрес сетевого адаптера |

Примечание Протокол IGMP описан в RFC 1112. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

Протокол ICMP оповещает об ошибках и управляет сообщениями для протокола IP. Маршрутизаторы могут посылать узлам сообщение ICMP Source Quench с предложением снизить скорость передачи, если эти узлы отправляют датаграммы слишком быстро.

IGMP информирует маршрутизаторы о доступности специальных групп узлов в данной сети.

# Занятие 4. Протокол IP

Протокол IP не ориентирован на соединение и предназначен для отправки и маршрутизации пакетов между узлами. На этом занятии описана маршрутизация пакетов протокола IP.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как протокол IP фрагментирует и маршрутизирует пакеты;
- ✓ описать структуру IP-пакета.

**Продолжительность занятия — 15 минут**

Протокол IP не ориентирован на соединение, поскольку он не устанавливает сеанс связи, перед тем как начать обмен данными. Протокол IP ненадежный — он не гарантирует доставку пакета, хотя делает для этого все возможное. По пути пакет может быть потерян, доставлен в неправильной последовательности, продублирован или задержан.

Протокол IP не требует подтверждения при приеме данных. Отправитель или получатель не информируется при потере пакета или доставке его в неправильной последовательности. Ответственность за подтверждение получения пакетов несут высокоуровневые транспортные протоколы, например TCP.

Поля IP-датаграммы в приведенной ниже таблице добавляются в заголовок пакета при его получении с транспортного уровня.

| Поле | Описание |
|---|---|
| Source IP-address (IP-адрес отправителя) | Идентифицирует отправителя датаграммы при помощи IP-адреса |
| Destination IP-address (IP-адрес получателя) | Идентифицирует получателя датаграммы при помощи IP-адреса |
| Protocol (Протокол) | Информирует протокол IP узла-получателя о том, какому протоколу верхнего уровня — TCP или UDP — его следует передать |
| Checksum (Контрольная сумма) | Легко вычисляемое значение для проверки целостности пришедшего пакета |

(*продолжение*)

| Поле | Описание |
|---|---|
| Time to live, или TTL (Время жизни) | Определяет, сколько секунд находится датаграмма в сети, перед тем как она будет *отвергнута* (discarded). Предотвращает бесконечное блуждание пакетов по сети. Маршрутизаторы должны уменьшать TTL на количество секунд, проведенных датаграммой в маршрутизаторе. TTL уменьшается по меньшей мере на одну секунду каждый раз, когда датаграмма проходит через маршрутизатор. По умолчанию в Windows NT 4.0 TTL равно 128 секундам |

Примечание Протокол IP описан в RFC 791. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

Если протокол IP идентифицирует адрес получателя как *локальный*, то он передаст пакет на этот узел напрямую. Если же IP-адрес получателя идентифицирован как удаленный, IP начнет искать маршрут к удаленному узлу в локальной таблице маршрутизации. Если он не найдет подходящего маршрута, то отправит пакет на шлюз по умолчанию, заданный в конфигурации узла-отправителя. *Шлюз по умолчанию* (default gateway) также называют *маршрутизатором* (router).

## Реализация IP на маршрутизаторе

Маршрутизатор обрабатывает полученные им IP-пакеты следующим образом.

1. Уменьшает значение TTL на 1 с или больше, если пакет надолго задерживается на маршрутизаторе.

   Если значение TTL достигает нуля, пакет отвергается.
2. Пакет может быть фрагментирован, если его размер слишком велик для сети дальнейшего следования.
3. Если пакет фрагментирован, то IP создает для каждого нового пакета (фрагмента) отдельный заголовок, устанавливая:
   - Flag (Флаг), указывающий, что существуют и другие фрагменты, которые будут отправлены вслед;
   - Fragment ID (Идентификатор фрагмента), идентифицирующий все фрагменты, составляющие один пакет;

- Fragment Offset (Смещение фрагмента), обеспечивающий правильную сборку пакета на узле-получателе.

4. Вычисляет новую контрольную сумму.
5. Определяет адрес сетевого адаптера следующего маршрутизатора.
6. Направляет пакет дальше в сеть.

На следующем узле пакет попадает по стеку протоколов к TCP или UDP. Этот процесс повторяется на каждом маршрутизаторе до тех пор, пока пакет не дойдет до адресата; там протокол IP собирает из фрагментов пакет в первоначальном виде.

## Структура IP-пакета

Поля заголовка IP-пакета (для IP версии 4) приведены в таблице.

| Поле | Описание |
|---|---|
| Version (Версия) | 4 бита используются для отображения версии протокола IP. Текущая версия — четвертая. Следующей будет шестая (см. главу 4) |
| Header Length (Длина заголовка) | 4 бита используются для отображения количества 32-битных слов в заголовке IP-пакета. Минимальный размер заголовка — 20 байт, следовательно, длина минимального заголовка — 0x5. Опции IP могут увеличить минимальный размер заголовка на 4 байта. Если опция не использует их все, то оставшиеся биты заполняются нулями, поэтому длина заголовка всегда кратна 4 байтам |
| Type of Service (Тип обслуживания) | 8 бит используются для обозначения требуемого для этой датаграммы качества обслуживания при доставке через маршрутизаторы объединенной IP-сети. В них есть биты, выделенные для приоритета, задержки, пропускной способности и характеристик надежности |
| Total Length (Общая длина) | 16 бит используются для отображения общей длины датаграммы протокола IP (заголовок IP-пакета + его содержание). Сюда не включен заголовок сетевого кадра |

(*продолжение*)

| Поле | Описание |
|---|---|
| Identification (Идентификация) | 16 бит используются в качестве идентификатора данного IP-пакета. Если IP-пакет фрагментирован, то все фрагменты имеют одинаковые идентификаторы, используемые при сборке узлом-получателем |
| Fragmentation Flags (Фрагментационные флаги) | 3 бита зарезервированы для флагов фрагментации; однако только 2 бита определены для текущего использования. Один флаг служит для обозначения фрагментированного пакета, другой — для идентификации последнего фрагмента |
| Fragment Offset (Смещение фрагмента) | 13 бит используются как счетчик смещения для указания положения фрагментов относительно начала поля данных IP-пакета. Если фрагментации нет, то смещение равно 0x0 |
| Time to Live (Время существования) | 8 бит используются в качестве индикатора времени (транзитов IP-пакета), максимально допустимого перед тем, как пакет будет отвергнут. Поле TTL используется как счетчик времени (в секундах), проведенного пакетом на маршрутизаторе, который соответственно уменьшает TTL. Современные маршрутизаторы почти всегда перенаправляют датаграммы менее чем за 1 с, однако, по требованиям RFC 791, они должны уменьшать TTL не менее чем на единицу. Поэтому TTL становится счетчиком максимального числа транзитов |
| Protocol (Протокол) | 8 бит используются в качестве идентификатора протокола, данные которого инкапсулированы в IP-пакет. Поле протокола применяется для передачи Р-пакета протоколу Iверхнего уровня |

(*продолжение*)

| Поле | Описание |
|---|---|
| Header checksum (Контрольная сумма заголовка) | 16 бит используются в качестве контрольной суммы заголовка IP-пакета. Данные пакета не учитываются и могут иметь свою собственную контрольную сумму для проверки ошибок. Когда узел получает IP-пакет, он проводит проверку контрольной суммы и при несовпадении значений отвергает пакет. Когда маршрутизатор пересылает IP-пакет, он, как минимум, уменьшает TTL. Поэтому контрольная сумма вычисляется снова при каждом транзите на пути от отправителя к получателю |
| Source Address (Адрес отправителя) | 32 бита используются для хранения IP-адреса узла-отправителя |
| Destination Address (Адрес получателя) | 32 бита используются для хранения IP-адреса узла-получателя |
| Options and Padding (Опции и заполнение) | Для хранения опций используется кратное 32 число бит. Если же опции не занимают этот бит целиком, остаток заполняется нулями. Таким образом, длина IP-заголовка всегда может быть выражена количеством четверок байт и записана в поле Header Length |

## Резюме

Протокол IP не ориентирован на соединение, он отправляет и маршрутизирует пакеты между узлами. IP — ненадежный протокол, поскольку не гарантирует доставку. Если пакет отправлен по адресу в локальной сети, то он посылается непосредственно на узел. Если IP-адрес получателя удален, IP ищет маршрут в локальной таблице маршрутизации.

# Занятие 5. Протокол TCP

Протокол TCP предоставляет надежную, ориентированную на соединение службу доставки. На этом занятии описано, как протокол TCP передает данные, а также даны определения порта и сокета.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать, как протокол TCP передает данные;
- ✓ дать определение порта и сокета.

**Продолжительность занятия — 25 минут**

Данные протокола TCP передаются сегментами, и соединение должно быть установлено до того, как узлы начнут обмениваться данными. TCP использует потоки, в которых данные представлены в виде последовательности байт.

TCP обеспечивает надежность, присваивая *номера последовательности* (sequence number) каждому передаваемому сегменту. Если сегмент разбивается на мелкие пакеты, то узел-получатель сможет узнать, все ли части получены. Для этого используются подтверждения. Для каждого отправленного сегмента узел-получатель должен вернуть отправителю *подтверждение* (acknowledgement, ACK) в течение определенного времени.

Если отправитель не получил ACK, данные передаются повторно. Если сегмент поврежден, узел-получатель отвергает его. Поскольку ACK в этом случае не посылается, отправитель передает сегмент еще раз.

Примечание TCP описан в RFC 793. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Порты

Приложения, использующие сокеты, идентифицируют себя на компьютере посредством *номера порта протокола* (protocol port number). Например, FTP-сервер использует определенный TCP-порт, поэтому другие приложения могут связаться с ним.

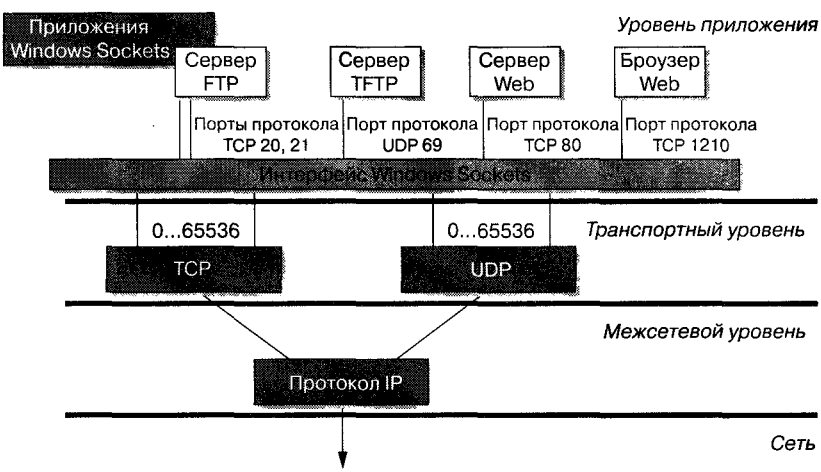
Порты могут иметь любой номер от 0 до 65 536. Номера портов для приложений клиентов динамически назначаются операционной системой при обработке запроса на обслуживание. *Известные* (well-known) номера портов для приложений-серверов назначаются группой Internet Assigned Numbers Authority (IANA) и не меняются.

Совет Вы можете узнать номера портов, просмотрев файл \systemroot\System32\Drivers\Etc\Services.

Номера известных портов расположены в интервале от 1 до 1 024. Окончательный список известных номеров портов задокументирован в RFC 1700. Копия этого документа находится на Web-странице Course Materials прилагаемого к курсу компакт-диска.

## Сокеты

*Сокет* (socket) во многом аналогичен дескриптору файла (file handle). Он обеспечивает конечную точку сетевого соединения. Приложение, создавая сокет, указывает три параметра: IP-адрес узла, тип обслуживания (протокол TCP — для ориентированного на соединение обслуживания и UDP — для не ориентированного) и порт, используемый приложением.




Приложение может создать сокет и использовать его для отправки не ориентированного на соединение трафика удаленным приложениям или же подключить его к сокету другого приложения. Во втором случае данные будут посланы по надежному соединению.

### Порты протокола TCP

Порт протокола TCP указывает место доставки сообщений. Номера портов, меньшие 256, определены как широко используемые. В таблице перечислены некоторые из таких портов.

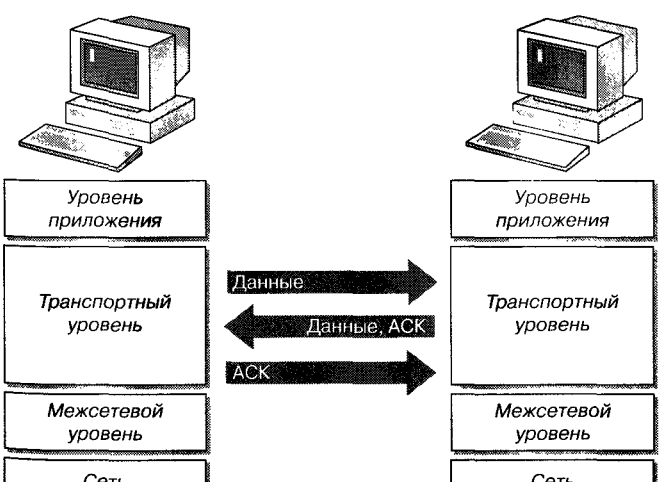
| Номер порта | Описание |
|---|---|
| 21 | FTP |
| 23 | Telnet |
| 53 | Доменная система имен (DNS) |
| 139 | Сервис NetBIOS |

## Установка связи по протоколу TCP

Инициализация TCP-соединения происходит в три этапа. Делается это для синхронизации отправки и получения сегментов, извещения другого узла о количестве данных, которые можно послать за один раз, и установки виртуального соединения.

Ниже перечислены операции, из которых состоит этот процесс.

1. Узел-отправитель запрашивает соединение, посылая сегмент с установленным флагом синхронизации (SYN).
2. Узел-адресат подтверждает получение запроса, отправляя обратно сегмент с:
   - установленным флагом синхронизации;
   - порядковым номером начального байта сегмента, который он может послать, или *номером последовательности* (sequence number);
   - подтверждением, включающим порядковый номер следующего сегмента, который он ожидает получить.
3. Запрашивающий узел посылает обратно сегмент с подтверждением номера последовательности и *номером своего подтверждения* (acknowledgement number).



Для завершения соединения TCP действует аналогично. Это гарантирует, что оба узла закончат передачу и примут все данные.

## Скользящие окна протокола TCP

Протокол TCP буферизует данные для передачи между двумя узлами, используя *скользящие окна* (sliding windows). Каждый TCP/IP-узел поддерживает два скользящих окна: одно — для приема данных, а другое — для отправки. Размер окна определяет объем данных, которые могут быть буферизованы на компьютере.

### Видеоролик: скользящие окна протокола TCP

Здесь показано, как работают скользящие окна протокола TCP и как размер скользящего окна влияет на производительность.

▶ **Запуск видеоролика**

1. Вставьте прилагаемый к курсу компакт-диск в CD-ROM-дисковод, запустится Microsoft Internet Explorer и откроется страница *The Internetworking with Microsoft TCP/IP on Microsoft Windows NT 4.0*,

   или

   запустите Windows NT Explorer, выберите прилагаемый к курсу компакт-диск, затем дважды щелкните файл Open.htm.
2. Щелкните пиктограмму начальной страницы.
3. Щелкните **Course Materials**.
4. Щелкните **Multimedia Presentation**.
5. Щелкните **TCP Sliding Windows**.

   Появится диалоговое окно Internet Explorer с вопросом, хотите Вы открыть файл или записать его на диск.
6. Выберите **Open**, затем щелкните **OK**.
7. Щелкните **Yes**, если появится окно системы безопасности.

   Начнется показ видеоролика. Если на Вашем компьютере нет звуковой платы или динамиков, щелкните кнопку **Text On**.

### Структура TCP-пакета

Все пакеты протокола TCP имеют две части — данные и заголовок. В таблице приведены поля заголовка TCP-пакета.

| Поле | Описание |
|---|---|
| Source Port (Порт отправителя) | TCP порт узла-отправителя |
| Destination Port (Порт получателя) | TCP порт узла-получателя. Определяет конечную точку соединения |
| Sequence Number (Порядковый номер) | Номер последовательности пакета. Используется для проверки получения всех байт соединения |
| Acknowledgment Number (Номер подтверждения) | Порядковый номер байта, который локальный узел планирует получить следующим |
| Data Length (Длина данных) | Длина TCP-пакета |
| Reserved (Зарезервировано) | Зарезервировано для будущего использования |
| Flags (Флаги) | Это поле описывает содержимое сегмента |
| Window (Окно) | Показывает, сколько места доступно в настоящий момент в окне протокола TCP |
| Checksum (Контрольная сумма) | Проверяет, поврежден ли заголовок |
| Urgent Pointer (Указатель срочности) | Когда отправляются срочные данные (указано в поле Flags), в этом поле задается конечная граница области срочных данных в пакете |

## Резюме

Протокол TCP предоставляет надежную, ориентированную на соединение службу доставки. Приложения, применяющие сокеты, используют уникальные номера портов. Сокет — это конечная точка сетевого соединения. Номера портов и сокетов выбираются из соответствующего диапазона.

Сеанс протокола TCP начинается и заканчивается одной и той же трехэтапной последовательностью действий. Протокол TCP использует скользящие окна для буферизации данных, передаваемых между двумя узлами. Размер окна показывает количество данных, которые могут быть буферизованы на компьютере.

# Занятие 6. Протокол UDP

Протокол User Datagram Protocol (UDP) обеспечивает не ориентированную на соединение службу доставки датаграмм по принципу «максимального усилия». Это означает, что получение всей датаграммы или правильной последовательности отправленных пакетов не гарантируется.

**Изучив материал этого занятия, Вы сможете:**

- определить протокол UDP и описать структуру UDP-пакета.

**Продолжительность занятия — 5 минут**

Протокол UDP используется приложениями, не требующими подтверждения. Обычно такие приложения передают данные небольшого объема за один раз. Примеры служб и приложений, использующих UDP: сервис имен NetBIOS, сервис датаграмм NetBIOS и сервис SNMP.

## Порты протокола UDP

Для использования протокола UDP приложение должно знать IP-адрес и номер порта получателя. Порт — место назначения при доставке сообщений — идентифицируется уникальным номером. Порт действует как мультиплексная очередь сообщений, то есть он может получать несколько сообщений одновременно. Важно отметить, что порты протокола UDP, перечисленные в таблице, отличаются от портов TCP, несмотря на использование тех же значений номеров.

| Номер порта | Ключевое слово | Описание |
|---|---|---|
| 15 | NETSTAT | Состояние сети |
| 53 | DOMAIN | Сервер имен домена |
| 69 | TFTP | Протокол TFTP |
| 137 | NETBIOS-NS | Сервис имен NetBIOS |
| 138 | NETBIOS-DGM | Сервис датаграмм NetBIOS |
| 161 | SNMP | Сетевой монитор SNMP |

Примечание Протокол UDP описан в RFC 768. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Структура пакета протокола UDP

Поля 8-байтного заголовка UDP-пакета перечислены в таблице.

| Поле | Описание |
|---|---|
| Source Port (Порт отправителя) | UDP-порт узла-отправителя. Его задавать не обязательно. Если не используется, то устанавливается равным нулю |
| Destination Port (Порт получателя) | UDP порт узла-получателя. Указывает конечную точку соединения |
| Message Length (Длина сообщения) | Размер сообщения. Минимальный UDP-пакет содержит только информацию заголовка (8 байт) |
| Checksum (Контрольная сумма) | Проверяет заголовок на предмет повреждения |

## Резюме

Протокол UDP обеспечивает не ориентированную на соединение службу доставки датаграмм, которая не гарантирует успешную доставку пакетов. Протокол UDP используется приложениями, не требующими подтверждения получаемых данных.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие уровни используются в четырехуровневой модели TCP/IP?

2. Какие основные протоколы обеспечиваются в транспортном драйвере протокола Microsoft TCP/IP?

3. Какой протокол используется для информирования клиента о недоступности сети-получателя?

4. Как изменяется датаграмма протокола IP при прохождении через маршрутизатор?

5. Когда используется протокол UDP?

6. На какой адрес отправляются ARP-запросы?

7. Какой адрес выясняется при помощи ARP-запроса при отправке пакета на локальный узел? На удаленный узел?

# Дополнительная информация

- Изучите все RFC, находящиеся на прилагаемом компакт-диске.

# IP-адресация



## В этой главе

В этой главе описаны компоненты IP-адреса, поддерживаемые Microsoft Windows NT классы IP-адресов и основы IP-адресации. На занятиях Вы изучите локальные сети. Выполняя упражнения этой главы, Вы научитесь определять корректность IP-адресов, присваивать IP-адреса узлам и выявлять проблемы, связанные с IP-адресацией.

## Прежде всего

Задания этой главы не требуют предварительной подготовки.

# Занятие 1. IP-адрес

IP-адрес определяет местонахождение узла в сети подобно тому, как адрес дома указывает его расположение в городе. Как и обычный адрес, IP-адрес должен быть уникальным и иметь единый формат.

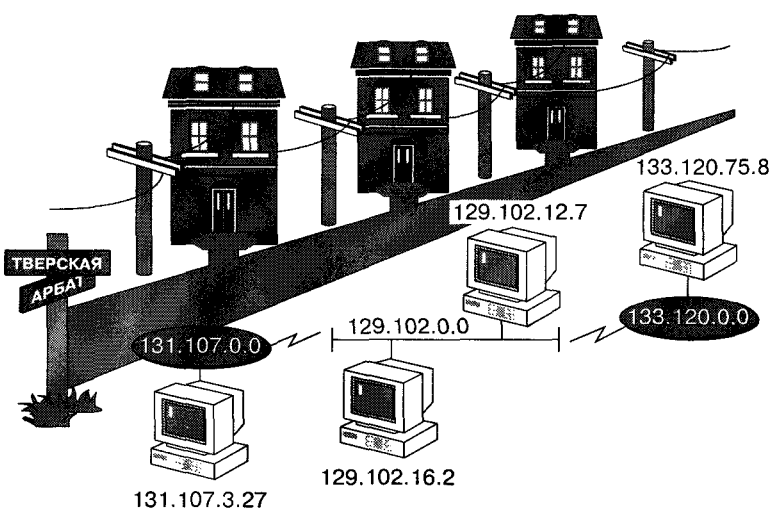
**Изучив материал этого занятия, Вы сможете:**

- ✓ определить идентификатор сети и узла в IP-адресе;
- ✓ преобразовать IP-адрес из двоичного представления в десятичное.

**Продолжительность занятия — 25 минут**

Каждый IP-адрес состоит из двух частей — *идентификатора сети* (network ID) и *идентификатора узла* (host ID). Первый определяет физическую сеть. Он одинаков для всех узлов в одной сети и уникален для каждой из сетей, включенных в объединённую сеть.

Идентификатор узла соответствует конкретной рабочей станции, серверу, маршрутизатору или другому TCP/IP-узлу в данной сети. Он должен иметь уникальное значение в данной сети. Каждый узел TCP/IP однозначно определяется по своему логическому IP-адресу. Такой адрес необходим всем сетевым компонентам, взаимодействующим по TCP/IP.

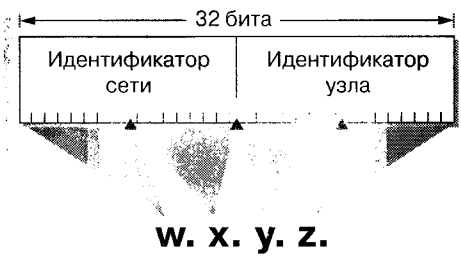


## Идентификаторы сетей и узлов

IP-адрес может быть записан в двух форматах — *двоичном* (binary) и *десятично-точечном* (dotted decimal). Каждый IP-адрес имеет длину 32 бита и состоит из четырёх 8-битных полей, называемых *октетами* (octets), которые отделяются друг от друга точками. Каждый октет представляет десятичное число в диапазоне от 0 до 255. Эти 32 разряда IP-адреса содержат идентификатор сети и узла.

Формат записи адреса в виде четырех десятичных чисел, разделенных точками, наиболее удобен для восприятия. Далее показаны различные формы записи IP-адреса.

| Двоичный формат | Десятично-точечный формат |
|---|---|
| 10000011 01101011 00000011 00011000 | 131.107.3.24 |

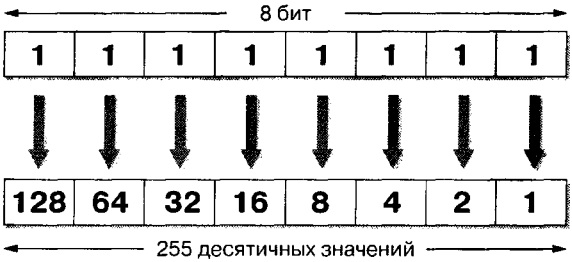



Пример: **131.107.3.24**

## Преобразование IP-адреса из двоичного формата в десятичный

Вы должны уметь определять значения битов в октетах и преобразовывать их в десятичные числа. В двоичном формате каждому биту в октете сопоставлено определенное десятичное число. Максимальное десятичное значение октета равно 255 (участвует каждый бит). Каждый октет преобразуются в число отдельно от других.

Бит, установленный в 0, всегда соответствует нулевому значению. Бит, установленный в 1, может быть преобразован в десятичное число. Младший бит октета представляет десятичное число 1, а старший — 128. Максимальное значение октета достигается, когда каждый его бит равен 1.




В следующей таблице показано, как биты одного октета преобразуются в десятичное число.

| Двоичная запись | Значения бит | Десятичное число |
|---|---|---|
| 00000000 | 0 | 0 |
| 00000001 | 1 | 1 |
| 00000011 | 1+2 | 3 |
| 00000111 | 1+2+4 | 7 |
| 00001111 | 1+2+4+8 | 15 |
| 00011111 | 1+2+4+8+16 | 31 |
| 00111111 | 1+2+4+8+16+32 | 63 |
| 01111111 | 1+2+4+8+16+32+64 | 127 |
| 11111111 | 1+2+4+8+16+32+64+128 | 255 |

## Упражнения

В этом упражнении Вам предстоит преобразовать двоичную запись в десятичное число и наоборот.

1. Переведите следующие двоичные числа в десятичные.

| Двоичное значение | Десятичное значение |
|---|---|
| 10001011 | |
| 10101010 | |
| 10111111 11100000 00000111 10000001 | |
| 01111111 00000000 00000000 00000001 | |

Совет Вы можете использовать калькулятор (в научном режиме) из папки Accessories для преобразования двоичных чисел в десятичные и обратно. Однако Вы лучше освоите этот процесс, если выполните несколько действий вручную.

2. Переведите следующие деятичные числа в двоичные.

| Десятичное значение | Двоичное значение |
|---|---|
| 250 | |
| 19 | |
| 109.128.255.254 | |
| 131.107.2.89 | |

## Резюме

Каждый узел TCP/IP идентифицируется по логическому IP-адресу, а уникальный IP-адрес необходим каждому узлу и сетевому компоненту, использующим TCP/IP. IP-адрес, состоящий из идентификаторов сети и узла, имеет длину 32 бита и содержит четыре 8-битных поля (октета).

# Занятие 2. Классы IP-адресов

Каждый класс IP-адресов определяет, какая часть адреса отводится под идентификатор сети, а какая — под идентификатор узла. На этом занятии Вы узнаете о различных классах IP-адресов.

**Изучив материал этого занятия, Вы сможете:**

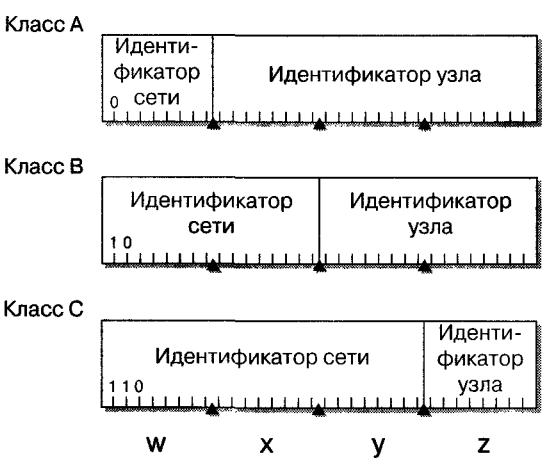
- ✓ определить идентификатор сети и узла в IP-адресе класса A, B или C;
- ✓ определить, к какому классу относится заданный IP-адрес.

**Продолжительность занятия — 15 минут**

Сообщество Интернета определило пять классов IP-адресов в соответствии с различными размерами компьютерных сетей. Microsoft TCP/IP поддерживает адреса классов A, B и C. Класс адреса определяет, какие биты относятся к идентификатору сети, а какие — к идентификатору узла. Также он определяет максимально возможное количество узлов в сети.

Класс IP-адреса идентифицируют по значению его первого октета, 32-разрядные IP-адреса могут быть присвоены в общей совокупности 3 720 314 628 узлам. Ниже показано, как определяются поля в IP-адресах разных классов.

| Класс | IP-адрес | Идентификатор сети | Идентификатор узла |
|---|---|---|---|
| A | w.x.y.z | w | x.y.z |
| B | w.x.y.z | w.x | y.z |
| C | w.x.y.z | w.x.y | z |



## Класс A

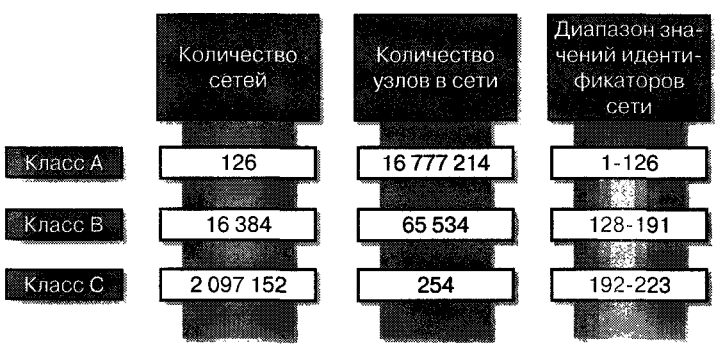
Адреса класса A назначаются узлам очень большой сети. Старший бит в адресах этого класса всегда равен нулю. Следующие семь бит первого октета представляют идентификатор сети. Оставшиеся 24 бита (три октета) содержат идентификатор узла. Это позволяет иметь 126 сетей с числом узлов до 17 миллионов в каждой.

## Класс B

Адреса класса B назначаются узлам в больших и средних по размеру сетях. В двух старших битах IP-адреса класса B записывается двоичное значение 10. Следующие 14 бит содержат идентификатор сети (два первых октета). Оставшиеся 16 бит (два октета) представляют идентификатор узла. Таким образом, возможно существование 16 384 сетей класса B, в каждой из которых около 65 000 узлов.

## Класс C

Адреса класса C применяются в небольших сетях. Три старших бита IP-адреса этого класса содержат двоичное значение 110. Следующие 21 бит составляет идентификатор сети (первые три октета). Оставшиеся 8 бит (последний октет) отводится под идентификатор узла. Всего возможно около 2 000 000 сетей класса C, содержащих до 254 узлов.




Примечание В качестве идентификатора сети не может использоваться значение 127. Оно зарезервировано для диагностики и используется в качестве локальной заглушки.

## Класс D

Адреса класса D предназначены для рассылки групповых сообщений. Группа получателей может содержать один, несколько или ни одного

узла. Четыре старших бита в IP-адресе класса D всегда равны 1110. Оставшиеся биты обозначают конкретную группу получателей и не разделяются на части. Пакеты с такими адресами рассылаются избранной группе узлов в сети. Их получателями могут быть только специальным образом зарегистрированные узлы. Micorosoft поддерживает адреса класса D, применяемые приложениями для групповой рассылки сообщений, включая WINS и Microsoft NetShow™.

## Класс E

Класс E — экспериментальный. Он зарезервирован для использования в будущем и в настоящее время не применяется. Четыре старших бита адресов класса E равны 1111.

Примечание Дополнительную информацию о групповой рассылке см. в статье *Multicasting*, в рубрике *Additional Readings* Web-страницы *Course Materials* прилагаемого к курсу компакт-диска.

## Упражнения

Определите, к какому классу принадлежат указанные IP-адреса.

1. Укажите классы следующих IP-адресов.

| Адрес | Класс |
|---|---|
| 131.107.2.89 | |
| 3.3.57.0 | |
| 200.200.5.2 | |
| 191.107.2.10 | |

2. В сетях каких классов IP-адресов более 1 000 узлов?

3. В сетях каких классов IP-адресов только 254 узла?

## Резюме

Всего существует пять классов IP-адресов. Microsoft поддерживает назначение узлам адресов классов A, B и C. Каждый класс соответствует сетям определенного размера.

# Занятие 3. Назначение IP-адресов

Хотя и не существует строгих правил назначения IP-адресов, Вам следует учитывать некоторые тонкости, чтобы выбирать корректные идентификаторы узлов и сетей. На этом занятии объясняется, как присваивать IP-адреса в локальной сети.

**Изучив материал этого занятия, Вы сможете:**

- ✓ понять, как назначать корректные IP-адреса;
- ✓ определять сетевые компоненты, которым необходим идентификатор сети;
- ✓ определять, каким узлам необходим идентификатор узла.

**Продолжительность занятия – 35 минут**

Существует несколько основных моментов, которые необходимо учитывать при назначении IP-адресов.

- Идентификатор сети не может равняться 127. Это значение зарезервировано для локальной заглушки и диагностики.
- Все биты идентификатора сети или узла не могут быть одновременно установлены в 1. Такой идентификатор применяется для широковещательных сообщений.
- Все биты идентификатора сети или узла не могут быть одновременно установлены в 0, так как в этом случае идентификатор означает всю локальную сеть.
- Каждый идентификатор узла должен быть уникальным для соответствующего идентификатора сети.

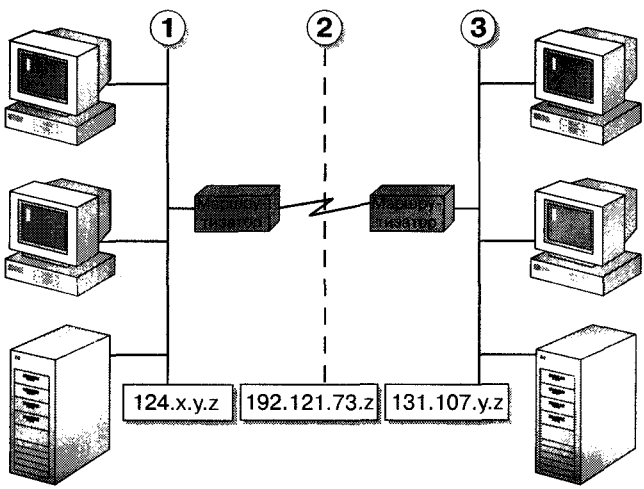
## Назначение идентификаторов сетей

Уникальный идентификатор необходим каждой сети и каждому внешнему соединению. Если Ваша сеть подключена к Интернету, Вам надо получить идентификатор сети от *Информационого Центра Интернета* (Internet Network Information Center, InterNIC). Если же Вы не планируете подключаться к Интернету, то можете использовать любой корректный идентификатор сети.

Идентификатор сети обозначает узлы TCP/IP, подключенные к одной физической сети. Поэтому, чтобы взаимодействовать друг с другом, все узлы одной физической сети должны иметь одинаковый идентификатор сети.

Если несколько сетей соединены через маршрутизаторы, уникальный идентификатор сети необходим для каждой из них. Такая ситуация проиллюстрирована ниже:

- сети 1 и 3 соединены через маршрутизаторы;
- маршрутизаторы соединяются через глобальную сеть 2;
- для сети 2 необходим отдельный идентификатор, чтобы соответствующие ей интерфейсы маршрутизаторов могли иметь уникальные идентификаторы узлов.

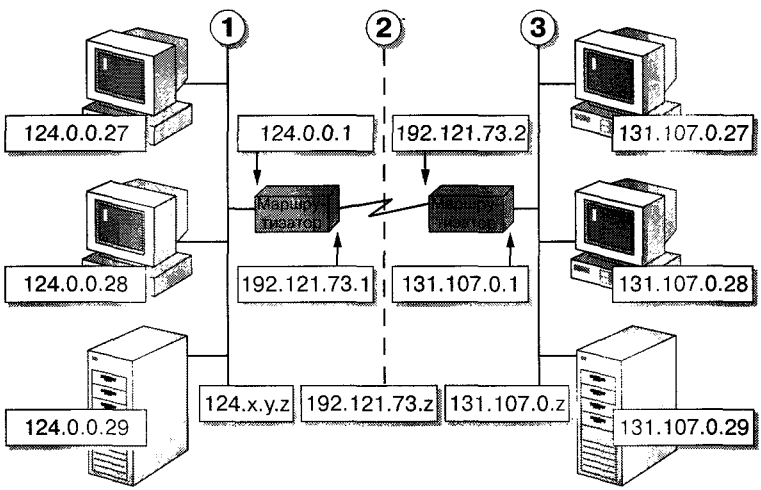



Примечание Если Вы собираетесь подключить свою сеть к Интернету, Вам необходимо официально получить идентификатор сети, чтобы гарантировать его уникальность. Для регистрации имен доменов и получения идентификаторов сетей Вы можете воспользоваться интерактивной службой регистрации InterNIC по адресу http://internic.net. По всем возникающим вопросам обращайтесь в службу поддержки по телефону (703) 742-4777.

Пространство IP-адресов, предназначенных для использования в изолированных сетях, определено в RFC 1918. Копия этого документа находится на страничке Course Materials прилагаемого к курсу компакт-диска.

## Назначение идентификаторов узлов

Идентификатор узла служит для обозначения TCP/IP-узла в некоторой сети и должен иметь уникальное значение для данного идентификатора сети. Всем TCP/IP-узлам, включая интерфейсы маршрутизаторов, необходимы уникальные идентификаторы. Идентификатор узла для маршрутизатора соответствует значению IP-адреса, указываемого в качестве адреса шлюза по умолчанию в конфигурации рабочей станции. Например, для узла из подсети 1, имеющего IP-адрес 124.0.0.27, адресом шлюза по умолчанию будет 124.0.0.1.




### Корректные идентификаторы узлов

В таблице указаны корректные значения идентификаторов узлов в сети.

| Класс адресов | Начало диапазона | Конец диапазона |
|---|---|---|
| Класс A | w.0.0.1 | w.255.255.254 |
| Класс B | w.x.0.1 | w.x.255.254 |
| Класс C | w.x.y.1 | w.x.y.254 |

### Методика назначения IP-адресов

Не существует конкретных правил назначения правильных IP-адресов. Вы можете назначать их последовательно или же выбирать легко запоминающиеся значения:

- назначать IP-адреса, группируя узлы по типу, например серверы и рабочие станции;
- выделять специальные IP-адреса маршрутизаторам.

Подобный подход позволит Вам избежать конфликтов, вызываемых повторением IP-адресов.

## Упражнения

Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

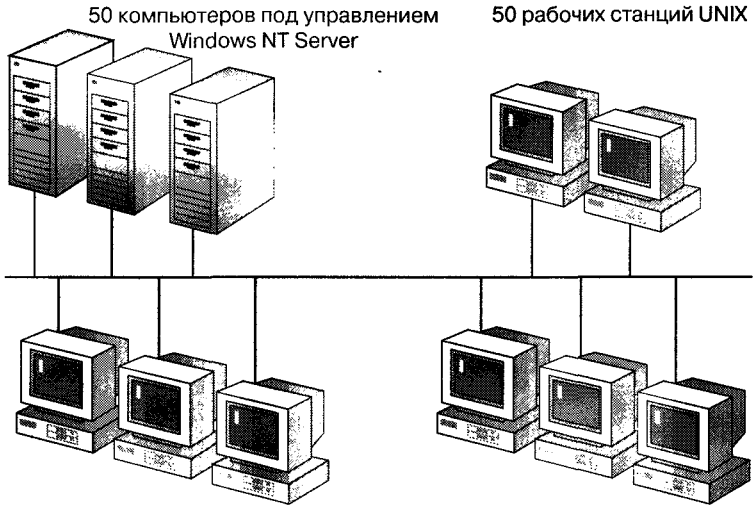
A. 131.107.256.80_____
B. 222.222.255.222_____
C. 231.200.1.1._____
D. 126.1.0.0_____
E. 0.127.4.100_____
F. 190.7.2.0_____
G. 127.1.1.1_____
H. 198.121.254.255_____
I. 255.255.255.255_____

А сейчас определите, каким сетевым компонентам TCP/IP необходим IP-адрес. Если указан тип протокола, предполагается, что это единственный протокол, поддержка которого установлена на данном узле. Рассмотрите перечисленные ниже сетевые компоненты и отметьте буквы, соответствующие компонентам, которым необходим IP-адрес.

A. Компьютер под управлением ОС Windows NT, использующий TCP/IP.
B. Рабочая станция, использующая LAN Manager и соединяющаяся с компьютером под управлением Windows NT с поддержкой TCP/IP.
C. Компьютер под управлением ОС Windows 95, которому необходим доступ к общим ресурсам на компьютере с Windows NT, использующем TCP/IP.
D. Хост UNIX, к которому Вы хотите осуществлять доступ с помощью утилит TCP/IP.
E. Принтер с сетевым интерфейсом, поддерживающим TCP/IP.
F. Маршрутизатор для соединения с удаленной IP-сетью.
G. Адаптер Ethernet на маршрутизаторе для локальной сети.
H. Рабочая станция, которая использует Microsoft LAN Manager и пытается соединиться с сервером LAN Manager, применяющим NetBEUI.
I. Компьютер под управлением ОС Windows for Workgroups, которому необходим доступ к общим ресурсам на сервере LAN Manager, поддерживающем NetBEUI.
J. Плоттер, подключенный к последовательному порту компьютера под управлением ОС Microsoft Windows NT, использующего TCP/IP.
K. Сетевой принтер, совместный доступ к которому осуществляется с помощью сервера LAN Manager, использующего NetBEUI.

L. Коммуникационный сервер, предоставляющий терминальный доступ к узлам TCP/IP.
M. Шлюз по умолчанию в Вашей сети.

Сейчас определите, какой класс адресов необходим для указанной IP-сети. Затем назначьте IP-адреса каждому типу узлов (UNIX, рабочие станции Windows NT, серверы), чтобы облегчить их идентификацию. Все компьютеры находятся в одной подсети.




Какие классы адресов могут быть использованы для данной сети?

---

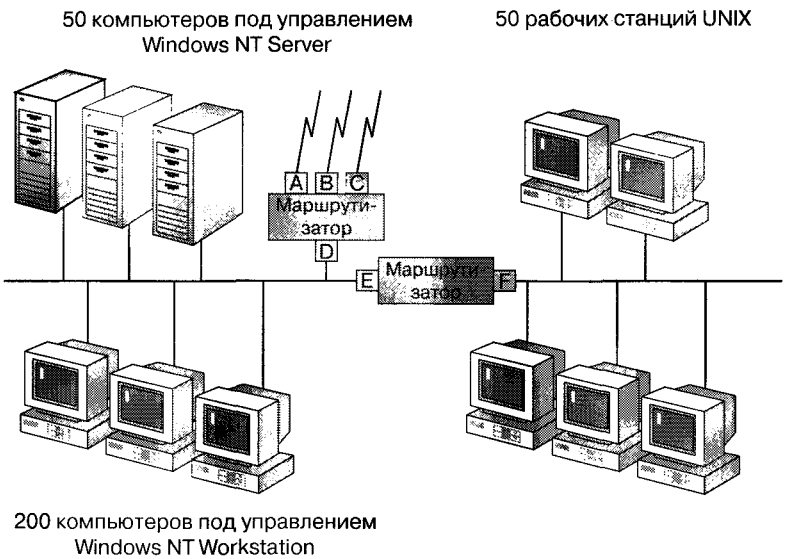
Какой из перечисленных ниже IP-адресов может быть использован для данной сети?

A. 197.200.3.0
B. 11.0.0.0
C. 221.100.2.0
D. 131.107.0.0

Используя выбранный Вами идентификатор сети, назначьте диапазон идентификаторов узлов каждому типу компьютеров так, чтобы можно было легко отличить друг от друга серверы и рабочие станции под управлением Windows NT и рабочие станции под управлением UNIX.

| Тип TCP/IP узла | Диапазон IP-адресов |
|---|---|
| Сервер Windows NT | |
| Рабочая станция Windows NT | |
| Рабочая станция UNIX | |

Определите, сколько идентификаторов узлов и сетей необходимо для сети, изображенной ниже.




Сколько идентификаторов сетей нужно для этого сетевого окружения?

Сколько идентификаторов узлов нужно для этого сетевого окружения?

Какой шлюз по умолчанию (интерфейс маршрутизатора) должен быть указан для рабочих станций с ОС Windows NT, которые связываются, в основном, только с рабочими станциями UNIX?

## Резюме

Для назначения корректных IP-адресов следует учитывать определённые соображения. Чтобы все узлы одной сети взаимодействовали друг с другом, они должны иметь одинаковые идентификаторы сети. Каждому узлу TCP/IP, включая интерфейсы маршрутизаторов, необходим уникальный идентификатор узла.

# Занятие 4. IP-адреса и маски подсетей

Маска подсети необходима каждому узлу TCP/IP. На этом занятии рассматривается назначение маски подсети и ее роль в маршрутизации IP-пакетов. Дополнительно о масках подсетей рассказывается в главе 5.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать назначение и роль маски подсети;
- ✓ использовать операцию логического «И» для определения IP-адреса назначения.

**Продолжительность занятия – 15 минут**

Маска подсети — это 32-разрядное значение, используемое для выделения (маскирования) из IP-адреса его частей: идентификаторов сети и узла. Такая процедура необходима при выяснении того, относится тот или иной IP-адрес к локальной или удаленной сети.

Каждый узел TCP/IP должен иметь маску подсети — либо задаваемую по умолчанию (в том случае, когда сеть не делится на подсети), либо специальную (если сеть разбита на несколько подсетей).

## Маска подсети, задаваемая по умолчанию

Задаваемая по умолчанию маска подсети используется в том случае, если сеть TCP/IP не разделяется на подсети. Даже в сети, состоящей из одного сегмента, всем узлам TCP/IP необходима маска подсети. Значение маски подсети по умолчанию зависит от используемого класса IP-адресов.

В маске подсети биты, соответствующие идентификатору сети, устанавливаются в 1. Таким образом, значение каждого октета будет равно 255. Все биты, соответствующие идентификатору узла, устанавливаются в 0.

| Класс адресов | Биты, используемые для маски подсети | Десятичная запись с точками |
|---|---|---|
| Класс A | 11111111 00000000 00000000 00000000 | 255.0.0.0 |
| Класс B | 11111111 11111111 00000000 00000000 | 255.255.0.0 |
| Класс C | 11111111 11111111 11111111 00000000 | 255.255.255.0 |

*Пример для класса B*

| | | |
|---|---|---|
| IP-адрес | 131.107. | 16.200 |
| Маска подсети | 255.255. | 0.0 |
| Идентификатор сети | 131.107. | y.z |
| Идентификатор узла | w.x. | 16.200 |

## Определение адреса назначения пакета

Протокол IP использует операцию логического «И» для определения того, какому узлу предназначен пакет — расположенному в локальной или удаленной сети. Эта операция осуществляется за счет внутренних механизмов протокола IP, и Вам, возможно, не придется ее выполнять.

Когда инициализируется поддержка TCP/IP, IP-адрес узла складывается с его маской подсети с помощью логического «И». Перед отправкой каждого IP-пакета, IP-адрес назначения точно так же складывается с той же маской подсети. Если результаты двух перечисленных выше операций совпадают, это означает, что получатель пакета находится в локальной сети. В противном случае пакет отправляется на IP-адрес маршрутизатора.

Для того чтобы выполнить операцию логического «И», TCP/IP сравнивает попарно соответствующие биты адреса и маски. Если оба бита равны 1, результат также равен 1. В остальных случаях результирующий бит равен 0.

| Сопоставление бит | Результат |
|---|---|
| 1 «И» 1 | 1 |
| 1 «И» 0 | 0 |
| 0 «И» 0 | 0 |
| 0 «И» 1 | 0 |

| | |
|---|---|
| *IP-адрес* | 10011111 11100000 00000111 10000001 |
| *Маска подсети* | 11111111 11111111 00000000 00000000 |
| *Результат* | 10011111 11100000 00000000 00000000 |

## Упражнения

Выполните логическую операцию «И» с перечисленными ниже IP-адресами и маской подсети и определите, принадлежит ли IP-адрес получателя к локальной или удаленной сети.

| | |
|---|---|
| IP-адрес отправителя | 10011001 10101010 00100101 10100011 |
| Маска подсети | 11111111 11111111 00000000 00000000 |
| Результат | |
| IP-адрес получателя | 11011001 10101010 10101100 11101001 |
| Маска подсети | 11111111 11111111 00000000 00000000 |
| Результат | |

1. Получен ли одинаковый результат?

2. Принадлежит IP-адрес получателя к локальной или удаленной сети?

## Резюме

Маска подсети по умолчанию используется в сетях TCP/IP, которые не разделены на подсети. Специальное значение маски подсети используется в том случае, когда сеть состоит из нескольких подсетей. С помощью операции логического «И» протокол IP определяет, предназначен пакет узлу в локальной или удаленной сети.

# Занятие 5. IP-адресация в IP версии 6.0

Существующая в протоколе IP версии 4 схема 32-разрядной адресации привела к дефициту идентификаторов сетей. На этом занятии Вы узнаете о перспективных направлениях развития IP-адресации.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как протокол IP версии 6 позволяет решить существующие проблемы IP-адресации.

**Продолжительность занятия — 5 минут**

Используемый в настоящее время формат заголовка IP-пакета не изменялся с 70-х годов, что является несомненной заслугой его разработчиков. Однако они не рассчитывали на стремительный рост Интернета и, соответственно, то, что пространство адресов IP версии 4 будет исчерпано.

В новой версии протокола IP (IPv6), ранее именовавшейся *IP нового поколения* (IP — The Next Generation, IPng), воплощен ряд идей по обновлению IP.

IPv6 создавался специально для решения двух основных проблем — нехватки имеющегося пространства адресов и его возможного дефицита в будущем. В IPv6 адрес состоит из 16-ти октетов. На письме он изображается в виде восьми пар октетов, разделенных двоеточиями. Октеты записываются в шестнадцатеричном формате.

В IPv6 применена принципиально иная структура пакета, не совместимая с версией 4. Она имеет ряд преимуществ: расширенное адресное пространство, упрощенный формат заголовка, поддержку ориентированного на реальное время трафика и механизм добавления новых возможностей.

Расширенное адресное пространство — одна из ключевых особенностей IPv6. В этой версии используются 128-разрядные адреса получателей и отправителей (в 4 раза больше, чем в IPv4). В 128 разрядах содержится более $3x10^{38}$ возможных значений, что обеспечивает достаточно адресов на ближайшее и отдаленное будущее. Так может выглядеть адрес в IPv6:

```
4A3F:AE57:F240:56C4:3409:AE52:440F:1403
```

Заголовок пакета IPv6 разработан таким образом, чтобы минимизировать содержащуюся в нем информацию. Поля опций и поля, не являющиеся необходимыми, вынесены в специальные расширения, расположенные после заголовка. Все, что не входит в основное содержание заголовка IPv6, может быть размещено в следующих за ним расширениях.

Новое специальное поле позволяет предварительно выделять сетевые ресурсы на пути следования пакета, что гарантирует полосу пропускания с ограниченной задержкой для таких сервисов реального времени, как передача по сети голоса и видео.

И наконец, важнейшее преимущество IPv6 — возможность его расширения на случай появления непредвиденных функциональных возможностей. Оно достигается за счет расширений, располагаемых непосредственно после основного заголовка. Таким образом, обеспечивается встроенная поддержка новых аппаратных и программных средств.

Примечание Протокол IPv6 описан в RFC 1883. Копия этого документа находится на Web-страничке *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

В адресном пространстве текущей версии IP возник дефицит адресов. В IPv6 используется принципиально иная структура пакета, имеющая ряд преимуществ: расширенное адресное пространство, упрощенный формат заголовка, поддержку ориентированного на реальное время трафика и механизм добавления новых функциональных возможностей.

# Закрепление материала



Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

2. Какие значения не могут быть использованы в качестве идентификаторов сетей и почему? Какие значения не могут быть использованы в качестве идентификаторов узлов? Почему?

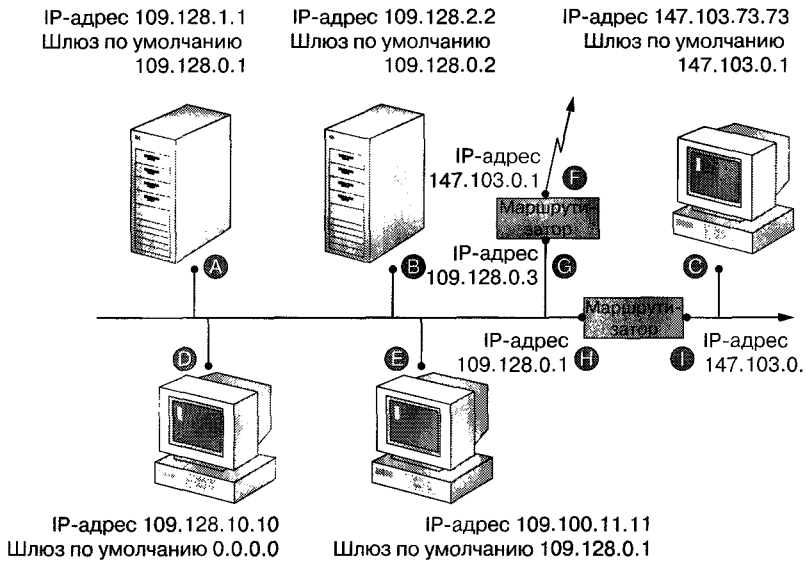
3. Когда необходим уникальный идентификатор сети?

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

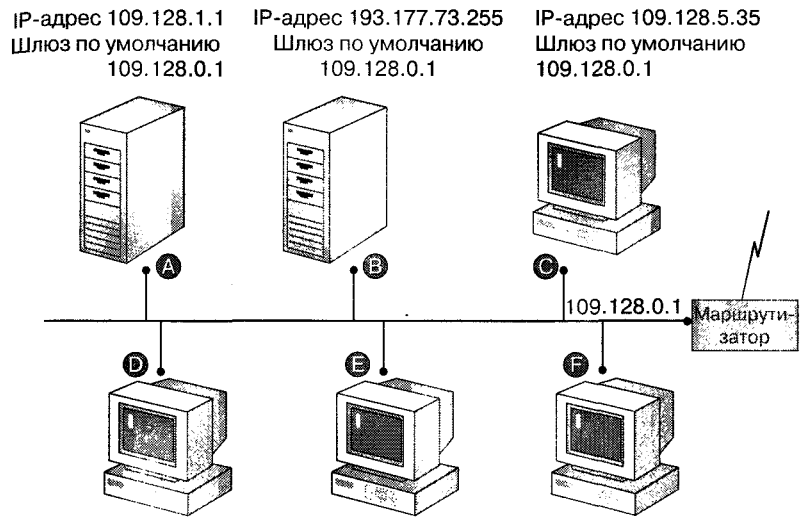
## Упражнения

Рассмотрите две IP-сети, определите скрытые проблемы, связанные с IP-адресацией, и объясните их возможные последствия.

Изучите следующую иллюстрацию, перечислите все проблемы IP-адресации и объясните, как каждая из них может повлиять на сетевые соединения. Правильно ли выбраны IP-адреса и шлюзы по умолчанию в каждом из следующих случаев?




Изучите следующую иллюстрацию, перечислите все проблемы IP-адресации и объясните, как каждая из них может повлиять на сетевые соединения. Правильно ли выбраны IP-адреса и шлюзы по умолчанию в каждом из следующих случаев?




## Дополнительная информация

- Заново просмотрите все упомянутые документы RFC — на прилагаемом к курсу компакт-диске.

# Подсети



## В этой главе

Вы узнаете, как назначать IP-адреса в нескольких TCP/IP сетях, используя единственный идентификатор сети. В занятиях этой главы рассматриваются основные концепции построения сетей на основе объединения подсетей. Выполняя упражнения, Вы поймете, когда необходимо применять подсети, когда следует пользоваться маской подсети по умолчанию, а когда — специальной маской и как ее определить, а также каким образом задать диапазон IP-адресов для подсети.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- изучить материал главы 4;
- установить Microsoft Windows NT Server 4.0 с поддержкой TCP/IP.

# Занятие 1. Общие сведения о подсетях

*Подсеть* (subnet) — это физический сегмент TCP/IP сети, в котором используются IP-адреса с общим идентификатором сети. Как правило, организации получают идентификатор сети от *Информационого Центра Интернета* (Internet Network Information Center, InterNIC). Сейчас Вы узнаете о том, какие условия нужно соблюдать при построении подсетей.

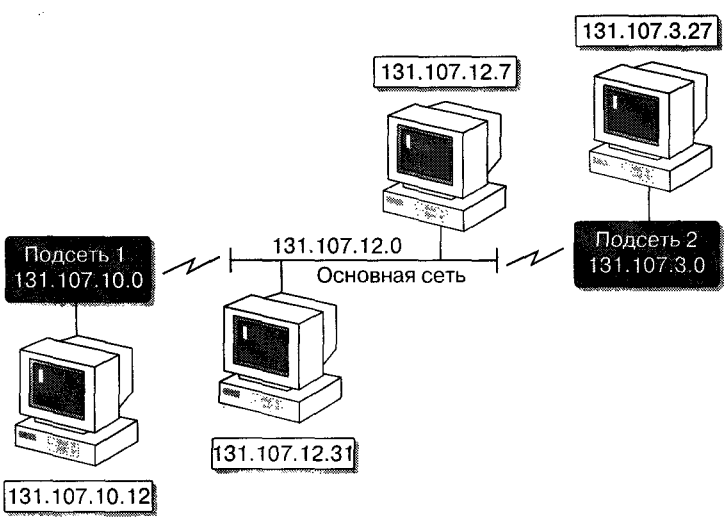
**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить назначение подсетей и преимущества их использования.

**Продолжительность занятия – 10 минут**

Для того чтобы разделить сеть на несколько подсетей, необходимо использовать различные идентификаторы сети (в данном случае подсети) для каждого сегмента. Как показано на рисунке, уникальные идентификаторы подсетей создаются путем разбиения идентификатора узла на две группы бит.

Первая из них служит для идентификации сегмента объединенной сети, вторая — для идентификации конкретного узла. Такой механизм называется *делением на подсети* (subnetting или subnetworking). Деление на подсети не является необходимым в изолированной сети (т.е. не имеющей выхода в Интернет).



Использование подсетей имеет целый ряд преимуществ. В организациях подсети применяют для объединения нескольких физических сегментов в одну логическую сеть. Применяя подсети, Вы можете:

- совместно использовать различные сетевые технологии (такие как Ethernet, Token Ring);
- преодолеть существующие ограничения, например на максимальное количество узлов в одном сегменте;
- уменьшить нагрузку на сеть, перенаправляя сетевой трафик и сокращая число широковещательных пакетов.

Примечание Деление сетей на подсети описано в RFC 950. Копия этого документа находится на Web-страничке *Course Materials* прилагаемого к курсу компакт-диска.

## Использование подсетей

Перед началом работы с подсетью необходимо определить, каким требованиям должна отвечать Ваша сеть сейчас и каким — в будущем. Воспользуйтесь следующей схемой.

1. Определите число физических сегментов Вашей сети.
2. Определите количество IP-адресов, необходимое для каждого сегмента. Каждому узлу TCP/IP нужен по крайней мере один IP-адрес.
3. В соответствии с Вашими требованиями определите:
   - одну маску подсети для всей Вашей сети;
   - уникальные идентификаторы подсети для каждого физического сегмента;
   - диапазон идентификаторов узлов для каждой подсети.

## Биты маски подсети

Перед тем как сформировать маску подсети, приблизительно определите, сколько сегментов и узлов в сегменте Вам потребуется в будущем.

Задав больше бит для маски подсети, Вы сможете увеличить количество подсетей, но максимальное число узлов в каждой из них сократится. Следующий пример для сети класса B, иллюстрирует эту зависимость:

3 бита = 6 подсетей = 8 000 узлов в подсети

8 бит = 254 подсети = 254 узла в подсети

Если Вы используете больше бит, чем необходимо, это позволит в будущем увеличить число подсетей, но ограничит количество узлов в каждой из них.

Используя меньше бит, Вы оставите возможность для увеличения числа узлов в подсети, но лимитируете количество подсетей.

## Резюме

Подсеть — это физический сегмент TCP/IP сети, в котором используются IP-адреса с одним идентификатором сети. Механизм назначения IP-адресов для подсетей называется делением на подсети. Количество бит, отводимых для маски подсети, определяет максимальное число подсетей и узлов в них.

# Занятие 2. Определение маски подсети

Задание маски подсети состоит из трех этапов. На этом занятии Вы узнаете, из каких именно, и выполните несколько упражнений на определение маски подсети.

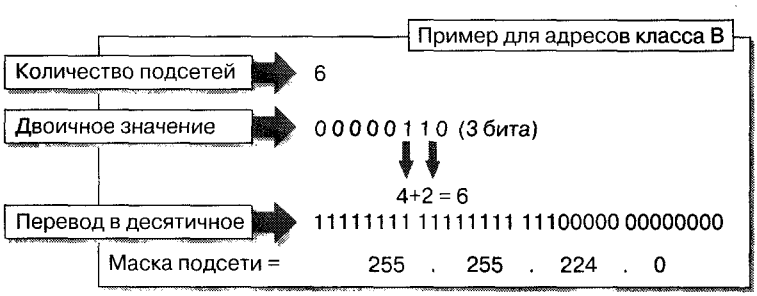
**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить назначение специальной маски подсети;
- ✓ задать правильную маску подсети в зависимости от ситуации.

**Продолжительность занятия — 45 минут**

Задание маски подсети необходимо, если Вы разбиваете сеть на подсети. Для этого выполните следующие операции.

1. Определите количество физических сегментов в Вашей сети и переведите это значение в двоичный формат.
2. Подсчитайте, сколько бит необходимо для записи полученного значения в двоичном формате. Например, если в Вашей сети шесть сегментов, двоичное значение равно 110, и для его записи в двоичном формате требуется 3 бита.
3. Запишите эти биты единицами (количество требуемых бит равно количеству записываемых единиц), дополнив их справа нулями до одного байта. Переведите полученное двоичное значение в десятичный формат. В рассматриваемом примере для идентификатора подсети потребовалось 3 бита. Переведя 11100000 в десятичное число, получим 224. Тогда маска подсети будет иметь вид 255.255.224.0 (для адресов класса B).




## Последовательность бит маски подсети

Так как подсети определяются соответствующей маской, администратор может использовать в качестве идентификатора подсети любую совокупность

бит. Когда деление на подсети впервые описывалось в RFC 950, было рекомендовано использовать старшие биты для формирования идентификаторов подсети. На сегодняшний день лишь немногие производители маршрутизаторов поддерживают идентификаторы подсети, состоящие из младших или не записанных последовательно бит. Более того, формирование идентификатора подсети из совокупности последовательных старших бит той части маски подсети, которая соответствует локальному адресу, стало обязательным требованием.

## Таблицы преобразования

Ниже перечислены маски подсетей для сетей класса A, заданные с использованием одного октета.

| Количество подсетей | Требуемое число бит | Маска подсети | Количество узлов в подсети |
|---|---|---|---|
| 0 | 1 | Не используется | Не используется |
| 2 | 2 | 255.192.0.0 | 4 194 302 |
| 6 | 3 | 255.224.0.0 | 2 097 150 |
| 14 | 4 | 255.240.0.0 | 1 048 574 |
| 30 | 5 | 255.248.0.0 | 524 286 |
| 62 | 6 | 255.252.0.0 | 262 142 |
| 126 | 7 | 255.254.0.0 | 131 070 |
| 254 | 8 | 255.255.0.0 | 65 534 |

В следующей таблице перечислены маски подсетей для сетей класса B, заданные с использованием одного октета.

| Количество подсетей | Требуемое число бит | Маска подсети | Количество узлов в подсети |
|---|---|---|---|
| 0 | 1 | Не используется | Не используется |
| 2 | 2 | 255.255.192.0 | 16 382 |
| 6 | 3 | 255.255.224.0 | 8 190 |
| 14 | 4 | 255.255.240.0 | 4 094 |
| 30 | 5 | 255.255.248.0 | 2 046 |
| 62 | 6 | 255.255.252.0 | 1 022 |
| 126 | 7 | 255.255.254.0 | 510 |
| 254 | 8 | 255.255.255.0 | 254 |

В следующей таблице перечислены маски подсетей для сетей класса С, заданные с использованием одного октета.

| Количество подсетей | Требуемое число бит | Маска подсети | Количество узлов в подсети |
|---|---|---|---|
| Не используется | 1 | Не используется | Не используется |
| 2 | 2 | 255.255.255.192 | 62 |
| 6 | 3 | 255.255.255.224 | 30 |
| 14 | 4 | 255.255.255.240 | 14 |
| 30 | 5 | 255.255.255.248 | 6 |
| 62 | 6 | 255.255.255.252 | 2 |
| Не используется | 7 | Не используется | Не используется |
| Не используется | 8 | Не используется | Не используется |

## Использование нескольких октетов

До этого момента Вы задавали маски подсети, используя только один октет. Иногда же полезно применять более одного октета, т.е. больше 8 бит. Таким образом Ваша схема адресации станет гибче.

Предположим, Вы конфигурируете интрасеть крупной организации, которая планирует объединить в общую сеть все свои подсети в Европе, Северной Америке и Азии. В совокупности в 30 географических регионах около 1 000 подсетей, состоящих приблизительно из 750 узлов каждая.

В этом случае можно использовать несколько идентификаторов для сетей класса В и делить на подсети каждую из них. В соответствии с требуемым количеством узлов в подсети Вам следует использовать маску 255.255.252.0. Для нужного числа подсетей Вам понадобится по меньшей мере 16 адресов класса В.

Однако существует более простое решение. Так как Ваши компьютеры находятся в интрасети, Вы можете использовать частную сеть, т.е один из специально зарезервированных идентификаторов сетей. Если Вы выберете значение 10.0.0.0 в качестве идентификатора сети класса А, то сможете и удовлетворить существующие требования, и обеспечить будущее расширение сети. Очевидно, что для деления на 1 000 подсетей в этом случае недостаточно только одного октета. Используя второй и часть третьего октета, Вы обойдетесь одним идентификатором сети.

| Идентификатор сети | Маска подсети | Маска подсети в двоичном формате |
|---|---|---|
| 10.0.0.0 | 255.255.248.0 | 11111111 11111111 11111000 00000000 |

Используя 13 бит для идентификатора подсети при разбиении на подсети сетей класса A, Вы получаете 8 190 подсетей, в каждой из которых может быть до 2 046 узлов.

Таким образом, Ваше решение и отвечает поставленным требованиям, и не лимитирует дальнейшее расширение.

## Упражнения

Определите необходимую маску подсети для различных ситуаций. Помните, что деление на подсети применяется не всегда.

1. Адрес класса A в локальной сети.

2. Адрес класса B в локальной сети, состоящей из 4 000 узлов.

3. Адрес класса C в локальной сети, состоящей из 254 узлов.

4. Адрес класса A в сети, содержащей 6 подсетей.

5. Адрес класса B в сети, содержащей 126 подсетей.

6. Адрес класса A, если в настоящее время сеть содержит 30 подсетей, в следующем году планируется увеличить их число до 65, причем в каждой подсети будет более 50 000 узлов?

7. Какой запас на случай будущего расширения сети обеспечивает маска подсети из предыдущего задания?

8. Адрес класса B, если в настоящее время сеть содержит 14 подсетей, в течение следующих двух лет размер каждой подсети может увеличиться вдвое, причем в каждой подсети будет не более 1500 узлов.

9. Какой запас на случай будущего расширения сети обеспечивает маска подсети из предыдущего задания?

Рассмотрите две некорректно заданные маски подсети и определите, что произойдет при попытке установить соединение с узлом из локальной или удаленной сети.

Используя приведенную ниже информацию, преобразуйте IP-адреса двух Ваших компьютеров в двоичный формат. Применив логическое «И», сложите их с маской подсети и определите, почему она задана неправильно.

| | | |
|---|---|---|
| Ваш IP-адрес | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.255.248 | 11111111 11111111 11111111 11111000 |
| Результат | | |
| IP-адрес получателя | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.255.248 | 11111111 11111111 11111111 11111000 |
| Результат | | |

Можно ли по результату выполнения операции сказать, принадлежат адреса отправителя и получателя к одной сети или к разным?

---

Объясните, почему Вы не смогли бы успешно выполнить Ping шлюза по умолчанию?

---

Используя приведенную ниже информацию, преобразуйте IP-адрес Вашего компьютера и IP-адрес удаленного узла в двоичный формат. Применив логическое «И», сложите их с маской подсети и определите, почему она задана неправильно.

| | | |
|---|---|---|
| Ваш IP-адрес | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.0.0 | 11111111 11111111 00000000 00000000 |
| Результат | | |
| IP-адрес | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.0.0 | 11111111 11111111 00000000 00000000 |
| Результат | | |

Свидетельствует ли результат, что IP-адрес получателя и маска подсети принадлежат удаленной сети или локальной сети?

---

Почему Вы не смогли бы успешно выполнить Ping удаленного узла?

---

Сравните результаты, полученные из-за применения неправильной маски подсети. Попытайтесь понять различие в поведении TCP/IP в случаях,

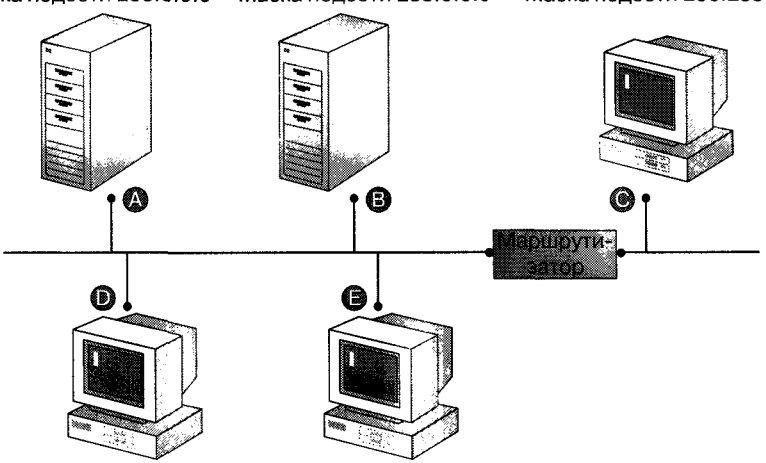
когда маска подсети относится к локальной или удаленной сети. Какие выводы можно сделать о том, как TCP/IP использует маску подсети?

Рассмотрите два примера, определите, какие проблемы могут возникнуть, и объясните их возможное проявление.

IP-адрес 109.128.1.1
Маска подсети 255.0.0.0

IP-адрес 109.128.2.2
Маска подсети 255.0.0.0

IP-адрес 147.103.73.73
Маска подсети 255.255.0



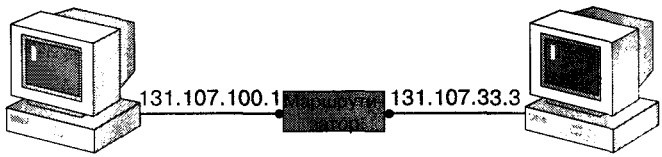

IP-адрес 109.128.10.10
Маска подсети 255.255.0.0

IP-адрес 109.100.11.11
Маска подсети 255.255.0.0

Для каких узлов маска подсети задана неправильно?

Как неправильное значение маски подсети влияет на работу этих узлов?

Каково правильное значение маски подсети?




IP-адрес 131.107.100.27
Маска подсети 255.255.0.0
Шлюз по умолчанию 131.107.100.1

IP-адрес 131.107.33.7
Маска подсети 255.255.0.0
Шлюз по умолчанию 131.107.3

Что неправильно в этой маске подсети?

Как это влияет на соединения?

Каково правильное значение маски подсети?

## Резюме

Если Вы хотите разделить свою сеть на подсети, необходимо задать маску подсети. Это можно сделать так: преобразовать количество физических сегментов сети в двоичный формат; подсчитать требуемое для его двоичной записи число бит; перевести его в десятичный формат. Для задания маски подсети можно использовать больше 8 бит — это увеличит гибкость схемы адресации.

# Занятие 3. Определение идентификаторов подсетей

Для задания идентификаторов подсетей используется то же число бит, что и для соответствующей маски подсети. Определить диапазон идентификаторов подсетей, входящих в объединенную сеть, можно несколькими способами. На этом занятии рассмотрены два из них.

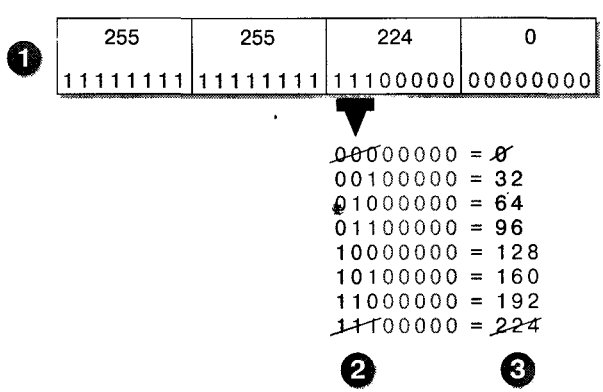
**Изучив материал этого занятия, Вы сможете:**

- ✓ различными способами определить диапазон идентификаторов подсетей, входящих в объединенную сеть;
- ✓ определить общую маску подсети для использования в глобальной сети, состоящей из множества подсетей.

**Продолжительность занятия — 20 минут**

Возможные идентификаторы подсети комбинируются из тех бит в адресе узла, которые используются в маске подсети. Определите количество возможных комбинаций этих бит и выпишите их в десятичном формате. Ниже приведена процедура, необходимая для определения диапазона идентификаторов подсетей последовательность действий.

1. Выпишите все возможные комбинации бит, используемых для формирования маски подсети.
2. Вычеркните комбинации, где значения всех бит одновременно равны 0 и 1. Это нужно сделать потому, что они представляют недопустимые IP-адреса: комбинация «все 0» означает всю локальную сеть, а «все 1» совпадает с маской подсети.
3. Перевелите в десятичный формат значения комбинации бит для каждой подсети. Каждое такое значение представляет одну сеть и используется для определения диапазона идентификаторов узлов в ней.



## Адреса подсетей специального назначения

Идентификаторы подсетей, состоящие из одних нулей или одних единиц, называются *адресами подсетей специального назначения* (special-case subnet addresses). Идентификатор из одних единиц применяется для широковещания в подсети. Идентификатор из одних нулей обозначает локальную подсеть. При делении на подсети такие идентификаторы использовать не рекомендуется. Однако их применение возможно, когда все маршрутизаторы и прочее оборудование Вашей сети поддерживает их. Ограничения, связанные с их использованием, описываются в RFC 950.

## Быстрый способ определения идентификаторов подсетей

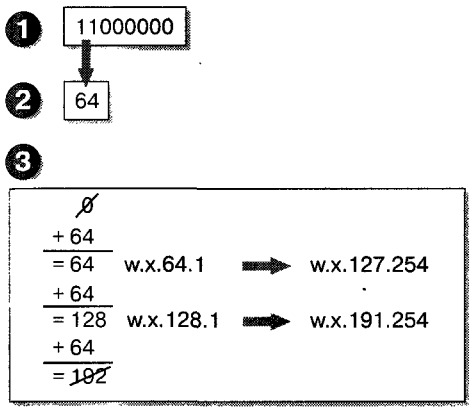
Описанный выше способ определения идентификаторов подсетей неэффективен, если Вы отводите под маску подсети больше 4 бит. В таком случае Вам придется выписывать и преобразовывать большое количество битовых комбинаций. Ниже показано, как быстро определить диапазон идентификаторов подсетей.

1. Запишите единицами количество бит, необходимых для идентификаторов подсетей, и дополните их справа нулями до одного байта. Например, если Вы используете 2 бита для идентификаторов подсетей, запишите это значение как 11000000.
2. Преобразуйте наименее значимый бит в десятичное число. Вы получите приращение для каждой очередной подсети. В предыдущем примере оно равно 64.
3. Начиная с нуля, выпишите последовательно получаемые с помощью приращения значения, пока не дойдете до 256.

---

Совет Если Вам известно необходимое число бит, Вы можете возвести число 2 в степень, соответствующую числу бит, и вычесть из результата 2, чтобы получить количество возможных битовых комбинаций.

---




## Упражнения

Определите маску подсети, соответствующую указанному диапазону IP-адресов.

1. Диапазон адресов от 128.71.1.1 до 128.71.254.254.

2. Диапазон адресов от 61.8.0.1 до 61.15.255.254.

3. Диапазон адресов от 172.88.32.1 до 172.88.63.254.

4. Диапазон адресов от 111.224.0.1 до 111.239.255.254.

5. Диапазон адресов от 3.64.0.1 до 3.127.255.254.

## Резюме

Для определения диапазона идентификаторов подсетей можно использовать два способа — короткий и длинный. Последний неэффективен, если для маски подсети используется более 4 бит.

# Занятие 4. Определение идентификаторов узлов в подсети

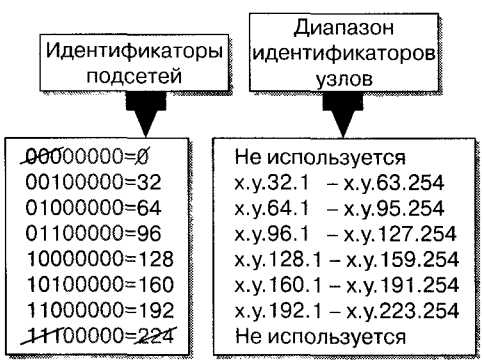
Количество узлов в подсети можно определить с помощью короткой процедуры. Фактически, когда Вы определяли идентификаторы подсетей, Вы тем самым задали также идентификаторы узлов в каждой из них. На этом занятии показано, как определять идентификаторы узлов в подсети. Выполняя упражнения, Вы закрепите полученные навыки.

**Изучив материал этого занятия, Вы сможете:**

- ✓ определить диапазон идентификаторов узлов в подсети, используя для этого идентификатор подсети.

**Продолжительность занятия — 30 минут**

Каждое очередное значение идентификатора подсети, увеличенное на единицу (см. предыдущее занятие), — не что иное, как начало диапазона идентификаторов узлов в подсети. Следующее по порядку возможное значение идентификатора подсети, уменьшенное на единицу, дает конечное значение диапазона. Это проиллюстрировано ниже.




В таблице указан допустимый диапазон идентификаторов узлов для сети класса B в случае, когда для маски подсети используется 3 бита.

| Значения бит | Десятичное значение | Начало диапазона | Конец диапазона |
|---|---|---|---|
| **00**000000 | 0 | Не используется | Не используется |
| **00**100000 | 32 | x.y.32.1 | x.y.63.254 |
| **01**000000 | 64 | x.y.64.1 | x.y.95.254 |
| **01**100000 | 96 | x.y.96.1 | x.y.127.254 |
| **10**000000 | 128 | x.y.128.1 | x.y.159.254 |
| **10**100000 | 160 | x.y.160.1 | x.y.191.254 |
| **11**000000 | 192 | x.y.192.1 | x.y.223.254 |
| **11**100000 | 224 | Не используется | Не используется |

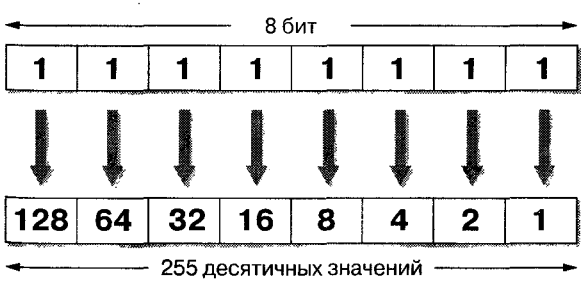
▶ **Определение количества узлов в подсети**

1. Подсчитайте число бит, которые можно использовать для идентификаторов узлов. Например, если Ваша сеть — класса B, и 16 бит используются для идентификатора сети, а еще 2 — для идентификаторов подсетей, то для идентификаторов узлов остается 14 бит.
2. Запишите это число двоичными единицами и преобразуйте полученное значение в десятичный формат. В рассматриваемом примере 11111111111111 имеет десятичное значение 16383.
3. Вычтите из него 1.

Совет Если Вам известно необходимое для идентификаторов узлов число бит, Вы можете возвести число 2 в степень, соответствующую числу бит и вычесть из полученного значения 2.

## Упражнения

Далее Вы попрактикуетесь в определении диапазона идентификаторов сетей, используя приведенную ниже иллюстрацию.



Определите идентификаторы подсетей для объединенной сети, состоящей из двух сетей, используя 2 бита маски подсети класса B.

1. Выпишите все возможные битовые комбинации для указанной ниже маски подсети. Переведите их в десятичный формат, чтобы определить начальное значение идентификаторов узлов для каждой подсети.

| 255 | 255 | 192 | 0 |
|---|---|---|---|
| 11111111 | 11111111 | 11000000 | 00000000 |
| Не используется | 00000000 | = | 0 |
| Подсеть 1 | _____ | = | __ |
| Подсеть 2 | _____ | = | __ |
| Не используется | 11000000 | = | 192 (маска подсети) |

2. Выпишите диапазон идентификаторов узлов для каждой подсети.

| Подсеть | Начальное значение | Конечное значение |
|---|---|---|
| Подсеть 1 | w.x.____.1 | w.x._____.254 |
| Подсеть 2 | w.x.____.1 | w.x._____.254 |

Определите диапазон идентификаторов сетей для объединенной сети, состоящей из 14 подсетей, используя 4 бита маски подсети класса B.

1. Выпишите все возможные битовые комбинации для указанной ниже маски подсети. Переведите их в десятичный формат, чтобы определить начальное значение идентификаторов узлов для каждой подсети.

| 255 | 255 | 240 | 0 |
|---|---|---|---|
| 11111111 | 11111111 | 11110000 | 00000000 |
| Не используется | 00000000 | = | 0 |
| Подсеть 1 | _____ | = | ___ |
| Подсеть 2 | _____ | = | ___ |
| Подсеть 3 | _____ | = | ___ |
| Подсеть 4 | _____ | = | ___ |
| Подсеть 5 | _____ | = | ___ |
| Подсеть 6 | _____ | = | ___ |
| Подсеть 7 | _____ | = | ___ |
| Подсеть 8 | _____ | = | ___ |
| Подсеть 9 | _____ | = | ___ |
| Подсеть 10 | _____ | = | ___ |

*(продолжение)*

| | | | |
|---|---|---|---|
| Подсеть 11 | _____ | = | ___ |
| Подсеть 12 | _____ | = | ___ |
| Подсеть 13 | _____ | = | ___ |
| Подсеть 14 | _____ | = | ___ |
| Не используется | 11110000 | = | 240 (маска подсети) |

2. Выпишите диапазон идентификаторов узлов для каждой подсети.

| Подсеть | Начальное значение | Конечное значение |
|---|---|---|
| Подсеть 1 | w.x._____.1 | w.x._____.254 |
| Подсеть 2 | w.x._____.1 | w.x._____.254 |
| Подсеть 3 | w.x._____.1 | w.x._____.254 |
| Подсеть 4 | w.x._____.1 | w.x._____.254 |
| Подсеть 5 | w.x._____.1 | w.x._____.254 |
| Подсеть 6 | w.x._____.1 | w.x._____.254 |
| Подсеть 7 | w.x._____.1 | w.x._____.254 |
| Подсеть 8 | w.x._____.1 | w.x._____.254 |
| Подсеть 9 | w.x._____.1 | w.x._____.254 |
| Подсеть 10 | w.x._____.1 | w.x._____.254 |
| Подсеть 11 | w.x._____.1 | w.x._____.254 |
| Подсеть 12 | w.x._____.1 | w.x._____.254 |
| Подсеть 13 | w.x._____.1 | w.x._____.254 |
| Подсеть 14 | w.x._____.1 | w.x._____.254 |

Используйте быстрый метод для определения диапазона идентификаторов сетей для 14 сетей. Сравните результаты с полученными в предыдущем задании. Они должны совпадать. Первый пункт этого упражнения уже выполнен.

1. Запишите двоичными единицами количество бит, используемых для маски подсети, дополнив его справа нулями до одного байта.

| 255 | 255 | 240 | 0 |
|---|---|---|---|
| 11111111 | 11111111 | 11110000 | 00000000 |

2. Укажите десятичное значение самого младшего бита из установленных в 1.

_____

3. Запишите двоичными единицами количество бит, используемых для маски подсети, переведите полученную запись в десятичный формат и вычтите 1. Вы получите возможное количество подсетей.

4. Начиная с нуля, добавляйте приращение, полученное в п. 2, столько раз сколько возможно различных битовых комбинаций (вычислено в п. 3).

Определите диапазон идентификаторов узлов для каждой из перечисленных подсетей.

1. Идентификатор сети — 75.0.0.0, маска подсети 255.255.0.0, две подсети.

2. Идентификатор сети — 150.17.0.0, маска подсети 255.255.255.0, четыре подсети.

3. Идентификаторы сетей — 107.16.0.0 и 107.32.0.0, маска подсети 255.240.0.0, две подсети.

4. Идентификаторы сетей — 190.1.16.0, 190.1.32.0, 190.1.48.0, 190.1.64.0, маска подсети 255.255.248.0, четыре подсети.

5. Идентификаторы сетей — 154.233.32.0, 154.233.96.0 и 154.233.160.0, маска подсети 255.255.224.0, три подсети.

## Резюме

Для того чтобы определить количество узлов в подсети, необходимо выполнить три операции: подсчитайте число бит, доступных для использования в идентификаторах узлов, переведите это записанное единицами значение в десятичный формат и вычтите 1.

# Занятие 5. Объединение нескольких сетей

Чтобы пространство идентификаторов сетей не было исчерпано, организации, координирующие развитие Интернета, разработали схему *объединения сетей* (supernetting), с которой Вы и познакомитесь на этом занятии.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать концепции объединения сетей.

**Продолжительность занятия — 10 минут**

В отличие от деления на подсети, при объединении сетей часть бит идентификатора сети маскируется как идентификатор узла — это увеличивает эффективность маршрутизации. Например, вместо того чтобы предоставить 1 идентификатор сети класса B организации, имеющей 2 000 узлов, InterNIC выделяет ей 8 идентификаторов сетей класса C. Каждая такая сеть может содержать до 254 узлов, что в совокупности обеспечивает 2 032 идентификатора узлов.

Таким образом экономятся идентификаторы сетей класса B. Однако эта технология порождает новую проблему. При использовании обычных механизмов маршрутизации, маршрутизаторы в Интернете должны поддерживать еще 7 дополнительных записей в своих таблицах, чтобы направлять пакеты в сеть подобной организации. Для того чтобы разгрузить маршрутизаторы Интернета, была разработана технология *бесклассовой маршрутизации* (Classless Inter-Domain Routing, CIDR), которая позволяет объединить все 8 записей таблицы маршрутизации в 1, относящуюся одновременно ко всем выделенным организации сетям класса C.

До объединения сетей

| Таблица маршрутизации маршрутизатора B | | |
|---|---|---|
| 220.78.168.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.169.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.170.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.171.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.172.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.173.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.174.0 | 255.255.255.0 | 220.78.168.1 |
| 220.78.175.0 | 255.255.255.0 | 220.78.168.1 |

После объединения сетей

| Таблица маршрутизации маршрутизатора B | | |
|---|---|---|
| 220.78.168.0 | 255.255.248.0 | 220.78.168.1 |

Таким образом, было выделено 8 идентификаторов сетей класса C — с 220.78.168.0 до 220.78.175.0. Запись в таблице маршрутизации формируется, как показано ниже.

| Идентификатор сети | Маска подсети | Маска подсети в двоичном виде |
|---|---|---|
| 220.78.168.0 | 255.255.248.0 | 11111111 11111111 11111000 00000000 |

При объединении сетей та сеть, для которой предназначен пакет, определяется выполнением операции логического «И» с использованием маски подсети и IP-адреса получателя. Если результат операции совпадает с идентификатором сети, пакет отправляется в соответствующую сеть. Эта процедура рассматривалась на предыдущем занятии.

Примечание Технология CIDR описывается в RFC 1518 и 1519. Копии этих документов находятся на Web-страничке *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

При объединении сетей часть бит идентификатора сети маскируется как идентификатор узла для повышения эффективности маршрутизации.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Выполняя упражнения, Вы подготовитесь к реальным ситуациям.

1. Каково назначение маски подсети?

2. Когда необходима маска подсети?

3. Когда используется маска подсети по умолчанию?

4. Когда необходимо задать специальную маску подсети?

## Упражнения

Задайте схему деления на подсети в каждом из следующих сценариев. Для каждого сценария определите:

- маску подсети;
- диапазон корректных идентификаторов сетей;
- шлюз по умолчанию для узлов каждой сети.

После этого ответьте на вопросы.

InterNIC выделил Вам один адрес сети класса B: 131.107.0.0. Интрасеть Вашей организации в настоящий момент состоит из 5 подсетей, в каждой из которых около 300 узлов. В следующем году число подсетей увеличится в 3 раза. В трех подсетях число узлов может достигнуть 1 000.

1. Сколько бит Вы использовали для маски подсети?

2. Какой запас на случай появления дополнительных сетей Вы оставили?

3. Какой запас на случай увеличения числа узлов Вы оставили?

InterNIC выделил Вам один адрес сети класса A: 124.0.0.0. Изолированная сеть Вашей организации в настоящий момент состоит из 5 подсетей. В каждой из подсетей около 500 000 узлов. В ближайшем будущем Вы планируете разделить эти 5 подсетей на 25 меньших, чтобы облегчить управление ими. Число узлов в каждой из них может достичь 300 000.

1. Сколько бит Вы использовали для маски подсети?

2. Какой запас на случай появления дополнительных сетей Вы оставили?

3. Какой запас на случай увеличения числа узлов Вы оставили?

В Вашей сети 5 подсетей, в каждой из которых около 300 узлов. В течение полугода количество подсетей превысит 100. Число узлов в каждой из них вряд ли станет больше 2 000. Вы не собираетесь подключать свою сеть к Интернету.

1. Какой класс адресов Вы использовали?

2. Сколько бит Вы использовали для маски подсети?

3. Какой запас на случай появления дополнительных сетей Вы оставили?

4. Какой запас на случай увеличения числа узлов Вы оставили?

Поставщик услуг Интернета получил диапазон из 2 048 адресов сетей класса С, начиная с 192.24.0.0 до 192.31.255.0.

1. Какой IP-адрес должен использоваться в таблице маршрутизации для направления пакетов в объединенную сеть этого провайдера?
2. Какая маска подсети должна использоваться для объединения всех этих сетей?

Клиенты этого провайдера предъявляют следующие требования:

- клиент 1 собирается иметь не более 2 023 узлов;
- клиент 2 собирается иметь не более 4 047 узлов;
- клиент 3 собирается иметь не более 1011 узлов;
- клиент 4 собирается иметь не более 500 узлов.

Определите значения недостающих параметров для каждого клиента.

1. Клиент 1
   Начальный IP-адрес 192.24.0.1
   Конечный IP-адрес 192.24.7.8
   Маска подсети
   _____
2. Клиент 2
   Начальный IP-адрес
   _____
   Конечный IP-адрес 192.24.31.254
   Маска подсети 255.255.240.0
3. Клиент 3
   Начальный IP-адрес 192.24.0.1
   Конечный IP-адрес
   _____
   Маска подсети 255.255.252.0
4. Клиент 4
   Начальный IP-адрес 192.24.14.1
   Конечный IP-адрес 192.24.15.254
   Маска подсети
   _____

# Дополнительная информация

- Изучите все документы RFC на прилагаемом к курсу компакт-диске

# Реализация IP-маршрутизации



## В этой главе

В этой главе Вам предложен обзор концепций IP-маршрутизации и способы реализации IP-маршрутизации на компьютере, работающем под управлением Microsoft Windows NT 4.0. Занятия посвящены построению статической таблицы маршрутизации, конфигурированию Windows NT-компьютера для работы в качестве IP-маршрутизатора, определению неисправности шлюза по умолчанию и использованию утилиты Route для добавления статических маршрутов в таблицу маршрутизации.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить ОС Windows NT Server 4.0.

# Занятие 1. Общие сведения об IP-маршрутизации

*Маршрутизация* (routing) — процесс выбора пути для передачи пакетов. Маршрутизация осуществляется на узле TCP/IP в момент отправки IP-пакетов, а затем — на IP-маршрутизаторе.

*Маршрутизатор* (router) — это устройство, которое перенаправляет пакеты из одной физической сети в другую. Маршрутизаторы также называют *шлюзами* (gateways). На этом занятии Вы познакомитесь с основными концепциями IP-маршрутизации.

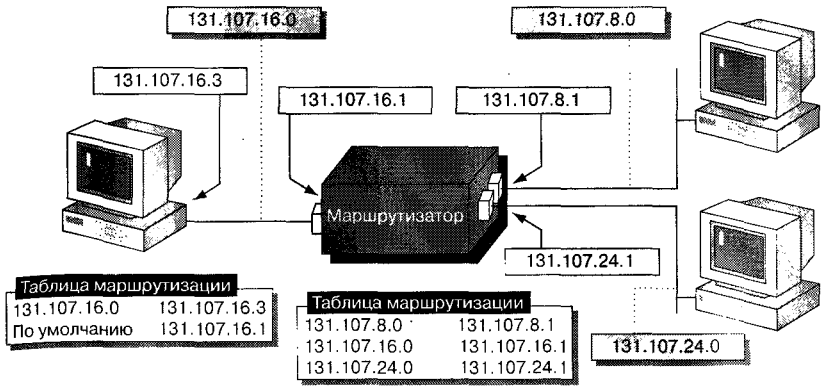
**Изучив материал этого занятия, Вы сможете:**

- ✓ понять основные концепции IP-маршрутизации;
- ✓ объяснить разницу между статической и динамической IP-маршрутизацией.

**Продолжительность занятия — 10 минут**

Решение перенаправить пакет должны принимать как узел-отправитель, так и маршрутизатор. Для принятия решения о маршрутизации IP-уровень обращается к хранящейся в памяти таблице маршрутизации (см. рис.). Она содержит записи с IP-адресами интерфейсов маршрутизатора, подключенных к сетям, с которыми он может связываться. По умолчанию маршрутизатор может посылать пакеты только в сети, для которых имеются сконфигурированные интерфейсы.

1. При попытке одного узла связаться с другим IP сначала определяет, является ли узел-получатель локальным или находится в другой сети.
2. Если узел-получатель находится в другой сети, IP ищет в таблице маршрутизации путь к удаленному узлу или удаленной сети.
3. Если прямой маршрут не обнаружен, то IP использует адрес шлюза по умолчанию для доставки пакета к маршрутизатору.
4. Маршрутизатор снова ищет путь к удаленному узлу или сети в таблице маршрутизации. Если путь не найден, пакет посылается по адресу шлюза, заданного по умолчанию для данного маршрутизатора.




При обнаружении очередного маршрута пакет посылается на следующий маршрутизатор — это называется *транзитом* (hop) — и в конце концов отправляется на узел-получатель. Если маршрут не найден, на узел-отправитель посылается сообщение об ошибке.

## Обнаружение неисправного шлюза

Протокол TCP может определить неисправность шлюза по умолчанию и внести необходимые изменения в таблицу IP-маршрутизации для использования другого шлюза. TCP пытается послать пакет на установленный по умолчанию шлюз до получения подтверждения. Однако, если значение *TcpMaxDataRetransmissions* превышено больше чем наполовину и в конфигурации компьютера указаны несколько шлюзов, TCP переключит IP на следующий в списке шлюзов по умолчанию.

Когда Вы конфигурируете компьютер, работающий под Windows NT, для использования нескольких IP-адресов шлюзов, обнаружение неисправного шлюза включено по умолчанию.

Примечание Реализованный Microsoft механизм определения неисправного шлюза включает повторные запросы TCP и метод триггерного повторного выбора, описанные в RFC 816. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Статическая и динамическая маршрутизация

Способ получения маршрутизатором информации зависит от используемого типа маршрутизации — статической или динамической. Статические маршрутизаторы требуют ручного построения и обновления таблиц маршрутизации. При изменении маршрута статические маршрутизаторы не информируют об этом друг друга. Они также не обмениваются маршрутами с динамическими маршрутизаторами.

Динамическая маршрутизация осуществляется такими протоколами, как *Routing Information Protocol* (RIP) и *Open Shortest Path First* (OSPF). Протоколы маршрутизации служат для периодического обмена информацией между динамическими маршрутизаторами. При изменении маршрута другие маршрутизаторы автоматически информируются об этом.

Windows NT Server версии 4.0 способен функционировать в качестве IP-маршрутизатора с использованием статической и динамической маршрутизации. Компьютер, работающий под управлением Windows NT, может быть сконфигурирован с несколькими сетевыми адаптерами, и сможет осуществлять маршрутизацию между ними. Такая система, идеальная для небольших корпоративных сетей, называется *компьютером с несколькими сетевыми интерфейсами* (multihomed computer).

Windows NT Server версии 4.0 может функционировать в качестве RIP-маршрутизатора, поддерживающего динамическое управление таблицами IP-маршрутизации. Протокол RIP исключает необходимость настраивать статические таблицы IP-маршрутизации.

Примечание Microsoft обеспечивает поддержку протоколов маршрутизации в Windows NT 4.0. Протокол RIP описан в RFC 1723. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

Маршрутизаторы пересылают пакеты из одной физической сети в другую. Уровень IP обращается к таблице маршрутизации, которая содержит записи с IP-адресами интерфейсов маршрутизаторов к другим сетям. При статическом способе требуется ручное построение и обновление таблиц маршрутизации. При динамическом маршрутизаторы автоматически получают информацию об изменении пути.

# Занятие 2. Статическая IP-маршрутизация

Статический маршрутизатор может связываться только с теми сетями, для которых имеет сконфигурированные интерфейсы. На этом занятии Вы научитесь конфигурировать статический маршрутизатор и модифицировать таблицу маршрутизации.

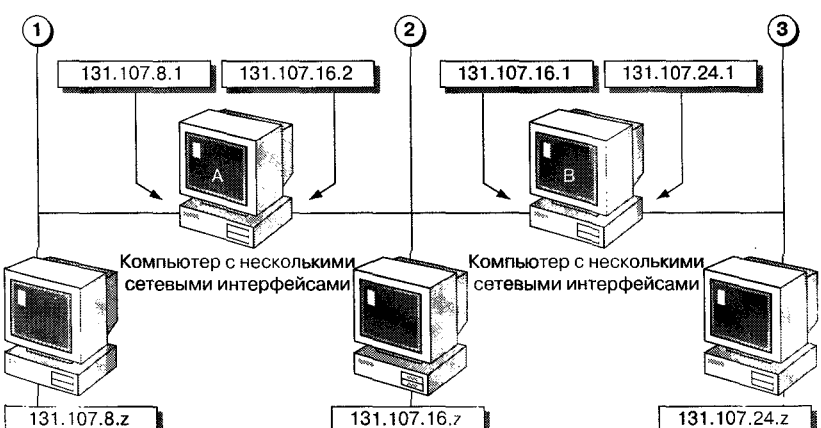
**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить требования к соединению со статическим IP-маршрутизатором;
- ✓ построить статическую таблицу маршрутизации.

**Продолжительность занятия — 25 минут**

Статический маршрутизатор надо предварительно настроить на маршрутизацию IP-пакетов в другие сети. В таблицу маршрутизации каждого маршрутизатора добавьте либо запись для каждой сети в корпоративной сети, либо адрес шлюза по умолчанию другого локального маршрутизатора.

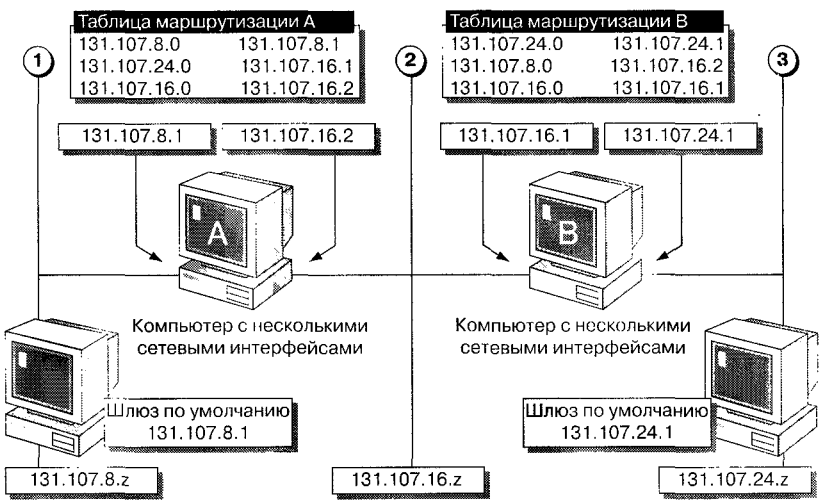
- Компьютер A локально соединен только с сетями 1 и 2. В результате узлы сети 1 могут соединяться с узлами сети 2, но не могут — с узлами сети 3.
- Компьютер B локально соединен только с сетями 2 и 3. Узлы сети 3 могут соединяться с узлами сети 2, но не могут — с узлами сети 1.



## Конфигурирование статических IP-маршрутизаторов

В корпоративной сети, имеющей по крайней мере один статический маршрутизатор, необходимо сконфигурировать записи статической таблицы маршрутизации для всех известных сетей на каждом маршрутизаторе.

- Запись статической таблицы маршрутизации создана на компьютере A. Она содержит идентификатор сети 3 и IP-адрес интерфейса (131.107.16.1), к которому компьютер A имеет прямой доступ и который может перенаправлять пакеты из сети 1 в сеть 3.
- Запись статической таблицы маршрутизации создана на компьютере B. Она содержит сетевой идентификатор сети 1, а также IP-адрес интерфейса (131.107.16.2), который напрямую доступен компьютеру B для того, чтобы перенаправлять пакеты из сети 3 в сеть 1.




Если в Вашей корпоративной сети более двух маршрутизаторов, и по крайней мере один из них является статическим, Вам необходимо сконфигурировать статическую таблицу маршрутизации на каждом компьютере с несколькими сетевыми интерфейсами.

Для того чтобы компьютер мог соединиться с другими в корпоративной сети, в его конфигурации адрес шлюза по умолчанию должен соответствовать IP-адресу локального интерфейса маршрутизатора.

### Использование адреса шлюза по умолчанию

Существует несколько методов конфигурирования статического маршрута без ручного добавления маршрутов в таблицу. Один из них — задать в качестве адреса шлюза по умолчанию для каждого компьютера с несколь-

ками сетевыми интерфейсами адрес локального интерфейса другого компьютера с несколькими сетевыми интерфейсами в той же сети. Этот метод эффективен в случае двух статических маршрутизаторов.

## Построение таблицы маршрутизации

Информацию в таблицу маршрутизации добавляют при помощи команды *route*. Команду *route print* используют для просмотра установленных по умолчанию записей в таблице маршрутизации. Статическая запись должна быть добавлена в таблицу маршрутизации статического маршрутизатора для всех сетей, для которых он не имеет сконфигурированных интерфейсов. Статическая запись включает в себя следующее:

- *адрес сети* (network address) — идентификатор сети или имя сети получателя; если используется сетевое имя, его поиск производится в файле Networks;
- *сетевую маску* (netmask) — маску подсети для адреса сети;
- *адрес шлюза* (gateway address) — IP-адрес или имя узла, являющегося интерфейсом к сети назначения; если используется имя узла, его поиск производится в файле Hosts.

Если Вы ссылаетесь на сетевое имя или на имя узла в таблице маршрутизации, оно должно быть описано в соответствующем файле. Оба файла находятся в каталоге *\systemroot*\System32\Drivers\Etc.

### Записи по умолчанию в таблице маршрутизации

Ниже перечислены записи по умолчанию, поддерживаемые таблицей маршрутизации Windows NT 4.0.

| Адрес | Описание |
|---|---|
| 0.0.0.0 | Обозначает маршрут по умолчанию к любой сети, не описанной в таблице маршрутизации |
| Широковещание в подсети (subnet broadcast) | Используется для широковещания в локальной подсети |
| Широковещание в сети (network broadcast) | Используется для широковещания по всей сети |
| Локальная заглушка (local loopback) | Используется для тестирования IP-конфигураций и соединений |
| Локальная сеть (local network) | Используется для направления пакетов на узлы локальной сети |
| Локальный узел (local host) | Адрес локального компьютера. Ссылается на адрес локальной заглушки |

## Добавление статических записей

Для добавления статических записей в таблицу маршрутизации используется команда *route*.

| Добавление или изменение статической записи | Функция |
|---|---|
| *route add* [*сеть*] *mask* [*сетевая маска*] [*шлюз*] | Добавляет маршрут |
| *route -p add* [*сеть*] *mask* [*сетевая маска*] [*шлюз*] | Добавляет постоянный маршрут |
| *route delete* [*сеть*] [*шлюз*] | Удаляет маршрут |
| *route change* [*сеть*] [*шлюз*] | Изменяет маршрут |
| *route print* | Показывает таблицу маршрутизации |
| *route -f* | Стирает все маршруты |

Например, для добавления маршрута, позволяющего устанавливать соединения с сетью 131.107.24.0 с компьютера из сети 131.107.16.0, Вы должны использовать следующую команду:

```
route add 131.107.24.0 mask 255.255.255.0 131.107.16.2
```

---

Примечание Если не указан параметр *-p*, то статические маршруты хранятся только в памяти, то есть не являются постоянными. *Постоянные* (persistent) маршруты хранятся в Реестре. Когда Вы перезапускаете компьютер, работающий под управлением Windows NT, необходимо воссоздавать все непостоянные маршруты.

---

# Упражнения

Используйте утилиту Route для просмотра записей в локальной таблице маршрутизации.

▶ **Просмотр таблицы маршрутизации**

- Наберите *route -p print* в командной строке и нажмите ENTER.

Какие адреса, отличные от Вашего IP-адреса и адреса заглушки отображены в поле **Gateway Address**? Если Вы работаете с компьютером, не подключенным к сети, то адрес шлюза не появится.

---

Удалите адрес шлюза по умолчанию. Тогда пакеты не смогут быть отправлены соответствующему маршрутизатору, и маршрутизация реализуется на основе имеющихся записей маршрутов.

▶ **Удаление адреса шлюза по умолчанию**

1. Дважды щелкните пиктограмму **Network** в **Control Panel**, затем — вкладку **Protocols**.
2. Щелкните **TCP/IP Protocol**, затем — **Properties**.
   Появится диалоговое окно **Microsoft TCP/IP Properties**.
3. Удалите адрес **Default Gateway**.
4. Нажмите кнопку **OK**, потом еще раз — **OK**.

▶ **Просмотр таблицы маршрутизации**

- Используйте команду *route print* в командной строке.

Показан ли адрес шлюза по умолчанию в поле **Gateway Address**?

---

Попытайтесь связаться с локальным и удаленным узлами.

---

Примечание Для этого Вам понадобится два сетевых компьютера.

---

▶ **Проверка сетевого соединения**

- Выполните Ping IP-адрес Вашего второго компьютера или компьютера Вашей локальной сети.

Была ли попытка успешной?

---

Возможен ли Ping IP-адреса удаленного узла, если не указан адрес шлюза в таблице маршрутизации?

---

Добавьте запись в статическую таблицу маршрутизации.

▶ **Добавление записи маршрута**

1. Наберите следующую команду:

```
route add 131.107.2.0 mask 255.255.255.0 131.107.2.1
```

2. Просмотрите записи в таблице маршрутизации и убедитесь в наличии этого маршрута.
3. Если бы Вы указали адрес узла из другой сети, был бы Ping успешным? Почему?

---

Восстановите адрес шлюза по умолчанию. Это позволит посылать пакеты на шлюз по умолчанию при отсутствии маршрута к сети назначения.

▶ **Восстановление адреса шлюза по умолчанию**

1. Переключитесь в диалоговое окно **Microsoft TCP/IP Properties**.
2. В окне **Default Gateway** наберите адрес Вашего шлюза по умолчанию.
3. Нажмите кнопку **OK**, потом еще раз — **OK**.

## Резюме

Статическая IP-маршрутизация является функцией IP. Это значит, что маршрутизаторы не обмениваются информацией о маршрутах автоматически. Статический маршрут может быть определен путем назначения шлюза по умолчанию или в виде записи в таблице конфигурации.

# Занятие 3. Динамическая IP-маршрутизация

При динамическом способе маршрутизаторы автоматически обмениваются путями к известным сетям. Если путь изменился, протоколы маршрутизации автоматически обновляют таблицу маршрутизации и информируют об этом другие маршрутизаторы объединенной сети. Такой способ очень важен для больших объединенных сетей.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить концепцию динамической IP-маршрутизации;
- ✓ объяснить требования к конфигурации узла для динамической маршрутизации;
- ✓ совместно использовать статическую и динамическую маршрутизацию.

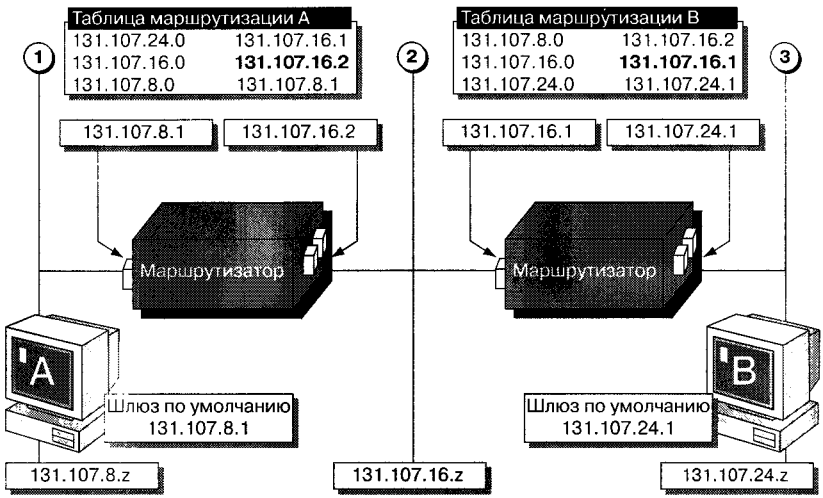
**Продолжительность занятия — 15 минут**

Обычно динамическая маршрутизация применяется в больших объединенных сетях, поскольку от администратора для управления сетью в этом случае требуются минимальные усилия. Для динамической маршрутизация необходим протокол RIP или OSPF.

## Конфигурация узла

Для связи узла с другими узлами объединенной сети его адрес шлюза по умолчанию должен соответствовать IP-адресу локального интерфейса маршрутизатора. Других настроек не требуется.

Как показано на рисунке, компьютеру A указан 131.107.8.1 (адрес локального интерфейса маршрутизатора) в качестве адреса шлюза по умолчанию. Компьютеру B в качестве адреса шлюза по умолчанию указывается 131.107.24.1. Узел сети 2 может использовать 131.107.16.2 или 131.107.16.1 в качестве адреса шлюза по умолчанию.




## Протокол RIP

Протокол маршрутизации Routing Information Protocol (RIP) для IP облегчает обмен информацией о маршрутизации в объединенной IP-сети. Все сообщения RIP передаются по протоколу UDP через порт 520.

RIP позволяет маршрутизаторам обмениваться *идентификаторами сетей* (network IDs), которых может достичь маршрутизатор, и расстоянием до этих сетей. В своей таблице маршрутизации RIP использует поле *подсчета транзитов* (hop count), или *метрику* (metric), для отображения расстояния до сети, обозначенной соответствующим идентификатором. Количество транзитов — это число маршрутизаторов, которые должны быть пройдены для достижения требуемого идентификатора сети. Максимальное количество транзитов для RIP-записи равно 15. Сетевые идентификаторы, требующие 16 и более транзитов, считаются недостижимыми. Количество транзитов может быть изменено для отображения медленных или перегруженных каналов. Если в таблице маршрутизации несколько записей для одного сетевого идентификатора, RIP-маршрутизатор выберет маршрут с наименьшим числом транзитов.

---

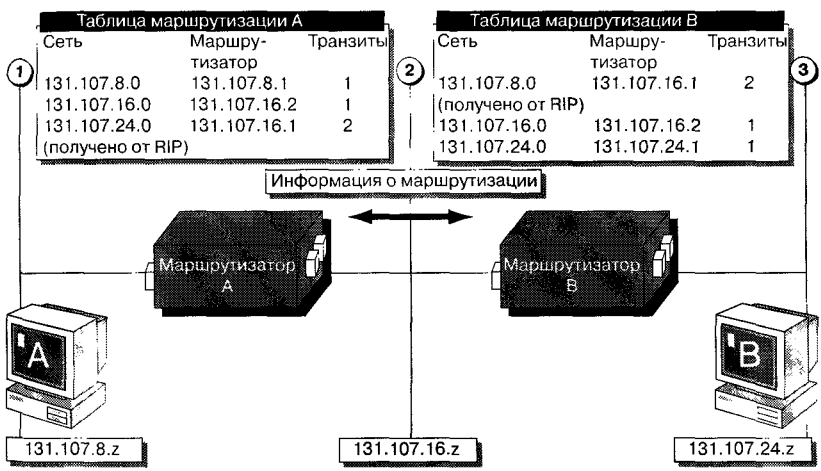
Примечание RIP-маршрутизатор, принимающий широковещательные RIP-сообщения, но не посылающий их, называется *молчащим RIP-маршрутизатором* (silent RIP router).

---

На рисунке показаны три подсети, связанные двумя компьютерами, работающими под управлением Microsoft Windows NT 4.0 с поддержкой

RIP-маршрутизации. Каждый маршрутизатор сконфигурирован с интервалом обновления по умолчанию, поэтому каждые 30 секунд каждый маршрутизатор посылает широковещанием свою таблицу маршрутизации. Маршрутизатор А посылает ограниченное широковещание в сеть 2 и всем маршрутизаторам с поддержкой RIP-маршрутизации сети 2, информируя их о сети 1. Затем В добавляет новые пути в свою таблицу маршрутизации. Если в ней есть запись, посылаемая А, В сравнит метрики обоих маршрутов. Если этот маршрут лучше, В обновит свою таблицу маршрутизации.

Маршрутизатор В также посылает ограниченное широковещание в сеть 2 всем ее RIP-маршрутизаторам, информируя их о сети 3. Затем В определяет количество новых записей и при необходимости обновляет свою таблицу маршрутизации.




## Недостатки RIP

Простой и широко поддерживаемый на практике протокол RIP для IP обладает некоторыми недостатками, связанными с тем, что он разрабатывался для локальных сетей. Из-за этого RIP хорошо работает только в малых объединенных IP-сетях с небольшим числом маршрутизаторов.

При использовании RIP таблица каждого маршрутизатора содержит полный список всех сетевых идентификаторов и возможных путей к ним. Она включает сотни или даже тысячи записей для большой объединенной IP-сети с многочисленными путями. Поскольку максимальный размер одного RIP-пакета — 512 байт, для отправки больших таблиц маршрутизации требуется множество RIP-пакетов.

RIP-маршрутизаторы объявляют содержимое своих таблиц через широковещание уровня MAC (Media Access Control) во всех подключенных сетях каждые 30 секунд. В больших IP-сетях осуществляется RIP-широковещание больших таблиц маршрутизации. Это иногда создает значительные проблемы для WAN-соединений, где существенные части полосы пропускания будут задействованы для трафика протокола RIP. Маршрутизация, основанная на RIP, не подходит для больших объединенных сетей или глобальных сетей (WAN).

В таблице маршрутизации каждой записи о маршруте, полученном по RIP, назначен 3-минутный тайм-аут (отсчитывается с момента получения), по истечении которого не обновленные записи удаляются. Если маршрутизатор выходит из строя, распространение изменений по объединенной сети может занять несколько минут. Это называется *проблемой медленной конвергенции* (slow convergence problem)*.

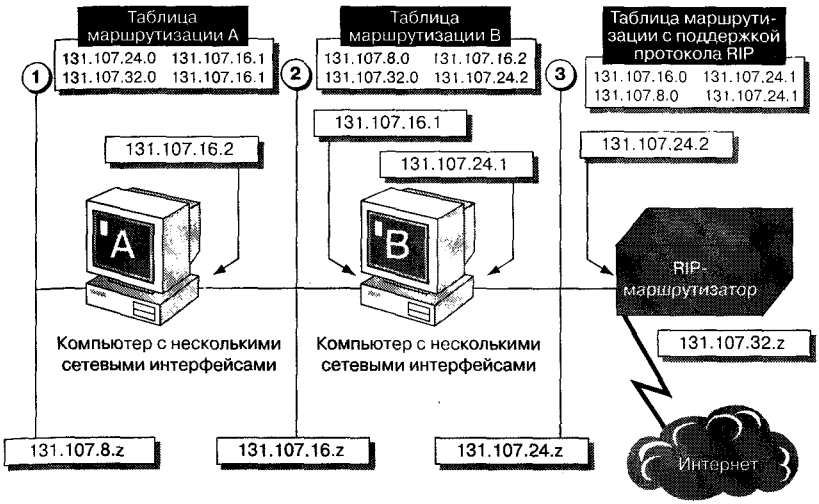
## Совместное использование статической и динамической маршрутизации

Статический маршрутизатор не обменивается информацией с динамическими. Для маршрутизации со статического маршрутизатора через динамический (IP-маршрутизатор с поддержкой RIP- или OSPF-маршрутизации) необходимо добавить статический маршрут в таблицы маршрутизации как на статическом, так и на динамическом маршрутизаторах.

- Необходимо добавить маршрут в таблицу маршрутизации компьютера A. Он должен содержать IP-адрес (131.107.16.1) интерфейса, имеющего доступ к выделенному IP-маршрутизатору для маршрутизации пакетов из сети 1 в Интернет.
- Для маршрутизации пакетов из сетей 2 и 3 в Интернет в таблицу маршрутизации компьютера B надо добавить статическую запись, содержащую IP-адрес (131.107. 24.2) интерфейса соответствующего IP-маршрутизатора для Интернета.
- Для связи компьютеров в Интернете с узлами сети 1 и 2 необходимо статически сконфигурировать динамический IP-маршрутизатор, указав IP-адрес интерфейса к компьютеру B. После этого компьютер B будет работать в качестве шлюза в другие подсети.

---

* Еще одна проблема состоит в том, что в Windows NT используется первая версия протокола RIP. В ней передаются только номера сетей, но не маски подсетей, что делает его непригодным для подсетей, длины масок которых не кратны 8 битам. Продукт Microsoft Routing and Remote Access Update позволяет использовать в Windows NT протокол RIP второй версии и OSPF. Этот продукт — бесплатное дополнение к Windows NT. — *Прим. перев.*




Примечание Некоторые реализации RIP не распространяют статические таблицы маршрутизации. В этом случае необходимо статически сконфигурировать удаленные маршрутизаторы в объединенной сети. Конфигурирование статического маршрута на RIP-маршрутизаторе отличается для каждого маршрутизатора. Подробности см. в документации на маршрутизатор, поставляемой производителем.

## Резюме

Динамическая маршрутизация важна для больших сетей. В качестве адреса шлюза по умолчанию для узла должен быть указан IP-адрес интерфейса локального маршрутизатора. Протокол RIP для IP позволяет обмениваться информацией о маршрутизации в объединенной сети на основе IP. Однако RIP хорош только для маленьких IP-сетей.

Статический маршрутизатор не обменивается информацией о путях с динамическими. Для маршрутизации со статического маршрутизатора через динамический Вам необходимо добавить статический маршрут в таблицы обоих маршрутизаторов.

# Занятие 4. Реализация маршрутизатора Windows NT

Статическая маршрутизация хорошо работает в маленьких сетях и на удаленных участках, но не в больших объединенных сетях, где существенно возрастает нагрузка, связанная с ручной поддержкой таблиц маршрутизации. Это занятие поможет Вам уяснить, что необходимо для установки Windows NT маршрутизатора.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как установить Windows NT маршрутизатор;
- ✓ объяснить, как утилита Tracert отслеживает маршрут пакета.

**Продолжительность занятия – 10 минут**

Установив поддержку протокола IP-маршрутизации RIP, Windows NT Server 4.0 можно использовать в качестве динамического IP-маршрутизатора. Использование RIP для IP в Windows NT 4.0 позволяет не конфигурировать таблицы маршрутизации вручную. RIP для IP подходит для объединенных сетей средних размеров, но не годится для больших объединенных сетей на основе IP из-за значительного объема широковещания.

► **Просмотр таблицы маршрутизации**

1. Установите несколько плат сетевых адаптеров и соответствующие драйверы или сконфигурируйте несколько IP-адресов на одной плате.
2. Сконфигурируйте плату(ы) адаптера с подходящим IP-адресом и маской подсети.
3. На вкладке **Routing** диалогового окна **Microsoft TCP/IP Properties** установите флажок **Enable IP Forwarding**.
4. В зависимости от имеющейся версии Windows NT:
   - на вкладке **Services** программы **Control Panel Network** добавьте сервис **RIP for Internet Protocol**

     или
   - добавьте статические маршруты в таблицу статического маршрутизатора.

## Утилита Tracert

Утилита Tracert проверяет маршрут, пройденный пакетом до получателя. Это полезно для обнаружения неисправного маршрутизатора. Если команда не выполняется успешно, Вы сможете определить, где прервался путь, и обнаружить неисправность, перегрузку или иной сбой маршрутизатора или WAN-канала.

Tracert также полезна для определения медленного маршрутизатора. Возвращаемое ей Время ответа показывает эффективность маршрутизатора или WAN-канала. Эту информацию используют для сравнения с данными о другом пути к тому же получателю.

Например, следующая команда выводит путь от локального узла до узла *www.microsoft.com* (207.68.137.36):

```
tracert www.microsoft.com
```

В результате работы команда проверила, что адрес маршрутизатора был использован на пути от локального узла до узла-получателя.

```
Tracing route to www.microsoft.com [207.68.137.36]
over a maximum of 30 hops:
1  <10 ms <10 ms  <10 ms 206.213.84.57
2  30 ms  40 ms   30 ms  fastl.accessone.com [206.213.95.11]
3  30 ms  80 ms   30 ms  198.68.188.1
4  30 ms  40 ms   30 ms  Fddil-0.GWI.SEA1.ALTER.NET [137.39.63.65]
5  40 ms  40 ms   40 ms  Distl-Sea.MOSWEST.MSN.NET [137.39.176.22]
6  40 ms  40 ms   40 ms  msftl-f0.moswest.msn.net [207.68.145.46]
7  231 ms 170 ms  170 ms www.microsoft.com [207.68.137.36]

Trace complete.
```

## Резюме

Windows NT Server 4.0 может работать в качестве динамического IP-маршрутизатора, если установлена поддержка протокола RIP для IP. Это устраняет необходимость вручную конфигурировать таблицы маршрутизации. Утилита Tracert позволяет обнаружить неисправный или медленный маршрутизатор.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Как осуществляется поддержка IP-маршрутизации?

2. Обязательно ли нужна таблица маршрутизации на компьютере с несколькими сетевыми интерфейсами, подключенном к корпоративной сети с двумя подсетями?

3. Когда надо создать статическую таблицу маршрутизации?

4. Какая информация необходима для таблицы маршрутизации?

5. Почему протокол RIP обычно не используется в большой сети?

# Дополнительная информация

- Изучите все RFC, находящиеся на прилагаемом к курсу компакт-диске.

# Протокол DHCP



## В этой главе

Вы научитесь использовать протокол DHCP для автоматического конфигурирования параметров TCP/IP и устранять возникающие при этом проблемы. На занятиях Вы установите и отладите сервер автоматической настройки узлов DHCP, протестируете конфигурацию DHCP, установите агент ретрансляции DHCP и получите IP-адрес с сервера DHCP.

## Прежде всего

Для выполнения заданий этой главы Вам необходимо:

- установить ОС Microsoft Windows NT Server 4.0 с протоколом TCP/IP.

# Занятие 1. Общие сведения о DHCP

Протокол настройки узла Dynamic Host Configuration Protocol (DHCP) автоматически назначает IP-адреса компьютерам. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP. На этом занятии Вашему вниманию представлен обзор DHCP и принципы его работы.

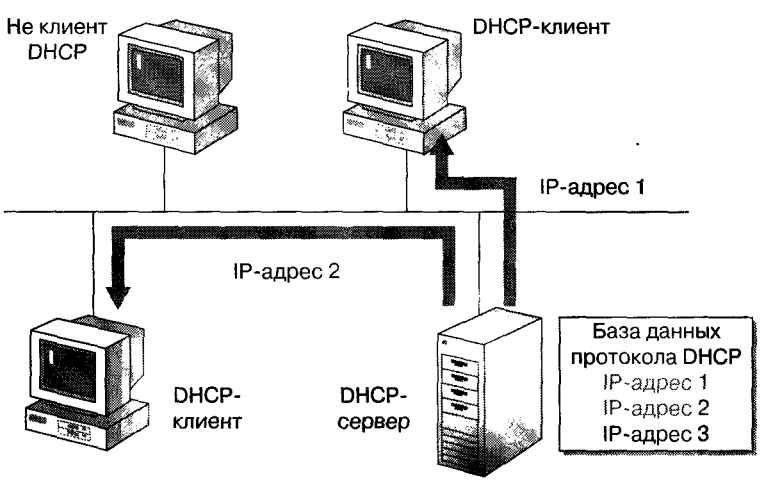
**Изучив материал этого занятия, Вы сможете:**

- ✓ описать назначение и преимущества протокола DHCP;
- ✓ объяснить, как DHCP-клиент получает IP-адреса с DHCP-сервера;
- ✓ объяснить, как утилита Ipconfig позволяет вручную обновлять или освобождать аренду IP-адреса.

**Продолжительность занятия — 35 минут**

Протокол автоматической настройки узла DHCP — расширение протокола BOOTP. Последний позволяет бездисковым клиентам запускать и автоматически конфигурировать протокол TCP/IP. DHCP централизованно управляет настройкой протокола TCP/IP при помощи автоматического назначения IP-адресов компьютерам, настроенным на использования протокола DHCP. Применение DHCP исключает некоторые проблемы, связанные с ручным конфигурированием протокола TCP/IP.

Как показано на рисунке, каждый раз при запуске DHCP-клиент запрашивает информацию с DHCP-сервера: IP-адрес, маску подсети и необязательные параметры, например адрес шлюза по умолчанию, адрес сервера DNS и адрес сервера имен NetBIOS.



Получив запрос, DHCP-сервер выбирает IP-адрес из пула адресов в своей БД и предлагает его DHCP-клиенту. Если тот принимает предложение, информация об IP-адресации, т. е. IP-адрес и остальные конфигурационные параметры TCP/IP, предоставляется в аренду клиенту на определенный срок. Если в пуле нет доступной информации об IP-адресации, то клиент не может инициализировать протокол TCP/IP.

Примечание Windows NT 4.0 Service Pack 2 поддерживает запросы клиентов по протоколу BOOTP.

Протокол BOOTP описан в RFC 1532, DHCP — в RFC 1533, 1534, 1541 и 1542. Копии этих документов находится на Web-странице Course Materials прилагаемого к курсу компакт-диска.

## Ручное и автоматическое конфигурирование

Чтобы понять преимущества протокола DHCP при конфигурации протокола TCP/IP на компьютерах клиентов, полезно сравнить ручной метод с автоматическим, использующим DHCP.

### Ручное конфигурирование протокола TCP/IP

Ручное конфигурирование протокола TCP/IP означает, что пользователь может выбрать любой случайный IP-адрес, вместо того чтобы получить его от сетевого администратора. Использование некорректных адресов вызывает в сети сбои, источник которых установить крайне трудно.

К тому же ошибка при выборе IP-адреса, маски подсети или шлюза по умолчанию иногда порождает различные сложности, начиная с проблем при подсоединении и заканчивая трудностями, связанными с дублированием IP-адреса.

Другой недостаток ручной конфигурации протокола TCP/IP — увеличение объема работы администратора в объединенных сетях, где компьютеры часто переносят из одной подсети в другую. Например, когда рабочую станцию перемещают в другую подсеть, IP-адрес и адрес шлюза по умолчанию надо изменить.

### Конфигурирование протокола TCP/IP при помощи DHCP

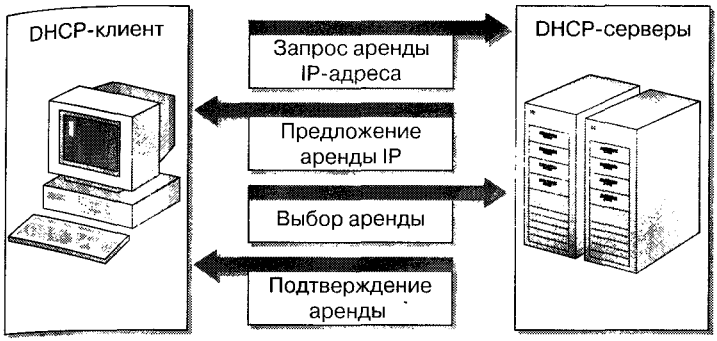
В результате использования протокола DHCP для автоматической настройки параметров протокола TCP/IP пользователи больше не нуждаются в сведениях от администратора для конфигурации TCP/IP. Сервер протокола DHCP предоставит всю необходимую информацию о конфигурации для всех клиентов протокола DHCP. Кроме того, исключается большинство трудно отслеживаемых сетевых неисправностей.

## Функционирование протокола DHCP

Протокол DHCP использует четырехэтапный процесс для конфигурации своего клиента. Если у компьютера несколько сетевых адаптеров, то каждый из них конфигурируется отдельно, и ему назначается уникальный IP-адрес. Передача данных между DHCP-клиентом и DHCP-сервером происходит по UDP через порты 67 и 68.

Большинство сообщений протокола DHCP передаются с использованием широковещания. Для связи DHCP-клиентов с DHCP-сервером в удаленной сети IP-маршрутизаторы должны поддерживать ретрансляцию широковещательных сообщений DHCP. В таблице отображены этапы конфигурирования протокола DHCP.

| Этап | Описание |
|---|---|
| Запрос аренды IP-адреса | Клиент инициализирует ограниченную версию протокола TCP/IP и посылает широковещательный запрос для поиска DHCP-сервера и информации об IP-адресации |
| Предложение аренды IP-адреса | Все серверы протокола DHCP, имеющие свободную информацию об IP-адресах, отправляют предложение клиенту |
| Выбор аренды IP-адреса | Клиент выбирает информацию об IP-адресации из первого полученного предложения и посылает широковещательное сообщение с запросом информации об аренде IP-адреса |
| Подтверждение аренды IP-адреса | DHCP-сервер, сделавший это предложение, отвечает на запрос, а все остальные серверы отзывают свои предложения. Клиенту назначается IP-адрес и сопутствующие параметры. |
| | Клиент завершает настройку и связывает TCP/IP с остальными компонентами системы. Поскольку автоматическая конфигурация выполнена, клиент может использовать все сервисы и утилиты протокола TCP/IP для связи с другими узлами TCP/IP |




## Запрос и предложение аренды IP-адреса

На первых двух этапах клиент запрашивает аренду у DHCP-сервера, а сервер предлагает клиенту IP-адрес.

### Запрос аренды

Когда клиент инициализируется в первый раз, он запрашивает аренду IP-адреса, посылая широковещательное сообщение всем DHCP-серверам. Поскольку клиент не имеет IP-адреса и не знает IP-адрес DHCP-сервера, он использует 0.0.0.0 в качестве адреса отправителя и 255.255.255.255 в качестве адреса получателя.

Запрос на аренду посылается в сообщении DHCPDISCOVER, которое также содержит аппаратный адрес сетевого адаптера клиента и имя его компьютера, поэтому DHCP-серверам известно, от какого клиента исходит запрос.

Процесс получения аренды начинается в следующих случаях:

- протокол TCP/IP инициализируется в первый раз как клиент протокола DHCP;
- клиенту отказано в запрашиваемом IP-адресе, возможно, из-за отмены аренды сервером протокола DHCP;
- клиент уже арендовал IP-адрес, затем отказался от него, и в данный момент ему нужна новая аренда.

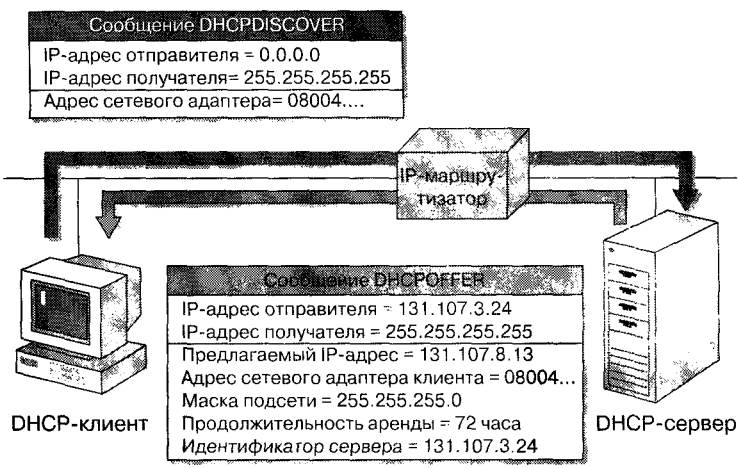
### Предложение аренды

Серверы протокола DHCP, принимающие запрос и имеющие свободную конфигурацию для клиента, посылают широковещательное предложение, в котором содержится:

- аппаратный адрес сетевого адаптера клиента;
- предлагаемый IP-адрес;
- маска подсети;
- срок аренды;
- идентификатор сервера (IP-адрес предлагающего аренду DHCP-сервера).

Поскольку клиент еще не имеет IP-адреса, используется широковещание. На рисунке изображена отправка предложения в сообщении DHCPOFFER.

DHCP-сервер резервирует предложенный IP-адрес, чтобы он не попал к другому DHCP-клиенту. DHCP-клиент выбирает IP-адрес из первого полученного предложения.




## Отсутствие работающих DHCP-серверов

DHCP-клиент ждет предложений в течение одной секунды. Если он их не получит, то не сможет инициализировать TCP/IP, и ему придется снова трижды посылать широковещательные запросы (с интервалами 9, 13 и 16 с и один раз со случайным интервалом в диапазоне от 0 до 1 000 мс). Если предложение так и не будет получено, клиент повторяет попытки каждые пять минут.

### Выбор аренды

На двух последних этапах клиент выбирает предложение, а DHCP-сервер подтверждает аренду.

Получив предложение хотя бы от одного DHCP-сервера, клиент посылает широковещательное сообщение о том, что выбор сделан на основе этого предложения.

Широковещательное сообщение DHCPREQUEST содержит идентификатор сервера (IP-адрес), предложение которого было выбрано. Все остальные DHCP-серверы отзывают свои предложения, чтобы их IP-адреса были доступны для следующего запроса.

### Подтверждение аренды

DHCP-сервер, приняв предложение, посылает широковещательное подтверждение клиенту — сообщение DHCPACK. Оно содержит арендованный IP-адрес и, иногда, другую конфигурационную информацию.

Когда DHCP-клиент получает подтверждение, протокол TCP/IP полностью инициализируется и рассматривается в качестве клиента протокола DHCP. После выполнения привязки клиент может использовать протокол TCP/IP для работы в сети.

Клиент сохраняет IP-адрес, маску подсети и другую информацию об IP-адресации в разделе реестра: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*adapter*\Parameters\Tcpip, где *adapter* — имя сетевого адаптера.

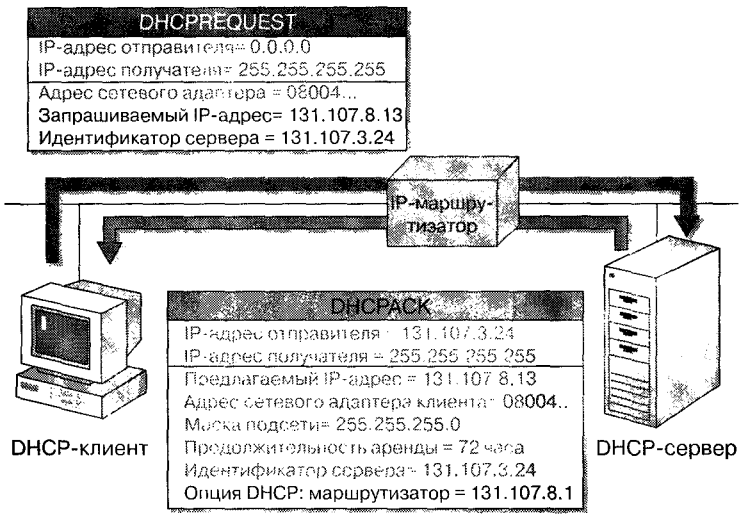
### Отказ в аренде

Широковещательное сообщение об отказе (DHCPNACK) посылается сервером, когда клиент пытается арендовать IP-адрес, ранее им использовавшийся, но теперь недоступный. Оно также посылается, если IP-адрес стал неправильным из-за физического перемещения клиента в другую подсеть*.

Как показано на иллюстрации, при получении отказа клиент заново запрашивает аренду протокола TCP/IP.

---

* После установки Service Pack версии 2 или выше DHCP-сервер отправляет DHCPNACK во всех случаях, когда запрос клиента, даже обращенный к другому DHCP-серверу, не является, с его точки зрения, корректным. Подробности — в разделе «Использование нескольких серверов DHCP» на стр. 132. — *Прим. перев.*




## Механизм обновления аренды

### Первая попытка обновления

Все клиенты DHCP пытаются обновить аренду по истечении половины ее срока и при каждом перезапуске системы. Для этого клиент посылает сообщение DHCPREQUEST на DHCP-сервер, предоставивший аренду.

Если DHCP-сервер доступен, то он обновляет аренду и посылает клиенту подтверждение (DHCPACK) с указанием времени новой аренды и, возможно, обновленными параметрами конфигурации.

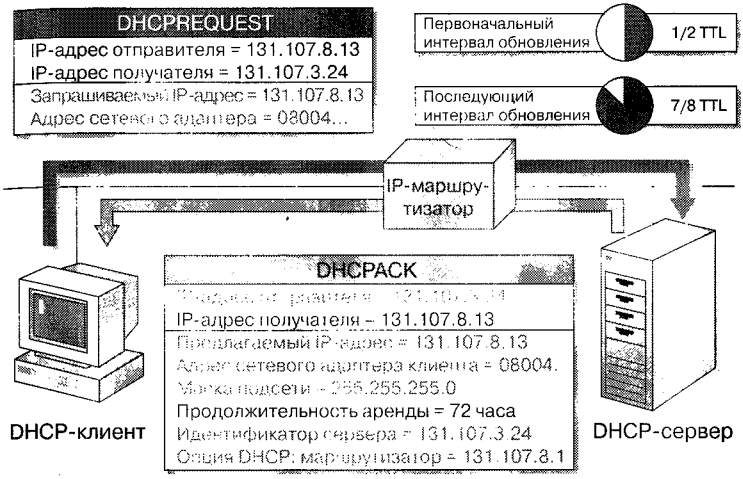
Получив подтверждение, клиент обновляет свою конфигурацию. Если он не может связаться с DHCP-сервером, генерируется сообщение о том, что аренда не обновлена. Тем не менее клиент может продолжать использовать свой IP-адрес, поскольку срок аренды истек только наполовину.

При перезапуске DHCP-клиент, как правило, пытается арендовать тот же IP-адрес с того же DHCP-сервера путем широковещательной передачи сообщения DHCPREQUEST, содержащего последний используемый клиентом IP-адрес. Если это не удается, но срок аренды еще не истек, DHCP-клиент продолжает использовать IP-адрес.

### Последующие попытки обновления

Если аренда не была обновлена DHCP-сервером по истечении половины ее срока, клиент попытается связаться со всеми доступными DHCP-серверами по истечении 87,5% времени аренды, отправляя широковещатель-

ое сообщение DHCPREQUEST (это проиллюстрировано ниже). Сервер HCP отвечает или сообщением DHCPACK (аренда обновлена) или со-бщением DHCPNACK (клиенту придется повторить инициализацию и рендовать другой IP-адрес).




Если аренда истекла или получено сообщение DHCPNACK, DHCP-лиент должен немедленно отказаться от использования IP-адреса. За-ем он попытается арендовать новый IP-адрес.

Если срок аренды истек, а клиент не может получить новую, связь по CP/IP прекращается до назначения нового адреса. Ошибка сети возвращается всем сетевым приложениям, пытающимся использовать ин-ерфейсы неинициализированного стека протоколов TCP/IP.

## Использование утилиты Ipconfig

Помимо проверки конфигурации протокола TCP/IP компьютера, утили-а Ipconfig используется для обновления конфигурационных параметров срока аренды, а также для повторного получения аренды. Для провер-и IP-адреса компьютера, маски подсети и шлюза по умолчанию наберите в командной строке:

```
ipconfig
```

Для проверки конфигурации протокола IP для операционной систе-мы и сетевого адаптера наберите в командной строке:

```
ipconfig /all
```

При помощи параметра */all* Вы получите следующую информацию о конфигурации протокола TCP/IP:

- имя узла, назначенное локальному компьютеру;
- IP-адреса всех серверов DNS, разрешенных для использования локальным компьютером;
- тип узла (режим работы) NetBIOS, например, широковещательный, гибридный, одноранговый, или «точка-точка», смешанный;
- идентификатор области видимости (Scope ID) имен NetBIOS;
- разрешена или нет IP-маршрутизация;
- доступен или нет доверенный агент WINS;
- используются ли при разрешении имен NetBIOS средства DNS или нет.

Параметр */all* позволяет получить сведения о конфигурации протокола IP для сетевого адаптера:

- описание платы адаптера, например EtherLink II;
- физический адрес платы адаптера;
- используется ли автоконфигурация по DHCP или нет;
- IP-адрес локального компьютера;
- маску подсети локального компьютера;
- шлюз по умолчанию локального компьютера;
- IP-адреса основного и запасного серверов WINS.

## Обновление аренды

Параметр */renew* задает отправку сообщения DHCPREQUEST на сервер DHCP для получения обновленных конфигурационных параметров и времени аренды. Если сервер DHCP недоступен, то клиент будет использовать текущую конфигурацию, предоставленную сервером DHCP. Наберите в командной строке:

```
ipconfig /renew
```

## Освобождение аренды

Параметр */release* задает отправку DHCP-клиентом сообщения DHCPRELEASE на сервер DHCP и освобождение аренды. Это полезно, когда клиент перемещается в другую сеть и больше не нуждается в аренде. После выполнения этой команды передача по протоколу TCP/IP прервется. Наберите в командной строке:

```
ipconfig /release
```

Клиенты Microsoft DHCP не отправляют сообщения DHCPRELEASE при выключении. Если клиент выключен на протяжении всего срока арен-

ды (и аренда не обновлялась), то по истечении ее срока DHCP-сервер может назначить IP-адрес этого клиента другому клиенту. Если клиент не посылает сообщение DHCPRELEASE, у него больше шансов получить тот же IP-адрес при очередной инициализации.

## Резюме

Протокол DHCP разработан для решения проблем путем централизации сведений об IP-конфигурации для назначения клиентам. Клиент его средствами конфигурируется в четыре этапа: запрос, предложение, выбор и подтверждение аренды.

Кроме проверки IP-конфигурации компьютера, Вы можете использовать утилиту Ipconfig для обновления конфигурационных параметров, времени аренды и для освобождения аренды.

# Занятие 2. Установка и конфигурация сервера протокола DHCP

Перед установкой протокола DHCP Вам придется ознакомиться с некоторыми тонкостями, касающимися его конфигурации. На этом занятии Вы узнаете о них, о требованиях к серверу и клиенту и научитесь устанавливать поддержку DHCP.

**Изучив материал этого занятия, Вы сможете:**

- ✓ определить, какие вопросы следует выяснить перед установкой протокола DHCP;
- ✓ установить протокол DHCP в объединенной сети;
- ✓ сконфигурировать диапазон адресов DHCP для нескольких подсетей.

**Продолжительность занятия — 75 минут**

Перед установкой протокола DHCP ответьте на следующие вопросы.

- Станут ли все компьютеры клиентами протокола DHCP? Учтите, что компьютеры, не являющиеся клиентами протокола DHCP, имеют статические IP-адреса, которые должны быть исключены из пулов серверов DHCP. Если надо, чтобы IP-адреса некоторых клиентов не менялись, их нужно зарезервировать.
- Будет ли сервер протокола DHCP поддерживать IP-адреса для нескольких подсетей? Если да, то учтите, что все маршрутизаторы, подключенные к подсетям, должны действовать как агенты ретрансляции протокола DHCP. Если Ваши маршрутизаторы не работают в качестве агентов ретрансляции протокола DHCP, то необходим по крайней мере один сервер протокола DHCP на каждую подсеть, имеющую клиентов протокола DHCP.
- Сколько надо серверов протокола DHCP? Имейте в виду, что сервер протокола DHCP не обменивается информацией с другими серверами DHCP. Поэтому необходимо, чтобы каждый DHCP-сервер назначал уникальные IP-адреса своим клиентам.
- Какую дополнительную информацию получат клиенты с сервера протокола DHCP? Возможные варианты адресной информации:
  - маршрутизатор;
  - сервер DNS;
  - сервер имен NetBIOS поверх TCP/IP;
  - идентификатор области видимости NetBIOS.

Выбрав дополнительные параметры, Вы определите, как сконфигурировать сервер протокола DHCP и будут ли они назначены для всех клиентов объединенной сети, клиентов определенной подсети или только отдельных клиентов.

## Использование нескольких серверов DHCP

Если Вашей объединенной сети нужно несколько серверов DHCP, то необходимо создать уникальный *диапазон адресов DHCP* (DHCP scope) для каждой подсети. Он определяет доступные для аренды IP-адреса.

Чтобы гарантировать клиентам аренду IP-адресов, потребуется несколько диапазонов адресов для каждой подсети, распределяемых между серверами протокола DHCP в объединенной сети, например:

- каждый сервер протокола DHCP должен иметь диапазон, содержащий примерно 75% IP-адресов для локальной подсети;
- каждому серверу протокола DHCP необходим диапазон действия для каждой удаленной подсети, содержащий приблизительно 25% доступных IP-адресов той подсети.

Когда сервер протокола DHCP недоступен, клиент может получить аренду с сервера протокола DHCP другой подсети, если маршрутизатор является агентом ретрансляции протокола DHCP.

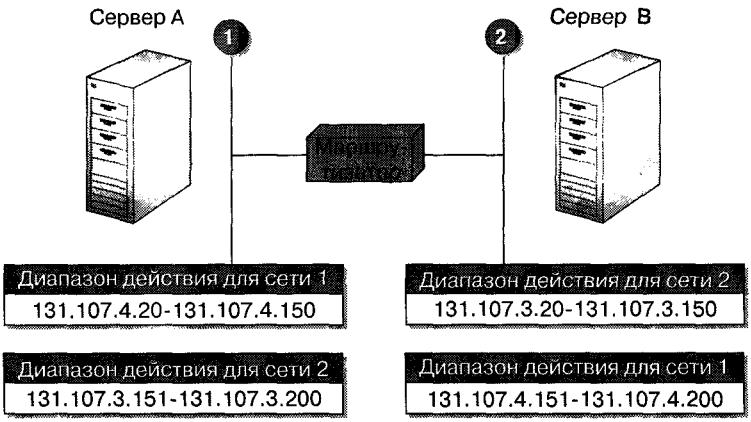
Предположим (см. рис.), сервер A имеет диапазон адресов для локальной подсети от 131.107.4.20 до 131.107.4.150 и сервер B — от 131.107.3.20 до 131.107.3.150. Каждый из них может сдавать в аренду IP-адреса клиентам своей подсети.

Вместе с тем у каждого сервера есть небольшой диапазон IP-адресов для удаленной подсети. Например сервер A имеет диапазон для подсети 2 от 131.107.3.151 до 131.107.3.200, сервер B — для подсети 1 от 131.107.4.151 до 131.107.4.200.

Когда клиент подсети 1 не может арендовать адрес у сервера A, он может арендовать адрес для своей подсети у сервера B, и наоборот*.

---

* Если Вы хотите использовать несколько логических подсетей на одном физическом сегменте при помощи DHCP-серверов, то Вам следует дополнительно ознакомиться с понятием *«наддиапазона»* (superscope), прочитав описание на Service Pack 2, а также внимательно изучить статьи *Q161571*, *Q169291*, *Q163055*, *Q124026* в Microsoft Knowledge Base (*http://support.microsoft.com*). — *Прим. перев.*




## Условия работы протокола DHCP

Для реализации протокола DHCP нужно настроить и сервер, и клиентов. Все маршрутизаторы, разделяющие подсети, в которых находятся серверы и клиенты, должны поддерживать RFC 1542 и действовать как агенты ретрансляции протокола BOOTP.

Для сервера протокола DHCP надо выполнить следующие условия.

- Сконфигурировать сервис DHCP Server хотя бы на одном компьютере в объединенной сети TCP/IP, работающем под управлением ОС Windows NT Server (он не должен быть контролером домена). Задать поддержку IP-маршрутизаторами RFC 1542. В противном случае Вам потребуется сервер протокола DHCP в каждой подсети.
- Сконфигурировать сервер протокола DHCP со статическим IP-адресом, подсетевой маской, шлюзом по умолчанию и другими параметрами (он не может быть клиентом протокола DHCP).
- Создать диапазон адресов на сервере протокола DHCP. Он содержит IP-адреса, которые сервер может назначить клиентам, например от 131.107.3.51 до 131.107.3.200.

Для клиента протокола DHCP требуется компьютер, работающий под управлением одной из следующих ОС с поддержкой DHCP:

- Windows NT Server 4.0;
- Windows NT Workstation 4.0;
- Microsoft Windows 95;
- Microsoft Windows for Workgroups 3.11, использующей протокол Microsoft TCP/IP-32 (поставляется на компакт-диске с Windows NT Server 3.5);

- Microsoft Network Client 3.0 for MS-DOS с драйвером реального режима протокола TCP/IP (находится на компакт-диске с Windows NT Server 3.5);
- Lan Manager 2.2c для MS-DOS, поставляемый на компакт-диске с Windows NT Server 3.5. Lan Manager 2.2c для OS/2 не поддерживается.

## Установка и конфигурация DHCP-сервера

Сервис DHCP Server предназначен для связи с клиентами протокола DHCP. Как только сервер протокола DHCP установлен и запущен, должны быть сконфигурированы некоторые опции. Далее перечислены основные действия для установки и конфигурирования протокола DHCP.

- Установите сервис Microsoft DHCP Server.
- Диапазон адресов или корректный IP-адрес надо сконфигурировать перед тем, как клиенты смогут арендовать IP-адреса у сервера.
- Глобальные опции, опции диапазона адресов и диапазона адресов клиента могут быть сконфигурированы для конкретного клиента.
- Сервер протокола DHCP может быть сконфигурирован для перманентного назначения одного и того же IP-адреса одному и тому же клиенту.

---

Примечание Сервер протокола DHCP не может быть клиентом протокола DHCP. Он должен иметь статический IP-адрес, маску подсети и адрес шлюза по умолчанию.

---

### Упражнение 1

Вы установите и настроите сервер протокола DHCP для автоматического назначения конфигурации протокола TCP/IP клиентам DHCP.

---

Примечание Для этого упражнения Вам потребуются два сетевых компьютера. Выполняйте его с компьютера, выбранного Вами в качестве сервера протокола DHCP (Server1). В следующем упражнении Вы будете настраивать второй компьютер (Server2) как клиент протокола DHCP.

---

Внимание! Не рекомендуется выполнять эти упражнения, если Ваш(и) компьютер(ы) являются частью большой сети. Установка сервера DHCP может конфликтовать с сетевыми операциями.

---

Определите физический адрес Вашей платы сетевого адаптера. Этот адрес используется для резервирования клиента.

▶ **Определение адреса сетевого адаптера**

- В командной строке наберите *ipconfig /all*, затем нажмите ENTER.

  Запишите физический адрес без дефисов (-). Он понадобится далее.

---

Существует как минимум два способа выяснения адреса Вашей платы сетевого адаптера. Назовите их.

---

---

▶ **Установка DHCP-сервера**

---

Примечание Выполните установку только на компьютере, назначенном Вами на роль сервера DHCP.

---

1. Щелкните кнопку **Start**, укажите на **Settings**, затем щелкните **Control Panel**.
2. Дважды щелкните пиктограмму **Network**.

   Появится диалоговое окно **Network Settings**.
3. Щелкните вкладку **Services**.
4. Щелкните кнопку **Add**.

   Появится диалоговое окно **Select Network Service.**
5. Выберите **Microsoft DHCP Server**, затем щелкните **OK**.

   Появится диалоговое окно **Windows NT Setup** с запросом о полном пути к установочным файлам Windows NT.
6. Наберите полный путь и щелкните **Continue**.

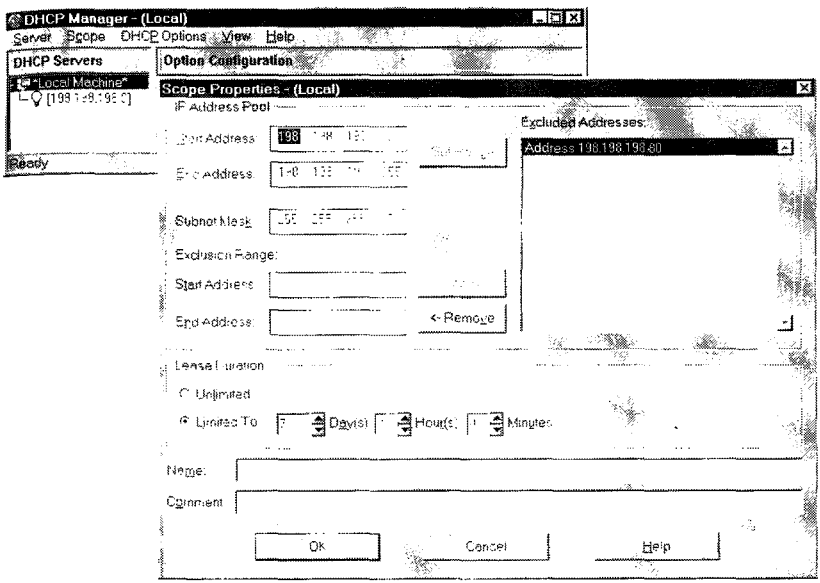
   Соответствующие файлы будут скопированы на Ваш компьютер, затем появится окно с сообщением, что для платы сетевого адаптера требуется статический IP-адрес.
7. Щелкните **OK**.

   Появится диалоговое окно **Network**.
8. Щелкните **Close**.

   Появится диалоговое окно **Network Settings Change**, предлагающее перезапустить компьютер для инициализации новой конфигурации.
9. Щелкните **Yes**.
10. Войдите в систему как *Administrator*.

## Конфигурация области видимости протокола DHCP

Когда сервер протокола DHCP установлен и запущен, сконфигурируйте диапазон адресов. Каждый сервер протокола DHCP требует как минимум одного диапазона IP-адресов, доступных клиентам для аренды. Вы можете создать несколько диапазонов для других серверов протокола DHCP в качестве резерва. Они также создаются для назначения IP-адресов, специфичных для конкретной подсети, например, адреса шлюза по умолчанию.




Примечание Для каждой подсети возможен только один диапазон адресов.

Поскольку серверы протокола DHCP не обмениваются информацией о диапазонах, важно, чтобы каждый диапазон действия содержал уникальные IP-адреса. Если два и более диапазонов действия содержат один и тот же IP-адрес, оба сервера могут назначить один IP-адрес разным клиентам протокола DHCP, что вызовет дублирование IP-адресов.

## Упражнение 2

Вы создадите диапазон адресов протокола DHCP, состоящий из одного IP-адреса (другого Вашего компьютера), со сроком аренды — один день.

Примечание Выполняйте данную процедуру на сервере протокола DHCP.

▶ **Создание диапазона действия протокола DHCP**

1. Щелкните **Start**, укажите на **Settings**, затем щелкните **Control Panel**.
2. Дважды щелкните пиктограмму **Services**. Каковы имена сервисов протокола DHCP?

---

3. Закройте диалоговое окно **Services**.
4. Щелкните кнопку **Start**, укажите на **Administrative Tools**, затем щелкните **DHCP Manager**.

   Появится диалоговое окно **DHCP Manager**.
5. Дважды щелкните ***Local Machine*** под **DHCP Servers**.
6. Щелкните **Create** в меню **Scope**.

   Появится диалоговое окно **Create Scope**. В таблице перечислены доступные опции.

| Опция | Описание |
|---|---|
| IP Address Pool Start Address (Начальный адрес пула IP-адресов) | Начальный IP-адрес, который может быть назначен DHCP-клиенту |
| IP Address Pool End Address (Конечный адрес пула IP-адресов) | Конечный IP-адрес, который может быть назначен DHCP-клиенту |
| Subnet Mask (Маска подсети) | Маска подсети, назначаемая DHCP-клиентам |
| Exclusion Range Start Address (Начальный адрес исключаемого диапазона) | Начальный IP-адрес, исключенный из пула IP-адресов. Адреса этого диапазона не будут назначаться DHCP-клиентам. Это необходимо, если у Вас есть статические IP-адреса, сконфигурированные для не DHCP-клиентов |

(*продолжение*)

| Опция | Описание |
|---|---|
| Exclusion Range End Address (Конечный адрес исключаемого диапазона) | Конечный IP-адрес, исключенный из пула IP-адресов. Адреса этого диапазона не будут назначаться DHCP-клиентам. Это необходимо, если у Вас есть статические IP-адреса, сконфигурированные для не DHCP-клиентов |
| Lease Duration Unlimited (Неограниченная продолжительность аренды) | Аренды DHCP, назначенные клиентам, не истекут никогда |
| Lease Duration Limited To (Продолжительность аренды, ограниченная до) | Количество дней, часов и минут, в течение которых аренда доступна DHCP-клиенту без обновления |
| Name (Имя) | Имя назначается диапазону адресов и отображается после IP-адреса в окне **DHCP Manager** |
| Comment (Комментарий) | Дополнительный комментарий для диапазона |

7. Сконфигурируйте диапазон действия, используя данные таблицы.

| Окно | Что следует набрать |
|---|---|
| **IP Address Pool Start Address** | IP-адрес второго компьютера |
| **IP Address Pool End Address** | IP-адрес второго компьютера |
| **Subnet Mask** | 255.255.255.0 |
| **Lease Duration Limited To (Days)** | 1 |

8. Щелкните кнопку **OK**.

   Появится диалоговое окно **DHCP Manager** с информацией о том, что диапазон был успешно создан и нуждается в активизации. Диапазон надо активизировать перед тем, как он станет доступным для аренды.

9. Для активизации диапазона щелкните кнопку **Yes**.

---

Примечание Другой способ активизации диапазона действия: выберите неактивный диапазон в окне **DHCP Manager**, затем в меню **Scope** щелкните **Activate**.

---

В окне **DHCP Manager** появится добавленный диапазон действия. Обратите внимание на желтую светящуюся лампочку, расположенную за IP-адресом, — она указывает, что диапазон активен. Окно сообщений информирует, что доступных данных больше нет.

---

Внимание! Если в объединенной сети есть компьютеры — не клиенты протокола DHCP, то надо исключить их статические IP-адреса из диапазона адресов сервера DHCP, иначе сервер DHCP может назначить клиенту протокола DHCP адрес, который приведет к дублированию.

---

10. Щелкните кнопку **OK**.

## Конфигурация опций диапазона адресов

Закончив создание диапазона адресов, Вы можете сконфигурировать опции для DHCP-клиентов в диалоговом окне **DHCP Options: Scope**.

- *Global* Глобальные опции доступны для всех клиентов DHCP. Они используются, когда всем клиентам во всех подсетях нужна одинаковая информация о конфигурации. Например, Вы можете сконфигурировать все клиенты для использования одного сервера WINS. Глобальные опции используются всегда, когда не сконфигурированы опции диапазона адресов или клиента.
- *Scope* Эти опции доступны только для клиентов, арендовавших адрес из диапазона сервера. Например, если Вы назначили отдельный диапазон адресов для каждой подсети, то сможете задать уникальный адрес шлюза по умолчанию для каждой подсети. Опции диапазона действия имеют больший приоритет по сравнению с глобальными.
- *Client* Эти опции назначаются для конкретного клиента, использующего постоянную аренду. Они всегда более приоритетны, чем опции диапазона адресов или глобальные.

---

Внимание! Несмотря на то что сервер протокола Microsoft DHCP может предложить все опции из списка, клиенты протокола Microsoft DHCP будут принимать только те, что приведены в таблице ниже. Клиенты, использующие другие реализации протокола DHCP, могут получать и использовать все опции.

---

| Опция | Описание |
|---|---|
| 003 Router | Описывает IP-адрес маршрутизатора, например адрес шлюза по умолчанию. Если у клиента есть локально определенный адрес шлюза по умолчанию, он будет использоваться вместо полученного по протоколу DHCP |
| 006 DNS Servers | Описывает IP-адрес сервера DNS |
| 046 WINS/NBT node type | Описывает используемый клиентом тип разрешения имен NetBIOS поверх TCP/IP. Возможные варианты:<br>1 = B-узел (широковещание)<br>2 = P-узел (точка-точка)<br>3 = M-узел (смешанный)<br>4 = H-узел (гибридный) |
| 044 WINS/NBNS servers | Описывает IP-адрес доступного клиентам сервера WINS. Если адрес сервера WINS конфигурируется вручную для клиента, то такая конфигурация приоритетнее, чем заданная этими опциями |
| 047 NetBIOS Scope ID | Описывает идентификатор локальной области видимости NetBIOS. NetBIOS поверх TCP/IP связывается только с узлами NetBIOS, имеющими тот же идентификатор области видимости |

## Упражнение 3

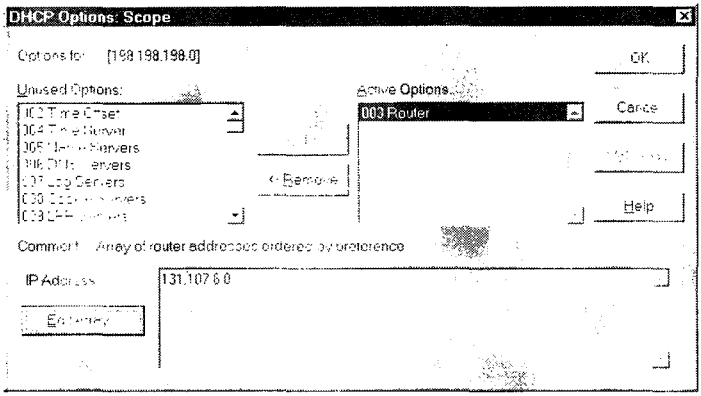
Вы настроите опцию диапазона адресов протокола DHCP, которая автоматически опишет адрес шлюза по умолчанию для клиентов протокола DHCP.

Примечание Выполняйте это упражнение с сервера протокола DHCP.

▶ **Конфигурация опций диапазона адресов протокола DHCP**

1. Щелкните пиктограмму с «горящей лампочкой» для только что созданного Вами диапазона.
2. В меню **DHCP Options** выберите **Scope**.

   Появится диалоговое окно **DHCP Options: Scope**.




3. Выберите **003 Router** в поле **Unused Options**, затем щелкните **Add**.
   Опция **003 Router** переместится в окно **Active Options**.
4. Щелкните кнопку **Value**.
   Раскроется диалоговое окно **Router IP Address**.
   Параметры окна **Router IP Address** описаны в таблице.

| Параметр | Описание |
|---|---|
| IP Address | Назначает добавляемый в опции IP-адрес сервера, например **003 Routers** |
| Long | Конфигурирует 32-разрядное числовое значение, например **035 ARP Cache Time-out** |
| String | Назначает строку из символов, например **015 Domain Name** |
| Word | Определяет 16-разрядное числовое значение для размеров некоторых блоков, например **022 Max DG Reassembly Size** |
| Byte | Назначает величину, состоящую из одного байта, например **046 WINS/NBT Node Type** |
| Binary | Описывает двоичную величину, например **043 Vendor-Specific Information** |

5. Щелкните кнопку **Edit Array**.
   Появится диалоговое окно **IP Address Array Editor**.
6. Под **New IP Address** наберите адрес Вашего шлюза по умолчанию (**131.107.2.1**), затем щелкните кнопку **Add**.
   Под **IP Addresses** появится новый IP-адрес.

7. Щелкните кнопку **OK** для возвращения в диалоговое окно **DHCP Options: Scope**.

   Новый маршрутизатор отобразится в списке IP-адресов.
8. Щелкните кнопку **OK**.

   Появится сообщение о том, что доступных данных больше нет.
9. Закройте окно **DHCP Manager**.

---

Примечание Вы должны завершить и перезапустить DHCP Manager для того, чтобы в левой панели появились новые опции.

---

## Резервирование информации для клиента

Вы можете сконфигурировать протокол DHCP таким образом, что сервер DHCP всегда будет назначать один и тот же IP-адрес одному и тому же клиенту. Это называется *резервированием информации для клиента* (client reservation).

Для некоторых клиентов протокола DHCP важно, чтобы IP-адрес не менялся при возобновлении аренды. Например, серверам в сети, где есть клиенты, не использующие WINS, требуются всегда одни и те же IP-адреса. Не WINS-клиенты должны использовать файл LMHOSTS для разрешения имен NetBIOS-узлов в удаленных сетях. Если IP-адрес сервера меняется, поскольку не зарезервирован, разрешение имени при помощи LMHOSTS не получится. Резервирование IP-адреса для сервера гарантирует, что этот адрес не изменится.

## Упражнение 4

Вы зарезервируете информацию для второго Вашего компьютера. В сетях с несколькими DHCP-серверами таким образом можно обеспечить один и тот же адрес для одного и того же клиента.

---

Примечание Выполняйте это упражнение только на сервере DHCP.

---

▶ **Резервирование информации для клиента**

1. Выполните Ping на IP-адрес Вашего второго компьютера, затем наберите *arp -a*, чтобы получить адрес его сетевого адаптера. Запишите его (без дефисов), так как он понадобится позднее.

---

2. Запустите DHCP Manager.
3. Дважды щелкните ***Local Machine***.

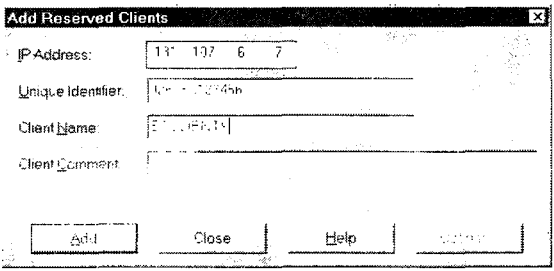
   Появится пиктограмма с «горящей лампочкой» и IP-адрес.

4. Щелкните эту пиктограмму.

   Окно **Option Configuration** отобразит активную опцию для диапазона адресов **003 Router**.

5. В меню **Scope** щелкните **Add Reservations**.

   Появится диалоговое окно **Add Reserved Clients**.




6. В окне **IP Address** наберите IP-адрес Вашего второго компьютера.
7. В окне **Unique Identifier** наберите адрес сетевого адаптера Вашего второго компьютера.

---

Примечание Адрес сетевого адаптера записывайте без дефисов.

---

Внимание! Если адрес в поле **Unique Identifier** набран неправильно, то он не совпадет с отправленным клиентом DHCP. В результате сервер протокола DHCP назначит клиенту произвольный доступный IP-адрес, несмотря на зарезервированный IP-адрес клиента.

---

8. В окне **Client Name** наберите *Server2* (где *Server2* — имя Вашего второго компьютера), затем щелкните **Add**.

   Это имя используется для идентификации в приложении DHCP Manager. Оно ассоциируется с адресом платы сетевого адаптера.

   Появится диалоговое окно **Add Reserved Clients**.

9. Для возврата в **DHCP Manager** щелкните **OK**.

---

Примечание Если в объединенной сети несколько серверов протокола DHCP, то важно, чтобы все они резервировали одинаковую информацию для своих клиентов. Тогда клиент сможет получить аренду с любого сервера DHCP, и ему будет гарантирован один и тот же IP-адрес.

---

## Упражнение 5

Вы протестируете конфигурацию сервера протокола DHCP, запустив клиент DHCP на Вашем втором компьютере и определив информацию о конфигурации протокола TCP/IP, назначенную ему DHCP-сервером.

---

Примечание Выполняйте это упражнение с Вашего второго компьютера. Он будет клиентом протокола DHCP, поэтому ему назначены адрес сетевого адаптера и имя, которые использовались для резервирования информации протокола DHCP.

---

▶ **Установка клиента протокола DHCP**

1. Щелкните вкладку **IP Address** в диалоговом окне **Microsoft TCP/IP**.
2. Щелкните **Obtain an IP address from a DHCP server**.

   Вам будет предложено активизировать протокол DHCP.
3. Щелкните кнопку **Yes**.
4. Щелкните кнопку **OK**.

   Это позволит установить и активизировать клиент DHCP.
5. Снова щелкните **OK**.

▶ **Проверка информации протокола TCP/IP, назначенной протоколом DHCP**

---

Примечание Выполняйте о упражнение только на компьютере-клиенте протокола DHCP.

---

1. В командной строке наберите *ipconfig /all* для просмотра конфигурации протокола DHCP.
2. Какой IP-адрес был назначен компьютеру клиента сервером протокола DHCP?

   _____

3. Каков адрес шлюза по умолчанию?

   _____

▶ **Просмотр адресов, назначенных протоколом DHCP**

Вы просмотрите список арендованных адресов сервера протокола DHCP.

---

Примечание Выполняйте это упражнение на сервере протокола DHCP.

---

1. В окне **DHCP Manager** выберите локальный диапазон адресов (отмечен пиктограммой с «горящей лампочкой»).
2. В меню **Scope** щелкните **Active Leases**.

   Появится диалоговое окно **Active Leases**, отображающее список IP-адресов, которые были арендованы клиентами.
3. Щелкните кнопку **Properties**.

   Появится диалоговое окно **Client Properties**. **Lease expires time** (время истечения аренды) отобразится как **infinite** (бесконечное).
4. Щелкните **OK** для возврата в диалоговое окно **Active Leases**.
5. Щелкните **OK** для возврата в окно **DHCP Manager**.

▶ **Обновление аренды протокола DHCP**

Вы обновите аренду, назначенную компьютеру клиента протокола DHCP.

---

Примечание Выполняйте данную процедуру только на компьютере клиента протокола DHCP.

---

1. В командной строке наберите *ipconfig /all*
2. Когда истекает срок аренды?

---

3. Для обновления аренды наберите *ipconfig /renew* в командной строке, затем нажмите ENTER.

   Отобразится информация о конфигурации протокола IP.
4. Наберите *ipconfig /all* для просмотра информации об аренде.
5. Когда истекает срок аренды?

---

## Резюме

Диапазон адресов — это совокупность IP-адресов для назначения клиентам. Несколько диапазонов и отдельные диапазоны для каждой подсети могут быть созданы для получения клиентами протокола DHCP корректных IP-адресов с любого сервера протокола DHCP. Для реализации протокола DHCP требуется программное обеспечение клиента и сервера. Каждому серверу DHCP нужен как минимум один диапазон адресов.

# Занятие 3. Агент ретрансляции протокола DHCP

Windows NT Server является RFC-совместимым агентом ретрансляции протокола DHCP. Агент ретрансляции, используемый совместно со статическим или динамическим маршрутизатором, передает сообщения протокола DHCP между клиентами протокола DHCP и серверами, расположенными в различных IP-сетях.

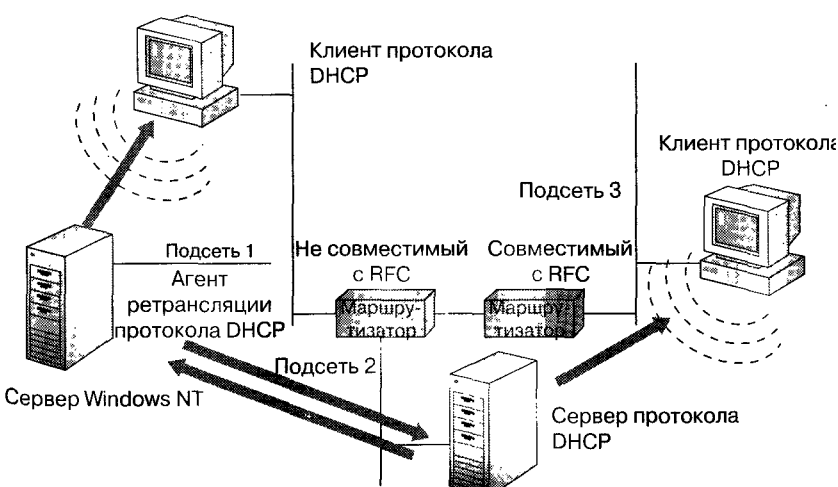
**Изучив материал этого занятия, Вы сможете:**

- ✓ установить и сконфигурировать агент ретрансляции протокола DHCP.

**Продолжительность занятия – 25 минут**

Если Ваши DHCP-клиенты и серверы разделены маршрутизаторами, Вы можете сконфигурировать Windows NT Server в качестве агента ретрансляции. Он будет перехватывать широковещательные сообщения протокола DHCP и пересылать их серверу протокола DHCP через IP-маршрутизаторы. Установить Microsoft DHCP Relay Agent можно через программу **Network** в **Control Panel**.

Когда клиент, использующий TCP/IP, в режиме DHCP-клиента запрашивает IP-адрес в подсети, где находится агент ретрансляции протокола DHCP, запрос принимается агентом. Он должен перенаправить запрос на компьютер, где работает сервис Windows NT DHCP Server. Этот компьютер возвращает IP-адрес непосредственно клиенту.



В конфигурации агента ретрансляции указывается IP-адрес компьютера, на котором работает Windows NT DHCP Server, поэтому он будет знать, куда пересылать запросы клиентов на аренду IP-адресов.

## Упражнения

Используя программу **Network** из **Control Panel**, установите агента ретрансляции протокола DHCP, а затем сконфигурируйте агента ретрансляции, используя окно свойств протокола DHCP для задания IP-адреса DHCP-сервера. Имейте в виду, что агент ретрансляции в реальной ситуации пересылает запросы между *разными* подсетями.

---

Примечание Выполняйте это упражнение на компьютере Server2.

---

▶ **Установка агента ретрансляции протокола DHCP**

1. Щелкните **Start**, укажите на **Settings**, затем щелкните **Control Panel**.
2. Дважды щелкните пиктограмму **Network**.

   Появится диалоговое окно **Network**.
3. Щелкните вкладку **Services**.

   Вкладка **Services** отобразит список **Network Services**, где указаны работающие в данный момент на компьютере сервисы.
4. Щелкните кнопку **Add**.

   В диалоговом окне **Select Network Service** отобразится список доступных сетевых сервисов.
5. Щелкните **DHCP Relay Agent**.

   **DHCP Relay Agent** в списке будет выделен.
6. Щелкните **OK**.

   Появится диалоговое окно **Windows NT Setup**.
7. Наберите путь к установочным файлам Windows NT Server, затем щелкните кнопку **Continue**.

   Появится диалоговое окно **Network**.
8. Щелкните кнопку **Close**.

   Появится диалоговое окно **Unattended Setup** с предложением добавить IP-адрес в список **DHCP Servers**.
9. Щелкните кнопку **Yes**.

   Появится диалоговое окно **TCP/IP Properties**.
10. Щелкните вкладку **DHCP Relay**, затем щелкните кнопку **Add**.

    Появится окно свойств **DHCP Relay Agent**.

11. Наберите IP-адрес сервера протокола DHCP и щелкните **Add**.
    IP-адрес добавится в список **DHCP Servers**.
12. Щелкните **OK**.
    Появится предложение перезапустить компьютер.
13. Щелкните кнопку **Yes**.
    Ваш компьютер перезапустится с активизированным агентом ретрансляции протокола DHCP.

Восстановите первоначальную конфигурацию компьютера для подготовки к следующим упражнениям.

▶ **Отключение агента ретрансляции протокола DHCP**

Примечание Выполняйте это упражнение на компьютере Server2.

1. Щелкните **Start**, укажите на **Settings**, затем щелкните **Control Panel**.
2. Дважды щелкните пиктограмму **Services**.
   Появится диалоговое окно **Services**.
3. Щелкните кнопку **DHCP Relay Agent**.
4. Щелкните вкладку **Startup**.
   Появится диалоговое окно **Service**.
5. Щелкните кнопку **Disabled**.
6. Щелкните **OK**.
7. Щелкните **Close**.
8. Выйдите из системы и перезагрузите компьютер.

▶ **Использование статического IP-адреса**

Примечание Выполняйте это упражнение на компьютере — DHCP-клиенте.

1. Войдите в окно **Microsoft TCP/IP Properties**.
2. Щелкните **Specify an IP address**.
3. Задайте конфигурацию, указанную в таблице.

| Параметр | Значение |
|---|---|
| IP-address (IP-адрес) | 131.107.2.211 |
| Subnet Mask (Маска подсети) | 255.255.255.0 |
| Default Gateway (Шлюз по умолчанию) | 131.107.2.1 |

4. Щелкните **OK**.
   Появится диалоговое окно **Network**.

5. Щелкните **OK**.
6. Выйдите из системы и перезагрузите компьютер.

## Резюме

Агент ретрансляции передает сообщения протокола DHCP между клиентами и серверами, расположенными в различных сетях.

# Занятие 4. Управление базой данных протокола DHCP

База данных автоматически сохраняется каждые 60 минут. Если Windows NT Server обнаружит повреждение базы данных, он автоматически восстановит ее по резервной копии. На этом занятии Вы узнаете, когда нужно сохранять вручную и сжимать базу данных.

**Изучив материал этого занятия, Вы сможете:**

- ✓ копировать и восстанавливать БД протокола DHCP;
- ✓ использовать утилиту Jetpack для сжатия БД протокола DHCP.

**Продолжительность занятия — 10 минут**

## Резервное копирование базы данных протокола DHCP

По умолчанию резервное копирование базы данных выполняется каждые 60 минут. Резервные копии хранятся в каталоге *\systemroot*\System32\Dhcp\Backup\Jet.

Интервал резервного копирования по умолчанию можно изменить, задав требуемое значение параметра **BackupInterval** и перезапустив сервис DHCP Server. Параметр **BackupInterval** находится в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters\BackupInterval.

Копия раздела реестра хранится в каталоге *\systemroot*\System32\Dhcp\Backup под именем DHCPCFG.

## Восстановление базы данных протокола DHCP

База данных может быть восстановлена вручную или автоматически. Для этого используется несколько методов.

- Перезапустите сервис DHCP Server. Если он обнаружит повреждение базы данных, то автоматически восстановит ее по резервной копии.
- Установите значение параметра **RestoreFlag** равным 1 и перезапустите сервис DHCP Server. Параметр **RestoreFlag** находится в разделе реестра HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters.

Поскольку база данных была успешно восстановлена, сервер автоматически поменяет значение на установленное по умолчанию — 0.

- Скопируйте содержимое каталога *systemroot*\System32\Dhcp\Backup\Jet в каталог *systemroot*\System32\Dhcp, затем перезапустите сервис DHCP Server*.

## Файлы базы данных протокола DHCP

Файлы, перечисленные в таблице, хранятся в каталоге *systemroot*\System32\Dhcp. Вам не следует исправлять или перемещать их.

| Файл | Описание |
|---|---|
| Dhcp.mdb | Файл базы данных протокола DHCP |
| Dhcp.tmp | Временный файл для хранения информации БД в течение работы сервиса DHCP Server |
| Jet.log и Jet*.log | Журнал всех транзакций, выполненных с базой данных. При необходимости используется протоколом DHCP для восстановления данных |
| System.mdb | Используется протоколом DHCP для хранения информации о структуре БД |

## Сжатие базы данных протокола DHCP

ОС Windows NT Server 4.0 автоматически сжимает базу данных протокола DHCP, поэтому, вероятнее всего, Вам не придется выполнять эту процедуру. Однако, если Вы используете ОС Windows NT Server 3.51 или более раннюю ее версию, то по истечении некоторого времени работы протокола DHCP может потребоваться сжать базу данных для увеличения производительности. Базу данных необходимо сжимать, если ее размер превышает 30 Мб.

## Упражнения

Для сжатия БД протокола DHCP Вы можете использовать утилиту Jetpack, поставляемую вместе с Windows NT Server. Это утилита работает в окне командной строки Windows NT Server.

### ▶ Сжатие базы данных протокола DHCP

1. Остановите сервис DHCP Server. Это может быть сделано из **Control Panel, Services, Microsoft DHCP Server** или из командной строки. В последнем случае используйте команду:

```
net stop dhcpserver
```

---

* Разумеется, сначала надо остановить сервис, затем скопировать файлы и, наконец, запустить сервис вновь. — *Прим. перев.*

2. В командной строке перейдите в каталог *\systemroot*\System32\Dhcp, затем запустите утилиту Jetpack (замените *имя_временного_файла* любым другим именем):

   ```
   jetpack dhcp.mdb имя_временного_файла.mdb
   ```

   Содержимое файла Dhcp.mdb будет сжато и помещено в файл с указанным Вами именем, этот файл будет скопирован под именем Dhcp.mdb, затем сам временный файл будет удален.
3. Перезапустите сервис DHCP Server из **Control Panel, Services, Microsoft DHCP Server** или из командной строки. В последнем случае используйте команду:

   ```
   net start dhcpserver
   ```

---

Примечание *Microsoft Windows NT Server Resource Kit* включает версию DHCP Manager для командной строки и утилиту, определяющую *нелегальные* (unautorized) серверы протокола DHCP*.

---

## Резюме

База данных протокола DHCP автоматически копируется каждые 60 минут. Однако в некоторых случаях необходимо сделать это вручную. Вы можете использовать утилиту Jetpack, поставляемую вместе с Windows NT Server, для сжатия базы данных протокола DHCP.

---

* Имеется в виду утилита DHCPLoc, которая помогает обнаружить появление в сети нового DHCP-сервера, установленного без санкции администратора и неизвестного ему. Эта утилита вообще полезна при отладке DHCP. — *Прим. перев.*

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Из каких этапов состоит аренда протокола DHCP?

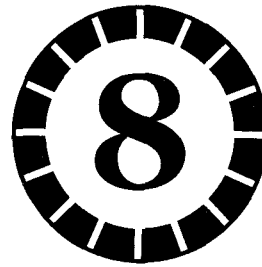
2. Когда клиенты протокола DHCP обновляют аренду?

3. Как надо сконфигурировать сервер протокола DHCP для получения аренды клиентом протокола DHCP?

4. В каких ситуациях требуется более одного сервера протокола DHCP в объединенной сети?

5. Как надо настроить DHCP-серверы, чтобы они «подстраховывали» друг друга?

6. Когда необходимо резервировать конкретный IP-адрес для клиента?



# NetBIOS поверх TCP/IP



## В этой главе

В предыдущей главе Вы изучили, как IP-адреса преобразуются в адреса сетевых адаптеров. В этой главе Вы познакомитесь с концепциями и методами распознавания имен NetBIOS, разрешением имен NetBIOS в IP-адреса с использованием механизма широковещания, файла LMHOSTS, сервера имен NetBIOS, *сервера имен домена* (Domain Name Server, DNS) и файла HOSTS. Выполняя упражнения, Вы научитесь настраивать и использовать файл LMHOSTS.

## Прежде всего

Прежде чем Вы приступите к выполнению заданий этой главы, нужно:

- установить ОС Microsoft Windows NT Server 4.0 с поддержкой протокола TCP/IP.

# Занятие 1. Общие сведения об именах NetBIOS

Имя NetBIOS назначается Вашему компьютеру. На этом занятии Вы познакомитесь с тем, как Windows NT использует его для взаимодействия другими компьютерами, поддерживающими NetBIOS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать NetBIOS и имена NetBIOS;
- ✓ перечислить виды служб, предоставляемых NetBIOS поверх TCP/IP;
- ✓ рассказать о регистрации, освобождении и обнаружении имен NetBIOS.

**Продолжительность занятия — 25 минут**

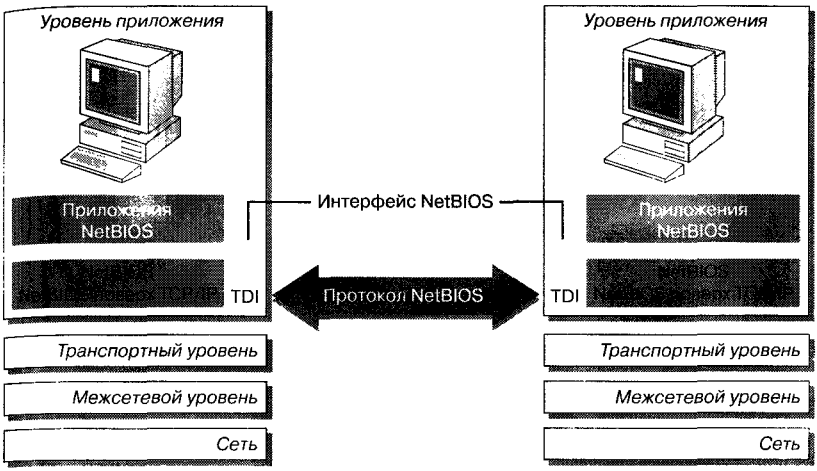
Стандарт NetBIOS, разработанный для IBM фирмой Sytek Corporation в 1983 году, позволяет приложениям взаимодействовать по сети. Этот стандарт определяет *интерфейс* сеансового уровня и *протокол* передачи данных и управления сеансом.

Интерфейс NetBIOS — доступный пользовательским приложениям стандартный API для отправки сетевого ввода/вывода и команд управления к ПО нижележащего протокола. Прикладная программа, использующая API интерфейса NetBIOS для сетевого взаимодействия, может работать с любым протоколом, поддерживающим интерфейс NetBIOS.

Стандартом NetBIOS определяется также протокол, действующий на сеансовом/транспортном уровне. Он реализуется в ПО нижележащего протокола, например NBFP (NetBEUI) или NetBT, где представлен весь набор команд сетевого ввода/вывода интерфейса NetBIOS. NetBIOS поверх TCP/IP, или просто NetBT, — это сетевая служба сеансового уровня.

NetBIOS поддерживает следующие команды и функции:

- регистрацию и проверку сетевых имен;
- запуск и завершение сеанса;
- надежную передачу данных сеанса, ориентированного на соединение;
- ненадежную передачу датаграмм (datagram) без установки соединения;
- возможность мониторинга и управления протоколом и адаптером.




## Имена NetBIOS

Имя NetBIOS — это уникальный 16-байтный адрес, используемый для идентификации в сети ресурса NetBIOS. Имена бывают *эксклюзивные* (exclusive) или *групповые — не эксклюзивные* (non-exclusive). Первые, как правило, используют для взаимодействия с некоторым процессом на компьютере, вторые — для передачи информации нескольким компьютерам одновременно.

Вы можете применить команду *nbtstat -n* для просмотра имен NetBIOS Вашего компьютера.

Например, имя NetBIOS используется службой сервера на компьютере, работающем под управлением Windows NT. При загрузке системы служба сервера регистрирует уникальное имя NetBIOS, основанное на имени компьютера. Точнее, имя, используемое сервером, — это 15-символьное имя компьютера плюс 16-й символ — шестнадцатеричное число 20. Остальные сетевые службы также используют имя компьютера для построения своих имен NetBIOS, поэтому 16-й символ применяется для однозначного определения таких служб, как *редиректор* (Redirector), *сервер* (Server) или *почтовая служба* (Messenger service).

Когда Вы подключаетесь к компьютеру под управлением Windows NT Server при помощи команды *net use*, поиск имени NetBIOS для службы сервера осуществляется посредством запросов Name Query.

Все сетевые службы Windows NT регистрируют свои имена NetBIOS. Все сетевые команды Windows NT (Windows NT Explorer, File Manager и команды *net*) используют имена NetBIOS для доступа к этим службам.

Имена NetBIOS также применяются в других системах, основанных на NetBIOS, например Windows for Workgroups, LAN Manager и LAN Manager для UNIX.

### Общие имена NetBIOS

Просмотр зарегистрированных имен полезен для определения служб, работающих на компьютере. В таблице описаны имена NetBIOS из базы данных WINS (Windows Internet Name Service) — сервиса Windows по распознаванию имен. Подробнее о WINS Вы узнаете в главе 9.

| Зарегистрированное имя | Описание |
|---|---|
| \\имя_компьютера[00h] | Имя, зарегистрированное для службы *рабочая станция* (Workstation) клиента WINS |
| \\имя_компьютера[03h] | Имя, зарегистрированное для служб Messenger клиента WINS |
| \\имя_компьютера[20h] | Имя, зарегистрированное для службы Server клиента WINS |
| \\имя_пользователя[03h] | Имя, под которым пользователь входит в систему. Оно регистрируется службой Messenger для того, чтобы пользователь мог получать сообщения, посланные на его имя командой *net send*. В том случае, если несколько пользователей вошли в систему под одним именем (например *Administrator*), только первый компьютер, с которого был осуществлен вход, зарегистрирует это имя |
| \\имя_домена[1Bh] | Имя домена регистрируется *главным контроллером домена* (Primary Domain Controller, PDC), дополнительно выполняющим функции *главного броузера домена* (Domain Master Browser). Это имя используется для удаленного просмотра доменов. Когда сервер WINS получает запрос на такое имя, он возвращает IP-адрес компьютера, зарегистрировавшего это имя |

## Регистрация, обнаружение и освобождение имен NetBIOS

Все узлы, использующие NetBIOS поверх TCP/IP, взаимодействуя с узлами NetBIOS, например с Windows NT, применяют регистрацию, обнаружение и освобождение имен.

### Регистрация имен

Начиная работу, узел NetBIOS поверх TCP/IP регистрирует имя NetBIOS при помощи *запроса регистрации имени* (name registration request) — широковещательного или направленного только к серверу имен NetBIOS.

Если какой-то узел пытается зарегистрировать уже зарезервированное имя NetBIOS, то либо узел с таким именем, либо сервер имен NetBIOS посылает *отказ в регистрации имени* (negative name registration response). Начинающий работу узел получает сообщение об ошибке инициализации.

### Обнаружение имен

*Обнаружение имени* (name discovery) в локальной сети осуществляется при помощи механизма широковещания или сервера имен NetBIOS. Когда узел Windows NT хочет связаться с другим узлом TCP/IP, он посылает *запрос на определение имени* (name query request), содержащий искомое имя NetBIOS, используя широковещательный пакет или адресуя запрос только серверу имен NetBIOS.

Узел, которому принадлежит искомое имя, или сервер имен NetBIOS отправляют обратно *положительный ответ об определении имени* (positive name query response).

### Освобождение имен

*Освобождение имени* (name release) происходит, если приложение или служба NetBIOS прекращает работу. Например, когда на узле останавливается служба Workstation, этот узел перестает посылать отказы в регистрации имен при попытке использовать зарезервированное им имя. В таком случае говорят, что имя NetBIOS *освобождено* (released), и его могут использовать другие узлы.

## Разделение пространства имен NetBIOS на области видимости

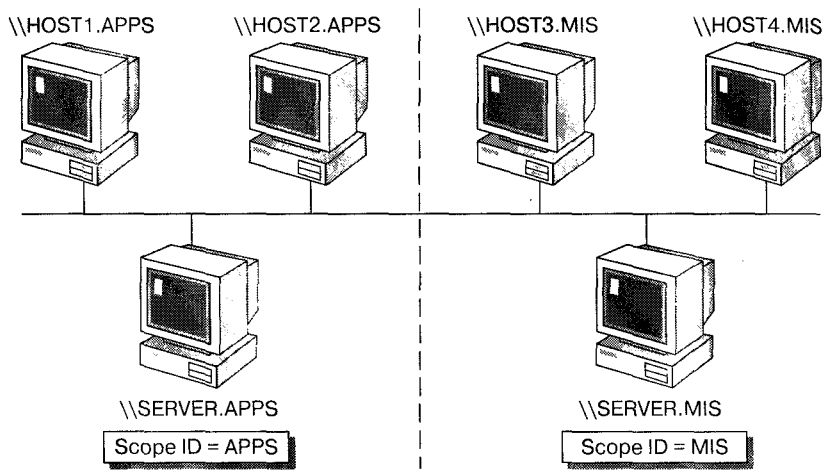
*Идентификатор области видимости NetBIOS* (NetBIOS Scope ID) применяют для сегментации пространства имен NetBIOS. Использование Scope ID не увеличивает производительность, но уменьшает количество пакетов, которые принимаются и обрабатываются узлом.

NetBIOS Scope ID — это строка символов, добавляемая к имени. Она позволяет разделить сплошное 16-символьное пространство имен NetBIOS на *области видимости* (scopes). Если такого деления нет, то имена должны быть уникальными для всех NetBIOS-ресурсов в сети. Задавая Scope ID, помните, что применять уникальные имена нужно только внутри одной области, а не во всем пространстве имен.

NetBIOS-ресурсы одной области видимости изолированы от всех остальных, внешних ресурсов. Если у двух узлов не совпадают Scope ID, то они не смогут взаимодействовать друг с другом посредством NetBIOS поверх TCP/IP. Значение Scope ID задается на вкладке **WINS Address** диалогового окна **Microsoft TCP/IP Properties**.

Две области — APPS и MIS — показаны на рисунке.

- HOST1.APPS и HOST2.APPS могут связаться с SERVER.APPS, но не с HOST3.MIS, HOST4.MIS или SERVER.MIS.
- Области видимости NetBIOS позволяют компьютерам использовать одинаковые имена (если, конечно, они имеют разные Scope ID). NetBIOS Scope ID становится частью имени, делая его уникальным. На рисунке два сервера имеют одинаковое NetBIOS-имя, но различные Scope ID.




Примечание NetBIOS Scope ID описан в документе RFC 1001. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

NetBIOS определяет интерфейс сеансового уровня и сеансовый протокол управления и передачи данных. Для взаимодействия с другими NetBIOS-узлами используются регистрация, освобождение и обнаружение имен. Параметр NetBIOS Scope ID применяется для сегментирования пространства имен NetBIOS.

# Занятие 2. Распознавание имен NetBIOS

Преобразование NetBIOS-имени компьютера в его IP-адрес называют *разрешением* (распознаванием) имени NetBIOS. Изучив материал этого занятия, Вы узнаете о разрешении имен NetBIOS и методах, применяемых в Windows NT для преобразования имен NetBIOS в IP-адреса. Также здесь коротко рассмотрены виды *узлов* (nodes) для распознавания имен NetBIOS, поддерживаемых Microsoft TCP/IP.

**Изучив материалы этого занятия, Вы сможете:**

- ✓ объяснить, как распознаются NetBIOS-имена узлов в удаленных сетях средствами файла LMHOSTS или сервера имен NetBIOS;
- ✓ объяснить, как распознаются NetBIOS-имена в локальной сети с помощью широковещания;
- ✓ описать типы узлов NetBIOS поверх TCP/IP.

**Продолжительность занятия — 25 минут**

*Разрешение* (resolution) NetBIOS-имени компьютера — процесс успешного отображения этого имени в IP-адрес. Прежде чем IP-адрес будет преобразован в адрес сетевого адаптера, NetBIOS-имя данного компьютера должно быть преобразовано в его IP-адрес.

В Microsoft TCP/IP возможны несколько методов разрешения имен NetBIOS. Использование конкретного метода зависит от того, является ли данный узел *локальным* (local) или *удаленным* (remote).

| Стандартные методы | Описание |
|---|---|
| Локальный кэш имен NetBIOS | В кэше содержатся NetBIOS-имена, которые уже распознавались локальным компьютером |
| Сервер имен NetBIOS (NetBIOS Name Server, NBNS) | Реализованный согласно RFC 1001 и RFC 1002 сервер для обеспечения распознавания имен NetBIOS. Свою реализацию фирма Microsoft назвала WINS |
| Локальное широковещание | Широковещательный запрос IP-адреса, соответствующего имени NetBIOS |

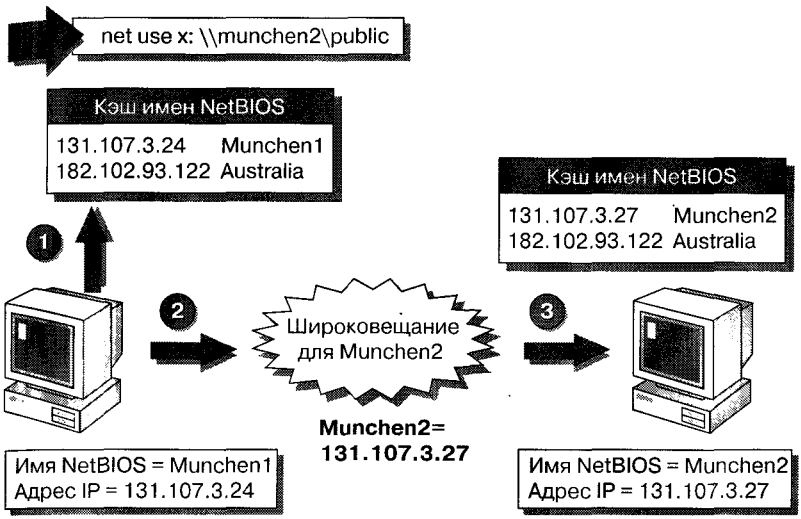
| Методы Microsoft | Описание |
|---|---|
| Файл LMHOSTS | Локальный текстовый файл, в котором IP-адреса отображены в имена NetBIOS для Windows-компьютеров в удаленных сетях |
| Файл HOSTS | Локальный текстовый файл, записанный в том же формате, что и файл \etc\hosts в BSD (Berkley Software Distribution) UNIX 4.3. В этом файле имена узлов отображены в IP-адреса. Он обычно применяется утилитами TCP/IP для разрешения имен узлов |
| Доменная система имен (Domain Name System, DNS) | Сервер, который поддерживает базу данных о соответствиях IP-адрес/имя узла |

## Разрешение локальных имен NetBIOS с применением широковещания

Когда запрашиваемый узел находится в локальной сети, NetBIOS разрешает его имя, используя механизм широковещания. Ниже этот процесс описан поэтапно.

1. Когда пользователь применяет команду Windows NT, например *net use*, IP-адрес, соответствующий NetBIOS-имени запрашиваемого узла, в первую очередь ищется в кэше имен NetBIOS. Если имя удаленного узла недавно использовалось, то соответствующий ему IP-адрес уже находится в кэше имен NetBIOS вызывающего узла, и широковещательный запрос не будет послан. Благодаря этому исключается повторение широковещательных запросов в сети.
2. Если NetBIOS-имя не разрешено при помощи кэша, то вызывающий узел посылает в локальную сеть широковещательный запрос об определении имени удаленного узла.
3. Каждый компьютер сети принимает этот запрос и ищет запрашиваемое имя в своей локальной таблице NetBIOS.

   Компьютер, которому принадлежит это имя, формирует *ответ об определении имени* (name query response). Перед его отправкой для определения адреса сетевого адаптера, запросившего ответ, используется протокол ARP (с применением кэша или широковещания). Как только выяснен адрес сетевого адаптера, посылается ответ об определении имени.




### Ограничения механизма широковещания

Не все маршрутизаторы перенаправляют широковещательные сообщения. Причем у тех, которые способны это делать, данная функция обычно отключена, так как сильно перегружает межсетевой трафик, что может привести к нарушению стабильности сети. В результате все широковещательные сообщения остаются в локальной сети.

---

Примечание Чтобы маршрутизатор мог перенаправлять широковещание, обязательно должна быть включена функция перенаправления широковещательных кадров для 137 и 138 портов UDP.

---

## Разрешение имен при помощи сервера имен NetBIOS

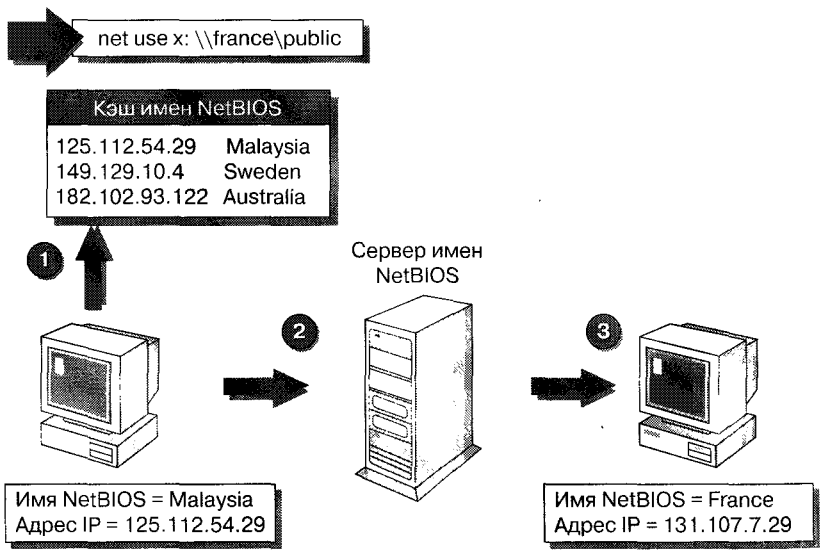
Обычно для разрешения имен NetBIOS в IP-адреса применяется сервер имен NetBIOS. Подробно такой процесс распознавания имени описан ниже.

1. Когда пользователь применяет команду Windows NT, например *net use*, начинается разрешение имени NetBIOS. Сначала имя NetBIOS удаленного узла ищется в кэше имен NetBIOS. Если оно там не обнаружено, клиент Windows NT пытается определить IP-адрес удаленного узла другим способом.
2. Если имя не может быть разрешено при помощи кэша имен NetBIOS локального узла, оно отсылается к серверу имен NetBIOS, который

указан в настройках локального узла. Когда имя NetBIOS разрешено в IP-адрес, он возвращается узлу, пославшему запрос.

По умолчанию клиент Windows NT пытается обнаружить *основной сервер WINS* (primary WINS server) три раза. Если ответ не приходит, клиент Windows NT пытается связаться с *резервным сервером WINS* (secondary WINS server). Однако, если основной сервер WINS ответил клиенту Windows NT, что не смог обнаружить в своей базе данных соответствие имя/IP-адрес для удаленного узла, клиент принимает это как ответ и не пытается связаться с резервным сервером WINS*.

3. После того как имя NetBIOS разрешено, вызывающий узел использует протокол ARP для разрешения IP-адреса в адрес сетевого адаптера.




## Разрешение имен NetBIOS в сетях Microsoft

Имена NetBIOS разрешают и при комбинации методов, поддерживаемых сетями Microsoft. Windows NT 4.0 и более поздние версии можно настроить так, что распознавание имен NetBIOS будет осуществляться не только при помощи широковещания и сервера имен NetBIOS. Дополнительно применяют DNS, а также файлы LMHOSTS и HOSTS. Если один из этих

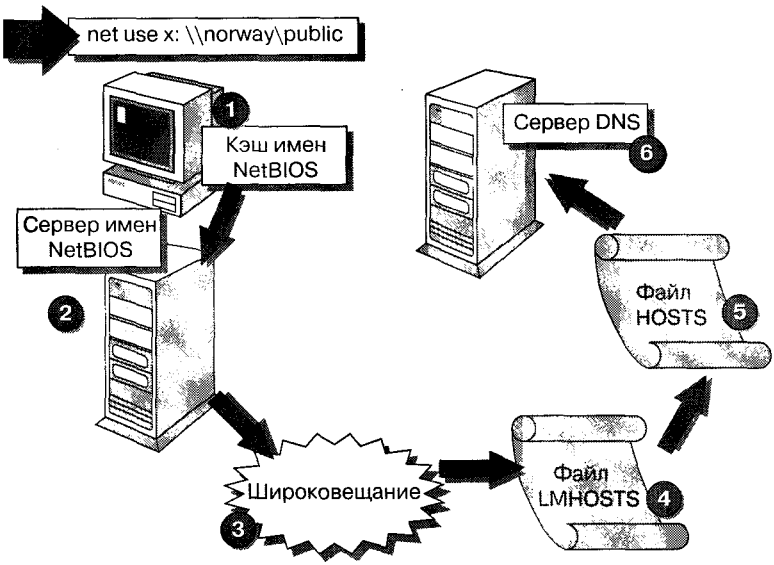
* Существует возможность убедиться в обратном. Если удалось связаться с основным сервером, но тот не обнаружил в своей базе данных нужного соответствия, резервный сервер все-таки запрашивается. — *Прим. перев.*

методов не сработает, другие подстрахуют. Вот как работают комбинированные методы.

1. Когда пользователь вводит команду Windows NT, например *net use*, IP-адрес, соответствующий NetBIOS-имени запрашиваемого узла, в первую очередь ищется в кэше имен NetBIOS. Если такое соответствие обнаружено, имя разрешается без использования сети.
2. Если указанный способ не дал результата, производится три попытки связи с сервером имен NetBIOS (если задан хотя бы один). После удачного разрешения имени возвращается IP-адрес.
3. Если имя не разрешилось при помощи сервера имен NetBIOS, клиент генерирует широковещательный запрос в локальную сеть. Если имя обнаружено в локальной сети, то возвращается IP-адрес.
4. Если имя NetBIOS не разрешилось при помощи широковещания, просматривается локальный файл LMHOSTS. После обнаружения имени в этом файле оно разрешается в IP-адрес.
5. Если имя NetBIOS не определяется через файл LMHOSTS, Windows NT пытается разрешить его, применяя другой механизм распознавания имен узлов. Для этого необходимо установить флажок **Enable DNS for Windows resolution** на странице **WINS Address Property** диалогового окна **TCP/IP**. В таком случае первый этап — это поиск на локальном узле в файле HOSTS.

   Если имя узла обнаружено в файле HOSTS, оно разрешается в IP-адрес. Файл HOSTS должен находиться на локальном компьютере.
6. Если имя не определилось через файл HOSTS, локальный узел отсылает запрос к серверу DNS, указанному в конфигурации. Если имя обнаружено сервером DNS, оно успешно разрешается в IP-адрес.

   Если сервер DNS не отвечает на запрос, производится несколько повторных запросов с интервалами 5, 10, 20 и 40 секунд.




Если перепробованы все приведенные методы, а имя NetBIOS все-таки не распознано, команда Windows NT сообщит пользователю об ошибке, указывая, что компьютер с данным именем обнаружить нельзя.

## Типы узлов разрешения имен при использовании NetBIOS поверх TCP/IP

В Windows NT 4.0 поддерживаются все типы узлов, описанные в RFC 1001 и 1002. Каждый из них распознает имена различными способами.

| Тип узла | Описание |
|---|---|
| B-узел, или широковещание (B-node) | Использует для регистрации и распознавания имен широковещательные сообщения (датаграммы UDP). Использование B-узла сопряжено с двумя основными проблемами: в крупномасштабной сети широковещательные сообщения перегружают сеть, маршрутизаторы обычно не выполняют перенаправление широковещательных сообщений, поэтому ответить на запрос смогут только компьютеры, находящиеся в одной локальной сети |

(*продолжение*)

| Тип узла | Описание |
|---|---|
| P-узел, или точка-точка (P-node, peer-peer) | Использует сервер имен NetBIOS (NBNS), например WINS, для распознавания имен. P-узел не использует широковещание, а напрямую запрашивает сервер имен. В этом случае компьютеры могут взаимодействовать через маршрутизаторы. Наиболее серьезная проблема при использовании P-узла в том, что всем компьютерам должен быть известен адрес NBNS, и если NBNS остановится, компьютеры не смогут установить связь, даже находясь в одной локальной сети |
| M-узел, или смешанный (M-node, mixed) | Является комбинацией B-узла и P-узла. По умолчанию M-узел работает как B-узел. Но если при помощи широковещания распознать имя не удалось, он использует NBNS как P-узел |
| H-узел, или гибридный (H-node, hybrid) | Является комбинацией P-узла и B-узла. По умолчанию H-узел работает как P-узел. Но если через сервер имен NetBIOS распознать имя не удалось, применяется широковещание |
| Расширенный B-узел Microsoft (Microsoft enhanced B-node) | В сетях Microsoft применяется для разрешения имен NetBIOS удаленных узлов. Файл LMHOSTS — статический файл, в котором NetBIOS-имена удаленных компьютеров отображены в их IP-адреса. Записи в файле LMHOSTS, начинающиеся с **#PRE**, сразу помещаются в кэш во время инициализации TCP/IP. Сначала соответствие NetBIOS-имя/IP-адрес ищется в кэше. Если оно не обнаружено, то посылается широковещательное сообщение. Если и это не дает положительного результата, тогда просматривается файл LMHOSTS |

Примечание Типы узлов для NetBIOS поверх TCP/IP определяются в RFC 1001 и 1002. Копии этих документов — на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

### Конфигурирование типа узла

Средствами следующего параметра реестра можно настроить способ, который будет применять NetBT для регистрации и разрешения имен:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

Примечание Если не указан ни один сервер WINS, то по умолчанию используется расширенный B-узел Microsoft. Если же указан хотя бы один сервер WINS, то по умолчанию используется H-узел.

### Утилита Nbtstat

Утилита Nbtstat позволяет проверять установленные при помощи NetBIOS поверх TCP/IP соединения, обновлять кэш LMHOSTS и определять зарегистрированное Вами имя и Scope ID. Эта программа также полезна при устранении неисправностей или для загрузки в память кэша имен NetBIOS.

| Команда | Описание |
|---|---|
| *nbtstat -n* | Отображает список всех зарегистрированных клиентом имен NetBIOS. |
| *nbtstat -c* | Отображает состояние кэша имен NetBIOS |
| *nbtstat -R* | Вручную перезаполняет кэш имен NetBIOS строками из файла LMHOSTS, начинающимися с параметра **#PRE** |

## Резюме

Разрешение имен NetBIOS — это процесс отображения NetBIOS-имени компьютера в его IP-адрес. В зависимости от конфигурации Вашей сети разрешать имена NetBIOS можно несколькими способами — посредством кэша имен NetBIOS, сервера имен NetBIOS (NBNS), широковещания в локальной сети, файла LMHOSTS, файла HOSTS и доменной системы имен.

В сетях Microsoft используется несколько методов разрешения имен NetBIOS. Если один не сработает, то другие предоставят резервный путь. В ОС Microsoft Windows NT 4.0 поддерживаются все типы узлов для NetBIOS поверх TCP/IP.

# Занятие 3. Применение файла LMHOSTS

Теперь, когда Вы познакомились с различными методами разрешения имен, сосредоточимся на расширенной реализации B-узла с применением файла LMHOSTS, в котором содержатся соответствия между IP-адресами и именами NetBIOS удаленных узлов.

**Изучив материалы этого занятия, Вы сможете:**

✓ сконфигурировать файл LMHOSTS для разрешения имен NetBIOS узлов удаленной сети.

**Продолжительность занятия — 35 минут**

LMHOSTS является статическим ASCII-файлом. Он применяется для разрешения NetBIOS-имен в IP-адреса удаленных компьютеров, работающих под управлением Windows NT, или других узлов, поддерживающих NetBIOS. Характеристики файла LMHOSTS:

- используется для разрешения NetBIOS-имен, применяемых в командах Windows NT;
- каждая запись в файле содержит одно имя NetBIOS и соответствующий ему IP-адрес;
- на каждом компьютере хранится собственная копия файла LMHOSTS; по умолчанию имя каталога, в котором он расположен, таково:

  *\systemroot*\System32\Drivers\Etc

  (в этом же каталоге в качестве примера приведен файл Lmhosts.sam);
- используется утилитами Windows NT.

Пример файла LMHOSTS:

```
#This file is used by Microsoft TCP/IP
122.107.9.10      Mexico      # Sales Server
131.107.7.29      France      # Database Server
191.131.54.73     UK          # Training Server
149.129.10.4      Sweden      #PRE  # Main Office Server
182.102.93.122    Australia   #PRE  # MIS Server
```

## Ключевые слова

В файле LMHOSTS могут содержаться ключевые слова, они начинаются со знака #. Если Вы используете LMHOSTS совместно с устаревшей реализацией NetBIOS поверх TCP/IP, например, в системе LAN Manager, ключевые слова игнорируются, поскольку со знака # начинаются приме-

чания. Все возможные ключевые слова для файла LMHOSTS приведены в таблице.

| Ключевое слово | Описание |
|---|---|
| **#PRE** | Указывает, какие записи необходимо загрузить в кэш имен во время инициализации и не удалять их оттуда. Эти записи сокращают число широковещательных сообщений в сети, поскольку просмотр кэша — самый первый шаг при разрешении имени. Записи, отмеченные **#PRE**, загружаются автоматически при инициализации или вручную посредством команды *nbtstat -R*, введенной из командной строки |
| **#DOM:***[имя домена]* | Добавляется после элемента и ассоциирует элемент с указанным доменом. Это ключевое слово предназначено для обеспечения процессов в домене: работы броузеров (browsers), т.е. просмотра списка ресурсов сети, регистрации в сети через маршрутизатор и синхронизации учетных записей пользователей |
| **#NOFNR** | Запрещает использование прямых запросов Name Query при взаимодействии с устаревшими UNIX-системами на основе LAN Manager |
| **#BEGIN_ALTERNATE**<br>**#END_ALTERNATE** | Используется для указания альтернативных мест расположения файлов LMHOSTS. Для включения удаленных файлов рекомендуется применять ключевое слово **#INCLUDE** и *UNC-имя* (Universal Naming Convention name). Естественно, что UNC-имя должно быть указано в файле LMHOSTS с соответствующим ему IP-адресом |
| **#INCLUDE** | Загружает и просматривает записи в файле, отличном от заданного по умолчанию LMHOSTS. Обычно #INCLUDE-файл — совместно используемый файл LMHOSTS, поддерживаемый централизованно |
| **#MH** | Указывает дополнительные записи для компьютера, который может иметь несколько сетевых интерфейсов |

Примечание Файл и кэш имен NetBIOS всегда просматриваются последовательно. Поэтому рекомендуется записи для наиболее часто используемых компьютеров указывать в начале списка. Записи с ключевым словом **#PRE** указывайте в конце списка, потому что после инициализации TCP/IP доступ к ним уже не нужен.

## Проблемы при разрешении имен с использованием файла LMHOSTS

Большинство проблем при разрешении имен NetBIOS возникают из-за некорректных записей в файле LMHOSTS.

| Проблема | Решение |
|---|---|
| В файле LMHOSTS нет записи для удаленного узла | Убедитесь, что в файл LMHOSTS занесены соответствия IP-адрес/имя NetBIOS для всех узлов, к которым необходимо иметь доступ |
| В файле LMHOSTS неправильно указано NetBIOS-имя компьютера | Проверьте правильность записи (посимвольно) всех используемых имен |
| Для имени NetBIOS указан неверный IP-адрес | Проверьте, всем ли именам NetBIOS соответствуют корректные IP-адреса |
| Указано несколько записей для одного имени NetBIOS | Убедитесь, что каждая запись файла LMHOSTS уникальна. Если имя повторяется, то для его разрешения используется первая обнаруженная запись. Если в ней указан неверный IP-адрес, следующие записи просматриваться не будут |

Совет После добавления записей в файл LMHOSTS примените команду *net* с каждым из указанных имен NetBIOS для проверки правильности записей.

## Упражнения

В первом упражнении Вы настроите файл LMHOSTS для разрешения имен NetBIOS в IP-адреса.

Примечание Если Вы раньше не сделали этого, удалите NWLink IPX/SPX Compatible Transport Protocol в диалоговом окне **Select Network Protocol**.

Выполняйте задание на главном компьютере (Server1).

▶ **Настройка файла LMHOSTS**

1. Откройте окно командной строки.
2. При помощи команды *edit* откройте файл:
   *\systemroot*\System32\Drivers\Etc\Lmhosts.sam
3. Прочтите в начале файла LMHOSTS инструкции по добавлению записей.
4. Перейдите в конец файла, а затем добавьте следующую запись:
   *131.107.2.211 Server2*
5. Сохраните файл как LMHOSTS*.
6. Запустите Windows NT Explorer.
7. В меню **Tools** щелкните **Map Network Drive**.
8. В окне **Path** наберите \\Server2 и щелкните **OK**.

Каков ответ?

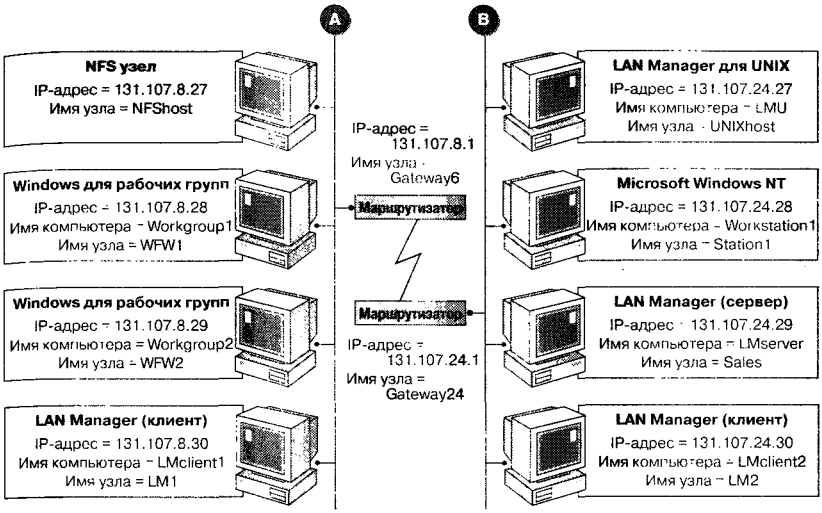
---

Если Вы получили сообщение об ошибке, то проверьте синтаксис команд и записей в файле LMHOSTS.

Взгляните на рисунок и определите, какие записи необходимо добавить в файлы LMHOSTS для каждой сети так, чтобы все узлы сети A могли взаимодействовать с узлами сети B и наоборот.

---

* Будьте внимательны! Если Вы вместо *edit* попытаетесь воспользоваться *notepad*, то, вероятно, не получите ожидаемого результата. Дело в том, что *notepad* по умолчанию сохраняет файлы с расширением .txt, а в списках каталогов по умолчанию, известные расширения имен файлов не отображаются.— *Прим. перев.*




Добавьте необходимые записи в приведенные файлы LMHOSTS так, чтобы узлы в обеих сетях могли взаимодействовать друг с другом.

**Файл LMHOSTS для узлов сети A**

| IP-адрес | Имя |
|---|---|

**Файл LMHOSTS для узлов сети B**

| IP-адрес | Имя |
|---|---|

## Резюме

Файл LMHOSTS содержит соответствия IP-адресов и имен NetBIOS удаленных узлов. В Windows NT файл LMHOSTS может содержать ключевые слова, которые упрощают процесс разрешения имен.

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие методы применяются для разрешения имен NetBIOS?

2. Каково назначение файла LMHOSTS?

# Windows Internet Name Service (WINS)



## В этой главе

В предыдущих главах рассматривались различные методы разрешения NetBIOS-имен. Из этой главы Вы узнаете, как установить службу WINS и как ее средствами уменьшить сетевой трафик за счет широковещательных запросов, вызванных работой NetBIOS поверх TCP/IP в режиме B-узла.

Выполняя занятия этой главы, Вы попрактикуетесь в установке и конфигурировании сервера, клиента и доверенного агента WINS.

Кроме того, Вы освоите управление средой WINS. В занятиях обсуждается поддержка базы данных и её репликация (копирование) между серверами WINS. Также Вы научитесь конфигурировать передающий и принимающий партнеры репликации и делать резервную копию базы данных WINS.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить ОС Windows NT Server 4.0;
- понять основные концепции NetBIOS, изложенные в главе 8.

# Занятие 1. Общие сведения о службе WINS

Служба Windows Internet Name Service (WINS) не применяет широковещание при разрешении имен компьютеров в IP-адреса, а использует динамическую базу данных, содержащую соответствия имен и IP-адресов. На этом занятии Вы узнаете о возможностях и назначениях WINS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как сервер WINS разрешает имена NetBIOS;
- ✓ показать преимущества использования WINS.

**Продолжительность занятия — 5 минут**

Сервер WINS — это усовершенствованный *сервер имен NetBIOS* (NetBIOS Name Server, NBNS), разработанный фирмой Microsoft для снижения широковещательного сетевого трафика, вызванного работой протокола NetBIOS поверх TCP/IP в режиме B-узла. Он применяется для регистрации имен NetBIOS и разрешения их в IP-адреса как для локальных, так и для удаленных узлов.

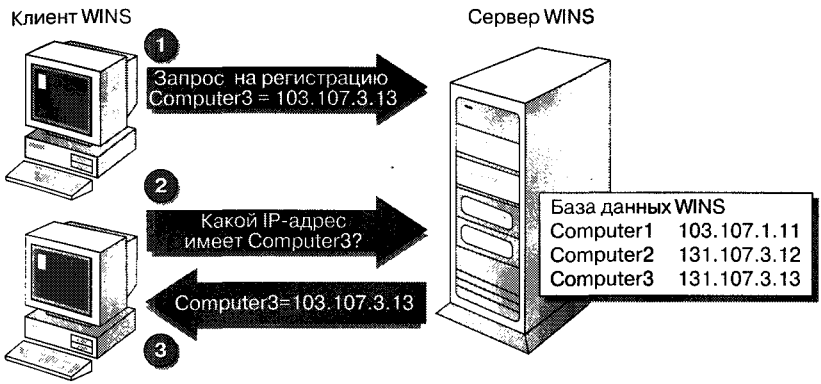
Использование WINS имеет ряд преимуществ. Во-первых, клиентские запросы на разрешение имен поступают непосредственно на сервер WINS. Если ему удается разрешить имя, IP-адрес направляется прямо к клиенту. В результате отпадает необходимость в широковещании и уменьшается сетевой трафик. Однако, если сервер WINS недоступен, клиенты могут применить широковещание для разрешения имени.

Во-вторых, база данных сервера WINS обновляется динамически, поэтому устаревшие сведения своевременно удаляются, а значит, отпадает необходимость в файле LMHOSTS. Кроме того, WINS обеспечивает возможности обзора многодоменной сети.

Прежде чем два использующих NetBIOS узла начнут взаимодействовать, имя узла назначения должно быть разрешено в IP-адрес. Это необходимо, поскольку для работы по протоколу TCP/IP требуется IP-адрес компьютера, а в NetBIOS используются имена компьютеров. Процесс разрешения имени описан далее.

1. Каждый раз при запуске в среде WINS клиент WINS регистрирует у сервера WINS, который задан в его конфигурации, соответствие своего имени NetBIOS IP-адресу.
2. Когда клиент WINS выполняет команду Windows NT для связи с другим узлом, запрос на определение имени посылается по локальной сети непосредственно к серверу WINS; широковещание при этом не используется.

3. Если сервер WINS находит в своей базе данных соответствующее имя NetBIOS и IP-адрес, то этот IP-адрес возвращается клиенту WINS. Поскольку БД сервера WINS динамически обновляется, она всегда содержит реальные соответствия имен NetBIOS и IP-адресов.




## Резюме

Преимущества использования WINS очевидны. Главное из них — уменьшение широковещательного трафика, поскольку запросы на разрешение имен направляются прямо на сервер WINS.

# Занятие 2. Разрешение имени при помощи WINS

В службе WINS применяются стандартные методы регистрации, обновления и освобождения имен. На этом занятии рассматриваются фазы разрешения имени NetBIOS в IP-адрес при помощи WINS.

**Изучив материалы этого занятия, Вы сможете:**

- ✓ описать, как в WINS происходит регистрация, обновление и освобождение имен.

**Продолжительность занятия — 25 минут**

Способ, используемый WINS для разрешения и сбора имен NetBIOS, аналогичен способу, применяемому в режиме B-узла. Метод обновления имен специфичен для режимов работы узлов NetBIOS, использующих сервер имен NetBIOS. Служба WINS представляет собой расширение стандарта, описанного в документах RFC 1001 и 1002. Дальнейшие примеры иллюстрируют процессы, применяемые при разрешении имен NetBIOS.

Примечание NetBIOS поверх TCP/IP описывается в RFC 1001 и 1002. Копии этих документов можно найти на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Регистрация имени

В конфигурационных параметрах каждого клиента WINS указан IP-адрес главного и, возможно, резервного серверов WINS. При запуске клиент WINS регистрирует на сервере WINS свои NetBIOS-имя и IP-адрес. В базе данных сервера сохраняются все зарегистрированные соответствия имен NetBIOS и IP-адресов.

## Обновление имени

Все имена NetBIOS регистрируются временно. Это значит, что любое имя может быть присвоено другому узлу после того, как предыдущий владелец откажется от него.

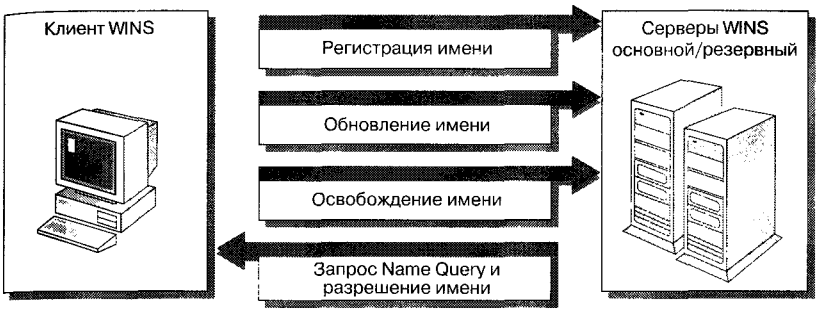
## Освобождение имени

Все клиенты WINS сами ответственны за продление *аренды* (lease) своего имени. Если имя больше не используется, например, при выключении компьютера, клиент WINS посылает серверу WINS сообщение с предложением освободить имя.

### Распознавание имени

После регистрации своего имени NetBIOS и IP-адреса на сервере WINS клиент WINS может взаимодействовать с другими узлами, получая IP-адреса, соответствующие их NetBIOS-именам, от сервера WINS.

Все сетевые сообщения, необходимые для работы WINS, передаются по протоколу UDP на порт 137.

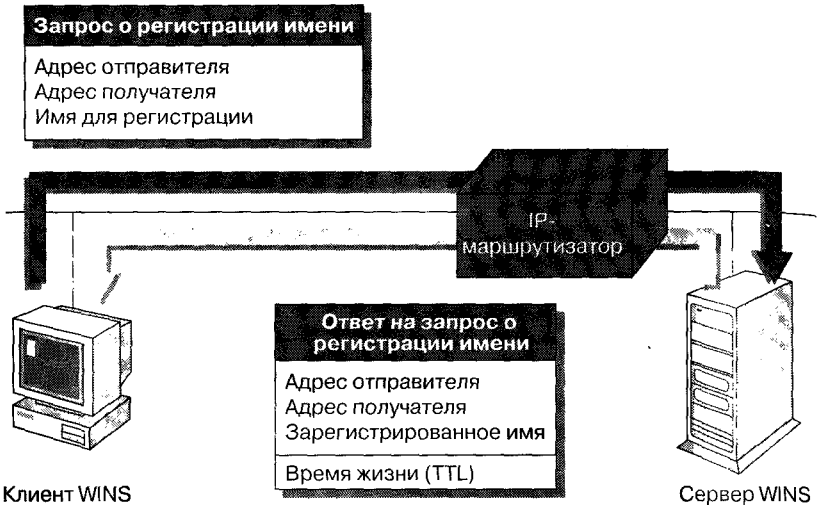



## Регистрация имени

В отличие от реализаций NetBIOS поверх TCP/IP в режиме B-узла, когда имена регистрируются средствами широковещания, клиенты WINS регистрируют свои NetBIOS-имена на серверах WINS.

При инициализации клиент WINS посылает запрос о регистрации имени NetBIOS непосредственно на сервер WINS, заданный в конфигурации клиента. Имена NetBIOS регистрируются при запуске сетевых служб или приложений, например, служб Workstation, Server и Messenger.

Если сервер WINS доступен и запрошенное имя не используется другим клиентом WINS, то данный клиент получит сообщение об успешной регистрации имени. В нем будет указано *время жизни* — TTL (Time To Live) имени клиента. Дальше показан процесс регистрации.




## Обнаружение повторяющегося имени

Если регистрируемое имя уже занесено в базу данных WINS, сервер WINS посылает текущему владельцу имени *запрос на определение имени* (name query request) в качестве проверки. Это делается три раза с интервалом 500 миллисекунд.

Если зарегистрированный компьютер имеет несколько сетевых адаптеров, сервер WINS опробует все заданные для него IP-адреса.

Если текущий владелец имени ответит серверу WINS, сервер пошлет отказ о регистрации клиенту, пытающемуся зарегистрировать это имя. Если же текущий владелец имени не ответит, сервер WINS позволит новому клиенту зарегистрировать это имя.

## Недоступность сервера WINS

Клиент WINS трижды пытается обнаружить главный сервер WINS (при помощи протокола ARP). Если ему это не удается, после третьей попытки запрос о регистрации имени посылается резервному серверу (если он задан). Если же ни один из серверов не доступен, клиент WINS может использовать широковещание для регистрации своего имени.

# Обновление имени

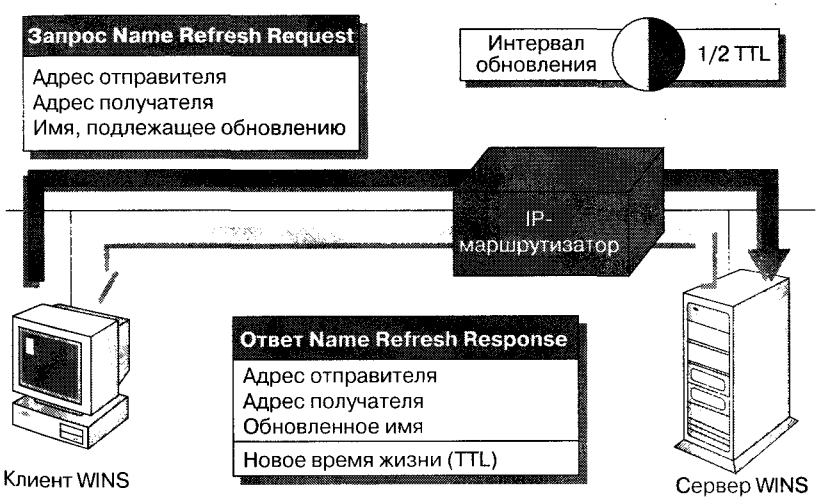
Чтобы продолжать использование имени NetBIOS, клиент должен продлить аренду, прежде чем закончится ее срок. Если клиент WINS не подтвердит дальнейшее использование имени, сервер WINS сделает это имя доступным для других клиентов.

### Запрос Name Refresh Request

Первую попытку обновления имени клиент WINS производит по истечении 1/8 TTL, посылая серверу *запрос на обновление имени* (Name Refresh Request). Если клиент не получит *подтверждение об обновлении имени* (Name Refresh Response), он будет повторять запросы каждые две минуты, пока не истечет 1/2 TTL.

Если подтверждение не поступит, клиент WINS попытается обновить регистрацию имени на резервном сервере WINS. При переключении на резервный сервер WINS процедура обновления имени происходит так, как будто это первая попытка. Затем клиент снова переключается на главный сервер WINS.

После первого успешного обновления имени дальнейшие запросы Name Refresh Request генерируются по истечении половины TTL (после каждого успешного обновления имени TTL также обновляется). На рисунке показано, как клиент WINS продлевает аренду для дальнейшего использования того же имени NetBIOS.




### Ответ на запрос Name Refresh Request

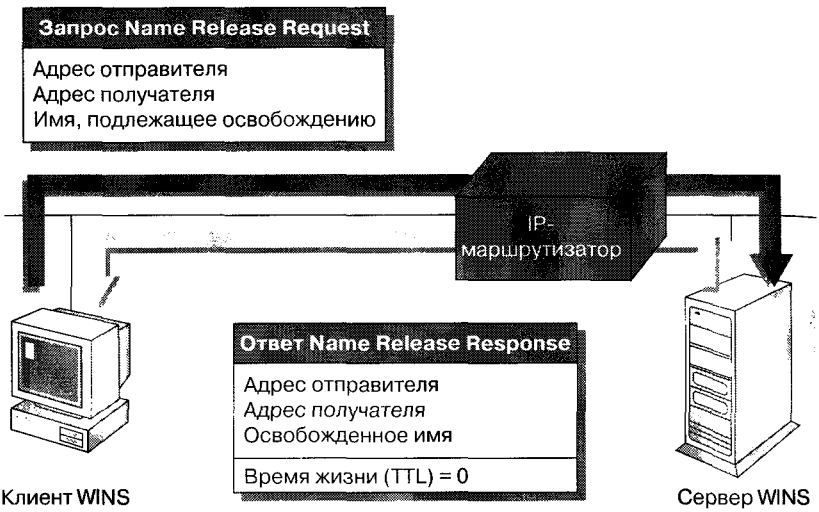
Когда сервер WINS получает запрос Name Refresh Request, он посылает клиенту подтверждение об обновлении имени и новое значение TTL.

## Освобождение имени

### Запрос Name Release Request

По завершении работы клиент WINS посылает серверу WINS *запросы на освобождение* (Name Release Requests) каждого зарегистрированного им

имени. Этот запрос содержит IP-адрес клиента и NetBIOS-имя, которое надо удалить из базы данных WINS. Освобожденное имя становится доступным для использования другими клиентами.




### Ответ на запрос Name Release Request

При получении запроса Name Release Request сервер WINS в первую очередь ищет это имя в своей базе данных. Если его там нет или ему сопоставлен другой IP-адрес, сервер WINS посылает клиенту *отказ в освобождении имени* (negative name release).

В нормальной ситуации сервер WINS отправляет *подтверждение об освобождении имени* (positive name release), а затем отмечает это имя в базе данных как неактивное. Подтверждение об освобождении имени содержит само освобожденное имя и значение TTL равное нулю.

## Сообщения Name Query и Name Response

Обычно разрешение имен NetBIOS в IP-адреса осуществляется на сервере имен NetBIOS, например WINS. По умолчанию клиент WINS сконфигурирован как H-узел протокола NetBIOS поверх TCP/IP. Сервер имен NetBIOS всегда перед началом широковещания ищет в своей базе данных соответствие имени NetBIOS IP-адресу. Этот процесс описан ниже.

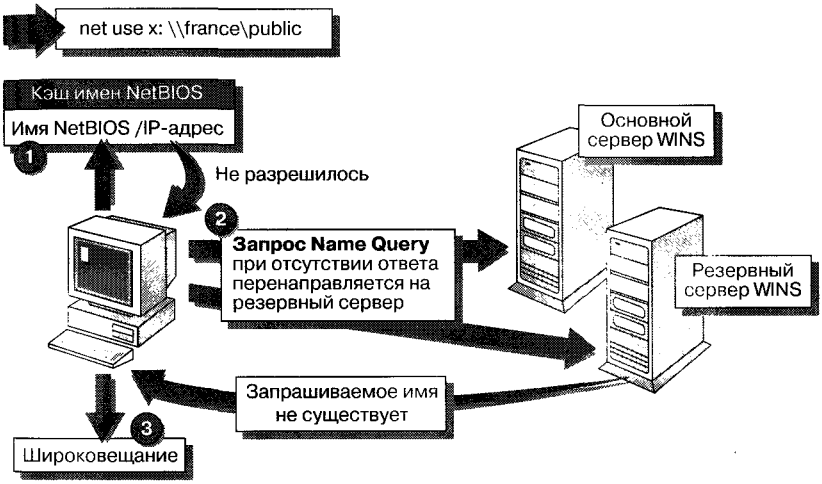
1. Когда пользователь хочет выполнить команду Windows NT, например *net use*, первым для разрешения имени узла назначения просматривается кэш имен NetBIOS.
2. Если имя не удалось разрешить через кэш, запрос Name Query посылается прямо на основной для данного клиента сервер WINS.

Если основной сервер WINS не отвечает, клиент еще два раза посылает запрос, а затем переключается на резервный сервер WINS*.

Если хотя бы один из серверов сумеет разрешить имя, он отсылает узлу-отправителю сообщение, содержащее соответствующий этому имени IP-адрес.

3. Если же ни один из серверов не сумел разрешить имя, клиенту WINS отсылается ответ «Запрашиваемое имя не существует» («Requested name does not exist») и применяется широковещание.

   Если не удается разрешить имя при помощи сервера WINS или широковещания, имя пытаются разрешить посредством просмотра файлов LMHOSTS и HOSTS или при помощи DNS.




## Резюме

Сервис WINS использует стандартные методы регистрации, обновления и освобождения имен. Чтобы продолжать использовать то же самое имя NetBIOS, клиент должен продлить аренду, пока не истечет время жизни. При отключении клиент WINS извещает сервер о том, что ему больше не требуется имя NetBIOS.

---

* Клиент запрашивает резервный сервер не только тогда, когда основной не отвечает. Когда основной сервер сообщает об отсутствии в его базе искомой записи, клиент пытается обратиться к резервному серверу. – *Прим. перев.*

# Занятие 3. Внедрение службы WINS

На этом занятии рассмотрены основные этапы реализации службы WINS — ее установка, задание статических отображений и настройка *доверенного агента службы WINS* (WINS proxy agent).

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать условия, необходимые для реализации сервера и клиента WINS;
- ✓ объяснить процедуру задания статических отображений для не WINS-клиентов;
- ✓ настроить доверенного агента WINS и сервер DHCP для совместного использования с WINS.

**Продолжительность занятия — 60 минут**

Перед применением WINS в объединенной сети следует определить необходимое число серверов WINS. Вообще-то, достаточно одного сервера WINS, поскольку запросы на разрешение имен являются направленными датаграммами, которые могут проходить через маршрутизаторы. Однако применение двух серверов гарантирует наличие резервной системы и обеспечивает отказоустойчивость: если один сервер вышел из строя, для разрешения имен можно обратиться к другому.

Придерживайтесь следующих рекомендаций при использовании сервера WINS.

- Хотя в службе WINS нет встроенных ограничений на обрабатываемое число запросов, но типичные показатели таковы — 1 500 зарегистрированных имен и около 4 500 запросов Name Query Request в минуту.
- Используйте один основной сервер WINS и по одному резервному на каждые 10 000 клиентов WINS.
- Многопроцессорные компьютеры повышают производительность примерно на 25% для каждого дополнительного процессора поскольку на каждом из них запускается отдельный поток WINS.
- Если отключено ведение журнала изменений базы данных (это можно сделать при помощи WINS Manager), регистрация имен происходит гораздо быстрее. Однако в случае какого-либо отказа Вы рискуете потерять несколько последних изменений.

## Требования к службе WINS

Перед началом установки службы WINS Вам необходимо убедиться в том, что компьютеры, назначенные на роли серверов и клиентов, удовлетворяют определенным требованиям к их конфигурации.

## Требования к серверу WINS

В сети, использующей протокол TCP/IP, служба сервера WINS должна быть установлена, как минимум, на одном компьютере, работающим под управлением Windows NT Server (не обязательно контроллере домена).

На сервере необходимо задать IP-адрес, маску подсети, шлюз по умолчанию и другие параметры TCP/IP. Их можно получить от сервера DHCP, но лучше использовать статически назначенные параметры.

## Требования к клиенту WINS

Внедрение WINS — это настройка клиентов, а также установка и конфигурирование службы WINS Server.

Клиентом может быть компьютер под управлением одной из следующих ОС:

- Windows NT Server 4.0 или 3.5*x*;
- Windows NT Workstation 4.0 или 3.5*x*;
- Windows 95;
- Windows for Workgroups 3.11 с протоколом Microsoft TCP/IP-32;
- клиент сетей Microsoft для MS-DOS;
- LAN Manager 2.2c для MS-DOS.

Клиенту необходимо указать IP-адрес основного сервера WINS, адрес резервного сервера может быть указан дополнительно.

## Конфигурация службы WINS Server

- Установите WINS.
- Задайте статические соответствия имен NetBIOS и IP-адресов всех не WINS-клиентов. Это нужно для того, чтобы удаленные клиенты WINS могли взаимодействовать с ними.
- Настройте доверенный агент WINS, чтобы у не WINS-клиентов была возможность разрешать имена через сервер WINS.
- Настройте на сервере DHCP поддержку WINS.

## Конфигурация клиента WINS

Конфигурация клиента задается на вкладке **WINS** диалогового окна **Microsoft TCP/IP Properties**. Для этого достаточно указать IP-адрес основного сервера WINS и — в качестве опции — резервного.

## Упражнение

Вы настроите сервер WINS на автоматическое разрешение имен NetBIOS в IP-адреса для клиентов WINS.

---

Примечание Выполните настройку на компьютере, который Вы решили сделать сервером WINS (Server1).

▶ **Установка службы WINS Server**

1. Щелкните **Start**, укажите на **Settings**, а затем щелкните **Control Panel**.
2. В **Control Panel** дважды щелкните пиктограмму **Network**, выберите вкладку **Services**, а затем — **Add**.
3. Выберите **Windows Internet Name Service** и щелкните **OK**.

   На экране появится диалоговое окно **Windows NT Setup** с приглашением ввести путь к установочным файлам Windows NT.
4. Задайте полный путь к установочным файлам Windows NT, а затем щелкните **Continue**.

   Необходимые файлы будут скопированы на Ваш компьютер, а затем снова появится диалоговое окно **Network**.
5. Щелкните **Close**.

   Вы увидите диалоговое окно **Network Settings Change.** Для вступления в силу новых параметров компьютер необходимо перезагрузить.
6. Щелкните **Yes**.
7. Войдите в систему под именем *Administrator**.

## Задание статических записей для не WINS-клиентов

Необходимо зарезервировать IP-адреса для тех клиентов DHCP, которым необходим постоянный IP-адрес.

В объединенной сети, в которой есть не WINS-клиенты, чаще всего удобнее задавать статические соответствия IP-адресов именам NetBIOS для каждого такого клиента. Это гарантирует, что имя NetBIOS не WINS-клиента будет успешно распознаваться клиентами WINS без просмотра локального файла LMHOSTS. Например, когда клиент WINS пытается выполнить команду *net use* с именем не WINS-клиента удаленной сети, IP-адрес не может быть поставлен в соответствие имени, поскольку не WINS-клиент не зарегистрировал его на сервере WINS.

▶ **Задание статических записей**

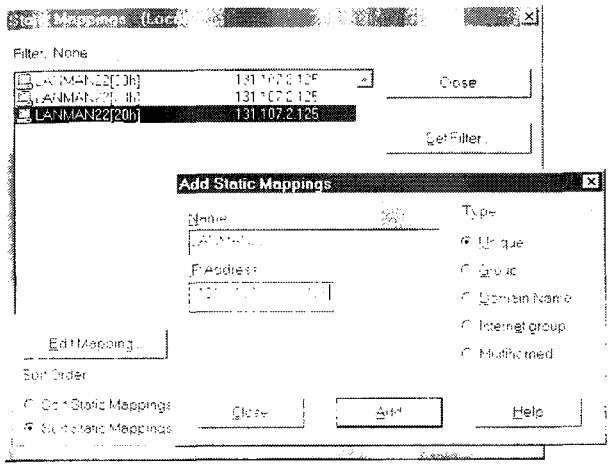
1. Щелкните кнопку **Start**, укажите на **Programs**, выберите **Administrative Tools**, а затем щелкните **WINS Manager**.
2. В меню **Mappings** щелкните **Static Mappings**.

   Появится диалоговое окно **Static Mappings**.
3. Щелкните **Add Mappings**.

   Появится диалоговое окно **Add Static Mappings**.

---

* Необходимо еще настроить компьютер, являющийся сервером имен, как WINS-клиент, то есть указать его собственный IP-адрес в поле **Primary WINS Server** конфигурации TCP/IP. — *Прим. перев.*




4. В строке **Name** укажите имя компьютера, не являющегося клиентом WINS.
5. В строке **IP Address** укажите IP-адрес этого компьютера.
6. В поле под заголовком **Type** укажите, является эта запись уникальным именем или именем группы. В таблице описаны опции **Type**.

| Тип | Описание |
|---|---|
| Unique (Уникальное) | Уникальное имя, соответствующее одному IP-адресу |
| Group (Групповое) | Иногда называется *нормальной группой* (normal group). Когда Вы при помощи WINS Manager добавляете запись в группу, Вы должны ввести имя компьютера и IP-адрес. Однако IP-адреса отдельных членов группы не хранятся в базе данных WINS, поэтому количество членов одной группы не ограничено. Для взаимодействия с членами группы применяются широковещательные пакеты |

(*продолжение*)

| Тип | Описание |
|---|---|
| Domain Name (Имя домена) | Это запись соответствия имени NetBIOS IP-адресам; в ней 16-й байт имени равен 0x1C. Группа домена может содержать до 25 IP-адресов её членов. При попытке регистрации 26-го адреса WINS заносит его на место *адреса-реплики* (replica address) — о репликации см. ниже, — а если таких адресов нет, то на место самой старой регистрации |
| Internet Group (Межсетевой группы) | Межсетевые группы определяются пользователем для объединения ресурсов, например принтеров, в целях упрощения их поиска и применения. Межсетевая группа содержит до 25 адресов своих членов. Однако динамические записи не могут заместить статические, которые добавлены при помощи WINS Manager или импортированы из файла LMHOSTS |
| Multihomed (Компьютера с несколькими сетевыми интерфейсами) | Уникальное имя, которому соответствует более одного IP-адреса. Используется для компьютеров с несколькими сетевыми интерфейсами. Каждая такая группа может содержать до 25 IP-адресов. При попытке регистрации 26-го WINS заносит его на место адреса-реплики, а если ее нет, то на место самой старой регистрации |

7. Щелкните **Add**.

   Эта запись немедленно будет добавлена в базу данных, а все строки ввода опустеют, и Вы сможете ввести очередную запись.

8. Повторите этот процесс для каждой статической записи, а затем щелкните **Close**.

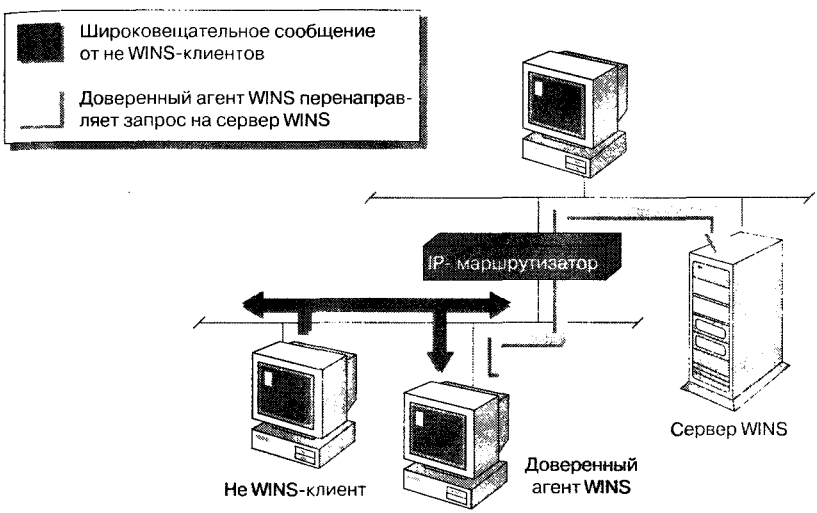
---

Внимание! Каждая статическая запись заносится в БД щелчком кнопки **Add**, но отменить ввод из этого диалогового окна нельзя. Поэтому, если Вы допустили ошибку при наборе имени или IP-адреса, необходимо вернуться в диалоговое окно **Static Mappings** и оттуда удалить эту запись.

---

## Конфигурирование доверенного агента WINS

Если в Вашей объединенной сети есть компьютеры, которые не являются клиентами WINS, они тоже смогут разрешать имена NetBIOS, используя сервер WINS, но только при помощи *доверенного агента WINS* (WINS Proxy Agent). Это средство расширяет возможности сервера WINS по разрешению имен и делает его доступным для не WINS-клиентов: широковещательные запросы о регистрации и разрешении имен прослушиваются и затем пересылаются на сервер WINS. На приведенной ниже иллюстрации показано, как доверенный агент WINS перенаправляет широковещательные сообщения к серверу WINS.




Настраивая доверенный агент WINS, Вы при помощи *редактора реестра* (Registry Editor) открываете раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters и устанавливаете значение параметра **EnableProxy** равным 1. Тип этого параметра — REG_DWORD.

### Регистрация имени NetBIOS

Когда не WINS-клиент посылает широковещательный запрос на регистрацию имени, доверенный агент WINS перенаправляет его на сервер WINS, чтобы проверить, не используется ли это имя другими клиентами WINS. Но имя NetBIOS не регистрируется, а лишь проверяется.

## Разрешение имени NetBIOS

Когда доверенный агент WINS получает *широковещательный запрос на распознавание имени* (name resolution broadcast), он сначала пытается разрешить это имя, используя кэш имен NetBIOS. Если же имени в кэше нет, посылается запрос к серверу WINS. Последний отправляет ответ, содержащий IP-адрес для запрашиваемого имени NetBIOS. Доверенный агент WINS возвращает эту информацию не WINS-клиенту.

## Требования к внедрению

Чтобы использовать WINS Proxy Agent для расширения возможностей сервера WINS необходимо следующее:

- как минимум, по одному доверенному агенту WINS на каждую подсеть, в которой имеются не WINS-клиенты. Это не обязательно, если маршрутизаторы настроены для пересылки широковещательных сообщений (включены 137 и 138 порты UDP), но рекомендуется для сокращения широковещательного трафика;
- не более двух доверенных агентов WINS на одну подсеть;
- в качестве доверенного агента WINS может выступать любой клиент WINS, но не сервер WINS.

### ▶ Настройка доверенного агента WINS

Прежде чем настраивать доверенный агент WINS, займитесь клиентом WINS.

1. Щелкните кнопку **Start**, а затем — **Run**.
2. В строке **Open** наберите *regedt32.exe* и щелкните **OK**.
   Появится окно **Registry Editor**.
3. Разверните окно **HKEY_LOCAL_MACHINE**.
4. Откройте следующий раздел реестра:
   SYSTEM\CurrentControlSet\Services\NetBT\Parameters
5. Дважды щелкните значение **EnableProxy**.
   Появится диалоговое окно **DWORD Editor**.
6. В строке **Data** введите *1*.
7. Щелкните **OK**.
8. Закройте **Registry Editor**.
9. Откройте диалоговое окно **Microsoft TCP/IP Properties**.
10. Щелкните вкладку **WINS Address**.
11. В строке **Primary WINS Server** введите IP-адрес Вашего основного сервера WINS.
12. Щелкните **OK**.
13. Щелкните **Close**.
    Появится предложение перезагрузить компьютер.

14. Щелкните **Yes**.
15. Войдите в систему под именем *Administrator*.

▶ **Удаление доверенного агента WINS**

В этом упражнении Вы удалите доверенный агент WINS.

1. Щелкните кнопку **Start**, а затем — **Run**.
2. В строке **Open** наберите *regedt32.exe* и щелкните **OK**.
   Появится окно **Registry Editor**.
3. Разверните окно **HKEY_LOCAL_MACHINE**.
4. Откройте следующий раздел реестра:
   SYSTEM\CurrentControlSet\Services\NetBT\Parameters
5. Дважды щелкните **EnableProxy**.
   Появится диалоговое окно **DWORD Editor**.
6. В строке **Data** введите *0*.
7. Щелкните **OK**.
8. Закройте **Registry Editor**.
9. Откройте диалоговое окно **Microsoft TCP/IP Properties**.
10. Щелкните вкладку **WINS Address**.
11. В поле **Primary WINS Server** удалите IP-адрес.
12. Щелкните **OK**.
13. Щелкните **Close**.
    Появится предложение о перезагрузке компьютера.
14. Щелкните **Yes**.
15. Войдите в систему под именем *Administrator*.

## Конфигурация сервера DHCP для поддержки службы WINS

Если компьютер является клиентом DHCP, поддержку WINS можно настроить через DHCP. Для этого необходимо при помощи утилиты DHCP Manager добавить и указать значения следующих опций DHCP:

- **044 WINS/NBNS Servers** — задайте IP-адреса основного и резервного серверов имен NetBIOS;
- **046 WINS/NBT Node** — задайте значение 0x8 (H-узел).

Когда клиент DHCP получает IP-адрес или продлевает его аренду, он получает и эти два параметра и, таким образом, настраивается на поддержку WINS.

---

Внимание! IP-адреса основного и резервного серверов WINS, явно заданные на локальном компьютере, имеют преимущество перед полученными при помощи DHCP.

---

## Упражнения

Здесь Вы настроите сервер DHCP так, чтобы он обеспечивал клиентов DHCP соответствующей адресной информацией о серверах WINS.

▶ **Запуск службы DHCP Server**

Примечание Выполняйте эту процедуру только на сервере DHCP.

1. Щелкните **Start**, укажите на **Settings**, а затем щелкните **Control Panel**.
2. Дважды щелкните пиктограмму **Services**.

   Появится диалоговое окно **Services**.
3. Щелкните **Microsoft DHCP Server**, а затем — **Start**.
4. Щелкните **Startup**.

   Появится диалоговое окно **Service**.
5. Щелкните **Automatic**, а затем — **OK**.
6. Щелкните **Close**.
7. Закройте **Control Panel**.

▶ **Настройка сервера DHCP для автоматической передачи IP-адресов серверов WINS**

В этом задании Вы настроите сервер DHCP так, чтобы он автоматически назначал клиентам DHCP адреса серверов WINS и тип узла NetBIOS.

Примечание Выполняйте эту процедуру только на сервере DHCP.

1. Щелкните кнопку **Start**, укажите **Programs**, выберите **Administrative Tools**, а затем щелкните **DHCP Manager**.

   Появится окно **DHCP Manager**.
2. Дважды щелкните ***Local Machine***.

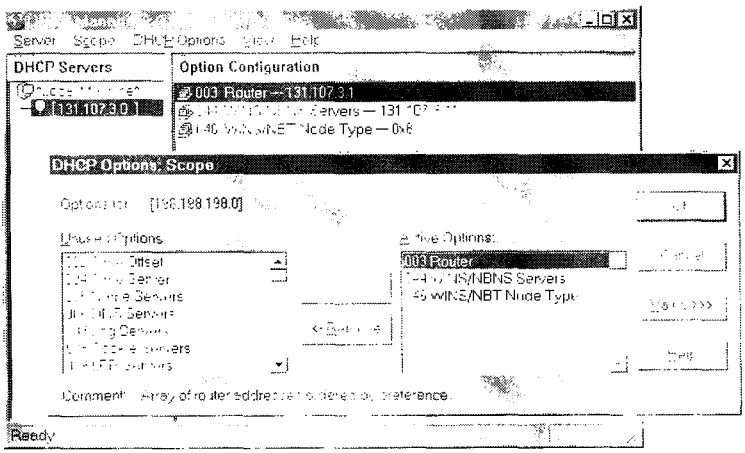
   Появится IP-адрес локальной области видимости.
3. Щелкните IP-адрес локальной области видимости.

   В окне **Option Configuration** появятся параметры локальной области видимости.
4. В меню **DHCP Options** щелкните **Scope**.

   Появится диалоговое окно **DHCP Options: Scope**.
5. В окне **Unused Options** выберите **044 WINS/NBNS Servers**, а затем щелкните **Add**.

   Появится окно **DHCP Manager** с сообщением о том, что для нормальной работы WINS Вы должны добавить параметр **046 WINS/NBT Node Type**.

6. Щелкните **OK**.
   Параметр **044 WINS/NBT Node Type** переместится в поле **Active Options**.
7. Щелкните **Value**.
   Раскроется окно **DHCP Scope: Options**.
8. Щелкните **Edit Array**.
   Появится диалоговое окно **IP Address Array Editor**.
9. В окне **New IP Address** введите IP-адрес Вашего сервера и щелкните **OK**.
   Новый IP-адрес появится в окне **IP Addresses**.
10. Чтобы вернуться в диалоговое окно **DHCP Options: Scope**, щелкните **OK**.
11. В окне **Unused Options** выберите **046 WINS/NBT Node Type**, а затем щелкните **Add**.




   Параметр **046 WINS/NBT Node Type** переместится в окно **Active Options** и появится строка ввода **Byte**.
12. В строке **Byte** введите *0x8*, а затем щелкните **OK**.
    Опять появится окно **DHCP Manager**, но уже с заданными параметрами области видимости для **003 Router**, **044 WINS/NBNS Servers** и **046 WINS/NBT Node Type**, перечисленными в поле **Option Configuration**.
13. Выйдите из DHCP Manager.

### ▶ Модификация клиента DHCP

Вы обновите аренду адреса клиентом DHCP, в результате он автоматически получит от сервера новые адреса серверов WINS и тип узла.

---

Примечание Выполняйте эти действия только на клиенте DHCP.

---

1. В командной строке введите *ipconfig /all* и нажмите ENTER.

   Вы увидите параметры **Windows IP Configuration**. Значение параметра **Node Type** — **broadcast**, а адрес основного сервера WINS не задан.
2. Переключитесь в диалоговое окно **Microsoft TCP/IP Properties**.
3. Щелкните **Obtain an IP address from a DHCP Server** .

   Появится окно подтверждения установки службы DHCP.
4. Щелкните **Yes**.
5. Два раза щелкните **OK**.
6. В командной строке введите *ipconfig /all* и нажмите ENTER.

   Вы увидите параметры **Windows IP Configuration**. Значения параметров **Node Type** и **primary WINS server** обновлены.

► **Использование службы WINS для разрешения имен**

В этом задании Вы используете службу WINS для разрешения имен NetBIOS. Однако разрешение будет ограничено локальной подсетью, поскольку удаленные узлы не зарегистрированы в базе данных локального сервера WINS.

1. Убедитесь что кэш имен NetBIOS пуст. Для этого в командной строке наберите *nbtstat -c* и нажмите ENTER.
2. Если появятся какие-нибудь записи, то очистите кэш имен NetBIOS. Для этого наберите *nbtstat -R* и нажмите ENTER.
3. Запустите Windows NT Explorer и попытайтесь соединиться с другим компьютером в локальной сети.

   Была ли попытка успешной?

   _____

   Установится ли соединение с удаленным узлом?

   _____

## Резюме

Чтобы установить и использовать WINS, необходимо настроить сервер и клиент. Задание статических записей для не WINS-клиентов позволит удаленным клиентам WINS взаимодействовать с ними. Для разрешения имени NetBIOS, запрошенного не WINS-клиентом, доверенный агент WINS просматривает свой кэш имен. Если имя не распознается таким образом, запрос пересылается к серверу WINS. Как минимум один, а максимум — два доверенных агента WINS необходимы для каждой подсети, в которой есть не WINS-клиенты.

# Занятие 4. Репликация базы данных между серверами WINS

Все серверы WINS в объединенной сети можно настроить так, чтобы они всегда *тиражировали* (replicate) на другие серверы записи из своей базы данных. Это гарантирует, что имя, зарегистрированное на одном сервере WINS, будет продублировано на всех остальных. На этом занятии объясняется, каким образом база данных одного сервера WINS тиражируется на других серверах WINS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, когда необходимо настроить сервер WINS в качестве передающего или принимающего партнера;
- ✓ настроить сервер WINS для репликации базы данных.

**Продолжительность занятия — 40 минут**

Репликация базы данных происходит при любом ее изменении, в том числе при освобождении имени. Дублирование баз данных позволяет серверу WINS распознавать NetBIOS-имена узлов, зарегистрированных на других серверах WINS. Например, если узел из подсети 1, зарегистрированный на сервере WINS той же подсети, пытается взаимодействовать с узлом из подсети 2, зарегистрированным на другом сервере WINS, имя NetBIOS не будет разрешено до тех пор, пока оба сервера WINS не продублируют друг другу свои базы данных.

Чтобы обмениваться записями базы данных, каждый из серверов WINS должен быть настроен как передающий или принимающий партнер хотя бы для одного сервера WINS. *Передающий партнер* (push partner) — это сервер WINS, который при изменении записей в его базе данных посылает своим принимающим партнерам сообщения с уведомлениями. Когда принимающие партнеры сервера WINS отвечают на уведомления, сервер WINS посылает им *копии новых записей* (replicas) своей базы данных.

*Принимающий партнер* (pull partner) — это сервер WINS, который запрашивает копии элементов базы данных у своих передающих партнеров. Он запрашивает и получает версии записей более поздние, чем полученные во время последней репликации.

---

Примечание Серверы WINS тиражируют только обновленные записи своих баз данных. Целиком база данных при репликации не копируется.

---

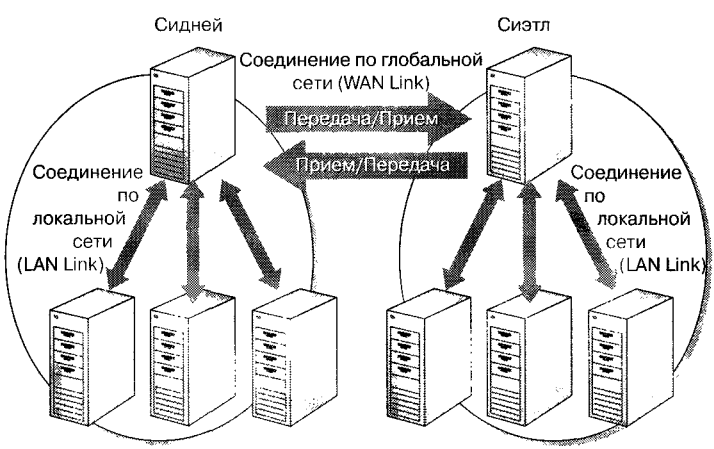
## Настройка передающего или принимающего сервера WINS

Выбор того, каким партнером по репликации (передающим или принимающим) будет сервер WINS, зависит от Вашего сетевого окружения. Выбирая способ репликации, придерживайтесь следующих правил:

- сделайте сервер WINS передающим партнером, если серверы связаны высокоскоростными соединениями, поскольку передача происходит всегда при обновлении заданного числа записей;
- сделайте принимающими партнерами удаленные узлы, если они связаны низкоскоростными линиями, поскольку прием можно настроить так, чтобы он происходил через заданные промежутки времени;
- чтобы полностью синхронизировать БД двух серверов, настройте их в качестве принимающего и передающего партнеров друг для друга*.

Эти правила мы применим далее в примере и иллюстрации.

- Предположим, в Сиднее и Сиэтле все серверы WINS всех узлов передают обновленные записи своих баз данных на один узел в своем городе.
- Эти выделенные серверы настроены как принимающие партнеры друг друга, поскольку линия связи, соединяющая их, относительно медленная. Репликация между ними может происходить, когда линия связи наименее загружена, например ночью.




* В конфигурации TCP/IP каждого сервера имен, участвующего в репликации оба поля адреса WINS-сервера, **Primary WINS Server** и **Secondary WINS Server**, должны содержать собственный IP-адрес. – *Прим. перев.*

Примечание Настройка сервера WINS в качестве передающего или принимающего партнера осуществляется при помощи программы WINS Administration tool.

## Настройка репликации базы данных

Репликация базы данных подразумевает, что, как минимум, один компьютер является передающим партнером и один — принимающим*.

Вот четыре возможных условия начала репликации базы данных.

1. При запуске системы: с того момента, как настроены партнеры по репликации, при каждом запуске сервера WINS осуществляется автоматическое обновление базы данных. Сервер WINS можно настроить так, чтобы при каждом запуске он информировал приемники об изменениях в своей базе данных.
2. Через заданные промежутки времени, например, через каждые 5 ч.
3. Когда количество регистраций и изменений в базе данных WINS достигает заданного предела: сервер WINS информирует всех своих принимающих партнеров, и они запрашивают обновленные записи.
4. Принудительное начало репликации из диалогового окна **WINS Manager Replication Partners**.

### Упражнения

В этих заданиях Вы настроите сервер WINS для репликации базы данных с другим сервером WINS.

Примечание Чтобы выполнить эти задания, настройте второй компьютер (Server2) как сервер WINS. Для этого выполните задание по установке службы WINS Server.

▶ **Настройка партнеров по репликации**

В этом задании Вы настроите второй компьютер (сервер WINS) как партнера по репликации.

1. В окне **WINS Manager** выберите меню **Server**, а потом щелкните **Replication Partners**.

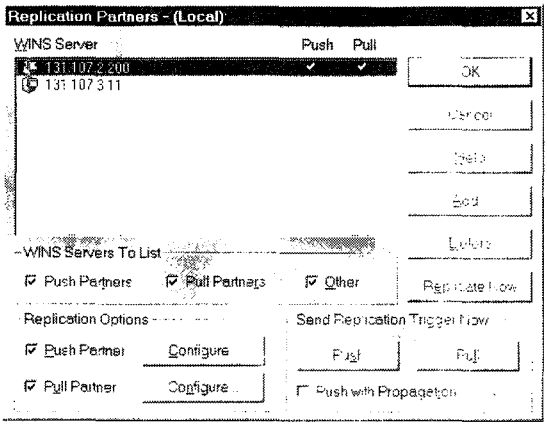
   Появится диалоговое окно **Replication Partners**.

2. Щелкните **Add**.

   Вы увидите диалоговое окно **Add WINS Server**.

* Еще возможны конфигурации, когда оба партнера настроены как передающие или как принимающие. В обоих случаях тиражирование происходит в обе стороны, но в первом каждый сам сообщает об изменениях, а во втором репликация происходит только по расписанию. — *Прим. перев.*

3. В строке **WINS Server** введите *131.107.2.200*, а затем щелкните **OK**. Появится диалоговое окно **Replication Partners**, в котором введенный IP-адрес добавлен к списку серверов WINS.




Внимание! На этом компьютере Вы должны указать основной сервер WINS в качестве партнера по репликации.

4. В списке **WINS Server** щелкните Ваш IP-адрес.
5. В группе **Replication Options** щелкните кнопку **Configure**, расположенную рядом с **Pull Partner**.

   Вы увидите диалоговое окно **Pull Partner Properties**.

   Установленный интервал репликации — 30 минут.

Примечание Для передающего партнера в строке **Update Count** задайте число обновлений записей базы данных, по достижении которого сервер WINS уведомит принимающих партнеров. Конкретное значение зависит от количества регистраций, поддерживаемых сервером. Сервер WINS, который получает сотни запросов о регистрации при подключении пользователей к сети, должен быть настроен для репликации большого числа обновлений.

Также Вы можете установить флажок **Push with Propagation**. Это заставит выбранные серверы WINS запрашивать все новые записи базы данных у сервера WINS, пославшего это сообщение. То есть, когда выбранный сервер получит какие-либо новые записи, он в свою очередь объявит о появлении изменений всем своим принимающим партнерам. Если выбранный сервер WINS не получает ни одной новой записи, он не распространяет сообщение об изменениях.

6. Щелкните **OK**.

▶ **Принудительная репликация**

В этом задании Вы заставите WINS тиражировать базу данных на другой сервер WINS.

1. В диалоговом окне **Replication Partners** щелкните **Replicate Now**.
   Появится сообщение **WINS Manager** о получении запроса репликации.
2. Щелкните **OK**.
3. Щелкните **OK**, чтобы вернуться в окно **WINS Manager**.
   Вы увидите окно **WINS Manager**, где IP-адрес указан как WINS-сервер.
4. В списке **WINS Server** выберите локальный сервер WINS.
5. В меню **Mappings** щелкните **Show Database**.
   Появится окно **Show Database**. Убедитесь, что в список **Select Owner** добавлены имена всех серверов, известных партнеру по репликации.

---

Примечание Если *номер версии* (version ID) тиражируемой БД равен 0, повторите пункты 1—3, чтобы произвести репликацию снова.

---

6. В списке **Select Owner** выберите Ваш IP-адрес.
   В списке **Mappings** Вы увидите список имен зарегистрированных на сервере WINS.
7. Просмотрите информацию в базах данных других серверов, а затем щелкните **Close**, чтобы вернуться в **WINS Manager**.

## Автоматические партнеры репликации WINS

Если Ваша сеть поддерживает групповую адресацию, сервер WINS можно настроить на автоматический поиск других серверов WINS в сети путем регулярной посылки групповых сообщений на IP-адрес 224.0.1.24. Тогда любой найденный в сети сервер WINS будет автоматически настроен как принимающий и передающий партнер репликации, а интервал *репликации приема* (pull replication) будет установлен равным двум часам. В этом случае, при нормальном выключении одного из компьютеров, он исключается из списка партнеров. Если сетевые маршрутизаторы не поддерживают групповую адресацию, данный сервер WINS сможет обнаружить только серверы WINS той же подсети.

По умолчанию автоматическое взаимодействие между серверами WINS отключено. Для ручного отключения этой функции используйте редактор реестра, чтобы установить значение параметра **UseSelfFndPnrs** равным 0, а значение **McastIntvl** — достаточно большим*.

---

* Для ручного включения этой функции используйте редактор реестра, чтобы установить значение параметра **UseSelfFndPnrs** равным 1, а значение **McastIntvl** — не меньше 2 400 секунд (то есть 40 минут — значение по умолчанию). — *Прим. перев.*

## Резюме

Все серверы WINS в одной сети можно настроить для обмена информацией друг с другом, чтобы имя, зарегистрированное на одном из них, стало известно другим. Принимающий партнер репликации сам запрашивает об обновлении базы данных WINS, передающий же информирует своих принимающих партнеров о том, что в базе данных WINS произошли изменения.

# Занятие 5. Поддержка базы данных сервера WINS

На этом занятии Вы научитесь просматривать базу данных и искать интересующие Вас записи. Вы также подробно познакомитесь с методами резервного копирования и восстановления базы данных WINS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ настроить сервер WINS для автоматического удаления устаревших записей из базы данных;
- ✓ делать резервную копию и восстанавливать базу данных WINS;
- ✓ применять утилиту Jetpack для сжатия базы данных WINS.

**Продолжительность занятия — 40 минут**

Утилита WINS Manager позволяет просматривать содержимое базы данных WINS и искать заданные записи.

## Упражнения

В этом задании Вы просмотрите все соответствия имен NetBIOS и IP-адресов, которые зарегистрированы в базе данных WINS.

Примечание Выполняйте это задание только на сервере WINS.

▶ **Запуск WINS Manager**

1. В командной строке наберите *nbtstat -R* для очистки кэша имен NetBIOS (*-R* следует набирать прописными буквами).

   Это гарантирует, что перед использованием сервиса WINS все записи из кэша имен NetBIOS будут удалены.
2. В **Control Panel** дважды щелкните пиктограмму **Services**.

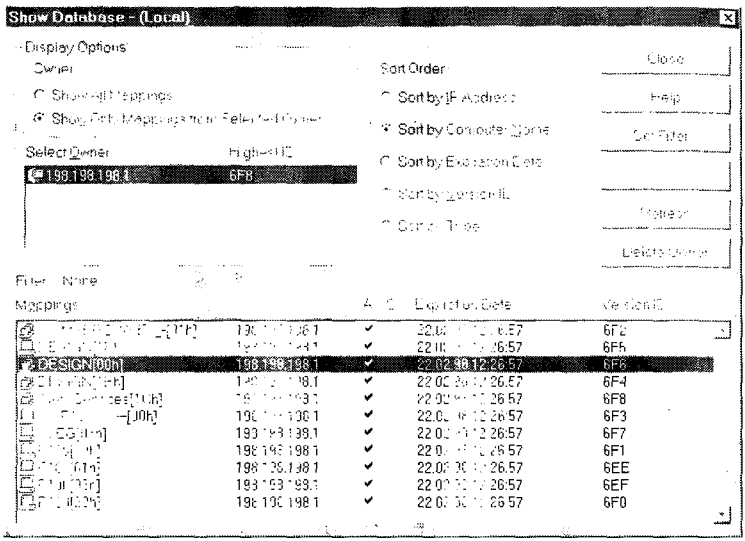
   Появится диалоговое окно **Services**.
3. Просмотрите список служб, чтобы убедиться, что сервис WINS работает.
4. Закройте диалоговое окно **Services**.
5. Щелкните кнопку **Start**, выделите **Programs**, затем укажите **Administrative Tools** и щелкните **WINS Manager**.

   Появится окно **WINS Manager**.

▶ **Просмотр содержимого базы данных WINS**

1. В меню **Mappings** окна **WINS Manager** щелкните **Show Database**.

Появится диалоговое окно **Show Database,** в котором показаны все имена NetBIOS, зарегистрированные в службе WINS.




2. Чтобы просмотреть имена, зарегистрированные на другом сервере WINS, выберите **Show Only Mappings from Selected Owner**, а затем в списке **Select Owner** выделите тот сервер WINS, который Вы хотите просмотреть.
3. С помощью опции **Sort Order** выберите необходимый Вам тип сортировки — по IP-адресам, именам компьютеров, времени отображения, номеру версии или типу.
4. Если Вы хотите просмотреть диапазон записей, щелкните **Set Filter** и укажите IP-адреса или имена NetBIOS.
5. Просмотрите данные в списке **Mappings**. Их элементы описаны в приведенной ниже таблице.

| Элемент | Описание |
|---|---|
|  | Показывает, что запись является уникальным именем |
|  | Представляет группу, межсетевую группу или компьютер с несколькими сетевыми интерфейсами |
| Имя | Зарегистрированное имя NetBIOS |

(*продолжение*)

| Элемент | Описание |
|---|---|
| IP-адрес | IP-адрес, который соответствует зарегистрированному имени |
| A либо S | Показывает, является запись динамической (A) или статической (S). Если в колонке A стоит крестик, значит, имя не является активным и скоро будет удалено из базы данных |
| Дата окончания срока (Expiration Date) | Показывает, когда закончится срок действия записи. При репликации записи дата окончания ее срока устанавливается равной текущему времени на принимающем сервере WINS плюс время обновления имен |
| Номер версии (Version ID) | Уникальное шестнадцатеричное число, присвоенное сервером WINS при регистрации имени. Оно используется принимающим партнером при репликации для определения обновленных записей |

6. Какие NetBIOS-имена клиент регистрирует на сервере WINS?

7. Как долго существуют такие имена?

8. Есть ли записи для удаленных узлов на сервере WINS?

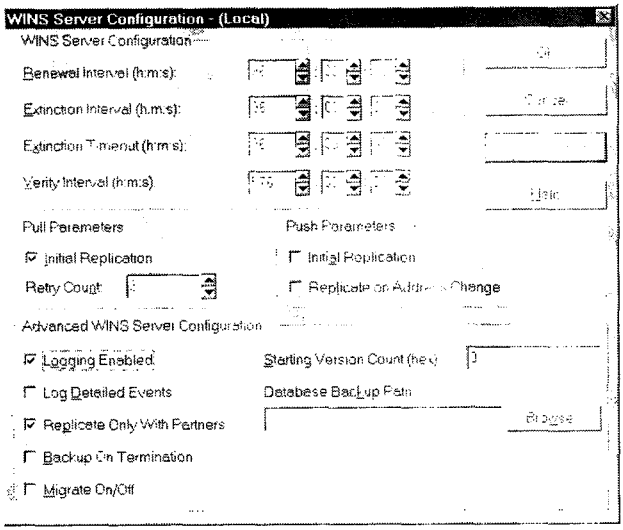
9. Чтобы удалить сервер WINS и все записи в базе данных, которыми он владеет, выделите его в списке **Select Owner** и щелкните **Delete Owner**.
10. Щелкните **Close**.

## Настройка сервера WINS

Базу данных каждого сервера WINS необходимо периодически очищать от записей, которые были освобождены или перерегистрированы на другом сервере WINS, но не были удалены. Эту процедуру выполняют вручную, выбрав **Initiate Scavenging** в меню **Mappings**. Администратор WINS может настроить сервер на автоматическую *очистку* (clean up) через определенные промежутки времени.

► **Определение времени пребывания имен NetBIOS в различных состояниях**

1. В меню **Server** окна WINS Manager щелкните **Configuration**. Появится диалоговое окно **WINS Server Configuration**.




2. Чтобы увидеть все параметры в этом окне, щелкните **Advanced**.
3. В группе **WINS Server Configuration** задайте каждый из перечисленных интервалов времени.

| Интервал | Описание |
|---|---|
| Интервал обновления (Renewal Interval) | Как часто клиент WINS должен обновлять регистрацию своего имени на сервере WINS. Значение по умолчанию — 144 часа |
| Время до исчезновения (Extinction Interval) | Время до момента, когда имя, помеченное как *освобожденное* (released), — оно более не является зарегистрированным — пометят как *исчезнувшее* (extinct). Значение по умолчанию — 144 часа |
| Время до удаления (Extinction timeout) | Время до момента, когда имя, помеченное как *исчезнувшее,* будет физически удалено из базы данных. Значение по умолчанию равно интервалу обновления, но не может быть меньше 24 часов |

(*продолжение*)

| Интервал | Описание |
|---|---|
| Время проверки (Verify Interval) | Время, по истечении которого сервер WINS проверяет активность имен, *не* принадлежащих ему (они получены с другого сервера WINS). Значение по умолчанию — 576 часов (24 дня). Это минимальное значение, принимаемое WINS Manager |

Примечание Значения по умолчанию, приведенные в этой таблице, являются корректными. Ваша версия документации или Справка (Help) могут содержать неверные значения по умолчанию для интервала обновления и времени до исчезновения.

Сервер WINS при каждом запуске компьютера запрашивает у своих партнеров по репликации сведения об обновлении базы данных, поскольку по умолчанию флажок **Initial Replication** в группе **Pull Parameters** отмечен.

4. Чтобы сервер при каждом запуске компьютера сообщал партнерам по репликации о состоянии своей базы данных, отметьте флажок **Initial Replication** в группе **Push Parameters**.
5. Когда закончите, нажмите **OK**.

Примечание В комплект *Microsoft Windows NT Server Resource Kit* входит утилита Winscl.exe, которая позволит Вам удалять отдельные динамические записи из базы данных WINS.

## Дополнительные параметры настройки

Приведенные в таблице параметры определяют поведение партнеров по репликации при запуске системы и позволяют дополнительно конфигурировать эту систему.

| Дополнительный параметр | Описание |
|---|---|
| Logging enabled (Запись журнала изменений) | Задает включение журнала всех изменений базы данных |
| Log Detailed Events (Подробное описание событий) | Задает ведение подробного журнала. Для увеличения производительности рекомендуется отключать |
| Replicate Only With Partners (Проводить репликацию только с партнерами) | Задает ведение репликации только с зарегистрированными партнерами. По умолчанию — включено |

(*продолжение*)

| Дополнительный параметр | Описание |
|---|---|
| Backup On Termination (Создавать резервную копию при остановке) | Задает автоматическое резервное копирование базы данных при выходе из WINS Manager |
| Migrate On/Off (Переход на другую платформу) | Если опция включена (On), то при конфликтах с новыми регистрациями или репликами статические записи для уникальных имен или имен с несколькими сетевыми интерфейсами рассматриваются как динамические. Это означает, что, если такая запись устарела, она будет перезаписана новой регистрацией или репликой. Включите этот параметр, если Вы переходите на платформу Windows NT с другой платформы |
| Starting Version Count (Начальный номер версии) | Задает наибольшее значение номера версии. Не стоит изменять это значение, если Ваша БД не повреждена или не требует восстановления |
| Database backup path (Путь для резервного копирования) | Задает каталог, в котором сохраняются резервные копии БД WINS. Этот каталог также используется при автоматическом восстановлении базы данных. Не задавайте здесь сетевой каталог |

## Резервное копирование и восстановление базы данных

Резервное копирование базы данных WINS очень важно. Оно позволит восстановить данные при сбое системы или повреждении данных. Когда Вы зададите каталог для резервного копирования, база данных WINS будет автоматически копироваться в него каждые 24 часа.

▶ **Задание каталога для резервного копирования**

1. В **WINS Manager** откройте меню **Mappings**, щелкните **Back Up Database**. Появится диалоговое окно **Select Backup Directory**.
2. Укажите место для сохранения резервных файлов.
3. Щелкните **OK**.

## Резервное копирование записей реестра WINS

Рекомендуется периодически проводить резервное копирование записей реестра, относящихся к службе WINS.

▶ **Создание резервной копии записей реестра WINS**

1. При помощи Registry Editor откройте раздел HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WINS
2. В меню **Registry** щелкните **Save Key**.
3. В диалоговом окне **Save Key** укажите каталог, в котором Вы сохраняете резервные файлы базы данных WINS.

## Восстановление поврежденной базы данных WINS

В случае повреждения базы данных WINS используйте один из следующих методов для восстановления ее содержимого:

- остановите и перезапустите службу WINS Server, если служба обнаружит повреждение в базе данных, она автоматически восстановит данные с резервной копии;
- в WINS Manager откройте меню **Mappings**, щелкните **Restore Database**.

Затем укажите каталог, в котором хранится резервная копия. База данных будет восстановлена с резервной копии.

## Файлы базы данных WINS

Перечисленные в таблице файлы расположены в каталоге *\systemroot* \System32\Wins.

| Имя файла | Описание |
|---|---|
| Wins.mdb | Файл базы данных |
| Winstmp.mdb | Временный файл, который создается при установке сервера WINS. Он может остаться в каталоге \Wins после программного или аппаратного сбоя |
| J50.log | Журнал всех транзакций, произведенных с базой данных. Этот файл при необходимости используется службой WINS для восстановления данных |
| J50.chk | Файл контрольной точки |

Внимание! Поскольку эти файлы необходимы для поддержки базы данных WINS, не изменяйте и не переносите их, за исключением случая ручного восстановления поврежденной базы данных WINS.

## Сжатие базы данных WINS

Поскольку Windows NT Server 4.0 может автоматически сжимать базу данных WINS, Вам не нужно вручную выполнять эти действия. Однако при необходимости Вы можете использовать утилиту Jetpack, поставляемую совместно с Windows NT Server, чтобы сжать базу данных WINS.

▶ **Сжатие базы данных WINS**

1. Остановите работу службы WINS Server при помощи **Control Panel**, **Services**, **Windows Internet Name Service** или из командной строки. В командной строке нужно ввести:

   ```
   net stop wins
   ```

2. Из каталога *systemroot*\System32\Wins запустите утилиту Jetpack при помощи команды (вместо *temporary_name* укажите любое имя файла):

   jetpack wins.mdb *temporary_name*.mdb

   Содержимое Wins.mdb будет сжато и записано в файл *temporary_name*, затем этот временный файл будет скопирован в файл с именем Wins.mdb. После этого временный файл удаляется.

3. Средствами **Control Panel**, **Services**, **Windows Internet Name Service** или из командной строки перезапустите службу сервера WINS. В командной строке необходимо ввести:

   ```
   net start wins
   ```

## Резюме

Средствами WINS Manager Вы сумеете просмотреть базу данных WINS или отыскать конкретные записи. Вы можете вручную удалить устаревшие записи или настроить сервер WINS на их автоматическое удаление. В Windows NT Server 4.0 включены инструменты для автоматического сжатия базы данных WINS.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Каковы основные преимущества службы WINS?

   _____

   _____

2. Какими двумя способами можно установить поддержку WINS на клиентском компьютере?

3. Сколько серверов WINS необходимо в сети, состоящей из 12 подсетей?

4. Какими способами не WINS-клиенты могут разрешать имена NetBIOS?

5. Когда необходимо использовать доверенный агент WINS?

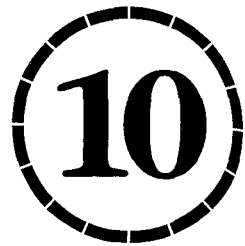
6. Как часто происходит резервное копирование базы данных WINS после установки WINS с параметрами по умолчанию?

7. Какие типы имен хранятся в базе данных WINS?

8. Как надо настроить репликацию WINS в глобальной сети с низкоскоростной связью и ограниченной полосой пропускания?

9. Как надо настроить репликацию WINS в локальной сети, не перегружая сетевой трафик?

10. Когда служба WINS использует групповую адресацию?



# Просмотр сетевых ресурсов и функции доменов



## В этой главе

В предыдущих главах обсуждалось распознавание имён NetBIOS при помощи файла LMHOSTS и сервиса WINS. В этой главе описан механизм просмотра NetBIOS-ресурсов в объединенной сети, применяющей протокол TCP/IP. Вы узнаете о просмотре ресурсов NetBIOS, регистрации в домене, изменении пароля для учетной записи пользователя и синхронизации доменов. Выполняя упражнения этой главы, Вы приобретете практические навыки настройки файла LMHOSTS для обзора сети и работы домена.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить Microsoft Windows NT Server 4.0 и протокол TCP/IP;
- изучить главу 8, «NetBIOS поверх TCP/IP».

# Занятие 1. Общие сведения

Чтобы эффективно работать с сетевыми ресурсами, пользователи должны уметь определять их доступность. В Windows NT для этого существует сервис Computer Browser, который поддерживает списки всех доступных в данный момент ресурсов. Здесь подробно рассматривается его работа.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать работу сервиса обзора компьютеров Windows NT: сбор и распределение информации, а также обработку клиентских запросов.

**Продолжительность занятия — 15 минут**

Сервис Computer Browser поддерживает совокупность списков, хранящих имена доступных ресурсов сети, или *списки просмотра* (browse lists). Они распределены между специально выделенными компьютерами, которые от имени клиентов выполняют обзор ресурсов.

Компьютеры, называемые *броузерами* (browsers), избавляют остальные компьютеры от необходимости создавать и обновлять список всех совместно используемых сетевых ресурсов. Назначая компьютеры на роль броузеров, сервис Computer Browser сокращает сетевой трафик, необходимый для построения и обновления списков ресурсов.

Броузеры различаются по типам — в соответствии с решаемыми задачами.

| Роль компьютера | Описание |
|---|---|
| Главный броузер (Master browser) | Компьютер, который создает и обновляет главный список доступных серверов своего домена или рабочей группы и список остальных доменов и рабочих групп. Он также распределяет этот список, называемый списком просмотра, между резервными броузерами |
| Резервный броузер (Backup browser) | Компьютер, который получает от главного броузера копию списка просмотра. Затем он передает этот список *клиентам просмотра* (browse clients) при поступлении от них соответствующих запросов |

*(продолжение)*

| Роль компьютера | Описание |
|---|---|
| Главный броузер домена (Domain master browser) | Кроме функций главного броузера выполняет дополнительные. Если в удаленных сетях несколько главных броузеров, то главный броузер домена синхронизирует списки просмотра всех главных броузеров в пределах данного домена |

Функции главного или резервного броузера могут выполнять компьютеры, работающие под управлением ОС Windows NT Workstation, Windows NT Server, Windows for Workgroups или Windows 95. Но на роль главного броузера домена может быть назначен только компьютер под управлением Windows NT Server, являющийся *главным контроллером домена* (primary domain controller, PDC).

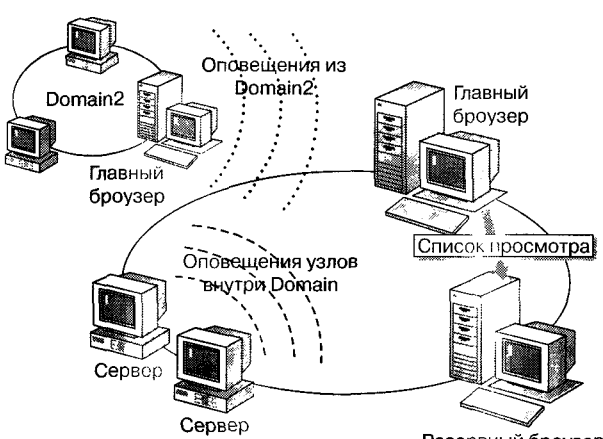
## Сбор и распределение информации

Работу служб обзора в Windows NT можно описать в терминах трех ключевых процессов:

- сбора информации о просмотре;
- распределения информации о просмотре;
- обслуживания клиентских запросов.

### Сбор информации

Осуществляется главным броузером. Этот процесс происходит непрерывно, а информация сохраняется в главном списке просмотра, куда включены списки всех серверов внутри данного домена и список остальных доменов и рабочих групп.



### Распределение информации

В процессе распределения информации о просмотре списки, составленные при сборе информации, передаются компьютерам, которые будут обрабатывать запросы клиентов. Этот процесс выполняется в двух случаях.

- При оповещении, отправляемом с главного броузера.

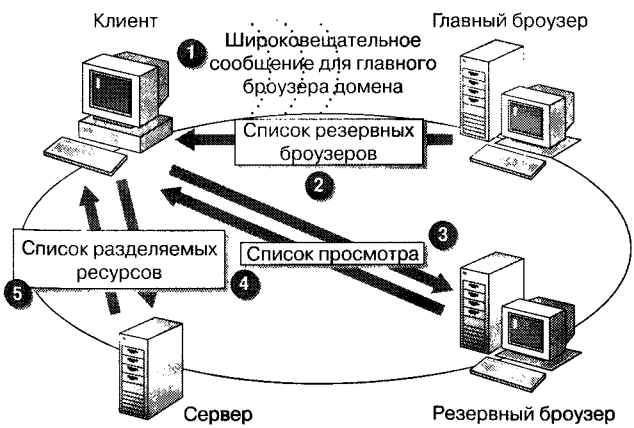
  Периодически главный броузер посылает широковещательный пакет оповещения, который информирует резервные броузеры о том, что главный ещё существует. Если же главный броузер не сделает этого в заданное время, то начнутся выборы нового главного броузера.
- При передаче списка просмотра от главного к резервному броузеру.

  Периодически каждый резервный броузер соединяется с главным броузером в своем домене и принимает от него список просмотра.

## Обслуживание клиентских запросов просмотра

С того момента, как список просмотра создан главным броузером и разослан резервным броузерам, все готово для обслуживания *клиентских запросов* (browsing requests).

1. Когда клиент пытается при помощи Windows NT Explorer получить доступ к домену или рабочей группе, он соединяется с главным броузером в этом домене или рабочей группе.
2. Главный броузер отправляет клиенту список, содержащий имена трех резервных броузеров.
3. После этого клиент запрашивает у резервного броузера список сетевых ресурсов.
4. Резервный броузер отсылает клиенту список серверов своего домена или рабочей группы.
5. Клиент выбирает сервер и получает его список доступных ресурсов.



## Резюме

Сервис Computer Browser в ОС Windows NT позволляет просматривать ресурсы сети. Типы броузеров различаются в соответствии с их ролями. Главный броузер постоянно поддерживает список всех серверов своего домена и список всех остальных доменов. Из них составляется список просмотра. С того момента, как список просмотра будет составлен и распределен между резервными броузерами, все готово для обслуживания клиентских запросов.

# Занятие 2. Просмотр ресурсов объединенной IP-сети

Для получения списка сетевых ресурсов сервис Computer Browser применяет механизм широковещания. На этом занятии обсуждаются проблемы, связанные с просмотром ресурсов корпоративной IP-сети.

**Изучив материал этого занятия, Вы сможете:**

- описать проблемы, связанные с просмотром ресурсов корпоративной IP-сети, и их возможные способы решения.

**Продолжительность занятия — 15 минут**

Поскольку широковещательные сообщения NetBIOS не маршрутизируются, то для обзора сети и работы домена в нескольких подсетях узлы необходимо настроить так, чтобы они использовали WINS или файл LMHOSTS. Однако это не нужно, если Ваш маршрутизатор может перенаправлять широковещательные пакеты NetBIOS.

Сервис Computer Browser использует серии широковещательных пакетов. При попытке обзора сети через IP-маршрутизаторы, которые не пересылают широковещательные пакеты, могут возникнуть некоторые проблемы. Чтобы обеспечить клиенту обзор всех сетевых ресурсов, в корпоративной IP-сети должны существовать механизмы для сбора и распределения списков просмотра, а также для обслуживания клиентских запросов на них.

## Просмотр с использованием IP-маршрутизатора

Некоторые маршрутизаторы можно настроить так, чтобы они пересылали широковещательные сообщения из одной IP-подсети в другую. Если IP-маршрутизатор пересылает эти сообщения, то сервис обзора сети работает как обычно, — как будто все домены и рабочие группы находятся в одной подсети. Главные броузеры знают обо всех серверах своего домена или рабочей группы, а также обо всех существующих доменах и рабочих группах. Поэтому все клиентские запросы просмотра могут быть удовлетворены.

Если этот режим включен на всех IP-маршрутизаторах Вашей объединенной сети (и сеть нормально функционирует – *прим. перев.*), то последующая информация для Вас несущественна. Однако пересылать широковещательные пакеты не рекомендуется, поскольку при этом весь широковещательный трафик протокола NetBIOS поверх TCP/IP распространяется по всей объединенной сети. А это снижает производительность всех узлов сети. Кроме того, пересылка широковещательных сообщений

может вызвать конфликты при выборах главного броузера — о них свидетельствуют записи об ошибках в журнале регистрации системных событий.

## Просмотр с использованием Windows NT

Обычно IP-маршрутизаторы не настроены для перенаправления широковещательных запросов NetBIOS. Это означает, что сбор и распределение информации и обслуживание клиентских запросов должны происходить на основе *направленного*, а не широковещательного IP-трафика. В Windows NT это осуществляется двумя способами.

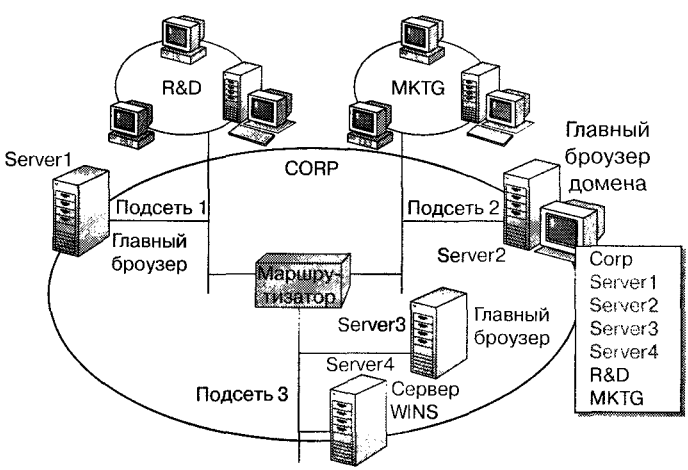
- Сервис WINS используют для сбора списков просмотра и обслуживания клиентских запросов.
- Записи в файле LMHOSTS обеспечивают распределение информации и обслуживание клиентских запросов.

## Обзор сети при помощи WINS

Сервис WINS решает проблемы широковещания путем динамической регистрации NetBIOS-имени компьютера и его IP-адреса и сохранения их в БД WINS. Когда клиент WINS взаимодействует с узлом TCP/IP через подсети, IP-адрес узла назначения может быть получен из базы данных без использования широковещания.

Сервис WINS улучшает механизм сбора имен доменов и рабочих групп, позволяя главному броузеру домена — клиенту WINS — периодически опрашивать сервер WINS и получать от него список всех доменов, зарегистрированных в базе данных WINS.

Преимущество WINS заключается в том, что главный броузер домена имеет полный список всех доменов, включая те, которые находятся в удаленных подсетях и не являются частью данного домена.

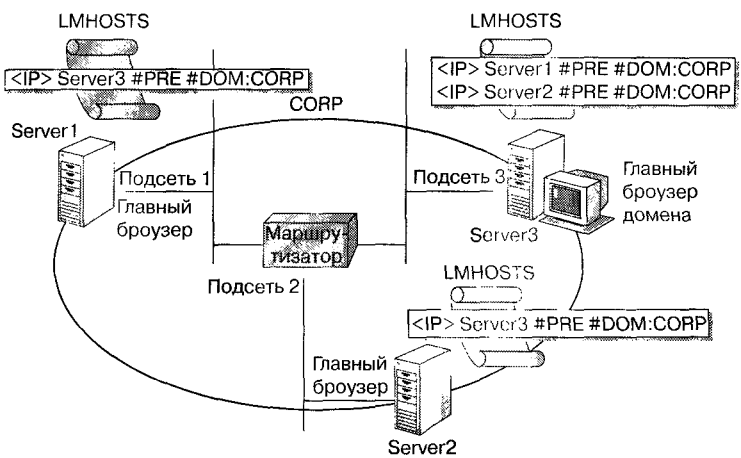


Примечание Список доменов, полученный от сервера WINS, содержит только имена доменов и соответствующие им IP-адреса, но не имена главных броузеров, которые объявили эти домены.

## Обзор сети с использованием файла LMHOSTS

Чтобы не WINS-клиенты, применяющие для регистрации имен широковещание, могли использовать прямые соединения между подсетями, им необходим файл LMHOSTS. В нем должны быть записаны IP-адреса и NetBIOS-имена контроллеров доменов, расположенных в удаленных подсетях.

Для прямого взаимодействия главных броузеров из удаленных подсетей и главного броузера домена в файле LMHOSTS необходимо задать NetBIOS-имена и IP-адреса компьютеров, являющихся броузерами (см. рисунок).




### Главные броузеры

В каждой подсети файл LMHOSTS на каждом главном броузере, работающем под управлением Windows NT, должен содержать:

- IP-адрес и имя компьютера, работающего главным броузером домена;
- имя домена с указанием префиксов **#PRE** и **#DOM**, например:

```
130.20.7.80 <имя_главного_броузера_домена> #PRE #DOM:<имя_домена>
```

### Главные броузеры домена

В файле LMHOSTS главного броузера домена обязательно присутствуют записи для каждого главного броузера каждой удаленной подсети.

На каждом главном броузере должны быть записи с префиксом **#DOM** для каждого главного броузера в данном домене. В таком случае, если один из главных броузеров будет выбран на роль главного броузера домена, не понадобится изменять файл LMHOSTS ни на одном из главных броузеров.

Если в файле LMHOSTS несколько записей с одинаковым именем домена, то главный броузер определит, какая из них соответствует главному броузеру домена, путем опроса каждого указанного IP-адреса. На опрос откликнется только главный броузер домена. Затем главный броузер соединится с главным броузером домена для обмена списками просмотра.

## Резюме

Сервис WINS решает проблемы, связанные с широковещанием NetBIOS-имен, за счет динамической регистрации NetBIOS-имени и IP-адреса компьютера и сохранения их в базе данных WINS.

# Занятие 3. Работа домена в корпоративной IP-сети

Здесь описано, как настроить файл LMHOSTS для обеспечения работы домена Microsoft.

**Изучив материал этого занятия, Вы сможете:**

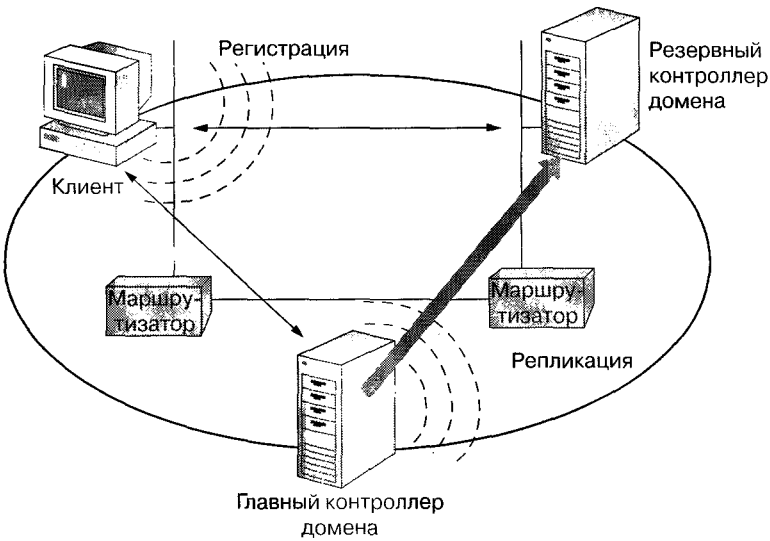
- ✓ описать, как в корпоративной IP-сети происходит *регистрация в домене* (domain logon), смена паролей и синхронизация доменов;
- ✓ спланировать реализацию файла LMHOSTS.

**Продолжительность занятия — 25 минут**

Кроме обзора сети, еще несколько программ, выполняемых сетевыми сервисами Windows NT, могут отправлять широковещательные сообщения всем компьютерам домена Microsoft. В их число входят:

- *регистрация в домене и изменение пароля* — широковещательный запрос по всему домену производится для обнаружения контроллера домена, который может аутентифицировать запрос на регистрацию, или для обнаружения PDC при смене пароля пользователя;
- *тиражирование базы данных с учетными записями пользователей домена, осуществляемое контроллерами домена* — широковещательное сообщение посылается от PDC к *резервным контроллерам домена* (backup domain controllers, BDC), заставляя их запрашивать репликацию обновленных значений из базы данных, содержащей учетные записи пользователей домена.

Поскольку такие широковещательные сообщения не пройдут через маршрутизатор, для выполнения этих задач необходимо использовать *направленную передачу* (directed traffic). Ниже показано, как при этом, кроме широковещательного сообщения в домен, посылаются сообщения к удаленным контроллерам домена. Список компьютеров, получающих направленные сообщения, определяется при помощи WINS или файла LMHOSTS.




## Использование файла LMHOSTS

Клиент не только отправляет широковещательное сообщение, но и ищет в файле LMHOSTS записи с префиксом **#DOM** с подходящим именем домена. Если он находит такую запись, сообщение дублируется для указанного компьютера.

Рекомендуется на каждом клиенте добавить в файл LMHOSTS записи с префиксом **#DOM**, соответствующие всем удаленным контроллерам домена. Таким образом, пользователь сможет зарегистрироваться, даже если отключены все локальные контроллеры домена. Если же локальных контроллеров домена нет вообще, запись с префиксом **#DOM** необходима для регистрации пользователя.

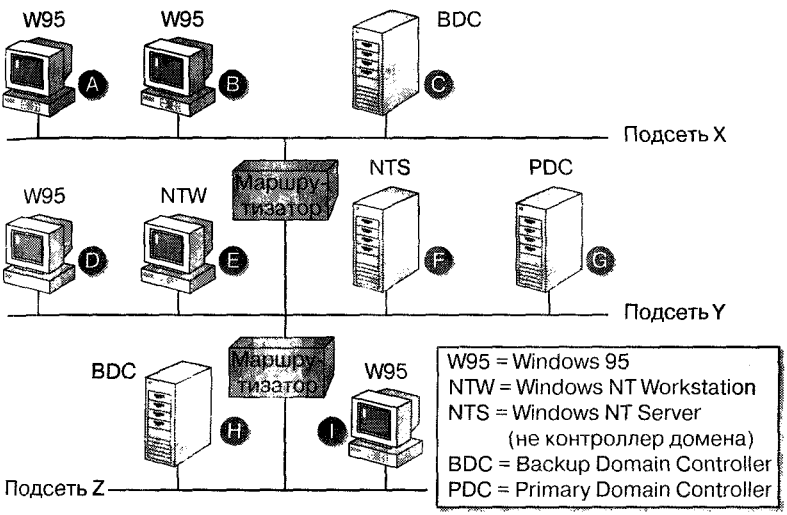
Если PDC не является клиентом WINS, то он должен иметь записи с префиксом **#DOM** для каждого BDC. На каждом BDC должна быть запись для PDC. Рекомендуется на каждом контроллере домена иметь записи с префиксом **#DOM** для всех остальных контроллеров домена. Таким образом, если BDC выбран на роль PDC, то у всех остальных BDC будет запись с префиксом **#DOM**, соответствующая новому PDC.

## Использование WINS

Клиент запрашивает у WINS список всех контроллеров данного домена. В ответ WINS отсылает список, называемый *межсетевой группой* (Internet group), содержащий до 25 контроллеров, зарегистрированных для данного домена. Затем клиент посылает сообщение непосредственно к этим контроллерам домена.

## Упражнения

В этих заданиях Вам придется решить, каким компьютерам необходим файл LMHOSTS для поддержки функций обзора сети, подтверждения регистрации, синхронизации домена и применения WINS, а также как настроить каждый файл LMHOSTS. Воспользуйтесь рисунком и сценарием.




Как показано на рисунке, домен охватывает несколько подсетей. В каждой подсети есть контроллер домена и другие компьютеры. Узлы в каждой подсети могут непосредственно просматривать ресурсы и взаимодействовать только с NetBIOS-узлами той же подсети, поскольку маршрутизаторы не перенаправляют широковещательные запросы.

1. Какие компьютеры используют файл LMHOSTS для поддержки обзора объединенной сети? Для каких компьютеров необходимо занести записи в файл LMHOSTS?

_____

_____

2. Какие компьютеры используют файл LMHOSTS для подтверждения регистрации? Для каких компьютеров необходимо занести записи в файл LMHOSTS?

_____

_____

3. Какие компьютеры используют файл LMHOSTS для поддержки синхронизации учетных записей домена? Для каких компьютеров необходимо занести записи в файл LMHOSTS?

4. Если сервер WINS установлен в подсети Y и все компьютеры настроены для использования WINS, каким из них понадобится файл LMHOSTS?

## Резюме

Некоторые задачи, выполняемые сетевыми службами Windows NT, могут отправлять широковещательные сообщения всем компьютерам домена Microsoft. Клиент посылает широковещательное сообщение в домен, а также ищет в файле LMHOSTS записи с префиксом **#DOM** с подходящим именем домена.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Почему возникают проблемы при обзоре ресурсов корпоративной IP-сети?

2. Каким образом главный броузер в подсети определяет IP-адрес главного броузера домена, если домен охватывает несколько подсетей?

3. Чем помогает сервис WINS при сборе информации о доменах и рабочих группах?

4. Что необходимо сделать на контроллерах домена, не являющихся клиентами WINS, чтобы обеспечить синхронизацию учетных записей, когда домен охватывает несколько подсетей?


# Разрешение имен узлов



## В этой главе

В этой главе рассматриваются концепции и проблемы разрешения имен узлов. Из занятий Вы узнаете, как для разрешения имен узлов используются сервер имен домена, сервер имен NetBIOS, широковещание и файл LMHOSTS. Вы научитесь настраивать и использовать файл HOSTS.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить ОС Microsoft Windows NT Server 4.0 и протокол TCP/IP.

# Занятие 1. Схемы именования в TCP/IP

Хотя для взаимодействия по протоколу TCP/IP необходимо задавать IP-адрес, к узлам чаще всего обращаются по их именам.

**Изучив материал этого занятия, Вы сможете:**

✓ объяснить различия в схемах именования узлов.

**Продолжительность занятия — 5 минут**

Узлы Windows NT и UNIX используют различные схемы именования. Узлу Windows NT можно назначить имя, но оно используется только утилитами TCP/IP. Узлу UNIX необходим лишь IP-адрес, но, по желанию, можно использовать имя узла или домена.

Перед установкой соединения каждый узел должен узнать IP-адрес своего партнера. От используемой схемы именования зависит формат обращения к узлу.

- При выполнении команды *net use* пользователь Windows NT обычно указывает NetBIOS-имя компьютера и гораздо реже — IP-адрес:

  ```
  net use x: \\имя_компьютера
  ```

  Сначала имя NetBIOS разрешается в IP-адрес, а затем протокол ARP по IP-адресу определяет адрес сетевого адаптера.
- Для обращения к узлу UNIX, поддерживающему TCP/IP, пользователь может указать IP-адрес, имя узла или имя домена. Если использовано имя узла или домена, то оно разрешается в IP-адрес. Если же задействован IP-адрес, то разрешения имени не требуется, и сразу определяется адрес сетевого адаптера.

Главное различие в способе обращения к двум указанным типам узлов в том, что при использовании сетевых команд Microsoft надо всегда указывать NetBIOS-имя, а не IP-адрес. Утилиты TCP/IP для взаимодействия с UNIX-узлами позволяют Вам использовать в этом случае IP-адрес.

---

Примечание ОС Windows NT 4.0 позволяет связаться с другим компьютером, работающим под управлением Windows NT, используя лишь IP-адрес. Например: `net use x: \\131.107.2.200\имя_ресурса`

---

## Резюме

Узлы под управлением Windows NT и UNIX используют различные схемы именования. ОС Windows NT и остальные сетевые ОС фирмы Microsoft требуют указывать имя NetBIOS для взаимодействия с другими узлами Windows NT.

# Занятие 2. Имена узлов

Имя упрощает обращение к узлу, поскольку его легче запомнить, чем IP-адрес. Имена узлов используются практически везде, где есть TCP/IP. На этом занятии объясняется механизм разрешения имен узлов.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как при помощи файла HOSTS разрешаются имена узлов как из локальной, так и из удаленной сети;
- ✓ объяснить, как имя узла разрешается в IP-адрес при помощи DNS и методов, поддерживаемых сетями Microsoft.

**Продолжительность занятия — 20 минут**

Имя узла — это псевдоним, назначенный администратором компьютеру для идентификации узла, поддерживающего TCP/IP. Имя узла иногда не совпадает с NetBIOS-именем данного компьютера и содержит до 256 символов. Одному узлу можно назначить несколько имен.

Имя узла TCP/IP облегчает взаимодействие с ним. Его можно использовать вместо IP-адреса, например, в программе Ping и других утилитах TCP/IP.

Имя узла всегда соответствует IP-адресу. Это соответствие может быть задано либо в файле HOSTS, либо в базе данных сервера имен NetBIOS или DNS. В ОС Windows NT для определения IP-адреса, соответствующего имени узла, иногда используют файл LMHOSTS.

Средства утилиты Hostname позволяют узнать имя, назначенное Вашей системе. По умолчанию для компьютера под управлением Windows NT имя узла совпадает с именем компьютера.

## Разрешене имени узла

*Разрешение имени узла* (host name resolution) — это процесс определения соответствующего ему IP-адреса. Только после этого IP-адрес может быть разрешен в адрес сетевого адаптера.

В ОС Windows NT для разрешения имен узлов предусмотрено несколько методов (см. главу 8); все их можно конфигурировать.

Методы, используемые протоколом Microsoft TCP/IP, перечислены в таблицах.

| Стандартные методы разрешения | Описание |
|---|---|
| Имя локального узла | Имя узла, заданное для данного компьютера. Имя запрашиваемого узла в первую очередь сравнивается с именем локального узла |
| Файл HOSTS | Локальный текстовый файл в формате, совпадающем с форматом файла \etc\hosts BSD UNIX 4.3. В этом файле указаны IP-адреса и соответствующие им имена узлов. Обычно этот файл используется утилитами TCP/IP для разрешения имен узлов |
| Сервер DNS | Сервер, на котором хранится база данных, содержащая соответствия имен компьютеров (имен узлов) IP-адресам |

| Методы Microsoft | Описание |
|---|---|
| Сервер имен NetBIOS, NBNS | Сервер, реализованный согласно спецификациям RFC 1001 и 1002 и обеспечивающий разрешение NetBIOS-имен компьютеров. Сервер WINS — это реализация NBNS от фирмы Microsoft |
| Локальное широковещание | Для определения IP-адреса соответствующего NetBIOS-имени используется широковещание в локальной сети |
| Файл LMHOSTS | Локальный текстовый файл, в котором указано соответствие IP-адресов и NetBIOS-имен компьютеров, находящихся в удаленных сетях |

## Разрешение имен при помощи файла HOSTS

В отличие от файла LMHOSTS, который использовался только для удаленных узлов, в файле HOSTS могут быть соответствия IP-адресов и имен как локальных, так и удаленных узлов. Процесс, описанный ниже, проиллюстрирован на следующей странице.

1. Разрешение имени начинается в тот момент, когда пользователь вводит команду, где указывает имя узла назначения.

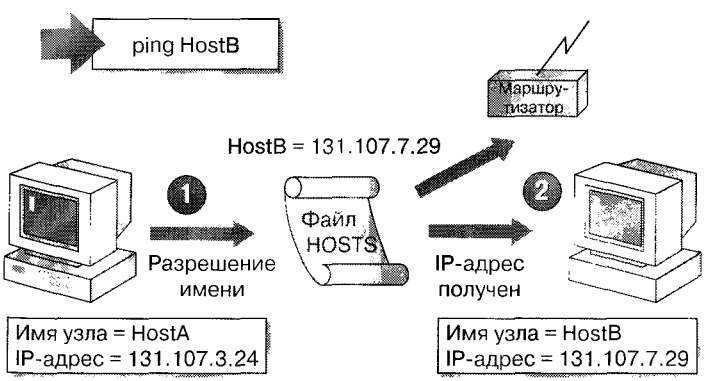
   Windows NT прежде всего проверяет, не совпадает ли указанное имя с именем локального узла. Если эти имена различны, то просматривается файл HOSTS. Если имя узла обнаружено в нем, то оно разрешается в IP-адрес.

   Если имя узла обнаружить не удалось, а другие методы разрешения имен, например DNS, сервер имен NetBIOS, или файл LMHOSTS, недоступны, процесс прекращается, а пользователь получает сообщение об ошибке.

2. После того как имя узла успешно разрешено в IP-адрес, делается попытка разрешить этот IP-адрес в адрес сетевого адаптера.

   Если узел назначения находится в локальной сети, адрес сетевого адаптера может быть получен из кэша протокола ARP или при помощи широковещания.

   Если же этот узел находится в удаленной сети, то ARP получает IP-адрес маршрутизатора, откуда запрос перенаправляется к узлу.




## Разрешение имен при помощи сервера DNS

Сервер *доменной системы имен* (Domain Name System, DNS) — это централизованная, обновляемая база данных, которая применяется в UNIX для разрешения *полностью определенных доменных имен* (fully qualified

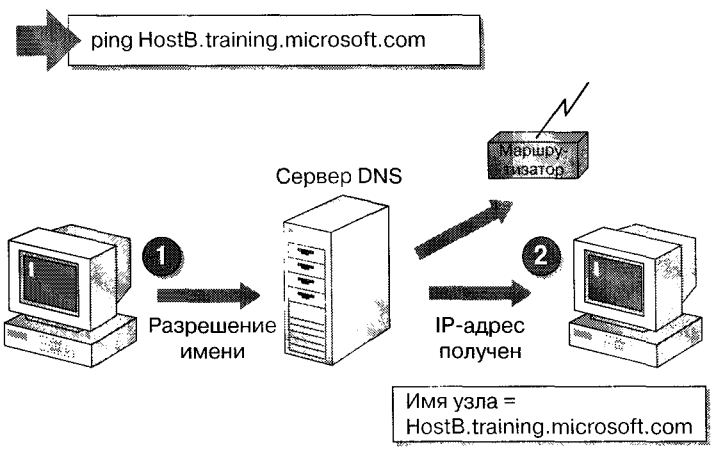
domain name, FQDN) и других имен узлов в соответствующие IP-адреса. ОС Windows NT 4.0 может использовать сервер DNS или сама выполняет его функции. Разрешение имен при помощи сервера DNS очень напоминает разрешение средствами файла HOSTS.

Если Windows NT для разрешения имен узлов использует сервер DNS, то процесс выполняется в два этапа.

1. Когда пользователь вводит команду, применяя FQDN или другое имя узла, сервер DNS ищет это имя в БД и разрешает его в IP-адрес.

   Если сервер DNS не отвечает на запрос, то с интервалами 5, 10, 20, 40, 5, 10 и 20 секунд выполняются повторные попытки. Если сервер DNS не отвечает и на эти запросы, а другие методы, например, сервер имен NetBIOS или файл LMHOSTS недоступны, процесс прекращается и генерируется сообщение об ошибке.
2. После того как имя узла разрешено, по протоколу ARP определяется адрес сетевого адаптера. Если узел назначения находится в локальной сети, это реализуется при помощи кэша ARP или широковещания. Если же узел-получатель находится в удаленной сети, ARP получает адрес маршрутизатора, который может перенаправить запрос.

   Если сервер DNS находится в удаленной сети, то перед разрешением имени ARP должен получить адрес сетевого адаптера маршрутизатора.




## Разрешение имен узлов в сетях Microsoft

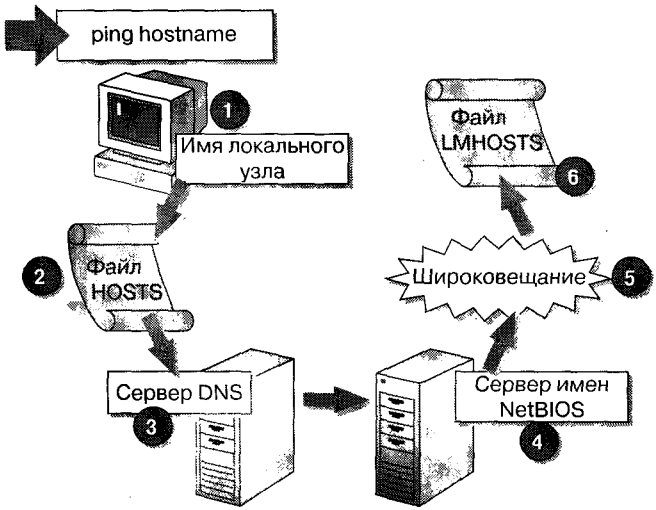
В ОС Windows NT для разрешения имен узлов используется не только файл HOSTS и сервер DNS, но и сервер имен NetBIOS, широковещание и файл LMHOSTS. Если один из этих методов не сработает, другие подстрахуют его, как показано в приведенном далее примере и на иллюстрации.

Последовательность действий при разрешении имени с использованием NBNS и LMHOSTS описана ниже.

1. Когда пользователь вводит команду и указывает имя узла, Windows NT сравнивает его с именем локального узла. При их совпадении имя разрешается и команда выполняется (сеть при этом не задействована).
2. Если введенное имя узла и имя локального узла не совпадают, то просматривается файл HOSTS. В случае обнаружения в нем указанного имени оно разрешается в IP-адрес, и начинается разрешение самого адреса. Файл HOSTS должен находиться в локальной системе.
3. Если имя узла не удалось разрешить при помощи файла HOSTS, узел-отправитель посылает запрос к указанным в его конфигурации серверам DNS. Обнаруженное сервером DNS, имя узла разрешается в IP-адрес, и начинается процесс разрешения адреса.

   Если сервер DNS не отвечает на запрос, то с интервалом в 5, 10, 20, 40, 5, 10 и 20 секунд посылаются повторные запросы.
4. Если сервер DNS не может разрешить имя узла, то перед попыткой связаться со своими серверами имен NetBIOS узел-отправитель просматривает локальный кэш имен NetBIOS. Если имя узла обнаружено в нем или зарегистрировано на сервере имен NetBIOS, то оно успешно разрешается в IP-адрес и начинается процесс разрешения адреса.
5. Если имя узла не было разрешено сервером имен NetBIOS, исходный узел посылает три широковещательных сообщения в локальную сеть. Обнаруженное в локальной сети, такое имя разрешается в IP-адрес и начинается процесс разрешения адреса.
6. Если не удалось разрешить имя при помощи широковещания, привлекается локальный файл LMHOSTS. Обнаруженное в этом файле имя узла разрешается в IP-адрес и начинается разрешение адреса.

   Если ни один из этих методов не позволил разрешить имя узла, то единственный способ связи — явно указать IP-адрес узла.




## Резюме

Имя узла используется для идентификации узла TCP/IP или шлюза по умолчанию. Разрешение имени узла — это процесс определения соответствующего ему IP-адреса. Эта процедура обязательна перед получением адреса сетевого адаптера при помощи протокола ARP.

# Занятие 3. Файл HOSTS

Теперь, когда Вы изучили различные методы разрешения имен, подробнее рассмотрим файл HOSTS. На этом занятии Вы настроите файл HOSTS для правильного разрешения имен узлов.

**Изучив материалы этого занятия, Вы сможете:**

- ✓ настроить и использовать файл HOSTS.

**Продолжительность занятия — 15 минут**

Файл HOSTS — это статический файл, используемый для хранения соответствий имен узлов и IP-адресов. Он совместим с файлом HOSTS из ОС UNIX. Файл HOSTS применяется программой Ping и другими утилитами TCP/IP для разрешения имен узлов, находящихся как в локальной, так и в удаленной сети. Кроме того, файл HOSTS может использоваться для разрешения имен NetBIOS (только в Microsoft TCP/IP-32).

Наличие файла HOSTS обязательно на каждом компьютере. Всякая его запись содержит IP-адрес и соответствующие ему одно или несколько имен узлов. По умолчанию в файле HOSTS есть запись с именем *localhost*.

Файл HOSTS просматривается при каждом обращении к именам узлов, которые считываются из него последовательно, поэтому наиболее часто используемые имена должны находиться в начале файла.

---

Примечание Файл HOSTS можно редактировать при помощи любого текстового редактора. Он находится в каталоге \systemroot\System32\Drivers\Etc.

Всякая запись может содержать до 255 символов, при этом регистр символов не учитывается.

---

Пример файла HOSTS:

```
# This file used by Microsoft TCP/IP utilities
127.0.0.1         localhost loopback
102.54.94.97      rhino.microsoft.com
131.107.2.100     unixhost UNIXHOST # LAN Manager UNIX Host
131.107.3.1 gateway GATEWAY   # Default Gateway
```

## Упражнения

Выполнив эти упражнения, Вы научитесь конфигурировать и применять файл HOSTS, настроите ОС Windows NT для использования DNS и выявите проблемы разрешения имен узлов и доменов. Вы собственноручно добавите имя узла и его IP-адрес в файл HOSTS. Далее он будет использован для разрешения имен узлов.

### ▶ Определение имени локального узла

В этом задании Вы определите имя локального узла, используемое утилитами TCP/IP.

1. Откройте окно командной строки;
2. Очистите кэш имен NetBIOS;
3. Введите *hostname* и нажмите ENTER.

   Вы увидите имя локального узла.

### ▶ Ping имени локального узла

В этом задании Вы при помощи утилиты Ping «прозвоните» имя локального узла, чтобы убедиться в том, что Microsoft TCP/IP может разрешать имя локального узла в отсутствие записей в файле HOSTS.

1. Введите *ping Server1* (где *Server1* — имя Вашего компьютера) и нажмите ENTER.

   Каков результат?

   _____

2. Введите *ping Server2* (где *Server2* — Ваш второй компьютер) и нажмите ENTER.

   Каков результат теперь?

   _____

### ▶ Ping имени компьютера в локальной сети

Примечание Выполняйте это задание на компьютере Server1.

- Введите *ping computertwo* и нажмите ENTER.

  Каков результат?

  _____

### ▶ Добавление записи в файл HOSTS

Примечание Выполняйте это задание на компьютере Server1.

1. Перейдите в указанный каталог:

   ```
   cd systemroot\system32\drivers\etc
   ```

2. При помощи редактора Edit измените файл HOSTS, введя:

   ```
   edit HOSTS
   ```

3. Добавьте в файл HOSTS следующую строку:

   ```
   131.107.2.211  computertwo
   ```

4. Сохраните файл и выйдите из редактора Edit.

▶ **Использование файла HOSTS для разрешения имен**

- Введите *ping computertwo* и нажмите ENTER.

  Каков результат?

_____

_____

## Резюме

В файле HOSTS задаются соответствия имен узлов IP-адресам, кроме того, этот файл совместим с файлом HOSTS из ОС UNIX.

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Что такое имя узла?

_____

_____

2. Для чего используется имя узла?

_____

_____

3. Из чего состоят записи файла HOSTS?

_____

_____

4. Что происходит раньше: разрешение IP-адреса или разрешение имени узла?

_____

# Доменная система имен



## В этой главе

В этой главе рассматриваются структура и составные части DNS, определение адресов TCP/IP, настройка файлов, используемых службой DNS, и регистрация DNS-сервера в *родительском домене* (parent domain). Во время занятий Вы получите навыки выбора оптимальных значений для различных параметров DNS. В их число входят количество доменов, серверов имен, зон, а также файлов, связанных с DNS.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить Windows NT 4.0 Server с протоколом TCP/IP.

# Занятие 1. Общие сведения о DNS

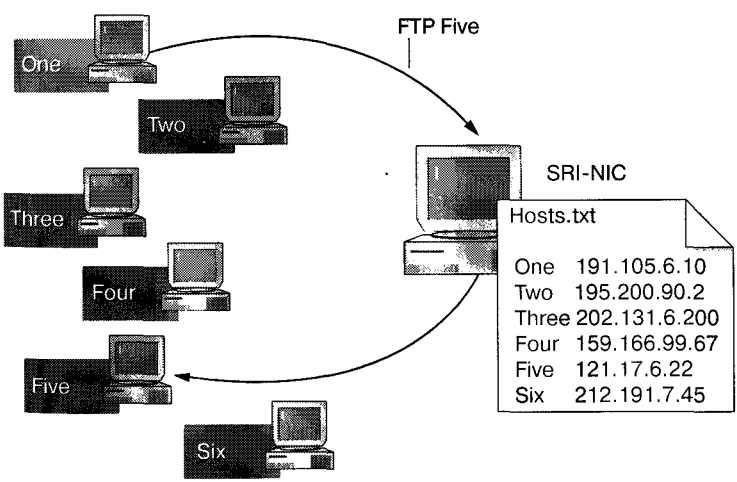
*Доменная система имен* (Domain Name System, DNS) похожа на телефонную книгу. При использовании DNS компьютер обращается к другому компьютеру по имени, а сервер имен домена преобразует имя в IP-адрес. На этом занятии Вы узнаете об архитектуре и структуре DNS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать структуру, архитектуру и составные части DNS;
- ✓ объяснить, как DNS используется для разрешения имен и IP-адресов.

**Продолжительность занятия — 30 минут**

До 1980 года сеть ARPANET состояла лишь из нескольких сотен компьютеров. Все соответствия имен и адресов компьютеров хранились в одном файле с именем Hosts.txt. Этот файл находился на компьютере центра Stanford Research Institute's Network Information Center (SRI-NIC) в Менло-Парк, штат Калифорния. Как показано на рисунке, остальные компьютеры сети ARPANET по мере надобности копировали из SRI-NIC файл Hosts.txt на свои узлы.




Поначалу эта схема работала достаточно хорошо, поскольку файл Hosts.txt нужно было обновлять один-два раза в неделю. Однако через несколько лет, когда сеть ARPANET заметно выросла, возникли проблемы:

- файл Hosts.txt стал очень большим;
- приходилось обновлять файл несколько раз в день;
- так как весь сетевой трафик маршрутизировался через SRI-NIC, поддержка файла Hosts.txt стала камнем преткновения для всей сети;
- сетевой трафик через SRI-NIC стал почти неуправляемым;
- в Hosts.txt использовалось *одноуровневое* (flat) пространство имен, поэтому имя компьютера в сети должно было быть уникальным.

Эти и другие проблемы заставили управление ARPANET искать другие способы распространения файла Hosts.txt. В результате была создана доменная система имен — DNS — распределенная база данных, использующая *иерархическое* (hierarchical) пространство имен.

Примечание Доменная система имен описана в документах RFC 1034 и 1035. Копии этих документов Вы найдете на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

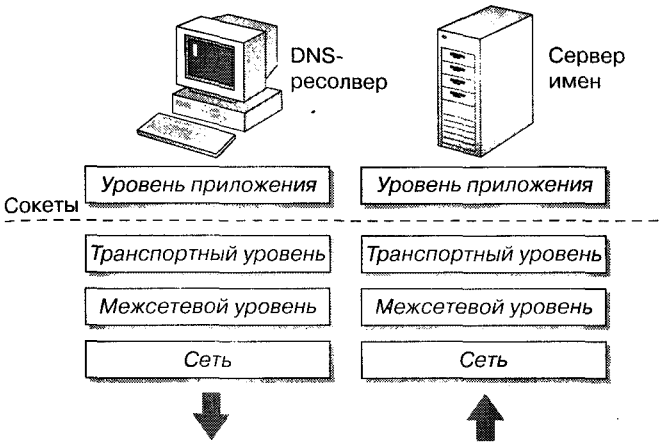
## Как работает DNS

В работе DNS участвует три основных компонента: клиенты DNS, или *программы разрешения имен* (resolvers), серверы имен и пространство имен домена.

В простейшем случае DNS-клиент посылает запросы серверу имен. Сервер возвращает либо требуемую информацию, либо указание на другой сервер имен, либо сообщение об отказе, если запрос не может быть удовлетворен.

Доменная система имен — это система управления иерархической распределенной базой данных, использующая технологию клиент-сервер. DNS работает на *прикладном уровне* (application layer) и использует UDP и TCP/IP как нижележащие протоколы.

Задача базы данных DNS — транслировать имена компьютеров в IP-адреса, что показано на следующей иллюстрации. DNS-клиентов часто называют *ресолверами* (resolvers), серверы — *серверами имен* (name servers).




Доменная система имен похожа на телефонную книгу. Пользователь находит имя человека или название организации, с которой хочет связаться, — рядом указан телефонный номер. Аналогично компьютер обращается к DNS, используя имя другого компьютера или домена, а сервер имен выдает соответствующий этому имени IP-адрес.

Сначала DNS-клиенты посылают серверам запросы по протоколу UDP (для повышения производительности), а переключаются на использование TCP только при потере информации.

### DNS-клиенты

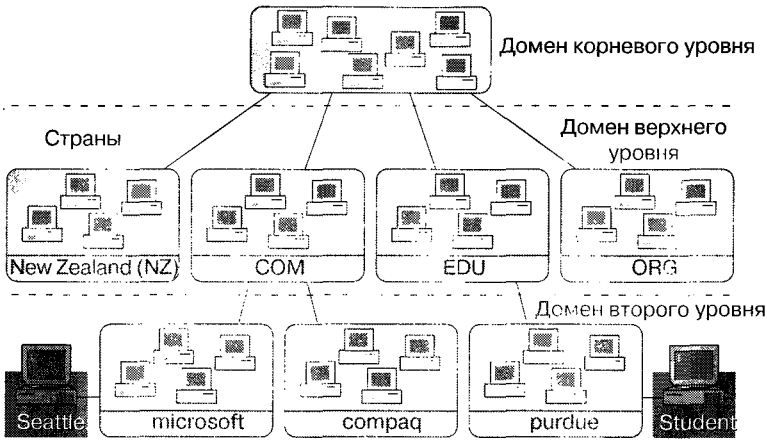
DNS-клиенты пересылают сообщения между приложениями и серверами имен. Сообщение содержит запрос, например IP-адрес Web-узла. Часто DNS-клиент встроен в приложение или работает на компьютере как библиотечная подпрограмма.

### Серверы имен

Серверы имен принимают сообщения от DNS-клиентов и преобразуют имена компьютеров (или доменов) в IP-адреса. Если сервер имен не в состоянии сам сделать это, то он может перенаправить запрос к другому серверу имен, который сможет разрешить его. Серверы имен сгруппированы по разным уровням — *доменам* (domains).

## Пространство имен домена

Это иерархически упорядоченная структура имен, напоминающая перевернутое дерево.




## Домены корневого уровня

Домены определяют различные уровни в иерархии. На самом верху — находится *корневой домен* (root domain). Он использует *пустую метку* (null lable), но ссылки на корневой домен можно задавать точкой (.).

## Домены верхнего уровня

Вот список *доменов верхнего уровня* (top-level domains)*:

- com — коммерческие организации;
- edu — образовательные учреждения и университеты;
- org — некоммерческие организации;
- net — сети (крупные сети, входящие в Internet);
- gov — невоенные правительственные учреждения;
- mil — военные правительственные учреждения;
- num — телефонные номера;
- arpa — *обратный* (reverse) DNS;
- *xx* — двухбуквенные обозначения стран.

В домены верхнего уровня могут входить узлы и домены второго уровня.

---

Примечание *Комитет Сообщества Интернета* (Internet Society committee) планирует ввести несколько новых доменов верхнего уровня, например .firm и .web.

---

* В настоящее время список доменов верхнего уровня расширяется. — *Прим. перев.*

### Домены второго уровня

В домены второго уровня входят узлы и другие домены, называемые *поддоменами* (subdomains). Так, в домен фирмы Microsoft *microsoft.com* включены как отдельные компьютеры, например *ftp.microsoft.com*, так и поддомены, например *dev.microsoft.com*. В последние также могут входить узлы, например *ntserver.dev.microsoft.com*.

### Имена узлов

Имена узлов обычно справа дополняются именем домена. Такая запись называется *полностью определенным доменным именем* (fully qualified domain name, FQDN). Например, узел *fileserver* в домене *microsoft.com* будет иметь FQDN-имя *fileserver.microsoft.com*.

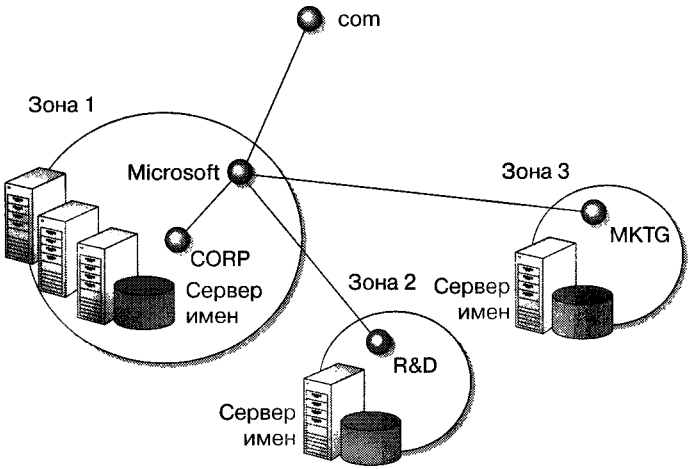
## Зоны ответственности

*Зона ответственности* (zone of authority) — это часть пространства имен домена, за которую отвечает конкретный сервер имен. Сервер имен хранит IP-адреса для всех имен из зоны его ответственности и обслуживает все запросы клиентов к этим именам.

Зона ответственности сервера имен охватывает, как минимум, один домен, который называют *корневым доменом зоны* (zone root domain). Зона ответственности может включать и поддомены корневого домена. Однако в одну зону не обязательно входят все поддомены, расположенные ниже корневого домена этой зоны.

На приведенной далее иллюстрации домен *microsoft.com* не укладывается в одной зоне. Часть домена выделена в отдельную зону *dev.microsoft.com*. Разбиение домена на несколько зон необходимо для раздельного управления группами в домене или для эффективного тиражирования данных.

Один DNS-сервер может управлять несколькими зонами. Каждая зона подчинена конкретному домену, который называют корневым доменом зоны.




## Роли DNS-серверов

DNS-серверы могут выполнять разные задачи.Они могут хранить и поддерживать свои базы данных различными способами. Далее описаны способы хранения данных своей зоны.

### Основной сервер имен

Основной сервер имен извлекает информацию из локальных файлов. Изменения в параметрах зоны, например добавление узла или домена, выполняются на основном сервере имен.

### Резервный сервер имен

Резервный сервер имен получает информацию о своей зоне от других серверов, которые ответственны за данную зону. Такой способ получения информации через сеть называют *зонной передачей* (zone transfer).

Существует три основные причины, по которым следует создавать резервные серверы имен.

- Избыточность — Вам необходимы, как минимум, один основной и один резервный сервер имен на каждую зону. Компьютеры должны быть как можно более независимы.
- Ускоренный доступ для удаленных клиентов — если у Вас есть несколько удаленных клиентов, то наличие резервных серверов имен (или других основных серверов имен в поддоменах) освободит их от использования низкоскоростных линий при распознавании имен.
- Снижение нагрузки — резервные серверы имен уменьшают загруженность основных серверов.

Поскольку информация о разных зонах хранится в разных файлах, разделение серверов на основные и резервные значимо только в пределах зоны. Другими словами, данный DNS-сервер может быть основным по отношению к одной зоне и резервным по отношению к другой.

### Главный сервер имен

При определении DNS-сервера на роль резервного сервера имен в данной зоне Вы должны указать DNS-сервер, от которого будет поступать зонная информация. Источник такой информации для резервного сервера имен в иерархии DNS называют *главным сервером имен* (master name server). Он может быть как основным, так и резервным DNS-сервером в своей зоне. При запуске резервный DNS-сервер связывается со своим главным сервером имен и запрашивает зонную передачу.

### Кэширующий DNS-сервер

Все DNS-серверы кэшируют запросы, на которые они отвечают. Кэширующие — это DNS-серверы, которые только перенаправляют запросы, кэшируют ответы и возвращают результаты. То есть, они не отвечают ни за какие домены (на них информация о зонах не хранится), а содержат лишь информацию, которая попала в кэш из ответов на запросы.

Обдумывая целесообразность использования такого DNS-сервера в Вашей организации, обратите внимание на то, что при начальном запуске кэш не содержит информации — она накапливается при обслуживании запросов. При этом отсутствует зональная передача и сильно снижается объем сетевого трафика. Это важно, если Вы работаете с низкоскоростными линиями связи.

## Резюме

Доменная система имен появилась в связи с увеличением размеров сети ARPANET. DNS-клиент посылает запросы серверу имен. Серверы имен принимают запросы и преобразуют имена компьютеров в IP-адреса. Пространство имен доменов включает иерархически сгруппированные корневые домены, домены верхнего уровня, домены второго уровня и имена узлов. Отдельные серверы отвечают за части пространства доменных имен. Эти части называются зонами ответственности.

# Занятие 2. Разрешение имен

Существует три типа запросов, которые клиент может направить к DNS-серверу: *рекурсивный* (recursive), *итеративный* (iterative) и *обратный* (inverse).

**Изучив материалы этого занятия, Вы сможете:**

- ✓ объяснить, как работают рекурсивный, итеративный и обратный запросы;
- ✓ описать, как запросы попадают в кэш для последующего использования.

**Продолжительность занятия — 10 минут**

## Рекурсивные запросы

DNS-сервер обязательно отвечает на рекурсивный запрос, посылая либо запрошенную информацию, либо сообщение об ошибке. Последнее означает, что запрошенные данные отсутствуют или указанного имени домена не существует. При этом DNS-сервер не может перенаправить клиента к другому DNS-серверу.

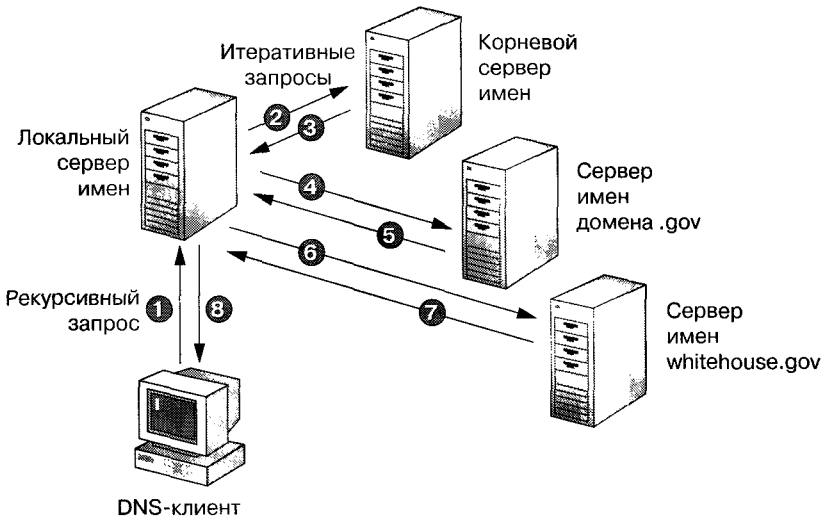
## Итеративные запросы

На итеративный запрос DNS-сервер выдает наилучший ответ из имеющихся у него. В нем может содержаться разрешенное имя или ссылка на другой DNS-сервер.

На следующей странице показан пример рекурсивного и итеративного запросов: клиент, находясь на работе, запрашивает у DNS-сервера IP-адрес, соответствующий узлу *www.whitehouse.gov*.

1. DNS-клиент посылает локальному DNS-серверу рекурсивный запрос, в котором просит определить IP-адрес для узла *www.whitehouse.gov*. Локальный сервер имен отвечает за распознавание имени и не может перенаправить клиента к другому DNS-серверу.
2. Локальный DNS-сервер просматривает свои зоны и не находит зону, содержащую указанное имя домена. Тогда он посылает к корневому серверу имен итеративный запрос об узле *www.whitehouse.gov*.
3. Корневой DNS-сервер, ответственный за корневой домен, возвращает IP-адрес сервера имен для домена верхнего уровня — *.gov*.
4. Локальный DNS-сервер посылает DNS-серверу домена *.gov* итеративный запрос о *www.whitehouse.gov*.
5. DNS-сервер домена *.gov* возвращает IP-адрес сервера имен, обслуживающего домен *whitehouse.gov*.

6. Локальный DNS-сервер посылает DNS-серверу домена *whitehouse.gov* итеративный запрос о *www.whitehouse.gov*.
7. DNS-сервер домена *whitehouse.gov* возвращает IP-адрес, соответствующий *www.whitehouse.gov*.
8. Локальный DNS-сервер посылает клиенту IP-адрес для *www.whitehouse.gov*.




## Обратные запросы

При обратном запросе клиент пытается узнать у DNS-сервера имя узла, соответствующего известному IP-адресу. Вообще-то, в пространстве имен DNS не установлено соответствие IP-адресов именам, и лишь сплошной просмотр всех доменов позволяет получить правильный ответ.

Чтобы избежать тотального просмотра всех доменов при обслуживании обратного запроса, был создан специальный домен, *in-addr.arpa*. Имена узлов этого домена совпадают с записью IP-адреса в виде четырех десятичных чисел, разделенных точкой. Но поскольку IP-адреса уточняются слева направо, а доменные имена справа налево, то при построении домена *in-addr.arpa* необходимо изменить порядок следования чисел IP-адреса. Согласно этому, управление нижележащими членами домена *in-addr.arpa* можно передать организациям, которым выделяются IP-адреса классов A, B и C.

В домен *in-addr.arpa* при его создании добавляются специальные ресурсы — *указательные записи* (pointer records, PTR), связывающие IP-адрес с именем узла. Например, чтобы определить имя узла, соответствующее IP-адресу 157.55.200.51, клиент обращается к DNS-серверу с запро-

сом указательной записи для 51.200.55.157.*in-addr.arpa*. Найденная указательная запись содержит имя узла и соответствующий IP-адрес 157.55.200.51. Эта информация отправляется обратно клиенту. В задачи администрирования DNS-сервера входит создание указательных записей для узлов данного домена.

## Кэширование и TTL

При обработке рекурсивного запроса иногда необходимо для получения ответа посылать несколько сообщений. Сервер имен сохраняет в кэше всю получаемую им информацию, но лишь на время, указанное в возвращаемых данных. Этот интервал называют *временем жизни* (time to live, TTL). Его определяет администратор DNS-сервера той зоны, в которой находятся указанные данные. Если информация о домене изменяется часто, то меньшее значение TTL гарантирует, что данные во всей сети не успевают устаревать. Однако это сильно загружает DNS-серверы.

Как только информация попадает в кэш, начинается обратный отсчет TTL. По истечении TTL она будет удалена из кэша DNS-сервера. DNS-клиенты также имеют кэш и учитывают TTL, поэтому они будут знать, когда данные устареют.

## Резюме

DNS-клиент (resolver) может посылать к DNS-серверу рекурсивные, итеративные и обратные запросы. Как только DNS-сервер ответит на запрос, эта информация помещается в кэш.

# Занятие 3. Конфигурирование файлов DNS

Типичный DNS-сервер использует четыре конфигурационных файла. Они будут детально описаны на этом занятии.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать содержимое файлов базы данных DNS.

**Продолжительность занятия – 25 минут**

Обычно для работы DNS-сервера необходимы файлы: базы данных, обратного просмотра (для обработки обратных запросов), кэш и загрузочный. С их помощью сервер выполняет большинство своих функций.

## Файл базы данных

Файл базы данных (Zone.dns) содержит исходные записи для домена. В комплект поставки ОС Windows NT 4.0 входит пример такого файла, Place.dns, с которым Вы можете работать. Прежде чем использовать этот файл на Вашем DNS-сервере, его необходимо отредактировать и переименовать — лучше всего по названию зоны, которую он описывает. Например, для зоны *microsoft.com* — microsoft.com.dns. Этот файл будет пересылаться от главных серверов имен к резервным.

Существует несколько типов записей, определенных для DNS. В документе RFC 1034 описаны следующие: SOA, NS, A, CNAME, PTR, MX и HINFO. Фирмой Microsoft дополнительно определены записи типа WINS и WINS-R.

### Запись Start of Authority

Первой в любом файле базы данных должна быть запись Start of Authority (SOA). Она определяет основные параметры зоны DNS. Ниже приведен пример записи SOA:

```
@ IN SOA nameserver1.microsoft.com. glennwo.microsoft.com.

    1   : serial number
    10800 : refresh [3 hours]
    3600   : retry [1 hour]
    604800    : expire [7 days]
    86400 : time to live [1 day]
```

Все записи SOA должны удовлетворять следующим требованиям:

- символ @ в файле базы данных означает «этот сервер»;
- IN означает запись для Интернета;

- любое, не оканчивающееся точкой (.) имя узла будет дополнено именем корневого домена;
- в адресе электронной почты администратора символ @ заменяется точкой (.);
- разрывы строк при переносе заключаются в круглые скобки.

### Запись Name Server

Запись Name Server (NS) служит для перечисления других серверов имен. Файл базы данных может содержать несколько записей Name Server. Пример записи NS:

```
@ IN NS nameserver2.microsoft.com
```

### Запись Host

Запись Host (A) статически привязывает имя узла к IP-адресу. Большая часть файла базы данных состоит из записей типа A (в них перечислены все узлы, расположенные в данной зоне). Пример записей типа A:

```
rhino       IN A 157.55.200.143
localhost   IN A 127.0.0.1
```

### Запись Canonical Name

Запись Canonical Name (CNAME) позволяет связать несколько имен узлов с одним IP-адресом. Такую операцию иногда называют *назначением псевдонимов* (aliasing). Вот пример записи типа CNAME:

```
FileServer1 CNAME rhino
www         CNAME rhino
ftp         CNAME rhino
```

Примечание Типы записей файла базы данных определены в документах RFC 1034, 1035 и 1183. Копию этих документов можно найти на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Файл обратного просмотра

Файл обратного просмотра (*z.y.x.w*.in-addr.arpa) позволяет DNS-клиенту определять имя узла,соответствующее заданному IP-адресу. Имя для файла обратного просмотра назначается в соответствии с названием зоны домена *in-addr.arpa*, для которой этот файл обрабатывает обратные за-

просы. Например, для обеспечения обратных запросов в IP-сети 157.57.28.0, необходимо создать файл обратного просмотра с именем 57.157.in-addr.arpa. В этом файле, как и во всех файлах базы DNS этой зоны, содержатся записи типов SOA и NS и, кроме этого, — *указательные записи* (pointer records).

Возможность обратного просмотра в DNS важна для тех приложений, которые контролируют безопасность на основе имен узлов. Например, когда клиент хочет связаться с томом *сетевой файловой системы* (network file system, NFS), на котором реализована такая защита, NFS-сервер обратится к DNS-серверу с обратным запросом на IP-адрес клиента. Если имя узла, полученное от DNS-сервера, не занесено в список доступа или если служба DNS не смогла обнаружить имя узла с таким IP-адресом, то в доступе к NFS тому будет отказано.

### Указательная запись

*Указательная запись* (pointer record, PTR) хранит соответствие IP-адреса и имени узла в пределах *зоны обратного просмотра* (reverse lookup zone). В ней IP-адрес записан в обратном порядке и справа дополнен строкой in-addr.arpa. Например, для определения имени, соответствующего 157.55.200.51, необходимо выполнить обратный запрос к имени 51.200.55.157.in-ddr.arpa. Указательная запись может выглядеть так:

```
51.200.55.157.in-addr.arpa. IN PTR mailserver1.microsoft.com.
```

## Кэш-файл

Файл Cache.dns содержит записи для серверов корневого домена. Кэш-файл должен существовать всегда, и он, фактически, одинаков для всех серверов имен. Когда сервер имен получает запрос извне своей зоны, он начинает процесс разрешения имени с обращения к этим серверам корневого домена. Пример записи в кэш-файле:

```
.                    3600000     IN    NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.  3600000     A           198.41.0.4
```

В кэш-файле хранится информация, необходимая для разрешения имен за пределами *ответственных доменов* (authoritative domains). Он содержит имена и IP-адреса корневых DNS-серверов. Файл, по умолчанию поставляемый с DNS-сервером в ОС Windows NT 4.0, содержит записи для всех корневых серверов сети Интернет. При установке на системы, не подключенные к Интернету, этот файл следует исправить так, чтобы в нем содержалась информация о доменах в корне Вашей сети.

Примечание Текущую версию кэш-файла для Интернета Вы найдете по адресу *ftp:\\rs.internic.net/domain/named.cache.*

## Загрузочный файл

В *загрузочном файле* (boot file) содержатся параметры для начального запуска Berkeley Internet Name Daemon (BIND) — одной из реализаций DNS. Этот файл содержит информацию, необходимую для разрешения имен, не входящих в контролируемый домен. Этот файл не определен в документах RFC и не нужен для совместимости с RFC. Но если администратору удобнее редактировать текстовые файлы, чем пользоваться DNS Manager, то в ОС Windows NT 4.0 есть возможность настроить DNS-сервер так, чтобы применялся загрузочный файл.

Загрузочный файл определяет поведение DNS-сервера во время старта. Команды в него записываются с начала строк, без предшествующих пробелов. Допустимы команды: *directory*, *cache*, *primary* и *secondary*.

| Команда | Описание |
|---|---|
| *directory* | Указывает на каталог, содержащий другие файлы, на которые ссылаются команды |
| *cache* | Указывает файл, при помощи которого DNS-сервер взаимодействует с серверами корневого домена. Эта команда обязательно должна присутствовать в загрузочном файле. Кэш-файл, пригодный для работы в Интернете, поставляется с Windows NT 4.0 |
| *primary* | Задает домен, за который отвечает данный сервер имен, и файл БД, содержащий исходные записи для этого домена (то есть файл зоны). В загрузочном файле может быть несколько таких команд |
| *secondary* | Задает домен, за который отвечает этот сервер имен (как резервный DNS-сервер), и список IP-адресов главных серверов, от которых можно получить зональную информацию. Кроме того, задает имя локального файла для кэширования этой зоны. В загрузочном файле может быть несколько таких команд |

В следующей таблице показаны синтаксис и примеры команд для загрузочного файла.

| Синтаксис | Пример |
|---|---|
| *directory* [*каталог*] | `directory c:\winnts\system32\dns` |
| *cache*.[*имя_файла*] | `cache.cache` |
| *primary* [*домен*] [*имя_файла*] | `primary microsoft.com microsoft.dns`<br>`primary dev.microsoft.com dev.dns` |
| *secondary* [*домен*] [*список_узлов*] [*имя локального_файла*] | `secondary test.microsoft.com 157.55.200.100 test.dns` |

## Резюме

Типичный DNS-сервер использует четыре конфигурационных файла. Файл базы данных содержит исходные записи для домена. Файл обратного просмотра необходим для разрешения обратных запросов. Кэш-файл содержит имена и адреса DNS-серверов, которые отвечают за корневой домен. Загрузочный — это файл начальных параметров для DNS-сервера Berkeley Internet Daemon Server.

# Занятие 4. Использование DNS

Конфигурация DNS-серверов зависит от таких факторов, как размер Вашей организации, ее расположение, а также от требований, предъявляемых к отказоустойчивости. На этом занятии Вы получите представление о настройке DNS для Вашего узла и изучите сценарии, по которым сможете оценить свои знания о планировании сетей.

**Изучив материал этого занятия, Вы сможете:**

- ✓ зарегистрировать DNS-сервер в родительском домене;
- ✓ оценить, сколько DNS-серверов, доменов и зон требуется для Вашей сети.

**Продолжительность занятия — 40 минут**

Организации, имеющей небольшую сеть, стоит использовать DNS-клиенты, которые взаимодействуют с DNS-сервером поставщика услуг Интернета (Internet Service Provider, ISP). Большинство из них будут готовы поддерживать Ваш домен за незначительную плату. Однако если Вы хотите сэкономить деньги или желаете полностью контролировать свой домен, то Вам придется создать собственный DNS-сервер.

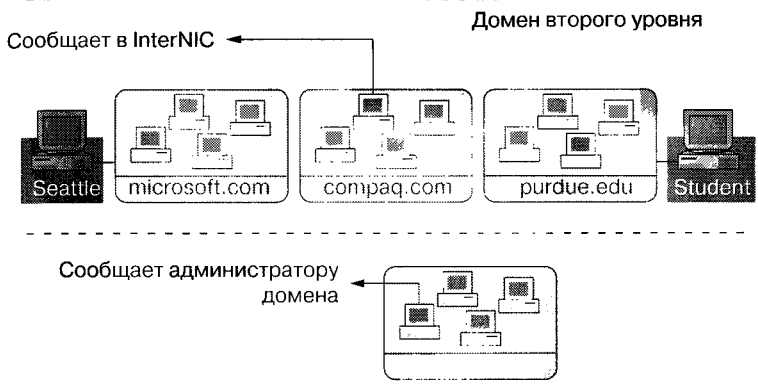
Чтобы войти в Интернет в качестве домена второго уровня, организация любого масштаба должна сообщить в InterNIC имя своего домена и IP-адреса, как минимум, двух DNS-серверов, обслуживающих этот домен. Установка и конфигурирование DNS-серверов внутри организации может проходить независимо от Интернета.

Для обеспечения надежности Microsoft рекомендует использовать в одном домене, как минимум, два DNS-сервера — основной и резервный. Первый поддерживает базу данных, которая дублируется (тиражируется) на втором. Такая схема позволяет обрабатывать запросы даже при выходе из строя одного DNS-сервера. Частоту тиражирования задают в соответствии с тем, как часто в домене изменяются имена, при этом необходимо, чтобы последние изменения были известны обоим серверам. Однако слишком частое тиражирование без надобности перегружает сеть и сами DNS-серверы.

## Регистрация в родительском домене

После установки и настройки DNS-сервера или серверов, Вам необходимо их зарегистрировать на DNS-сервере, который расположен уровнем выше в иерархической структуре DNS. На следующей иллюстрации приведен пример регистрации DNS-сервера в вышележащем домене. Родительской системе необходимо знать имена и IP-адреса Ваших DNS-серверов. Возможно, потребуется дополнительная информация, например

дата начала работы домена, а также имена и почтовые адреса ответственных за работу домена.




Если *родительский домен* (parent domain) расположен ниже второго уровня, необходимо выяснить у его администратора, какую информацию Вы должны предоставить.

Примечание Если Вы регистрируетесь в поддомене или выше, обратитесь в интерактивную регистрационную службу InterNIC — *http://internic.net*. Если у Вас возникли трудности или вопросы при регистрации, то позвоните в центр поддержки — (703) 742-477.

## Упражнения

Здесь приведены три сценария реализации DNS. Фабула такова: компания переходит на Windows NT Server и хочет использовать *службу каталогов* (directory services).

Вам придется оценить необходимое количество DNS-серверов, доменов и зон, а также разрешить несколько вопросов, связанных с проектированием конфигурации DNS для каждой компании.

Проработав эти сценарии, Вы реально оцените Ваши знания о планировании сетей, прежде чем приступите к установке DNS.

### Сценарий 1. Проектирование DNS для небольшой сети

Предположим, компания XYZ собирается менять устаревший компьютер среднего класса на компьютер, работающий под управлением Windows NT Server 4.0.

Прежде большая часть персонала получала к нему доступ посредством терминалов. Компьютеры одних сотрудников на базе i486, а других — на базе Pentium, но они не подключены к сети.

Сеть в основном собираются использовать для совместного доступа к файлам и принтерам, но планируется иметь один сервер Windows NT, на котором будет работать SQL Server. Большинству пользователей понадобится доступ к компьютеру, на котором выполняется Microsoft SQL Server. Рабочие приложения установят на локальных компьютерах но все файлы данных будут храниться на серверах.

Кроме того, компания XYZ желает подключиться к Интернету, чтобы использовать электронную почту.

Спланируйте основные характеристики сети, используя данные таблицы.

| Компоненты окружения | Описание |
|---|---|
| Пользователи | 100 человек |
| Расположение | В одном офисе |
| Администрирование | Один постоянный администратор |
| Серверы | 3 компьютера: два — Pentium-120, 32 Мб RAM, 3,2 Гб жесткий диск; один — Pentium-150, 128 Мб RAM, выделен под Exchange Server |
| Клиенты | Все компьютеры на базе Pentium или i486, работают под управлением Windows NT 4.0 или Windows 95 |
| Приложения Microsoft BackOffice | Exchange Server и DNS |
| Использование сервера | Хранение файлов и печать |

На принятие решений влияет:

- количество пользователей;
- количество административных единиц;
- количество узлов.

1. Сколько доменов Вам понадобится?

_____

2. Сколько поддоменов Вам понадобится?

_____

3. Сколько зон Вам понадобится?

_____

4. Сколько основных DNS-серверов Вам понадобится?

_____

5. Сколько резервных DNS-серверов Вам понадобится?

6. Сколько кэширующих DNS-серверов Вам понадобится?

## Сценарий 2. Проектирование DNS для сети среднего размера

Предположим, Вы консультант компании WXY, в которой 8 795 пользователей. Около 8 000 подключены к четырем основным узлам, а остальные работают в филиалах — в десяти крупных городах США. Компания решила перейти на серверы Windows NT. Кроме того, решено централизовать все учетные записи пользователей в одном месте — в главном офисе.

Четыре основных узла связаны линиями T1. Каждый филиал соединен с ближайшим из основных узлов линией 56 кбит/с.

Три из четырех основных узлов работают независимо от других. Четвертый — главный офис корпорации. От 25 до 250 пользователям в филиалах постоянно требуется доступ ко всем четырем основным узлам и изредка — к другим филиалам.

Кроме десяти филиалов компании принадлежит временный исследовательский центр, в котором работают 10 человек. Там установлен один сервер, который соединяется с сервером в Бостоне (см. рис.) по телефонным каналам при помощи маршрутизаторов, обеспечивающих при необходимости временные модемные соединения. Этот узел, работающий самостоятельно и нуждающийся в связи только для отправки сообщений, планируется закрыть в течение 6 месяцев.

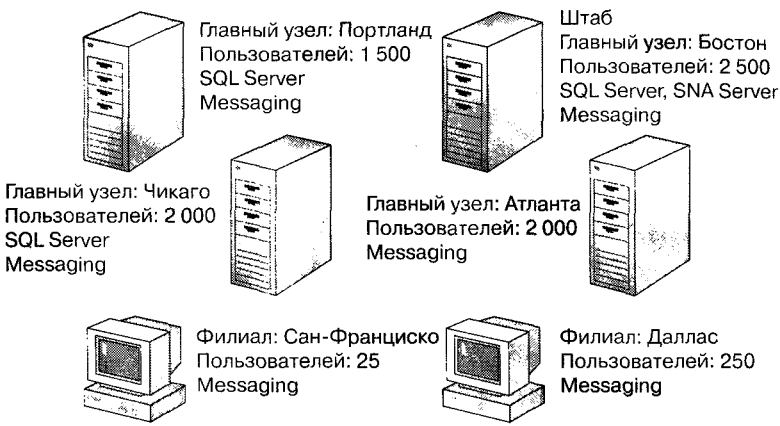
Предполагается, что главные узлы и филиалы продолжат работу на имеющемся оборудовании. В данный момент линии связи загружены на 60%. В ближайшие 12—18 месяцев существенно расширять сеть не собираются.

Спланируйте основные характеристики сети, используя данные таблицы.

| Компоненты окружения | Описание |
|---|---|
| Пользователи | 8 795 человек |
| Расположение | 4 главных узла и 10 филиалов в крупных городах США. Открытие зарубежных филиалов не планируется |
| Администрирование | Постоянные администраторы на каждом из четырех главных узлов. На некоторых небольших узлах администраторы работают по совместительству |

(*продолжение*)

| Компоненты окружения | Описание |
|---|---|
| Количество серверов имен | Надо определить |
| Количество кэширующих серверов | Для каждого района и его зоны нужен кэширующий DNS-сервер |
| Клиенты | Компьютеры на базе i386, i486 и Pentium, работают под управлением Windows NT и Windows 95 |
| Серверные приложения | SQL Server, Exchange Server и DNS |




В число других филиалов входят: Лос-Анджелес — 40 пользователей; Солт-Лейк-Сити — 25 пользователей; Монреаль — 30 пользователей; Новый Орлеан — 25 пользователей; Канзас-Сити — 25 пользователей; Вашингтон, округ Колумбия — 100 пользователей; Денвер — 200 пользователей; Майами — 75 пользователей.

На решение влияет:

- количество пользователей;
- количество административных единиц;
- количество узлов;
- скорость и качество линий связи между узлами;
- допустимая полоса пропускания линий связи;
- ожидаемые изменения в сети;
- набор приложений для бизнеса.

1. Сколько доменов Вам понадобится?

2. Сколько поддоменов Вам понадобится?

3. Сколько зон Вам понадобится?

4. Сколько основных DNS-серверов Вам понадобится?

5. Сколько резервных DNS-серверов Вам понадобится?

6. Сколько кэширующих DNS-серверов Вам понадобится?

7. Используя приведенную ниже таблицу расстояний (в милях), распределите филиалы по зонам: филиал должен находиться в той же зоне, что и ближайший к нему главный узел.

| Портланд, шт. Орегон | Бостон | Чикаго | Атланта |
|---|---|---|---|

| Таблица расстояний | Атланта | Бостон | Чикаго | Портланд, шт. Орегон |
|---|---|---|---|---|
| **Даллас** | 807 | 1 817 | 934 | 2 110 |
| **Денвер** | 1 400 | 1 987 | 1 014 | 1 300 |
| **Канзас-Сити** | 809 | 1 454 | 497 | 1 800 |
| **Лос-Анджелес** | 2 195 | 3 050 | 2 093 | 1 143 |
| **Майами** | 665 | 1 540 | 1 358 | 3 300 |
| **Монреаль** | 1 232 | 322 | 846 | 2 695 |
| **Новый Орлеан** | 494 | 1 534 | 927 | 2 508 |
| **Солт-Лейк-Сити** | 1 902 | 2 403 | 1 429 | 800 |
| **Сан-Франциско** | 2 525 | 3 162 | 2 187 | 700 |
| **Вашингтон** | 632 | 435 | 685 | 2 700 |

## Сценарий 3. Проектирование DNS для крупной сети

Во всех филиалах компании ABC работают 60 000 человек. Ее штаб расположен в Женеве (Швейцария). Головной офис для Северной и Южной Америки находится в Нью-Йорке, а для Австралии и Азии — в Сингапуре. Каждый из головных офисов полностью контролирует пользователей в своем регионе.

Работникам компании необходимо иметь доступ к ресурсам головных офисов всех регионов. Три региональных головных узла соединены линиями T1. В каждом из них есть набор приложений, которые должны быть доступны всем узлам своих регионов и офисам других регионов. В Малазийском и Австралийском филиалах находятся главные производственные мощности. К их узлам необходим доступ всех остальных филиалов.

Все деловые приложения выполняются под управлением ОС Windows NT Server. Эти компьютеры будут назначены серверами в своих доменах.

Линии связи между Сингапуром, Австралией и Малазией загружены на 90%. В Азиатском и Австралийском регионах имеется 10 дочерних компаний — в Австралии, Китае, Индонезии, Японии, Корее, Малазии, Новой Зеландии, Сингапуре, Таиланде и на Тайване.

В связи с ограничениями импорта в некоторые филиалы было решено предоставить им право самостоятельно закупать оборудование и поддерживать домены. В последнее время большая часть компьютеров, приобретенных филиалами, работает под управлением Windows NT Workstation. Компания позволяет при необходимости закупать дополнительное оборудование.

Для простоты вопросы будут касаться только Азиатско-Австралийского региона.

Спланируйте основные характеристики, используя данные таблицы.

| Компоненты окружения | Описание |
|---|---|
| Пользователи | 25 000 человек, которые иногда мигрируют между филиалами |
| Расположение | Региональный штаб находится в Сингапуре, 10 филиалов в Австралии, Китае, Индонезии, Японии, Корее, Малазии, Новой Зеландии, Сингапуре, Таиланде и на Тайване |
| Администрирование | Постоянные администраторы во всех региональных штабах и в каждом филиале |
| Количество доменов | Необходимо оценить |
| Клиенты | Все компьютеры на базе Pentium, i486 или i386, работают под управлением Windows NT Workstation или Windows 95 |
| Серверные приложения | SLQ Server, SNA Server, Systems Management Server, Messaging и DNS |
| Количество кэширующих серверов | Необходимо оценить |

На решение влияет:

- количество пользователей;
- количество административных единиц;
- количество узлов;
- скорость и качество линий связи между узлами;
- допустимая полоса пропускания линий связи;
- ожидаемые изменения в сети;
- набор приложений для бизнеса.

1. Сколько доменов Вам понадобится?

2. Сколько поддоменов Вам понадобится?

3. Сколько зон Вам понадобится?

4. Сколько основных DNS-серверов Вам понадобится?

5. Сколько резервных DNS-серверов Вам понадобится?

6. Сколько кэширующих DNS-серверов Вам понадобится?

## Резюме

Исходя из размера и структуры организации, Вы, возможно, захотите использовать DNS в Вашей сети. Однако, для небольшой сети лучше применять DNS-клиенты, которые используют DNS-сервер, поддерживаемый поставщиком услуг Интернета. Если организация собирается подключиться к Интернету, нужно сообщить об этом в InterNIC.

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Назовите три основных компонента DNS.

2. Объясните различие между основным, резервным и главным серверами имен.

3. Перечислите три причины, по которым надо создавать резервный сервер имен.

4. Опишите различие между доменом и зоной.

5. Чем отличаются рекурсивные и итеративные запросы?

6. Перечислите файлы, необходимые для реализации DNS в ОС Windows NT.

7. Каково назначение загрузочного файла?

# Дополнительная информация

- Paul Albitz and Cricket Liu. «DNS and BIND», издательство O'Reilly & Associates;
- Статья «DNS and Microsoft Windows NT 4.0».


# Внедрение DNS



## В этой главе

Из этой главы Вы узнаете об установке и конфигурировании DNS, интегрировании служб DNS и WINS, а также об использовании NSLOOKUP — утилиты для диагностики DNS. Во время занятий Вы установите и сконфигурируете DNS, настроите файлы, используемые DNS, и опробуете DNS-серверы для разрешения имен узлов в IP-адреса.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить Microsoft Windows NT Server 4.0 и протокол TCP/IP;
- освоить материал главы 12.

# Занятие 1. Сервер Microsoft DNS

В состав ОС Windows NT 4.0 входит стандартная служба DNS. На этом занятии описывается внедрение сервера Microsoft DNS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ установить службу Microsoft DNS Server;
- ✓ использовать утилиту Nslookup при решении проблем, связанных с DNS.

**Продолжительность занятия — 25 минут**

Microsoft DNS — это DNS-сервер, соответствующий RFC, поэтому он создает и использует стандартный файл зоны DNS и поддерживает все стандартные типы ресурсных записей. Он совместим с остальными DNS-серверами и включает в свой состав диагностическую утилиту — Nslookup. Microsoft DNS легко интегрируется с WINS, а управляется при помощи утилиты DNS Manager, имеющей стандартный графический интерфейс.

## Установка Microsoft DNS Server

Прежде чем устанавливать для ОС Microsoft Windows NT службу DNS Server, важно убедиться, что на сервере Windows NT 4.0 правильно сконфигурирован протокол TCP/IP. По умолчанию служба DNS Server получает в качестве имени узла и домена те значения, что заданы в диалоговом окне **Microsoft TCP/IP Properties**. Записи типа SOA и NS создаются на основе этих имен. Если же имя узла и домена не указаны, то будут созданы только записи типа SOA.

### Упражнения

Примечание Если Вы еще не установили Windows NT 4.0 Service Pack, сделайте это сейчас. В разделе «Инструкции по установке» статьи «Об этой книге» описано, как установить Service Pack с прилагаемого к курсу компакт-диска.

На этом занятии Вы установите службу Microsoft DNS Server. Настройкой DNS Вы займетесь на последующих занятиях.

Примечание Выполняйте это задание на компьютере, выполняющем роль DNS-сервера.

▶ **Задание порядка поиска для сервиса DNS Server**

1. Войдите в систему как *Administrator*.
2. В командной строке введите *ipconfig* и нажмите ENTER.
3. Запишите IP-адрес Вашего компьютера.

---

4. Перейдите в диалоговое окно **Microsoft TCP/IP Properties** и щелкните вкладку **DNS**.
5. В поле ввода **Domain** введите *Domain1* (или имя Вашего домена).
6. Щелкните кнопку **Add** под списком **DNS Service Search Order**.
7. В поле ввода **DNS Server** задайте IP-адрес Вашего компьютера и щелкните кнопку **Add**.
8. Щелкните **OK**.

   Появится диалоговое окно **Network**.
9. Щелкните **OK** для закрытия диалогового окна **Network**

▶ **Установка сервиса DNS Server**

1. В **Control Panel** дважды щелкните пиктограмму **Network**, а затем — **Services**.
2. Щелкните **Add**.

   Появится диалоговое окно **Select Network Service**.
3. В списке **Network Service** щелкните **Microsoft DNS Server**, а затем — **OK**.

   Программа установки Windows NT выведет диалоговое окно, в котором надо указать полный путь к установочным файлам Windows NT.
4. Введите путь к установочным файлам Windows NT, щелкните **Continue**.

   Все необходимые файлы, включая файлы примеров, будут скопированы на жесткий диск.
5. В диалоговом окне **Network** щелкните **Close**.
6. Когда появится предложение перезагрузить компьютер, щелкните **Yes**.

## Поиск и устранение проблем с DNS средствами Nslookup

Утилита Nslookup — основной диагностический инструмент для DNS, позволяющий Вам взаимодействовать с DNS-сервером. При помощи Nslookup можно просматривать ресурсные записи на DNS-серверах, в том числе и на серверах DNS под управлением UNIX. Эта утилита устанавливается совместно с протоколом TCP/IP.

### Режимы работы утилиты Nslookup

Утилита Nslookup может работать в двух режимах: интерактивном и пошаговом. Если Вы хотите просмотреть небольшое количество данных, то

используйте пошаговый режим (или режим командной строки), если же — большое количество, то лучше работать в интерактивном режиме.

## Параметры утилиты Nslookup

Синтаксис использования Nslookup выглядит так:

```
nslookup [-опция...][искомый_компьютер|-[сервер]]
```

| Параметр | Описание |
|---|---|
| *-опция* | Задает одну или несколько команд Nslookup. Полный список команд Вы получите, щелкнув пункт **Help** из меню Nslookup |
| *искомый_компьютер* | Если это — IP-адрес, а тип запрашиваемой записи A или PTR, то утилита возвратит имя компьютера. Если же это — имя, которое не оканчивается точкой, то оно будет дополнено именем текущего домена. Для исследования компьютера, расположенного за пределами текущего домена, необходимо после его имени поставить точку. Если вместо *искомый_компьютер* ввести дефис (-), то Nslookup перейдет в интерактивный режим |
| *сервер* | Задаст использование указанного сервера в качестве DNS-сервера. Если этот параметр не указан, то используется текущий DNS-сервер, заданный в параметрах системы |

▶ **Использование Nslookup в пошаговом режиме**

1. Измените свойства командной строки так, чтобы размер экранного буфера стал равным 50.

   Для этого используйте вкладку **Layout**.
2. Если окно командной строки не в полноэкранном режиме, нажмите ALT+ENTER.
3. Введите следующую команду:

   ```
   nslookup узел
   ```

   где *узел* — это имя узла в Вашем домене.

   Утилита Nslookup возвратит IP-адрес компьютера с именем *узел*, поскольку эта информация хранится в базе данных DNS.
4. Выйдите из командной строки.

### Описание команд Nslookup

Описание команд утилиты Nslookup Вы найдете в справочной системе Windows NT. Вызовите ее и задайте поиск по ключевому слову *nslookup*. Щелкните **Nslookup commands** для просмотра списка всех команд.

▶ **Использование Nslookup в интерактивном режиме**

1. В командной строке введите *nslookup* и нажмите ENTER.

   Появится значок приглашения ( > ).
2. Наберите *set all.*

   Эта команда выведет список всех текущих значений параметров утилиты Nslookup.
3. Обратитесь к справочной системе Windows NT, а затем, используя команду *set,* установите значение *time-out* (тайм-аут) равным 1 секунде, а значение *number of retries* (количество попыток) — равным 7 секундам. При помощи *set all* убедитесь, что эти значения изменились.

   ```
   Set ti=1
   Set ret=7
   ```
4. Переключитесь в DNS Manager и узнайте количество узлов в домене.
5. Переключитесь обратно в командную строку.
6. В ответ на приглашение ( > ) введите имена других компьютеров, после каждого нажимая ENTER.
7. Переключитесь в DNS Manager и нажмите F5.

   Имена всех компьютеров, которые можно определить, будут добавлены в базу данных зоны.
8. Выйдите из командной строки.
9. Закройте Windows NT Help и DNS Manager.

## Резюме

Служба Microsoft DNS совместима с другими DNS-серверами. Перед установкой службы DNS Server Вы должны убедиться, что протокол TCP/IP на сервере Windows NT 4.0 сконфигурирован корректно.

Утилита Nslookup — основное диагностическое средство для DNS. Она позволяет просматривать ресурсные записи на DNS-серверах.

# Занятие 2. Администрирование DNS-сервера

Администрировать DNS-сервер можно двумя способами — используя DNS Manager или вручную редактируя конфигурационные файлы. На этом занятии рассматриваются инструменты, используемые для администрирования DNS-сервера.

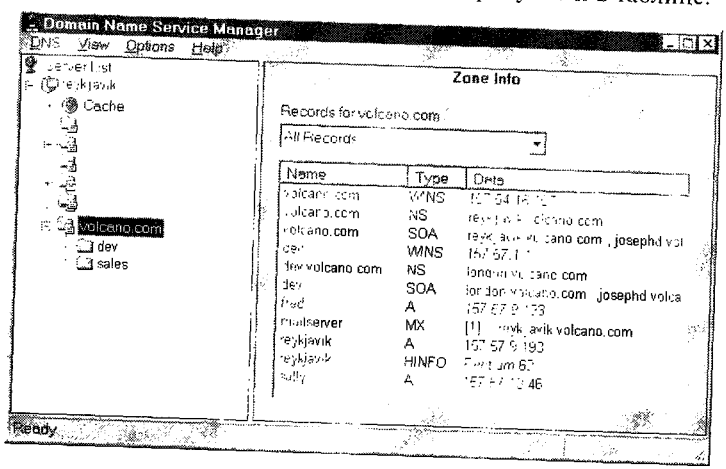
**Изучив материал этого занятия, Вы сможете:**

- ✓ администрировать DNS-сервер;
- ✓ создать файл зоны и заполнить его ресурсными записями.

**Продолжительность занятия — 60 минут**

## Настройка параметров сервиса DNS Server

Вы можете средствами DNS Manager задать свойства DNS-сервера Microsoft Windows NT. Поскольку изначально DNS-сервер не имеет никакой информации о сети пользователя, то он устанавливается как кэширующий сервер для работы в Интернете. Это означает, что DNS-сервер имеет только информацию о корневых серверах сети Интернет. Для выполнения большинства дополнительных функций необходима специальная информация, что показано на рисунке и в таблице.



| Свойство | Описание |
|---|---|
| Interfaces (Интерфейсы) | Определяет, с какими сетевыми интерфейсами работает DNS-сервер на компьютере, где установлено *несколько сетевых интерфейсов* (multihomed). По умолчанию используются все интерфейсы |
| Forwarders (Экспедиторы) | Заставляет Ваш сервер использовать другой сервер для перенаправления сообщений. Сервер имен может быть подчиненным для другого сервера, перенаправляющего сообщения |
| Boot method (Способ загрузки) | Определяет способ, которым сервер имен загружает параметры, — либо из реестра, либо из конфигурационных файлов |

## Упражнения

Вы сконфигурируете DNS, настроите файлы DNS, а также примените службу DNS для разрешения имен узлов в их IP-адреса.

Примечание Для выполнения этих упражнений Вам необходимы два компьютера: один — DNS-сервер, а другой — DNS-клиент.

Просмотрите службу Windows NT DNS Server, установленную по умолчанию.

▶ **Осмотр установленного по умолчанию DNS-сервера**

Примечание Выполняйте это задание на компьютере — DNS-сервере.

1. Войдите в систему как *Administrator*.
2. Щелкните кнопку **Start**, укажите на **Programs**, затем — на **Administrative Tools** и щелкните **DNS Manager**.
3. В меню **DNS** щелкните **New Server**.

   Появится диалоговое окно **Add DNS Server**.
4. В поле **Add DNS Server** введите *Server1* и щелкните **OK**.
5. Дважды щелкните кнопку **Cache**.

   Вы увидите всю информацию, которая содержится в кэше DNS-сервера. В нем всегда есть информация о корневых серверах Интернета.
6. В меню **Options** щелкните **Preferences**.

   Появится диалоговое окно **Preferences**.
7. Щелкните **Show Automatically Created Zones**, а затем — **OK**.

8. Щелкните имя Вашего компьютера и нажмите F5 для обновления содержимого окна **DNS Manager**.

   Вы увидите три зоны обратного просмотра: *0.in-addr.arpa*, *127.in-addr.arpa* и *255.in-addr.arpa*.

9. Дважды щелкните каждую из них.

   Какие типы записей они содержат?

   _____

10. Дважды щелкните *127.in-addr.arpa*.

    Появится папка под именем **0**.

11. Дважды щелкните папку **0**.

    Появится вторая папка **0**.

12. Дважды щелкните вторую папку **0**.

    Появятся записи типа PTR для локального узла. Они используются при обратном просмотре по адресу 127.0.0.1.

    В данный момент служба DNS Server, установленная на Вашем компьютере, сконфигурирована как кэширующий сервер имен.

### Ручное конфигурирование DNS

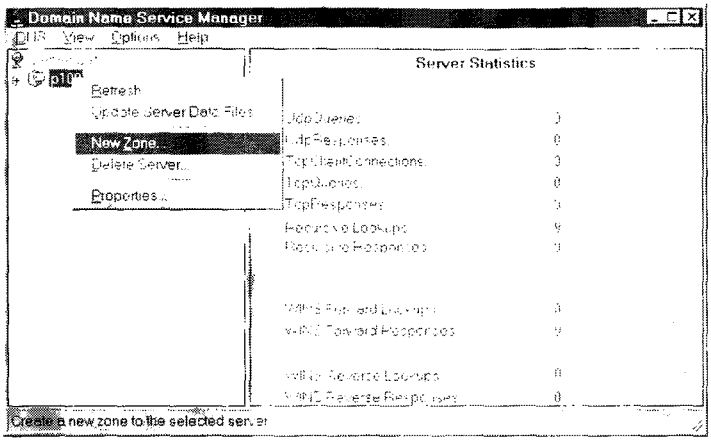
DNS-сервер можно настроить вручную, редактируя файлы, которые по умолчанию находятся в каталоге *\system_root*\System32\Dns. В этом случае администрирование аналогично администрированию традиционной службы DNS, описанной в RFC. Эти файлы можно изменять, используя обычный редактор текстов. После этого необходимо остановить и перезапустить службу DNS.

## Добавление доменов и зон

Первый шаг при конфигурировании DNS-сервера — определение иерархической структуры Ваших доменов и зон. Далее эту информацию необходимо при помощи DNS Manager внести в конфигурацию DNS.

### Добавление основных или резервных зон

Основные и резервные зоны добавляются при помощи DNS Manager, что показано на следующей иллюстрации. DNS Manager сгенерирует имя по умолчанию для файла зоны. Если он уже существует, то DNS Manager автоматически импортирует в него эти записи.




Соответствия имен и IP-адресов основной зоны хранятся локально. При настройке основной зоны Вам не понадобится никакая другая информация, кроме имени зоны.

Резервные зоны получают соответствия имен и IP-адресов от главного сервера путем зональной передачи. При настройке резервной зоны Вам понадобится имя зоны и имена главных серверов имен.

---

Примечание По соглашению, принятому Microsoft, в ОС Windows NT создается файл с именем *имя_зоны*.dns, что отличается от других DNS-серверов, которые создают файл с именем Db.zone.

---

## Добавление поддоменов

После того как в сервер занесена информация обо всех зонах, можно создавать поддомены. Для этого в контекстном меню выбранной зоны щелкните **New Domain**. Введите имя нового поддомена и щелкните **OK**.

Если нужно задать вложенные поддомены, создавайте каждый последующий, используя пункт **New Domain** контекстного меню предыдущего.

В реестре существуют разделы для каждой зоны ответственности DNS. Они являются подразделами в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zones

Для каждой зоны есть свой подраздел. В нем содержится имя файла базы данных, по которому можно определить, является ли DNS-сервер основным или резервным. Например, зоне *dev.volcano.com* в реестре соответствует следующая запись:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zones\dev.volcano.com

## Конфигурирование свойств зоны

| Свойство | Описание |
|---|---|
| General | Задает параметры файла зоны и указывает, является этот сервер основным или резервным сервером имен |
| SOA record | Конфигурирует параметры зональной передачи и почтовый ящик администратора сервера имен |
| Notify | Определяет, информировать ли резервные серверы при изменениях в базе данных основного сервера. Кроме того, Вы можете усилить защиту DNS-сервера, задав список резервных серверов, которые имеют право обращаться к этому серверу |
| WINS lookup | Включает использование WINS при разрешении имен. Список серверов WINS вы можете задать прямо в этом диалоговом окне — по принципу «для отдельного сервера имен» (per-name-server), отметив флажок **Settings Only Affect Local Server**. Если он не установлен, резервные серверы тоже смогут обращаться к заданным серверам WINS |

## Упражнения

В этом упражнении Вы зададите DNS-серверу основную зону.

▶ **Добавление зоны**

Примечание Выполняйте это упражнение на компьютере, работающем DNS-сервером.

1. Щелкните правой кнопкой мыши имя Вашего компьютера, а затем щелкните **New Zone**.

   Появится диалоговое окно **Creating New Zone for Server1**.
2. Щелкните **Primary**, а затем — **Next**.
3. В поле ввода **Zone Name** введите *zone1.com* (где *zone1.com* — имя Вашей зоны).
4. Нажмите клавишу TAB.

   В поле **Zone File** будет автоматически занесено *zone1.com.dns*.
5. Щелкните **Next**, а затем — **Finish**.

   Теперь в списке **Server List** есть имя зоны и добавлены записи **Zone Info**.

6. Щелкните каждую ресурсную запись.
   Какие типы записей содержит каждая из них?

7. Щелкните имя Вашей зоны.
8. В меню **DNS** щелкните **Properties**.
   Появится диалоговое окно **Zone Properties**.
9. Щелкните вкладку **Notify**.

Примечание Если бы Вы настроили резервный DNS-сервер для Вашего домена, его следовало бы указать в поле **Notify List** и щелкнуть **Add**.

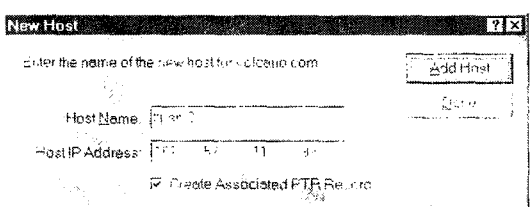
10. Щелкните **OK***.

## Добавление ресурсных записей

После того как были заданы зоны и поддомены, можно заносить ресурсные записи. Для этого выделите зону или поддомен и щелкните **DNS-New Host** или выберите **New Record** в меню.

### Новый узел

Для задания нового узла введите его имя и IP-адрес, затем установите флажок **Create Associated PTR Record,** чтобы в соответствующем домене обратного просмотра была создана необходимая запись.




### Новая запись

При создании новой записи необходимо указать ее тип. В диалоговом окне отражены соответствующие поля, характерные для выбранного типа записи, что показано на следующей иллюстрации. Поле TTL содержит значение времени жизни по умолчанию для записей типа SOA файла зоны. Само значение TTL сохраняется в записи, только если оно отличается от значения по умолчанию. Задайте всю информацию и щелкните **OK,** чтобы добавить ресурсную запись.

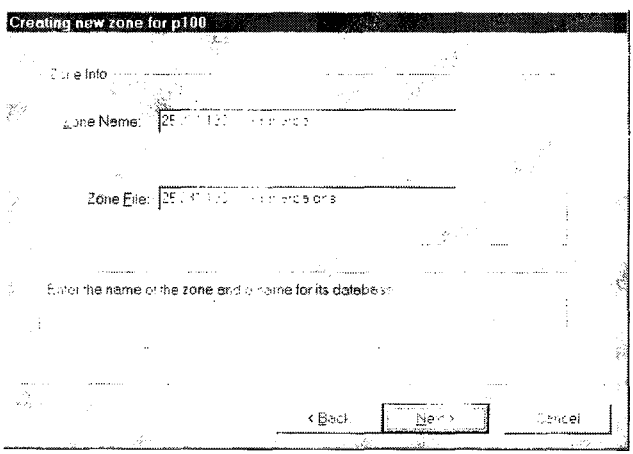
* Следует иметь ввиду, что удаление зоны при помощи DNS Manger не убирает файл с диска физически. Поэтому, чтобы после создать зону заново, необходимо удалить соответствующий файл. — *Прим. перев.*

## Настройка обратного просмотра

Для того чтобы по заданному IP-адресу находить имя узла, необходимо создать зоны обратного просмотра для каждой сети, в которой находятся узлы, занесенные в базу данных DNS. Создание зоны обратного просмотра практически идентично созданию зоны любого другого типа, только имя другое.

Например, если узел имеет IP-адрес 198.231.25.89, то в домене *in-addr.arpa* он будет представлен именем *89.25.231.198.in-addr.arpa*. Более того, чтобы клиент, который знает его IP-адрес, смог определить его имя, необходимо создать зону DNS с именем *25.231.198.in-addr.arpa*, что показано на иллюстрации.

Все указательные записи для сети 198.231.25.0 должны быть занесены в эту зону обратного просмотра.




### Упражнения

Вы создадите зону обратного просмотра, которая позволит службе DNS определить имя по полученному в запросе IP-адресу.

► **Задание зоны обратного просмотра на основном DNS-сервере**

Примечание Выполняйте это задание на компьютере — DNS-сервере.

1. Определите, какое имя надо дать зоне обратного просмотра на основном DNS-сервере. Для этого воспользуйтесь одним из перечисленных правил.

- Для адресов класса A, добавьте первое число IP-адреса к *.in-addr.arpa* (например, для IP-адреса класса A 29.122.15.88 зона обратного просмотра должна иметь имя *29.in-addr.arpa*).
- Для адресов класса B, добавьте первые два числа IP-адреса в обратном порядке к *.in-addr.arpa* (например, для IP-адреса класса B 129.122.15.88 зона обратного просмотра должна иметь имя *122.129.in-addr.arpa*).
- Для адресов класса C, добавьте первые три числа IP-адреса в обратном порядке к *.in-addr.arpa* (например, для IP-адреса класса C 219.122.15.88 зона обратного просмотра должна иметь имя *15.122.219.in-addr.arpa*).

Какое имя имеет Ваша зона обратного просмотра?

---

2. Откройте **DNS Manager** и щелкните имя Вашего компьютера.
3. В меню **DNS** щелкните **New Zone**.

   Появится диалоговое окно **Creating New Zone**.
4. Щелкните **Primary**, а затем — **Next**.
5. Введите имя зоны обратного просмотра в поле **Zone Name**.
6. При помощи клавиши TAB перейдите в поле **Zone File**.

   Имя файла будет автоматически подставлено в это поле.
7. Щелкните **Next**, а затем — **Finish**.

---

Примечание Если Вы настраиваете параметры зоны для резервного DNS-сервера, необходимо ввести его IP-адрес на вкладке **Notify** в диалоговом окне **Zone Properties**.

---

В этом задании Вы добавите имя узла в Ваш домен.

### ► Добавление другого компьютера в домен в качестве узла

---

Примечание Выполняйте это задание на компьютере — DNS-сервере.

---

1. Щелкните правой кнопкой мыши имя Вашей зоны.
2. В появившемся меню щелкните **New Host**.

   Появится диалоговое окно **New Host**.
3. В поле **Host Name** введите имя второго компьютера.
4. В поле **Host IP Address** укажите IP-адрес второго компьютера.
5. Щелкните **Create Associated PTR Record**, а затем — **Add Host**.
6. Щелкните **Done**.
7. Щелкните зону *107.131.in-addr.arpa* и нажмите F5.

Перед *107.131.in-addr.arpa* появится знак плюс (+).

8. Дважды щелкните *107.131.in-addr.arpa*.

   Под строкой *107.131.in-addr.arpa* появится значок папки.

9. Дважды щелкните значок папки.

   В поле **Zone Info** появится запись **PTR**.

10. Дважды щелкните запись **PTR**, просмотрите содержимое этой записи, а затем щелкните **OK**.

    Это автоматически созданная запись для обратного просмотра, поскольку была выбрана опция **Create Associated PTR Record**.

11. Повторите пункты с 1 по 10, чтобы добавить запись для Вашего компьютера и обновить списки.
12. Удостоверьтесь, что в Вашу зону были добавлены две записи типа A (одна — для первого Вашего компьютера, а другая — для второго).
13. Удостоверьтесь, что в зоне обратного просмотра (*107.131.in-addr.arpa*) есть две записи типа PTR (одна — для первого Вашего компьютера, а другая — для второго).

## Резюме

Первым шагом при настройке DNS-сервера Microsoft Windows NT является определение иерархии доменов и зон DNS. После задания зон и поддоменов можно заносить ресурсные записи. Для того чтобы по заданному IP-адресу находить имя узла, надо создать зоны обратного просмотра для каждой сети, в которой находятся узлы, занесенные в БД DNS.

# Занятие 3. Интеграция DNS и WINS

Службу WINS проще эксплуатировать, чем DNS, поскольку она динамически регистрирует соответствия имен и IP-адресов. На этом занятии объясняется, почему и каким образом WINS можно использовать совместно с DNS.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить, как можно объединить DNS и WINS;
- ✓ настроить клиент WINS;
- ✓ настроить разрешение имен и обработку обратных запросов службой WINS;
- ✓ задать псевдонимы для имени узла.

**Продолжительность занятия — 45 минут**

База данных DNS, содержащая соответствия имен и IP-адресов, является статической, и изменения в нее вносятся вручную. В DNS реализована иерархическая модель, что позволяет разбить на зоны администрирование и репликацию базы данных.

С другой стороны, WINS позволяет компьютерам динамически регистрировать для себя соответствия имени и IP-адреса, что упрощает эксплуатацию. Но пространство имен WINS — одноуровневое, и кроме того, необходимо репликацией обеспечить хранение полной базы данных на каждом WINS сервере.

## Запись WINS

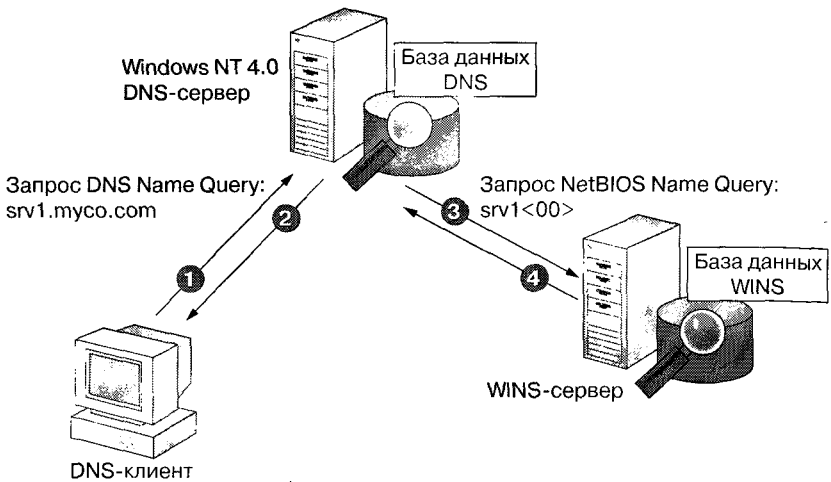
Новый тип записи — WINS — определен как часть файла базы данных и применяется только в Microsoft DNS. Для этого в корневой домен зоны вводится новая запись, сохраняемая в файле базы данных. Теперь, если в файле базы данных не найдено соответствие имени и IP-адреса, DNS обратится к базе данных сервера WINS.

1. Клиент связывается со своим DNS-сервером и запрашивает IP-адрес другого узла.

   DNS-сервер просматривает свою базу данных и не находит записи содержащей IP-адрес этого узла.

2. Поскольку в файле базы данных есть запись типа WINS, то DNS-сервер преобразует имя узла в NetBIOS-имя и посылает запрос на это имя серверу WINS.

3. Если сервер WINS может разрешить это имя, то он возвращает DNS-серверу IP-адрес.
4. DNS-сервер передает этот IP-адрес запрашивающему клиенту.

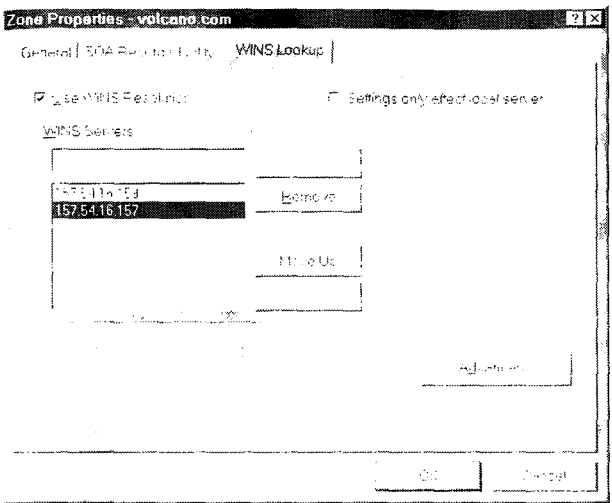



Примечание Если зона использует разрешение имен при помощи WINS, то все DNS-серверы, ответственные за эту зону, должны быть настроены на использование WINS.

## Возможность использования WINS

Включив WINS Lookup (Использовать WINS), Вы можете настроить DNS-сервер так: если он не может разрешить имя своими силами, то отправляет запросы серверу WINS.

Включите WINS Lookup посредством **DNS Manager**: выберите зону, откройте ее контекстное меню и укажите в нем **Properties**. Перейдите на вкладку **WINS Lookup**, установите флажок **Use WINS Resolution** и введите IP-адреса серверов WINS (это показано на иллюстрации).




## Обратный просмотр при помощи WINS

Присутствие записи типа WINS-R в корне зоны заставляет DNS-сервер использовать механизм *просмотра состояния адаптера узла NetBIOS* (NetBIOS node adapter status lookup). Этот механизм используется при выполнении запросов на обратное разрешение IP-адресов, для которых нет статически заданных PTR-записей.

Включение механизма обратного разрешения при помощи WINS осуществляется в DNS Manager. Надо вызвать свойства соответствующей зоны *in-addr.arpa*, перейти на страницу **WINS Reverse Lookup**, установить флажок **Use WINS Reverse Lookup** и затем — значение поля **DNS Host Domain**, которым будет дополняться обнаруженное NetBIOS-имя перед тем, как оно будет отправлено в качестве ответа клиенту.

## Время жизни для сервиса WINS

Значение WINS TTL можно задать на странице **Advanced**, которая вызывается с вкладки **WINS Lookup** окна свойств зоны. Когда сервер WINS успешно разрешает соответствие имени и IP-адреса, то IP-адрес сохраняется в кэше в течение времени **Cache Timeout Value**. По умолчанию это значение равно 10 минутам. Если этот IP-адрес пересылается другому DNS-серверу, то вместе с ним передается и TTL.

## Упражнения

В этих упражнениях Вы сконфигурируете сервер Windows NT, чтобы он использовал WINS для разрешения имен. В первом задании Вы настроите клиента WINS на использование основного сервера WINS.

► **Настройка клиента WINS**

Примечание Выполняйте это задание на компьютере — DNS-клиенте.

1. Перейдите в диалоговое окно **Microsoft TCP/IP Properties**.
2. Щелкните ярлык **WINS Address**.
3. В поле ввода **Primary WINS Server** введите IP-адрес WINS-сервера.
4. Щелкните **OK**, а затем — **Close**.

   Появится окно **Network Settings Change**, в котором Вам предлагается перезагрузить компьютер.
5. Щелкните **Yes**.

   Компьютер перезагрузится.
6. Войдите в систему как *Administrator*.

В этом задании Вы настроите DNS так, чтобы для имен, которые не удалось разрешить, применялся WINS.

► **Настройка разрешения имен при помощи WINS**

Примечание Выполняйте это задание на компьютере — DNS-сервере.

1. Запустите DNS Manager.
2. Щелкните правой кнопкой мыши имя Вашей зоны, затем щелкните **Properties**.

   Появится диалоговое окно **Zone Properties**.
3. Щелкните ярлык **WINS Lookup**.
4. Установите флажок **Use WINS Resolution**.
5. В поле **WINS Servers** введите IP-адрес Вашего WINS-сервера.
6. Щелкните **Add**, а затем — **OK**.

В этом упражнении Вы настроите DNS так, чтобы для тех IP-адресов, которые разрешить не удалось, применялся WINS.

► **Настройка обратного просмотра при помощи WINS**

Примечание Выполняйте это упражнение на компьютере — DNS-сервере.

1. Запустите DNS Manager.

2. Щелкните правой кнопкой мыши имя Вашей зоны обратного просмотра *107.131.in-addr.arpa*, а затем щелкните **Properties**.

   Появится диалоговое окно **Zone Properties**.
3. Щелкните ярлычок **WINS Reverse Lookup**.
4. Установите флажок **Use WINS Reverse Lookup**.
5. Введите имя вашей зоны в поле **DNS Host Domain, и щелкните OK**.

▶ **Тестирование обратного просмотра при помощи WINS**

Примечание Выполняйте это задание на компьютере — DNS-сервере.

1. В командной строке введите:

   ```
   nslookup 131.107.2.211
   ```

   где 131.107.2.211 — IP-адрес клиента.

   Утилита Nslookup покажет имя узла, поскольку в базе данных обратного просмотра есть запись для Вашего узла.
2. Введите:

   ```
   nslookup 131.107.2.200
   ```

   где 131.107.2.200 — IP-адрес Вашего сервера.

   Утилита NSLOOKUP покажет имя узла с IP-адресом 131.107.2.200, поскольку был включен обратный просмотр при помощи WINS. Кроме того, DNS автоматически добавит адресную запись в базу данных после разрешения IP-адреса.

## Резюме

Используя WINS, Вы можете настроить DNS сервер так, что, если соответствие имени и IP-адреса не определяется средствами DNS, запросы будут обрабатываться средствами сервера WINS. Включить использование WINS можно в диалоговом окне **Zone Properties** в DNS Manager.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Для чего необходимо задавать имя узла и имя домена в диалоговом окне настройки параметров DNS протокола TCP/IP *перед* установкой службы Microsoft DNS Server?

2. Каковы функции утилиты Nslookup?

3. Опишите процесс использования WINS.

4. Опишите ситуацию, когда полезно использовть WINS.

# Дополнительная информация

- Paul Albitz и Cricket Liu. «DNS and BIND», издательство O'Reilly and Associates.
- Статья «DNS and Microsoft Windows NT 4.0».


# Взаимодействие в гетерогенных средах



## В этой главе

В этой главе описано сетевое взаимодействие между компьютерами, применяющими NetBIOS и использующими другие механизмы, а также рассмотрены различные сетевые средства Microsoft Windows NT. Вы также узнаете, как устанавливать и конфигурировать Microsoft FTP-сервер и систему печати по TCP/IP.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо:

- установить Windows NT Server 4.0 с протоколом TCP/IP.

А также желательно иметь совместно используемый принтер для печати с применением протокола TCP/IP.

# Занятие 1. Общие сведения

Основное преимущество использования протокола TCP/IP в том, что он обеспечивает возможность взаимодействия с самыми различными типами компьютеров, например UNIX. Из этого занятия Вы узнаете о требованиях к соединениям с компьютерами, не поддерживающими NetBIOS и с применяющими NetBIOS в соответствии с RFC.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить требования к межсетевому взаимодействию в сетях Microsoft.

**Продолжительность занятия — 10 минут**

Протокол Microsoft TCP/IP, будучи общим, обеспечивает межсетевое взаимодействие со многими не поддерживающими NetBIOS компьютерами. Для связи с любым компьютером, например с системой на основе OS/2, UNIX, Solaris или VMS, Вам необходим общий сетевой протокол типа TCP/IP. Требуются также прикладные программы (обычно клиент/сервер) на компьютерах, между которыми устанавливается связь.

## Соединение с удаленным компьютером по сети Microsoft

Чтобы использовать стандартные команды и функции сети Microsoft (например, *net use*, Windows NT Explorer или File Manager) для соединения с удаленным компьютером, надо выполнить следующие требования:

- обеспечить *взаимодействие на уровне транспортного драйвера* (Transport Driver Connectivity): оба компьютера соединяются друг с другом, используя транспортный драйвер, например TCP/IP, NBF или IPX;
- обеспечить *взаимодействие посредством протокола SMB* (SMB Connectivity). Служба рабочей станции связывается с серверным процессом SMB на удаленном компьютере. SMB — это протокол *совместного использования файлов* (file-sharing protocol), применяемый во всех продуктах MS®-Net.

---

Примечание Если на удаленном компьютере установлен *идентификатор области видимости* NetBIOS (Scope ID), он должен соответствовать идентификатору области видимости Ваших компьютеров. В противном случае компьютеры не смогут установить связь, используя NetBIOS.

---

Многие производители реализовали NetBIOS поверх TCP/IP и SMB-серверы в своих операционных системах. Например, PATHWORKS для VMS компании Digital Equipment Corporation, LAN Server для OS/2 компании IBM и LAN Manager для UNIX.

### Соединение с сервером Windows NT с удаленного комьютера

Windows NT сервер обеспечивает файловые сервисы персональным компьютерам, используя протокол SMB (Server Message Block). Файловый сервис для UNIX-клиента доступен через протокол NFS (Network File System), FTP-сервис или при установке SMB-клиента.

Для Windows NT существуют NFS-серверы от сторонних производителей. С ними сервер Windows NT обеспечивает файловый сервис персональным компьютерам, рабочим станциям UNIX или другим системам, работающим как NFS-клиенты. Эти сервисы также поддерживают файловые системы NTFS, FAT, CDFS и HPFS.

## Утилиты Microsoft TCP/IP

Перечисленные в таблице утилиты Microsoft TCP/IP обеспечивают соединение с компьютерами на основе TCP/IP с использованием *Сокетов Windows* (Windows Sockets).

| Утилита | Функция |
|---|---|
| REXEC | Выполняет процесс на удаленном компьютере, на котором работает программное обеспечение REXEC-сервера. Обеспечивает безопасность путем парольной защиты |
| RSH (Remote Shell) | Обеспечивает выполнение команд на удаленном RSH-сервере без регистрации в системе. Не обеспечивает защиту паролями |
| Telnet | Обеспечивает эмуляцию терминала (DEC VT 100, DEC VT 52 и TTY) и аутентификацию на основе имени пользователя и пароля |
| RCP (Remote Copy) | Копирует файлы между компьютером под управлением Windows NT, и сервером, на котором работает RCP-демон, без регистрации в системе; не обеспечивает безопасность посредством аутентификации пользователя |
| FTP | Обеспечивает двустороннюю передачу файлов между компьютером, работающим под управлением Windows NT, и любым другим TCP/IP-компьютером, на котором работает программное обеспечение FTP-сервера. Поддерживает аутентификацию на основе имени пользователя и пароля |

(*продолжение*)

| Утилита | Функция |
|---|---|
| TFTP | Подпротокол FTP, использующий протокол пользовательских датаграмм [User Datagram Protocol (UDP)] вместо протокола TCP; обеспечивает двустороннюю передачу файлов между компьютером, работающим под управлением Windows NT, и TCP/IP-компьютером, работающим под управлением программного обеспечения TFTP сервера, не обеспечивает аутентификацию пользователя |
| Web-броузер (Web Browser) | Web-броузер получает доступ к документам, хранящимся на WWW-сервере и обеспечивает аутентификацию на основе имени пользователя и пароля |
| LPD | Обслуживает запросы LPR и посылает задания на печать; поддерживает аутентификацию на основе имени пользователя и пароля |
| LPR | Позволяет печатать документы на принтере, подключенном к серверу, на котором работает LPD; поддерживает аутентификацию на основе имени пользователя и пароля |
| LPQ | Обеспечивает возможность просмотра очереди печати на LPD-сервере; обеспечивает аутентификацию на основе имени пользователя и пароля |

## Резюме

TCP/IP позволяет Windows NT взаимодействовать со многими компьютерами, поддерживающими этот протокол. Утилиты TCP/IP фирмы Microsof предоставляют различные возможности для связи с другими компьютерами.

# Занятие 2. Утилиты удаленного выполнения

Некоторые утилиты TCP/IP обеспечивают соединение с удаленными компьютерами. На этом занятии Вы познакомитесь с требованиями к использованию утилит удаленного выполнения.

**Изучив материал этого занятия, Вы сможете:**

- ✓ понять, как соединиться с удаленным компьютером, используя сеть Microsoft.

**Продолжительность занятия — 10 минут**

## Утилита REXEC

Утилита Remote Execution (REXEC) обеспечивает удаленное выполнение программ с использованием аутентификации на основе имен и паролей пользователей. Когда выполняется команда *rexec*, появляется приглашение ко вводу пароля пользователя на удаленном компьютере. После соединения пользователя с удаленным компьютером пароль проверяется. Если он введен правильно, то выполняется указанная команда. REXEC обычно завершает свою работу, когда заканчивается выполнение удаленных команд. Синтаксис REXEC:

```
rexec tcpip-хост команда
```

## Утилита RSH

Утилита Remote Shell (RSH) используется для выполнения команд на удаленном сервере, где работает RSH-демон (в большинстве случаев — это UNIX-компьютер). RSH полезна при компиляции программ. Единственное средство обеспечения безопасности — наличие имени пользователя в файле .rhosts на UNIX-компьютере. RSH не выдает приглашения ко вводу пароля. Синтаксис RSH:

```
rsh unix-хост команда
```

## Утилита Telnet

Telnet — это протокол удаленного терминала, обеспечивающий эмуляцию терминалов Digital Equipment Corporation VT 100, Digital Equipment Corporation VT 52 или TTY. Telnet использует сервисы TCP, ориентированные на соединение. Любые выполняемые с помощью Telnet программы или команды обрабатываются Telnet-сервером, а не локальным компьютером.

Для использования Telnet на удалённом компьютере должен быть установлен Telnet-сервер, или *демон* (daemon) — эту программу Microsoft не поставляет. Вам также необходима учетная запись на компьютере, работающем под управлением Windows NT.

На компьютере-клиенте надо установить программное обеспечение Telnet-клиента (поставляемое вместе с Windows NT). Кроме того, требуется учетная запись пользователя на Telnet-сервере.

▶ **Установка связи с Telnet-сервером**

1. В командной строке запустите Telnet.exe. Откроется окно Telnet.
2. В меню **Connect** выберите **Remote System**. Появится диалоговое окно **Connect**.
3. В поле **Host Name** наберите имя или IP-адрес Telnet-сервера. Нажмите кнопку **OK**.
4. Когда появится приглашение, зарегистрируйтесь на Telnet-сервере используя имя и пароль.

Установив соединение, Вы сможете использовать команды удалённого компьютера так, как если бы работали за подключенным к нему терминалом. Любые запускаемые Вами программы выполняются Telnet-сервером, а не локальным компьютером.

Примечание Протокол Telnet описан в RFC 854. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Резюме

В TCP/IP входит ряд утилит удаленного выполнения. Утилита REXEC запускает процесс на удаленном компьютере. Для ее использования необходимо задать на нем учетную запись пользователя. Утилита RSH выполняет команды на удаленном компьютере. Для работы с ней необходимо наличие имени пользователя в файле .rhosts на UNIX-компьютере. Telnet выполняет команды в диалоговом режиме, эмулируя терминал удалённого компьютера.

# Занятие 3. Утилиты передачи данных

В TCP/IP существует ряд утилит передачи данных. К ним относится и широко применяемый протокол FTP (File Transfer Protocol). На этом занятии Вы познакомитесь с использованием каждой из этих утилит.

**Изучив материал этого занятия, Вы сможете:**

- ✓ понять, как используются утилиты передачи данных для установки связи и получения доступа к ресурсам на удалённом компьютере, поддерживающем TCP/IP;
- ✓ установить сервисы FTP из комплекта Microsoft® Internet Information Server (IIS);
- ✓ использовать программное обеспечение FTP-клиента для передачи файлов.

**Продолжительность занятия — 25 минут**

## Утилита RCP

Подобно RSH, RCP (Remote Copy Protocol) не требует от пользователя регистрации на сервере, на котором работает RCP-демон (в большинстве случаев — это UNIX-компьютер). Однако имя пользователя надо указать в файле .rhosts, расположенном на UNIX-компьютере, и этот пользователь должен обладать привилегией удалённого выполнения команд. RCP используется для копирования файлов между локальным и удаленным UNIX-компьютером или между двумя удаленными компьютерами. Эта утилита не выдает приглашения ко вводу пароля. Синтаксис RCP:

```
rcp хост1.пользователь1:откуда хост2.пользователь2:куда
```

## Утилита FTP

Утилита FTP, использующая протокол TCP в качестве своего транспорта, — одна из наиболее распространенных. Она обеспечивает передачу двоичных и текстовых файлов с FTP-сервера и на него. FTP-сервером может служить UNIX или компьютер под управлением Windows NT, на котором работает FTP-сервер (демон). Протокол FTP часто используется для получения файлов из Интернета.

Если FTP-сервер не поддерживает анонимные подключения, на нем необходимо задать учетную запись пользователя. В Интернете многие серверы разрешают анонимные подключения. Синтаксис команды FTP:

```
ftp [опции] хост команда
```

На удалённом компьютере должен работать FTP-сервер (поставляется с Windows NT) и задана учетная запись пользователя Windows NT.

На компьютере-клиенте должно работать ПО FTP-клиента (поставляется с Windows NT) и задана учетная запись пользователя.

## Команды FTP

Команды FTP могут быть введены в одной строке или с помощью командного интерпретатора. Если команда указана при запуске FTP в командной строке, то FTP немедленно попытается установить связь с FTP-сервером. В противном случае FTP запускает свой командный интерпретатор, в котором пользователь может набирать FTP-команды.

Наиболее распространенные команды FTP перечислены в таблице

| Команда | Назначение |
|---|---|
| *binary* | Изменяет тип передачи файла на двоичный |
| *get* | Копирует удаленный файл на локальный компьютер |
| *put* | Копирует локальный файл на удаленный компьютер |
| *!* | Временно возвращает пользователя в режим командной строки |
| *quit* или *bye* | Осуществляет выход из FTP |

## Утилита TFTP

Утилита TFTP (Trivial File Transfer Protocol) также позволяет передавать файлы между компьютерами. Она использует не ориентированные на соединение сервисы UDP и не поддерживает какую-либо аутентификацию пользователя. На удаленной системе файлы должны иметь атрибуты «чтение для всех» и «запись для всех» (world-readable и writable в UNIX).

Microsoft поставляет только программное обеспечение для TFTP-клиента. Используйте TFTP-сервер сторонних производителей для подключения к компьютеру, работающему под управлением Windows NT. Пример синтаксиса команды TFTP:

```
tftp -i хост get файл1 файл2
```

Примечание Протокол FTP описан в RFC 959, а TFTP — в RFC 1350. Копии этих документов находятся на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Упражнения

Здесь Вы установите Windows NT FTP-сервер на Вашу рабочую станцию, а затем, используя второй компьютер, получите доступ к нему по протоколу FTP. Далее Вы командой *netstat* получите информацию о состоянии FTP портов.

---

Примечание Для выполнения этих упражнений рекомендуется иметь два компьютера. Однако в большинстве случаев Вы можете начать сеанс FTP-связи с Вашим собственным сервером, набрав *ftp 127.0.0.1*

---

Определите, установлен ли Microsoft Internet Information Server (IIS) с FTP-сервисом

▶ **Исследование операционной среды Windows NT Server**

1. Зарегистрируйтесь под именем *Administrator*.
2. Нажмите кнопку **Start**, выберите **Settings**, а затем — **Control Panel**.
3. В **Control Panel** дважды щелкните пиктограмму **Services**.

   Появится диалоговое окно **Services**.
4. Проверьте, есть ли в списке сервис **FTP Publishing Service**.

   Если нет, Вам придется установить Internet Information Server (IIS) с FTP-сервисом, используя описанную ниже процедуру.
5. Закройте диалоговое окно **Services**.
6. Закройте **Control Panel**.

Выполните эту процедуру, если ранее Вы не устанавливали IIS с FTP-сервисом.

▶ **Установка Internet Information Server**

1. Зарегистрируйтесь под именем *Administrator*.
2. Дважды щелкните пиктограмму **Install Internet Information Server** на рабочем столе.

   Появится диалоговое окно **Internet Information Server Installation**.
3. В поле **Installed from** введите путь к установочным файлам Windows NT.

   Появится диалоговое окно **Microsoft Internet Information Server 2.0 Setup**.
4. Прочтите информацию в нем и нажмите кнопку **OK**.

   Появятся следующие установочные опции:

   - **Internet Service Manager**;
   - **World Wide Web Service**;
   - **WWW Service Samples**;
   - **Internet Service Manager (HTML)**;
   - **Gopher Service**;

- **FTP Service**;
- **ODBC Drivers and Administration**.

5. Убедитесь, что выбраны по крайней мере **Internet Service Manager** и **FTP Service**, и нажмите кнопку **OK**.
6. Когда появится предложение создать каталог C:\Winnt\System32\Inetsrv, нажмите кнопку **Yes**.

   Появится диалоговое окно **Publishing Directories** с указанием каталога, выбранного по умолчанию, — C:\Inetpub\Ftproot в поле **FTP Publishing Directory**.
7. Если каталог по умолчанию Вас устраивает, нажмите кнопку **OK**.
8. Когда появится предложение создать этот каталог, нажмите кнопку **Yes**. Программа установит **Internet Information Server FTP Service**.
9. Когда установка закончится, нажмите кнопку **OK**.

Используйте программное обеспечение FTP-клиента для копирования файла с FTP-сервера на FTP-клиент

▶ **Передача файла по протоколу FTP**

1. В командной строке наберите:

   ```
   Copy C:\Winnt\*.bmp C:\Inetpub\Ftproot
   ```

2. Создайте временный каталог C:\Ftptemp на Вашем компьютере.
3. Войдите в него.
4. Начните сеанс FTP-связи со вторым компьютером командой:

   ```
   ftp server2
   ```

5. Зарегистрируйтесь под именем *Anonymous*.
6. В ответ на запрос пароля нажмите ENTER.

   Появится приглашение командной строки *ftp>*.
7. Введите команду:

   ```
   dir
   ```

   Появится список всех доступных файлов на FTP-узле.
8. Используйте команду *get* для получения одного файла. Наберите:

   ```
   get lanma256.bmp
   ```

9. Для просмотра переданного на Ваш компьютер файла введите:

   ```
   !dir
   ```

10. Используйте команду *mget* для получения остальных файлов. Введите:

    ```
    mget *
    ```

11. Для завершения сеанса FTP-связи введите:

```
bye
```

Введите команду *netstat* в процессе FTP-связи для проверки состояния портов TCP

► **Запуск сеанса FTP**

1. Чтобы начать сеанс FTP-связи, в командной строке введите:

```
ftp server2
```

2. Зарегистрируйтесь под именем *Anonymous*.
3. В ответ на запрос пароля нажмите ENTER.

   Появится приглашение командной строки *ftp>*.
4. Введите следующую команду для вывода информации о текущих сетевых TCP-соединениях:

```
!netstat
```

5. Для вывода информации о текущих сетевых TCP-соединениях и текущем состоянии TCP-портов введите команду:

```
!netstat -n
```

   Какой TCP-порт используется протоколом FTP со стороны сервера?

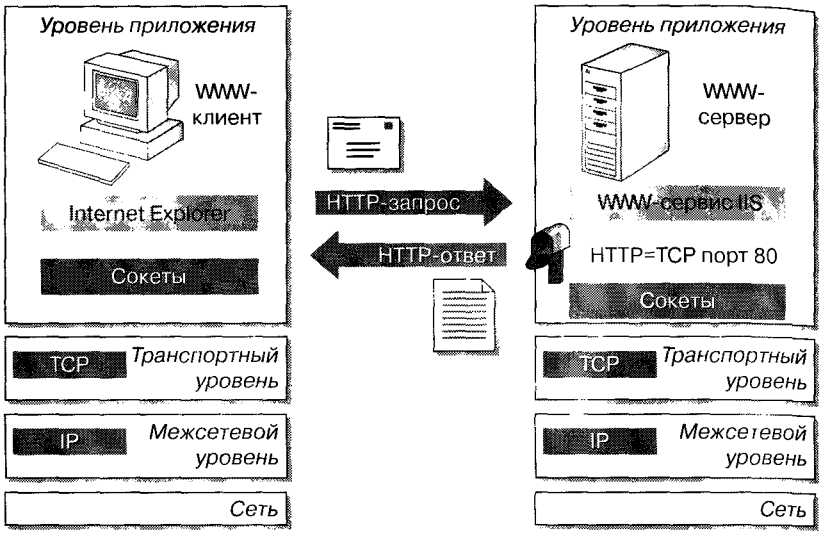
   _____

6. Для завершения сеанса FTP-связи введите:

```
Bye
```

## Средства просмотра Web

WWW («Всемирная паутина») на сегодня — один из наиболее распространенных путей передачи данных через Интернет. Средства просмотра Web — Web-броузеры, (Web-browsers) — позволяют получать доступ к документам, хранящимся на Web-серверах. WWW поддерживает модель клиент/сервер и использует *протокол передачи гипертекста* (Hypertext Transfer Protocol, HTTP) между клиентом и сервером (см. рис.).




На компьютере-клиенте должен работать Web-броузер. Существует множество Web-клиентов, некоторые из них можно бесплатно получить по Интернету. На компьютере-сервере должен работать WWW-сервис.

Сервер отвечает на запрос, высылая сообщение о состоянии транзакции («успешное» или «отсутствует») и запрошенные данные. После отправки данных соединение обрывается и сервер не запоминает его состояние. Каждый объект в HTTP-документе требует отдельного соединения.

Web-броузеры предпочтительны при передаче данных. Во-первых, они поддерживают множество типов данных — Web-броузер может автоматически передавать и отображать текстовые файлы и графику, проигрывать видео- и звуковые клипы и выполнять приложения, ассоциированные с известными типами файлов.

Во-вторых, они поддерживают несколько протоколов передачи данных, включая FTP, Gopher и Network News Transfer Protocol (NNTP).

## Резюме

RCP копирует файлы между удаленным и локальным компьютерами без аутентификации. FTP копирует файлы с помощью надежного протокола TCP и применяет аутентификацию на уровне пользователя. Web-броузеры, например Microsoft Internet Explorer, используют HTTP для передачи данных с Web-сервера. TFTP копирует файлы с помощью протокола UDP и не применяет аутентификацию на уровне пользователя.

# Занятие 4. Утилиты печати

Установив и сконфигурировав поддержку принтеров по протоколу TCP/IP, Вы можете соединиться с принтером, используя Print Manager или команду LPR — в зависимости от того, присоединен принтер к компьютеру под управлением Windows NT, или к UNIX-компьютеру. На этом занятии Вы узнаете о поддержке печати по протоколу TCP/IP.

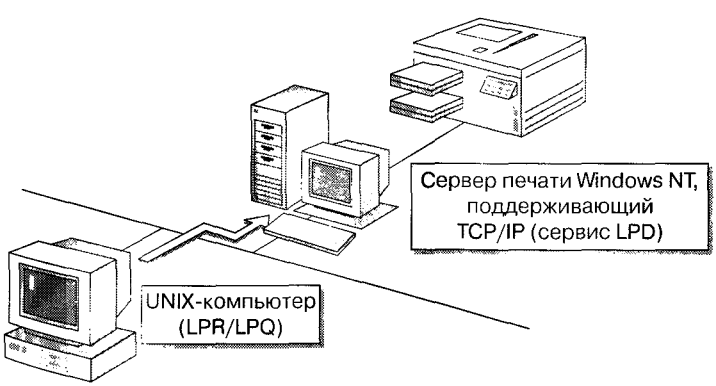
**Изучив материал этого занятия, Вы сможете:**

- ✓ установить и сконфигурировать поддержку печати по протоколу TCP/IP;
- ✓ установить связь с принтером, поддерживающим TCP/IP, и печатать на нем;
- ✓ использовать LPQ для просмотра очередей печати, а LPR — для печати файлов.

**Продолжительность занятия — 45 минут**

LPR и LPQ — программы-клиенты, устанавливающие связь с процессом LPD на сервере, как показано на рисунке.

- LPD — это сервис на компьютере, работающем под управлением Windows NT (LPDSVC), он позволяет другим компьютерам посылать задания на печать на этот компьютер, используя протокол TCP/IP и программу LPR.
- LPR — программа-клиент печати, дающая возможность компьютеру-клиенту под управлением Windows NT посылать задания на печать на любой компьютер, на котором работает сервис LPD.
- LPQ может быть использована для определения состояния принтера после отправки задания на печать.



Примечание Поддержка печати с использованием Microsoft TCP/IP описана в RFC 1179. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Работа сервера печати по протоколу TCP/IP (LPD)

Чтобы ОС Windows NT могла принимать задания на печать от LPR-клиентов, необходимо установить и запустить сервис сервера печати по протоколу TCP/IP (LPDSVC). Второе можно сделать, используя программу **Services** в **Control Panel**, командную строку или Server Manager.

Совет Рекомендуется автоматический запуск сервера печати по протоколу TCP/IP — из программы **Services** в **Control Panel** или из Server Manager.

### Параметры реестра для сервера печати по протоколу TCP/IP

Параметры сервера печати по протоколу TCP/IP расположены в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LPDSVC\Parameters.

## Использование LPR и LPQ

### Отправка заданий на печать

В зависимости от среды, из которой Вы посылаете задание на печать, используйте один из перечисленных методов:

- для Windows-приложений — Print Manager;
- при использовании командной строки или при печати с UNIX-компьютера — утилиту LPR (LPR.EXE).

LPR отправляет файлы для печати сервису LPD, работающему на сервере Windows NT или UNIX-компьютере, по следующему синтаксису:

```
lpr -Sip_адрес -Римя_принтера имя_файла
```

Чтобы отправить задание на печать, LPR устанавливает TCP-соединение с сервисом LPD, используя порты в диапазоне с 512 по 1023.

### Проверка состояния печати

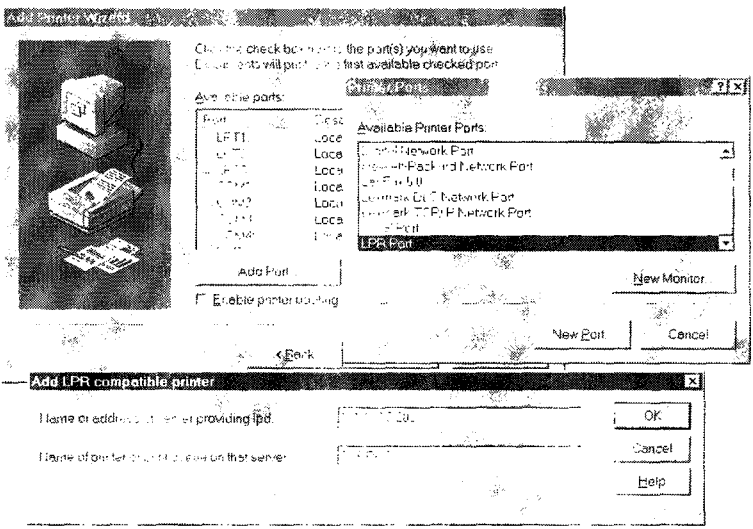
Отправив файл на печать с помощью LPR, Вы можете использовать утилиту LPQ (Lpq.exe) для проверки состояния очереди печати:

```
lpq -Sip_адрес -Римя_принтера -l
```

Примечание Параметры *-S* и *-P* в обеих командах должны быть указаны [illegible] буквами. Параметр *-l* (латинская буква l) может быть набран

### Конфигурирование Print Manager с помощью LPR Print Monitor

Чтобы сконфигурировать Windows NT Print Manager для использования сервера печати LPD, Вы должны добавить в протокол TCP/IP *поддержку печати* (printing support) и сконфигурировать принтер для использования *монитора печати* LPR (LPR print monitor). Пример конфигурации показан на иллюстрации.

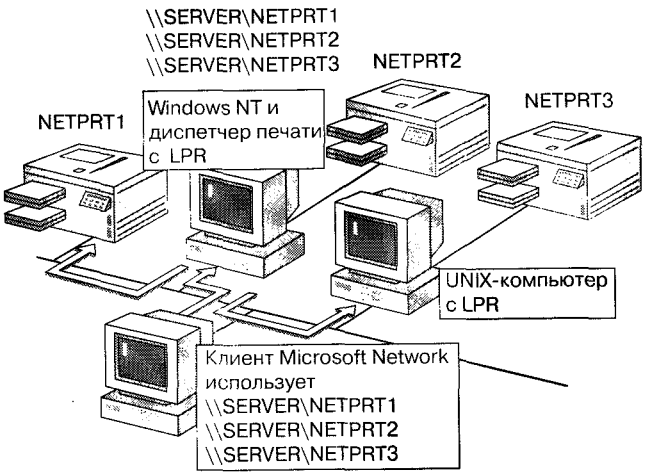



Примечание Опция **LPR Port** появится в диалоговом окне **Printer Port** менеджера печати Print Manager только в том случае, если на Вашем компьютере установлен компонент Microsoft TCP/IP Printing.

## Использование Windows NT в качестве шлюза печати

Компьютер под управлением Windows NT с установленными сервисами печати по протоколу TCP/IP (LPD) может выполнять две функции шлюза (они показаны на иллюстрации). Во-первых, получать задания на печать от клиентов Microsoft и затем пересылать их автоматически на TCP/IP-сервер печати, на котором работает утилита LPD. В этом случае не требуется наличия LPR или TCP/IP у клиента.

Во вторых, компьютер под управлением Windows NT может получать задания на печать от любого LPR-клиента и затем пересылать их на любой доступный ему принтер.




## Упражнения

Здесь Вы установите сервис печати по протоколу TCP/IP, создадите TCP/IP-принтер и затем используете утилиту LPR для печати на принтер. Для выполнения этих упражнений Вам потребуется совместно используемый принтер, а также его имя, тип и IP-адрес сервера печати.

### ► Установка TCP/IP-принтера

Сначала Вы установите сервис печати Microsoft TCP/IP Printing service, затем — TCP/IP-принтер, используя Print Manager.

1. В **Control Panel** дважды щелкните пиктограмму **Network**.
   Появится диалоговое окно **Network**.
2. Выберите вкладку **Services**.
   Появится диалоговое окно **Services property**.
3. Нажмите кнопку **Add**.
   Появится диалоговое окно **Select Network Service**.
4. Нажмите **Microsoft TCP/IP Printing** и затем — **OK**.
   Появится окно **Windows NT Setup**, с запросом о полном пути к установочным файлам Windows NT.
5. Введите путь к установочным файлам Windows NT и нажмите **Continue**.
   На Вашу рабочую станцию скопируются нужные файлы, и затем появится диалоговое окно **Network**.
6. Нажмите **Close**.
   Появится окно **Network Settings Change** с сообщением о том, что ком-

7. Нажмите **Yes**.
8. Зарегистрируйтесь под именем *Administrator*.
9. В окне **Control Panel** дважды щелкните **Services**.
   Появится диалоговое окно **Services**.
10. Выберите **TCP/IP Print Server** и нажмите **Start**.
11. Нажмите **Close**.

▶ **Создание TCP/IP-принтера**

1. В диалоговом окне **Control Panel** дважды щелкните пиктограмму **Printers**.
   Появится диалоговое окно **Printers**.
2. Дважды щелкните **Add Printer**.
   Появится диалоговое окно **Add Printer Wizard**.
3. Нажмите **My Computer**, а затем — **Next**.
4. Нажмите **Add Port**.
   Появится диалоговое окно **Printer Ports**.
5. Нажмите **LPR Port** и затем — **New Port**.
   Появится диалоговое окно **Add LPR compatible printer**.
6. В поле **Name or address of server providing lpd** введите Ваш IP-адрес.
7. В поле **Name of printer or print queue on that server** введите имя принтера и нажмите **OK**.
8. Нажмите **Close**.
9. Нажмите **Next**.
10. Завершите установку, используя данные таблицы.

| Когда появится приглашение ко вводу | Используйте эту информацию |
|---|---|
| Printer manufacturer and model | *Printer type* (тип принтера) |
| Printer name | *Printername* (имя принтера) |
| Shared/Not shared | Shared |
| Share name | *share* (имя принтера) |
| Test page | No |

В диалоговом окне **Insert Disk** появится просьба вставить диск в дисковод.

11. Нажмите **OK**.
    Появится диалоговое окно **Windows NT Setup**, запрашивающее полный путь к установочным файлам Windows NT Server.
12. Введите путь к установочным файлам Windows NT Server и нажмите **OK**.
    Появится пиктограмма с именем созданного TCP/IP-принтера.

В этом упражнении Вы установите связь с TCP/IP-принтером и пошлете задание на печать. Используйте программу Notepad для отправки файлов на печать. Затем Вы средствами утилиты командной строки LPQ просмотрите удаленную очередь печати.

▶ **Установка связи с TCP/IP-принтером посредством Print Manager**

1. В окне **Printers** дважды щелкните **Add Printer**.
   Появится диалоговое окно **Add Printer Wizard**.
2. Нажмите **Network printer server** и затем — **Next**.
   Появится диалоговое окно **Connect to Printer**.
3. В поле **Printer** введите путь и имя принтера и затем нажмите **OK**.
   Программа предложит Вам сделать этот принтер по умолчанию.
4. Нажмите **Yes**, а затем — **Next**.
5. Нажмите **Finish**.
   В окне **Printers** появится пиктограмма, изображающая совместно используемый компьютер.
6. Дважды щелкните пиктограмму, изображающую новый принтер.
   Имя принтера появится в окне **Printername on share**.
7. Запустите Notepad, создайте небольшой документ и отправьте его на печать на совместно используемый принтер.
8. Вернитесь в окно **Printername on share**.
   Появится диалоговое окно **Messenger Service** с уведомлением, что печать документа закончена.
9. Нажмите **OK**.
10. Закройте окно **Printername on share**.

▶ **Использование LPR и LPQ для получения доступа к TCP/IP-принтеру**

1. В командной строке посмотрите удаленную очередь печати. Наберите:

```
lpr -Sxxx.xxx.xxx.xxx -Римя_принтера -l
```

   где xxx.xxx.xxx.xxx — IP-адрес сервера печати, а имя_принтера — имя Вашего принтера.

---

Внимание! Параметры *-S* и *-P* набираются прописными буквами.

---

   Появится диалоговое окно **Window NT LPD Server print queue status**.
2. Отправьте новое задание в очередь печати. Наберите:

```
lpr -Sxxx.xxx.xxx.xxx -Римя_принтера c:\config.sys
```

   Программа отправит файл в очередь печати на совместно используемый принтер.

3. Просмотрите новые задания в удаленной очереди печати. Обратите внимание, что список новых заданий содержит документ LPR-клиента в виде имени задания.
4. Завершите работу с командной строкой.

## Резюме

LPD отвечает на запросы от LPR и LPQ и отправляет данные, которые необходимо распечатать, на устройство печати. LPR отправляет задание на печать серверу печати LPD. LPQ опрашивает список заданий на сервере печати LPD. Windows NT может выполнять роль шлюза печати для TCP/IP-узлов и узлов других типов.

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Что необходимо компьютеру под управлением Windows NT для соединения с другим узлом?

2. Что необходимо компьютеру под управлением Windows NT для соединения и взаимодействия с RFC-совместимым NetBIOS-узлом, например LAN Manager для UNIX?

3. Опишите два различия в обращении к ресурсам TCP-узлов посредством команд Windows NT или утилит TCP/IP.

4. Какие утилиты TCP/IP используются для копирования файлов?

5. Какие утилиты TCP/IP позволяют выполнять команды на удалённом компьютере?

6. Какие функции обеспечивает поддержка сетевой печати по протоколу TCP/IP?

# Использование SNMP-сервисов



## В этой главе

В этой главе вы познакомитесь с Simple Network Management Protocol (SNMP) — еще одним протоколом из семейства TCP/IP, а также с его функциями, выполняемыми *станциями управления* SNMP (management stations), и сервисом Microsoft SNMP (агентом SNMP). Выполняя упражнения, Вы установите, сконфигурируете и протестируете сервис SNMP.

## Прежде всего

Прежде чем приступить к изучению материалов этой главы, необходимо

- установить Windows NT Server 4.0 с протоколом TCP/IP;
- найти файл Snmputil.exe на прилагаемом к курсу компакт-диске.

# Занятие 1. Определение SNMP

Протокол SNMP предназначен для сбора и передачи *служебной информации* (status information) между различными компьютерами. На этом занятии Вы узнаете, что такое протокол SNMP и познакомитесь с системами управления и агентами.

**Изучив материал этого занятия, Вы сможете:**

- ✓ объяснить и описать сервис Microsoft SNMP;
- ✓ описать операции, выполняемые агентом SNMP и системой управления.

**Продолжительность занятия — 20 минут**

SNMP — это протокол из семейства TCP/IP. Первоначально он был разработан *Сообществом Интернета* (Internet community) для наблюдения и устранения неполадок в маршрутизаторах и *мостах* (bridges). SNMP позволяет наблюдать и передавать информацию о состоянии:

- компьютеров, работающих под управлением Windows NT;
- серверов LAN Manager;
- маршрутизаторов и шлюзов;
- мини-компьютеров или мэйнфреймов;
- терминальных серверов;
- концентраторов.

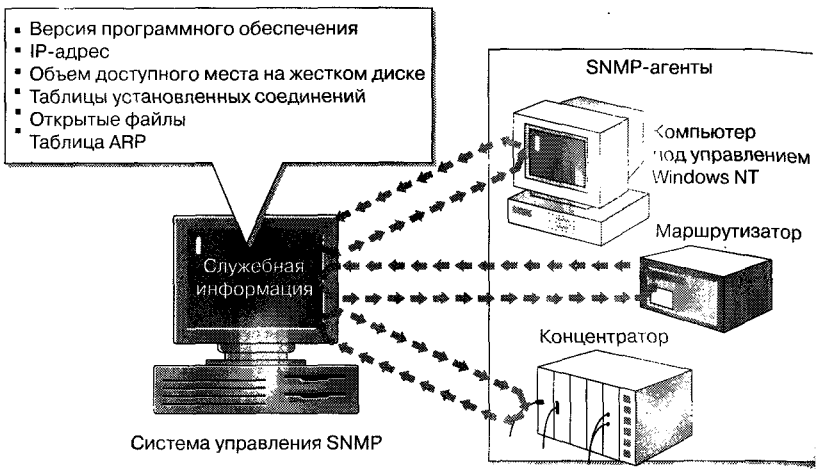
SNMP использует распределенную архитектуру, состоящую из *систем управления* (management systems) и *агентов* (agents). С помощью сервиса Microsoft SNMP компьютер, работающий под управлением Windows NT, может выдавать отчет о своем состоянии системе управления SNMP в сети, использующей протокол TCP/IP.

Сервис SNMP посылает информацию о состоянии одному или нескольким компьютерам по запросу или когда происходит важное событие, например, компьютеру не хватает места на жестком диске.

Примечание Протокол SNMP описан в RFC 1157. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## Системы управления и агенты

SNMP позволяет наблюдать за различными компьютерами с помощью систем управления и агентов, как показано на иллюстрации.




## Система управления SNMP

Основная функция системы управления — запрос информации от агентов. *Система управления* (management system) — это любой компьютер, на котором работает программное обеспечение управления SNMP. Система управления может выполнять операции *get, get-next* и *set*.

- Операция *get* запрашивает какой-либо параметр, например количество доступного пространства на жестком диске.
- Операция *get-next* запрашивает следующую величину, используется для просмотра таблицы объектов.
- Операция *set* изменяет значение, используется редко, потому что большинство параметров доступны только для чтения и не изменяются.

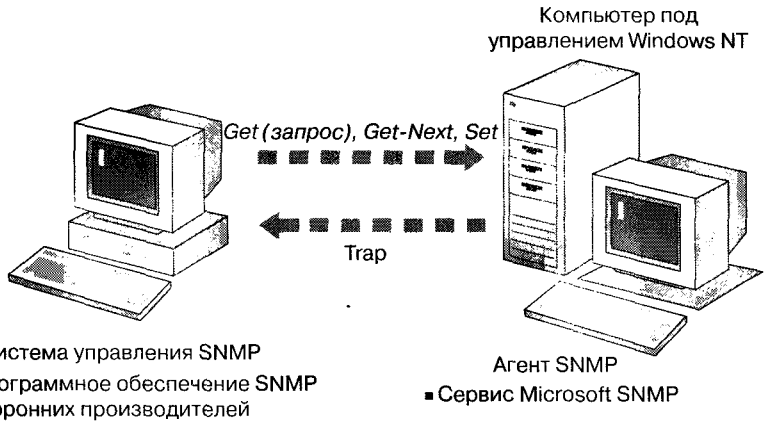
## Агент SNMP

Основная функция агента SNMP заключается в выполнении операций *get, get-next* и *set*, инициированных системой управления, как показано на иллюстрации ниже. Агент — это любой компьютер, на котором работает соответствующее программное обеспечение SNMP, как правило, сервер или маршрутизатор. Сервис Microsoft SNMP — это программное обеспечение агента SNMP.

Единственная операция, которая может быть инициирована агентом, — *trap*. Эта операция сигнализирует системам управления о необычном событии, например нарушении пароля*.

---

* Здесь имеется в виду обращение со стороны системы управления, не авторизованной на выполнение таких операций. — *Прим. перев.*




## Сервис Microsoft SNMP

Он обеспечивает сервисы агента SNMP любому компьютеру, на котором работает программа управления SNMP. Сервис SNMP:

- обрабатывает запросы служебной информации от компьютеров;
- сообщает о важных событиях [*ловушках* (traps)] нескольким компьютерам, как только они происходят;
- использует имена узлов и их IP-адреса для идентификации компьютеров, которым посылает информацию и с которых получает запросы;
- может быть установлен и использован на любом компьютере, работающем под управлением Windows NT с протоколом TCP/IP;
- позволяет применять счетчики для наблюдения за TCP/IP, используя Performance Monitor.

### Архитектурная модель SNMP

Сервис Microsoft SNMP написан с использованием интерфейса Windows Sockets. Это позволяет обращаться к нему из сетевых систем управления, созданных средствами этого интерфейса. Сервис SNMP посылает и принимает сообщения по протоколу UDP (порт 161) и использует IP для поддержки маршрутизации SNMP-сообщений.

SNMP позволяет применять дополнительные динамически подключаемые библиотеки агентов для поддержки других баз MIB. Сторонние производители могут разрабатывать собственные базы MIB для использования совместно с сервисом Microsoft SNMP. Microsoft SNMP включает модуль Microsoft Win32 API SNMP администратора для упрощения разработки SNMP-приложений.

## Резюме

SNMP позволяет наблюдать за компьютерами, работающими под управлением Windows NT, и сигнализировать системам управления о происходящих событиях.

Сервис Microsoft SNMP обеспечивает сервисы агентов, дополнительные библиотеки DLL и Win32 SNMP API администратора для упрощения разработки SNMP-приложений.

# Занятие 2. Management Information Base

Информация, которую система управления запрашивает от агентов, хранится в специальной *информационной базе данных* MIB (Management Information Base). На этом занятии дается определение баз данных MIB, поддерживаемых сервисом SNMP.

**Изучив материал этого занятия, Вы сможете:**

- ✓ описать базы данных MIB, поддерживаемые SNMP.

**Продолжительность занятия — 10 минут**

MIB — это набор контролируемых объектов, представляющих информацию об устройствах сети, например, о количестве активных сеансов или версиях сетевой операционной системы, работающей на компьютере. Главное то, что и агент SNMP, и база данных MIB одинаково интерпретируют контролируемые объекты. Таким образом, система управления с помощью базы данных MIB «знает», какую информацию можно запросить у агента и что характеризует тот или иной объект.

Сервис SNMP поддерживает Internet MIB II, LAN Manager MIB II, DHCP MIB и WINS MIB.

## Internet MIB II

Internet MIB II — это расширение предыдущего стандарта Internet MIB I. Оно определяет 171 объект, необходимый для поиска неисправностей и анализа конфигурации.

Примечание База данных Internet MIB II описана в RFC 1212. Копия этого документа находится на Web-странице *Course Materials* прилагаемого к курсу компакт-диска.

## LAN Manager MIB II

LAN Manager MIB II определяет около 90 объектов, включающих такие элементы, как статистическую, сеансовую, пользовательскую, регистрационную информацию и данные о совместно используемых ресурсах. К большинству объектов LAN Manager MIB II установлен доступ только для чтения в связи с отсутствием обеспечения безопасности в SNMP.

## DHCP MIB

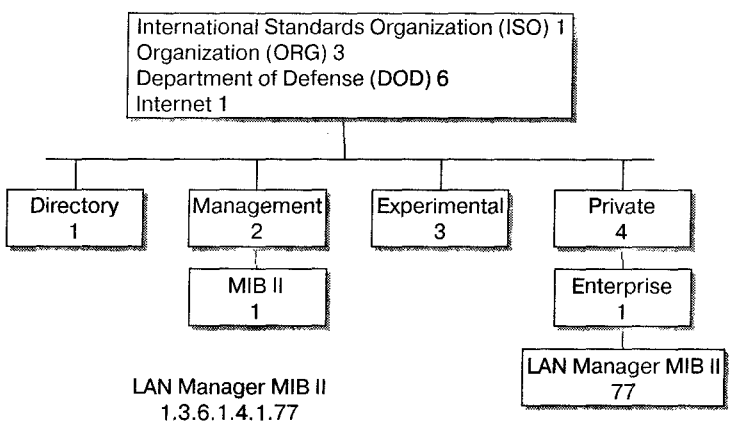
Windows NT 4.0 поставляется с DHCP MIB. Эта база определяет объекты для наблюдения за активностью DHCP-сервера. Модуль Dhcpmib.dll автоматически устанавливается при установке сервиса DHCP Server. Он наблюдает около 14 параметров DHCP, например, число полученных запросов DHCPDISCOVER, количество отказов или адресов, взятых в аренду клиентами, и др.

## WINS MIB

Windows NT 4.0 поставляется с WINS MIB. Эта база определяет объекты для наблюдения за активностью WINS-сервера. Модуль Winsmib.dll автоматически устанавливается при установке сервиса WINS Server. Он наблюдает приблизительно 70 параметров WINS, например, число запросов, на которые удалось успешно ответить, количество неуспешных запросов или дату и время последнего сеанса тиражирования базы данных.

# Дерево имен

Пространство имен MIB-объектов имеет иерархическую структуру. На иллюстрации видно, что оно организовано так, что каждому контролируемому объекту может соответствовать уникальное имя. Полномочия на управление частями пространства имен присваиваются отдельным организациям. Поэтому организации вправе назначать имена, не консультируясь с комитетом по Интернету. Например, 1.3.6.1.4.1.77 является пространством имен, присвоенным LAN Manager. Поскольку 1.3.6.1.4.1.77 присвоено LAN Manager, корпорации Microsoft присвоено 1.3.6.1.4.1.311, и все новые базы MIB будут созданы на этой ветви. Microsoft вправе назначать имена объектам где угодно в рамках этого пространства имен.



Идентификатор объекта в иерархии записывается как последовательность меток, начинающихся в корне и заканчивающихся самим объектом. Метки разделены точками. Например, идентификатор объекта для MIB II приведен ниже.

| Имя объекта | Номер объекта |
|---|---|
| iso.org.dod.internet.management.mibii | 1.3.6.1.2.1 |

А в следующей таблице — идентификатор объекта для LAN Manager MIB II.

| Имя объекта | Номер объекта |
|---|---|
| iso.org.dod.internet.private.enterprise.lanmanager | 1.3.6.1.4.1.77 |

Примечание Пространство имен, используемое для идентификаторов объектов, — уникально и отделено от иерархического пространства имен, присвоенного именам UNIX-доменов.

## Резюме

MIB — набор контролируемых объектов, представляющих служебную информацию, например, о количестве установленных сеансов на компьютере.

# Занятие 3. Установка и конфигурирование сервиса SNMP

Если Вы хотите контролировать TCP/IP с помощью Performance Monitor, Вам необходимо установить сервис SNMP. Чтобы использовать приложение сторонних производителей для наблюдения за компьютером, работающим под управлением Windows NT, Вам также придется сконфигурировать сервис SNMP.

**Изучив материал этого занятия, Вы сможете:**

- ✓ определить сообщество SNMP;
- ✓ установить и сконфигурировать сервис Microsoft SNMP;
- ✓ использовать программу SNMPUTIL для тестирования соединений для Microsoft SNMP сервиса.

**Продолжительность занятия — 50 минут**

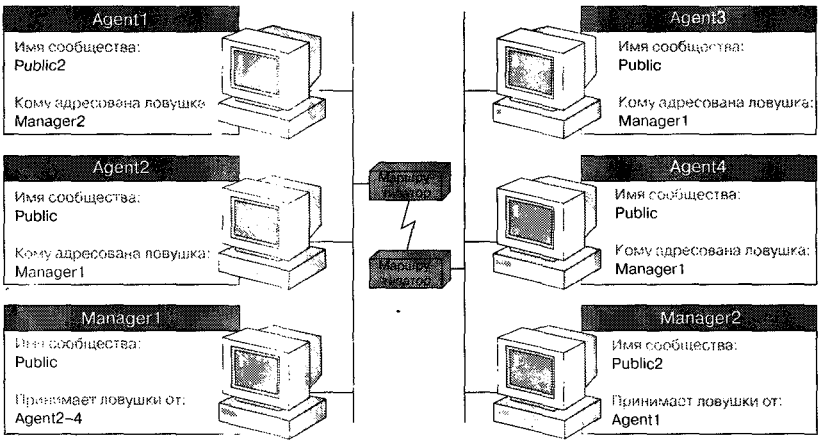
## Определение сообществ SNMP

Перед установкой SNMP Вам необходимо определить *сообщество* (SNMP community) — группу, к которой принадлежат компьютеры с сервисом SNMP. *Имя сообщества* (community name) идентифицирует сообщество. Оно обеспечивает простейшую безопасность и контекстную проверку для агентов, получающих запросы и инициирующих *прерывания* (traps), и для систем управления, инициирующих запросы и обрабатывающих прерывания. Агент не примет запрос от системы управления, сконфигурированной за пределами его сообщества.

SNMP-агент может быть членом нескольких сообществ одновременно, что позволит ему связываться с администраторами SNMP различных сообществ. Например, на иллюстрации ниже определены два сообщества — Public и Public2.

Только агенты и администраторы — члены одного сообщества — могут связываться друг с другом.

- Agent1 может получать и посылать сообщения Manager2, потому что они оба являются членами сообщества Public2.
- Agent2, Agent3 и Agent4 могут получать и посылать сообщения Manager1, потому что все они являются членами сообщества Public, принятого по умолчанию.




## Сбор информации

Инструкция и иллюстрация ниже показывают, как сервис SNMP реагирует на запросы системы управления.

1. Система управления SNMP посылает запрос агенту, используя имя узла агента (или его IP-адрес).

   Запрос отправляется приложением на UDP порт 161.

   Имя узла преобразуется в IP-адрес любым из доступных методов разрешения, включая файл HOSTS, DNS, WINS, широковещание или файл LMHOSTS.

2. Формируется SNMP-пакет, содержащий следующую информацию:
   - операцию *get*, *get-next* или *set* для одного или нескольких объектов;
   - имя сообщества и другую проверочную информацию.

   Пакет передается по сети агенту на UDP порт 161.

3. SNMP-агент получает пакет в свой буфер.

   Проверяется имя сообщества. Если оно неправильное или пакет некорректный, он отвергается.

   Если имя сообщества правильное, агент проверяет имя узла или IP-адрес отправителя. Агент должен быть уполномочен принимать пакеты от системы управления. В противном случае пакет отвергается.

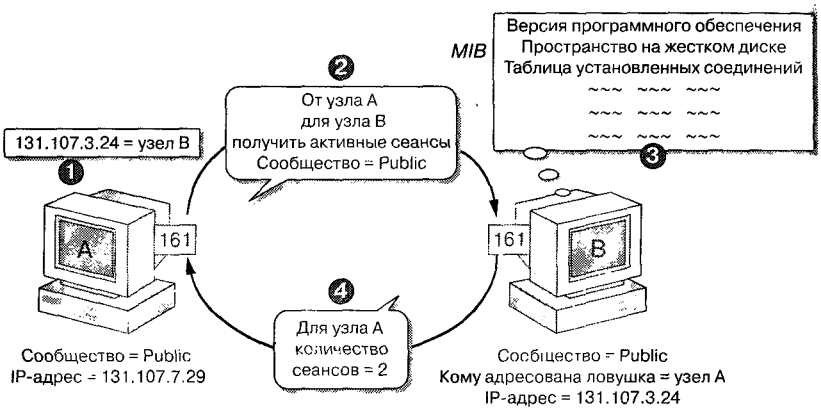
   Запрос передается соответствующей DLL.

| Если запрос для | Происходит следующее |
|---|---|
| объекта Internet MIB II | TCP DLL находит информацию |
| объекта LAN Manager MIB II | LAN Manager DLL находит информацию |
| объекта DHCP | DHCP MIB DLL находит информацию |
| объекта WINS | WINS MIB DLL находит информацию |
| расширенного агента MIB | DLL для этой MIB находит информацию |

Идентификатор объекта отображается в соответствующую функцию API, которая затем и вызывается.

DLL возвращает информацию агенту.

4. SNMP-пакет с требуемой информацией отправляется назад администратору SNMP.



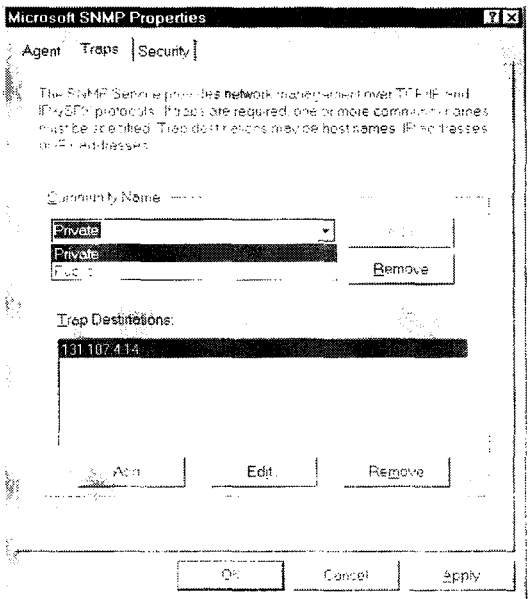

## Упражнения

В этом упражнении Вы установите и настроите сервис SNMP.

▶ **Установка сервиса SNMP**

1. В **Control Panel** дважды щелкните пиктограмму **Network**.
2. Выберите вкладку **Services** и нажмите **Add**.
   Появится диалоговое окно **Select Network Service**.
3. Щелкните **SNMP Service** и нажмите **OK**.
4. Введите на запрос путь к установочным файлам Windows NT.

5. После того как нужные файлы скопируются на компьютер, появится диалоговое окно **Microsoft SNMP Properties**.




6. Выберите имя сообщества Public.
7. Нажмите **OK**.

   Появится диалоговое окно **Network**.
8. Нажмите **Close**.

   Появится окно **Network Settings Change** с предупреждением о необходимости перезагрузить компьютер.
9. Нажмите **Yes**.
10. Войдите в систему под именем *Administrator*.

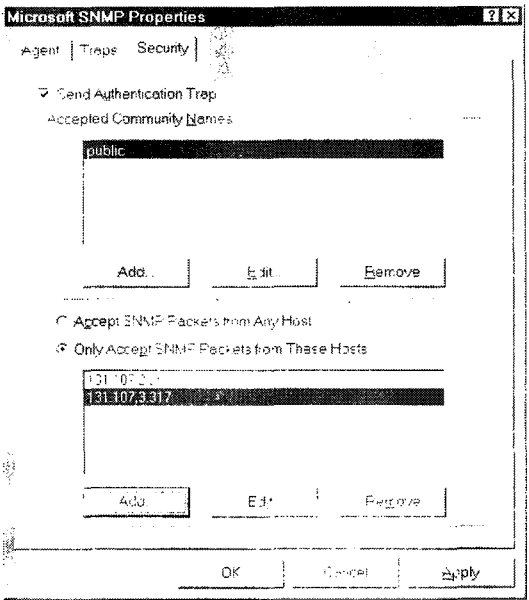
## Настройка безопасности

Сервис SNMP обеспечивает элементарную безопасность и контекстную проверку агентов, получающих запросы и инициирующих ловушки, и систем управления, инициирующих запросы и получающих ловушки. Агент не примет запрос от системы управления, не принадлежащей ни к одному из указанных в списке допустимых сообществ. Windows NT посылает системное прерывание аутентификации, принятое по умолчанию.

► **Конфигурирование безопасности SNMP**

1. В **Control Panel** дважды щелкните пиктограмму **Network**.
2. Выберите вкладку **Services**, нажмите **SNMP Services** и затем — **Properties**. Появится диалоговое окно **Microsoft SNMP Properties**.
3. Выберите вкладку **Security**.
4. Сконфигурируйте параметры, показанные в таблице.

| Параметр | Описание |
|---|---|
| Send Authentication Trap | Когда SNMP сервис получает запрос на информацию, не содержащий корректного имени сообщества или не совпадающий с подходящим именем узла для сервиса, сервис SNMP может отправить в ответ системное прерывание, указывающее, что запрос не аутентифицирован. Отметьте этот флажок, чтобы задать системное прерывание аутентификации |
| Accepted Community Names | Компьютер должен принадлежать сообществу, указанному в этом списке, чтобы сервис SNMP смог принимать запросы от него. Как правило, все компьютеры принадлежат сообществу Public, являющемуся стандартным именем для общего сообщества всех компьютеров |
| Accept SNMP Packets from Any Host | Если указана эта опция, пакеты SNMP не отвергаются на основе идентификаторов узлов-отправителей и указанного под опцией списка допустимых узлов |
| Only Accept SNMP Packets from These Hosts | Если выбрана эта опция, пакеты SNMP принимаются только с указанных в списке компьютеров |




## Настройка сервисов SNMP-агента

Сервис SNMP позволяет компьютеру, работающему под управлением Windows NT, информировать систему управления о деятельности на различных уровнях семейства протоколов Интернета.

▶ **Конфигурирование сервисов SNMP-агента**

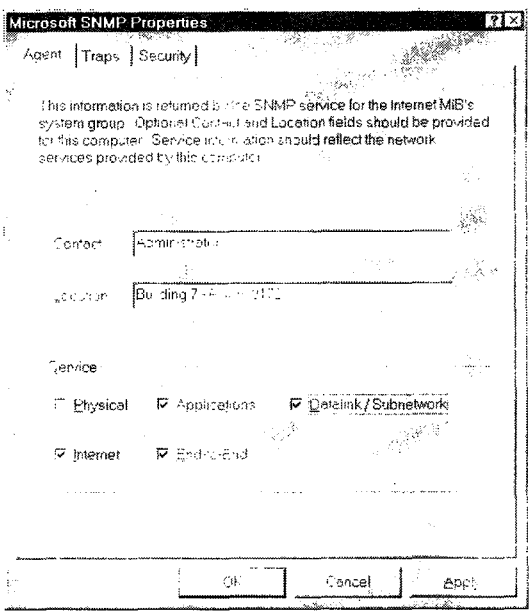
1. В диалоговом окне **Microsoft SNMP Properties** выберите вкладку **Agent**.
2. В поле **Contact** введите контактное имя.

   Обычно, это имя человека, использующего компьютер.
3. В поле **Location** введите описание места, где установлен компьютер.
4. В поле **Service** выберите сервисы, которые будут обеспечиваться агентом.

   Каждый сервис информирует о транзакции на разном уровне. Сервисы, выбранные по умолчанию: Applications, End-to-End и Internet.

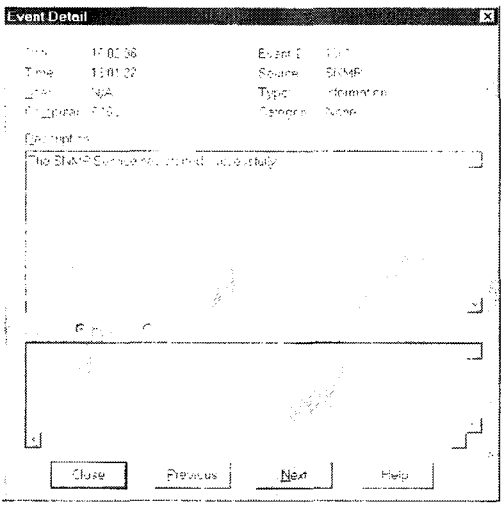
| Сервис | Выберите эту опцию, если |
|---|---|
| Physical | компьютер, работающий под Windows NT, управляет какими-либо физическими устройствами, например повторителями (repeaters) |
| Datalink/ Subnetwork | компьютер, работающий под Windows NT, управляет мостом |
| Internet | компьютер, работающий под управлением Windows NT, действует как IP-шлюз (маршрутизатор) |
| End-to-End | компьютер под управлением Windows NT, действует как IP-узел. Эта опция должна быть указана всегда |
| Applications | компьютер, работающий под управлением Windows NT, использует любое TCP/IP-приложение. Эта опция должна быть указана всегда |

5. Нажмите **OK**.
6. Нажмите **Close**.



## Обнаружение ошибок

Если сервис SNMP дал сбой по какой-либо причине, это будет отмечено в *системном журнале* (system log) в Event Viewer. Именно туда следует заглянуть в первую очередь при возникновении проблемы, связанной с сервисом SNMP.




▶ **Просмотр сообщения об ошибках SNMP в Event Viewer**

1. Щелкните кнопку **Start**, укажите на **Programs**, затем — на **Administrative Tools** и выберите **Event Viewer**.
2. Выберите пиктограмму сообщения, чтобы прочесть информацию об ошибке.

## Упражнения

В этих упражнениях Вы посредством Performance Monitor просмотрите объекты, добавленные в результате установки сервиса SNMP. Затем, используя Performance Monitor, посмотрите изменение счетчиков активности по протоколам ICMP и IP, связанное с выполнением команды Ping.

---

Примечание Для выполнения этих упражнений Вам необходимо установить SNMP, используйте инструкцию из этой главы.

---

► **Просмотр новых объектов в Performance Monitor**

1. Щелкните кнопку **Start**, укажите на **Programs**, затем на — **Administrative Tools** и выберите **Performance Monitor**.

   Появится окно **Performance Monitor**.
2. В меню **Edit** выберите **Add to Chart**.

   Появится диалоговое окно **Add to Chart**.
3. В поле **Object** нажмите стрелку, чтобы вывести список объектов.
4. Перечислите относящиеся к TCP/IP объекты.

► **Наблюдение за датаграммами IP с помощью Performance Monitor**

1. В поле **Object** выберите из списка **ICMP**.

   Появится список счетчиков ICMP.
2. В поле **Counters** выберите **Message/sec**.
3. В поле **Scale** установите *1.0* и нажмите **Add**.
4. В поле **Object** выберите **IP**.
5. В поле **Counters** выберите из списка **Datagrams Sent/sec**.
6. В поле **Scale** установите *1.0* и нажмите **Add**.
7. Нажмите **Done**.

   Ваш выбор появится в области отображения.
8. В меню **Options** выберите **Chart**.
9. Измените **Vertical Maximum** на *10* и нажмите **OK**.
10. Перетащите окно **Performance Monitor** в верхнюю часть экрана.
11. В командной строке выполните Ping по адресу второго компьютера.
12. Вернитесь в **Performance Monitor**, и Вы сможете наблюдать активность, вызванную выполнением Ping.

    Какая активность была отмечена в результате выполнения Ping?

    Сколько сообщений ICMP в секунду было записано?

    Сколько IP-датаграмм в секунду было послано?

    Почему сообщений ICMP послано в два раза больше чем IP-датаграмм?
13. Закройте **Performance Monitor**.

## Утилита SNMPUTIL

В составе *Microsoft Windows NT Resource Kit* поставляется утилита Snmputil (Snmputil.exe), которая проверяет корректность установки сервиса SNMP для связи с управляющими станциями SNMP. Snmputil выполняет те же самые вызовы, что и управляющая станция SNMP.

Вот ее синтаксис:

```
snmputil команда агент сообщество идентификатор_объекта_(OID)
```

Возможные команды:

*get* — позволяет получить значение запрашиваемого идентификатора объекта;

*getnext* — позволяет получить значение объекта, следующего за заданным идентификатором;

*walk* — позволяет переходить по ветви MIB, заданной идентификатором объекта.

Например, чтобы определить число предоставленных в аренду адресов сервером DHCP с именем DHCPserver в сообществе Public, Вам понадобится ввести команду:

```
snmputil getnext DHCPserver Public.1.3.6.1.4.1.311.1.3.2.1.1.1
```

Эта команда выдаст *идентификатор объекта* (OID) и значение счетчика для указанного в запросе идентификатора объекта, в приведенном случае — число взятых в аренду IP-адресов.

### Упражнения

В этом упражнении Вы, посмотрев описания объектов MIB, получите доступ к объектам SNMP для просмотра данных, собранных агентом SNMP и программой управления. В первой части упражнения Вы используйте утилиту Snmputil.exe, чтобы удостовериться, что Ваш агент SNMP сконфигурирован для установки связи с администратором SNMP.

▶ **Просмотр данных SNMP**

1. Скопируйте файл D:\LabFiles\Chapt15\Snmputil.exe в каталог C:\Winnt. Здесь D: — метка дисковода компакт-дисков.
2. Откройте командную строку.
3. С помощью Snmputil.exe определите относящиеся к DHCP объекты SNMP. Введите следующую команду в одной строке и затем нажмите ENTER: (*host_id* замените нужным значением).

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.3.2.1.1.1
```

Сколько адресов было арендовано?

4. Примените утилиту Snmputil.exe к объекту WINS 1.3.6.1.4.1.311.1.2.1.17. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.2.1.17
```

Сколько успешно разрешенных запросов было обработано WINS-сервером?

5. Примените утилиту Snmputil.exe к объекту WINS 1.3.6.1.4.1.311.1.2.1.18. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.2.1.18
```

Сколько неуспешных запросов было выполнено сервером WINS?

6. Примените утилиту Snmputil.exe к объекту LAN Manager 1.3.6.1.4.1.77.1.1.1. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.77.1.1.1
```

7. Примените утилиту Snmputil.exe к объекту LAN Manager 1.3.6.1.4.1.77.1.1.2. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.77.1.1.2
```

Какая версия Windows NT Server работает на компьютере?

## Резюме

Перед установкой SNMP Вам необходимо определить *сообщество* — группу, к которой принадлежит SNMP-компьютер. SNMP обеспечивает минимальный уровень безопасности и контекстную проверку для агентов. Вы можете использовать Event Viewer для обнаружения сбоев сервиса SNMP.

# Закрепление материала

? Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие четыре операции SNMP Вы знаете?

2. Какие операции SNMP инициируются системой управления? Какие инициируются агентом?

3. Какие виды MIB поддерживаются ОС Windows NT 4.0?

4. Какие методы разрешения имен узлов использует SNMP?

5. Для чего используется имя сообщества?

# Поиск и устранение неисправностей Microsoft TCP/IP



## В этой главе

Здесь кратко описан порядок диагностики IP-сети. Вы узнаете об утилитах Microsoft Windows NT и TCP/IP, которые бывают весьма полезными при решении различных проблем TCP/IP, а также о распространенных проблемах, возникающих при использовании TCP/IP, их симптомах и возможных причинах.

## Прежде всего

Для успешного изучения материалов этой главы не нужно выполнять никаких подготовительных операций.

# Занятие 1. Применение средств диагностики Windows NT

Для поиска и устранения связанных с TCP/IP проблем существует хорошо продуманный алгоритм. На этом занятии Вы познакомитесь с ним и узнаете об утилитах Windows NT, используемых при его применении.

**Изучив материал этого занятия, Вы сможете:**

- ✓ выявлять распространенные проблемы, связанные с TCP/IP;
- ✓ пользоваться утилитами для их диагностики и устранения;
- ✓ рассказать о том, как диагностировать TCP/IP.

**Продолжительность занятия — 20 минут**

Устранение неисправности значительно упрощается, если Вы можете определить источник ее возникновения. Проблемы, связанные с TCP/IP, могут быть сгруппированы по категориям.

| Причина проблемы | Общие характеристики проблемы |
|---|---|
| Конфигурация | Узел не инициализируется, или не запускается один из сервисов |
| IP-адресация | Не получается соединение с другими узлами. Возможно, Ваш узел не отвечает на их запросы |
| Деление на подсети | Команда Ping на Вашу рабочую станцию выполняется успешно, но Вы не можете получить доступ к локальным/удаленным узлам |
| Разрешение адреса | Команда Ping по IP-адресу Вашей рабочей станции выполняется успешно, но Ping не проходит на другие узлы |
| Разрешение имени NetBIOS | Вы можете получить доступ к узлу по его IP-адресу, но не можете установить соединение с помощью команды *net* |
| Разрешение имени узла | Вы можете получить доступ к узлу по его IP-адресу, но не можете сделать этого с использованием его имени |

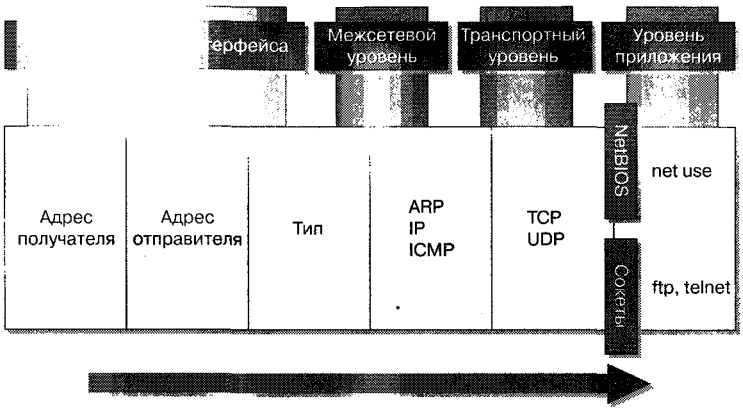
## Утилиты Windows NT

Windows NT включает несколько утилит, которые могут оказаться полезными при диагностировании проблем, связанных с TCP/IP.

| Название утилиты | Применение |
|---|---|
| Ping | Проверка правильности конфигурирования TCP/IP и доступности других узлов |
| Arp | Просмотр кэша ARP для обнаружения неверной записи |
| Netstat | Отображение статистики протокола и текущего состояния TCP/IP-соединений |
| Nbtstat | Контроль состояния соединений по протоколу NetBIOS поверх TCP/IP, обновление кэша LMHOSTS или определение зарегистрированного Вашим узлом имени и идентификатора области видимости (NetBIOS Scope ID) |
| Ipconfig | Проверка конфигурации TCP/IP, включая адреса серверов DHCP и WINS |
| Tracert | Регистрация маршрута до удаленного узла |
| Route | Отображение и модификация локальной таблицы маршрутизации |
| Nslookup | Отображение информации, получаемой от серверов DNS |
| Сервис Microsoft SNMP | Передача статистической информации системам управления, основанным на SNMP |
| Журнал событий | Отслеживание событий и ошибок |
| Performance Monitor | Анализ производительности и выявление узких мест |
| Network Monitor | Перехват входящих и исходящих пакетов для анализа проблемы |
| Редактор Реестра | Просмотр и изменение параметров конфигурации |

## Порядок диагностики

Диагностику TCP/IP рекомендуется проводить от нижнего уровня семейства протоколов Интернета к верхнему, как показано на иллюстрации. Цель такой диагностики — проверка способности протоколов каждого уровня связываться с протоколами верхнего и нижнего уровней.




Процедура состоит из двух этапов.

1. Проверьте, успешно ли выполняется команда Ping.

   Если да, то IP-связи между *уровнем сетевого интерфейса* (Network Interface layer) и *уровнем Интернета* (Internet layer) в норме. Утилита Ping использует протокол ARP для разрешения IP-адреса в адрес сетевого адаптера для каждого эхо-запроса и эхо-ответа.

2. Попробуйте установить соединение с другим узлом.

   Тем самым Вы проверите TCP/IP-соединения с уровня сетевого интерфейса до уровня приложения.

---

Примечание Если Вы не в состоянии самостоятельно устранить неисправность, Вам может понадобиться IP-анализатор (например, Microsoft Network Monitor) для просмотра сетевой активности на каждом уровне.

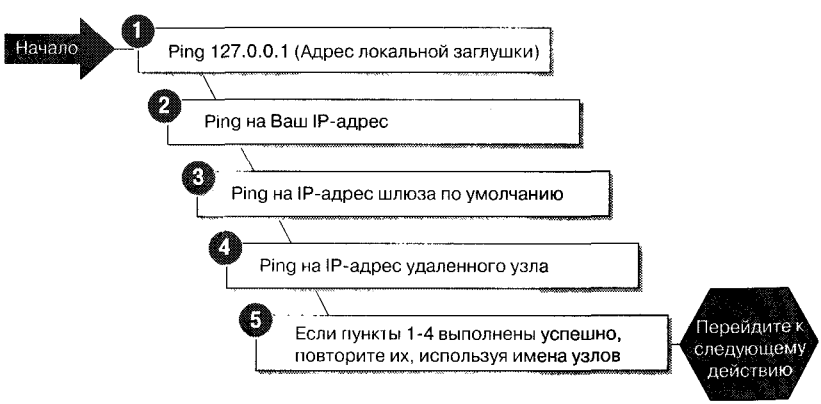
---

## Проверка IP-соединений

В самом начале при помощи утилиты Ping проверьте, как проходят сетевые пакеты. Этим Вы проконтролируете связь между уровнем сетевого интерфейса и уровнем Интернета. Рекомендуется при проверке использовать имя узла только после того, как Вы успешно выполнили Ping, указывая IP-адрес. Инструкция и иллюстрация показывают, как диагностировать соединения с помощью утилиты Ping.

▶ **Диагностика уровней сетевого интерфейса и Интернета средствами утилиты Ping**

1. Для проверки правильности установки и загрузки TCP/IP выполните Ping по адресу локальной заглушки. Если эта попытка оказалась неудачной, проверьте, была ли система перезагружена после установки и конфигурирования TCP/IP.
2. Выполните Ping, указав в качестве параметра свой IP-адрес, чтобы проверить, правильно ли он сконфигурирован. Если эта операция завершилась неудачей:
   - посмотрите конфигурацию, используя программу **Network** из **Control Panel** для контроля правильности введенного адреса.
   - проверьте корректность IP-адреса и его соответствие выбранной схеме адресации.
3. Выполните Ping по IP-адресу шлюза по умолчанию, чтобы удостовериться, что шлюз функционирует и правильно сконфигурирован и что внутри Вашей локальной сети возможна связь. Если эта операция завершилась неудачей, убедитесь в том, что Вы используете правильные IP-адрес и маску подсети.
4. Выполните Ping по IP-адресу удаленного узла для проверки связи с внешней сетью. Если эта операция завершилась неудачей:
   - убедитесь, что задан правильный IP-адрес шлюза по умолчанию;
   - убедитесь, что удаленный узел функционирует;
   - проверьте, работает ли соединение между маршрутизаторами.
5. После того как Вы установили, что команда Ping выполняется успешно при указании IP-адреса, повторите Ping, задав имя узла для проверки правильности конфигурирования имени в файле HOSTS.



## Проверка TCP/IP-соединений

Следующая задача при поиске неисправностей — проверка соединений от уровня Интернета до уровня приложения путем установки сеанса связи. Используйте один из методов, показанных на рисунке.

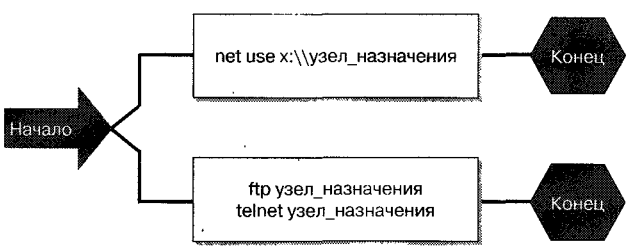
Для создания сеанса связи NetBIOS поверх TCP/IP с компьютером, работающим под управлением Windows NT, или другим совместимым с RFC узлом NetBIOS, установите соединение, используя команду *net use* или *net view*. Если эта операция завершилась неудачей:

- проверьте, поддерживает ли тот узел, с которым Вы пытаетесь связаться, протокол NetBIOS;
- убедитесь, что совпадают идентификаторы области видимости вызывающего узла и узла, с которым Вы устанавливаете связь;
- проверьте, правильность используемого имени NetBIOS;
- если узел, с которым Вы устанавливаете связь, находится в удаленной сети, удостоверьтесь, что необходимое Вам правильное отображение имени в IP-адрес возможно средствами WINS или файла LMHOSTS.

Чтобы установить сеанс связи с IP-узлом, используя Сокеты Windows, примените утилиту Telnet или FTP. Если эта операция завершилась неудачей:

- удостоверьтесь, что на узле, с которым Вы связываетесь, работает сервер Telnet или FTP;
- убедитесь, что Вы имеете соответствующие права на этом узле;
- при попытке установить соединение, используя имя узла, убедитесь, что на сервере DNS или в файле HOSTS есть соответствующая запись.

С узлом, поддерживающим NetBIOS в соответствии с RFC




С другим узлом, поддерживающим TCP/IP

## Резюме

Если Ping выполняется успешно, то связи от уровня сетевого интерфейса до уровня Интернета работоспособны. Если Вы можете создать сеанс связи, то связи от уровня Интернета до уровня приложения работоспособны.

# Закрепление материала

Эти вопросы помогут Вам лучше усвоить основные темы данной главы. Если Вы не сумеете ответить на вопрос, повторите материал соответствующего занятия.

1. Какие три утилиты Windows NT используются при диагностике проблем, связанных с TCP/IP?

2. Какие утилиты TCP/IP используются для проверки связей от уровня сетевого интерфейса до уровня Интернета?

3. Какие две процедуры диагностики IP-сети Вы знаете?

# Вопросы и ответы

## Глава 1. Основные сведения о TCP/IP

Стр. 8 **Закрепление материала**

1. Что акое TCP/IP?

   **TCP/IP — это набор протоколов, предоставляющий средства маршрутизации в глобальных сетях и позволяющий взаимодействовать различным узлам Интернета.**

2. Публикуются ли стандарты протокола TCP/IP в RFC? Все ли RFC описывают стандарты?

   **Да, стандарты TCP/IP всегда публикуются в RFC. Однако не все RFC описывают стандарты.**

## Глава 2. Установка и конфигурация TCP/IP

Стр. 21 **Закрепление материала**

1. Какие утилиты используются для проверки и тестирования конфигурации TCP/IP?

   **Ipconfig и Ping.**

2. Какие параметры должны в обязательном порядке назначаться компьютеру с ОС Windows NT, использующему TCP/IP в глобальной сети?

   **IP-адрес, маска подсети и IP-адрес шлюза по умолчанию.**

# Глава 3. Обзор архитектуры стека протоколов TCP/IP

## Ответы к упражнениям

► **Подробный просмотр кадра ARP-запроса**

Стр. 33

5. В окне **Detail** разверните **ETHERNET**.

   Появятся свойства кадра **ETHERNET**.

   Каков адрес получателя?

   **FFFFFFFFFFFF**

   Соответствует ли адрес получателя какому-нибудь адресу сетевого адаптера?

   **Нет, это адрес для широковещания.**

   Каков адрес отправителя?

   **Адрес сетевого адаптера Вашего компьютера.**

   Какой тип имеет этот кадр Ethernet?

   **0x0806 — ARP: Address Resolution Protocol (Протокол ARP).**

7. В окне **Detail** разверните **ARP_RARP**.

   Каков адрес сетевого адаптера отправителя?

   **Адрес может быть различным.**

   Каков адрес сетевого адаптера получателя?

   **Адрес 000000000000, поскольку это пакет запроса, и в данный момент адрес сетевого адаптера неизвестен.**

   Каков адрес протокола получателя?

   **131.107.2.211**

► **Подробный просмотр кадра ARP-ответа**

Стр. 34

2. В окне **Detail** разверните **ETHERNET:ETYPE**.

   Появятся свойства кадра **ETHERNET:ETYPE**.

   Каков адрес получателя?

   **Может быть различным**.

   Соответствует ли адрес получателя какому-нибудь адресу сетевого адаптера?

   **Да**.

   Каков адрес отправителя?

   **Адрес сетевого адаптера Вашего компьютера.**

Каков тип кадра Ethernet?

**0x0806 — ARP: Address Resolution Protocol.**

4. В окне **Detail** разверните **ARP_RARP**.

   Каков адрес сетевого адаптера отправителя?

   **Может быть различным.**

► **Просмотр кэша протокола ARP**

Стр. 35 2. Запомните запись для шлюза по умолчанию (если он сконфигурирован), например:

   131.107.2.1 08-00-02-6c-28-93

   **Записи могут быть разными.**

► **Ping на адрес локального узла**

Стр. 35 2. Просмотрите новую запись в кэше протокола ARP.

   Какая запись была добавлена?

   **Для узла, на адрес которого выполнялся Ping (для Вашего второго компьютера).**

   Какого она типа?

   **Dynamic (Динамическая).**

► **Добавление ARP-записи**

Стр. 36 2. Просмотрите кэш протокола ARP и убедитесь, что запись добавлена.

   Какого она типа?

   **Static (Статическая).**

   Почему тип этой записи отличается от предыдущих?

   **Потому что запись была добавлена вручную, а не в результате широковещания. Такие записи остаются в кэше до тех пор, пока компьютер не перезагрузится.**

Стр. 52 ## Закрепление материала

1. Какие уровни используются в четырехуровневой модели TCP/IP?

   **Уровень приложения (Application), транспортный (Transport), Интернета (Internet), или межсетевой, и сетевого интерфейса (Network Interface).**

2. Какие основные протоколы обеспечиваются в транспортном драйвере протокола Microsoft TCP/IP?

   **TCP, UDP, ICMP, IGMP, IP и ARP.**

3. Какой протокол используется для информирования клиента о недоступности сети-получателя?

   **ICMP.**

4. Как изменяется датаграмма протокола IP при прохождении через маршрутизатор?

   **Уменьшается TTL, обновляется значение контрольной суммы возможна фрагментация.**

5. Когда используется протокол UDP?

   **Когда приложению необходимо послать данные без установления соединения — обычно при отправке сообщений нескольким принимающим станциям.**

6. На какой адрес отправляются ARP-запросы?

   **На широковещательный адрес (FFFFFFFFFFFF).**

7. Какой адрес выясняется при помощи ARP-запроса при отправке пакета на локальный узел? На удаленный узел?

   **Для локального узла — это адрес сетевого адаптера этого узла Для удаленного узла — это адрес сетевого адаптера шлюза, к которому надо отсылать датаграммы (обычно это Ваш шлюз по умолчанию).**

# Глава 4. IP-адресация

## Ответы к упражнениям

Стр. 56

1. Переведите следующие двоичные числа в деятичные.

| Двоичное значение | Десятичное значение |
|---|---|
| 10001011 | **139** |
| 10101010 | **170** |
| 10111111 11100000 00000111 10000001 | **191.224.7.129** |
| 01111111 00000000 00000000 00000001 | **127.0.0.1** |

2. Переведите следующие деятичные числа в двоичные.

| Десятичное значение | Двоичное значсние |
|---|---|
| 250 | **11111010** |
| 19 | **00010011** |
| 109.128.255.254 | **01101101 10000000 11111111 11111110** |
| 131.107.2.89 | **10000011 01101011 00000010 01011001** |

Стр. 60 1. Укажите классы следующих IP-адресов.

| IP-адрес | Класс |
|---|---|
| 131.107.2.89 | **B** |
| 3.3.57.0 | **A** |
| 200.200.5.2 | **C** |
| 191.107.2.10 | **B** |

2. В сетях каких классов IP-адресов более 1 000 узлов?

   **В сетях класса A (16 777 214) и класса B (65 534).**

3. В сетях каких классов IP-адресов только 254 узла?

   **В сетях класса C.**

Стр. 64 Определите, какие IP-адреса не могут быть назначены узлам. Объясните, почему такие IP-адреса не являются корректными.

A. 131.107.256.80

   **Этот IP-адрес недопустим, поскольку значение одного числа (октета) не может превышать 255.**

B. 222.222.255.222

   **Это допустимый IP-адрес.**

C. 231.200.1.1

   **Этот IP-адрес недопустим, поскольку 231 определяет адреса класса D, которые не используются как IP-адреса узлов.**

D. 126.1.0.0

   **Это допустимый IP-адрес.**

E. 0.127.4.100

   **Ноль — недопустимое значение. Оно означает «только эта сеть»**

F. 190.7.2.0

   **Это допустимый IP-адрес.**

G. 127.1.1.1

   **Этот IP-адрес недопустим, поскольку адрес 127 зарезервирован для диагностических целей.**

H. 198.121.254.255

   **Этот IP-адрес недопустим, поскольку 255 в качестве номера узла означает широковещание.**

I. 255.255.255.255

   **Этот IP-адрес недопустим, поскольку 255 — это широковещательный адрес.**

Стр. 64 А сейчас определите, каким сетевым компонентам TCP/IP необходим IP-адрес. Если указан тип протокола, предполагается, что это единственный протокол, поддержка которого установлена на данном узле. Рассмотрите перечисленные ниже сетевые компоненты и отметьте буквы, соответствующие компонентам, которым необходим IP-адрес.

A. Компьютер под управлением ОС Windows NT, использующий TCP/IP.
B. Рабочая станция, использующая LAN Manager и соединяющаяся с компьютером под управлением Windows NT с поддержкой TCP/IP.
C. Компьютер под управлением ОС Windows 95, которому необходим доступ к общим ресурсам на компьютере с Windows NT, использующем TCP/IP.
D. Хост UNIX, к которому Вы хотите осуществлять доступ с помощью утилит TCP/IP.
E. Принтер с сетевым интерфейсом, поддерживающим TCP/IP.
F. Маршрутизатор для соединения с удаленной IP-сетью.
G. Адаптер Ethernet на маршрутизаторе для локальной сети.
H. Рабочая станция, использующая Microsoft LAN Manager и пытающаяся соединиться с сервером LAN Manager, который применяет NetBEUI.
I. Компьютер под управлением ОС Windows for Workgroups, которому необходим доступ к общим ресурсам на сервере LAN Manager, поддерживающем NetBEUI.
J. Плоттер, подключенный к последовательному порту компьютера под управлением ОС Microsoft Windows NT, использующего TCP/IP.
K. Сетевой принтер, совместный доступ к которому осуществляется с помощью сервера LAN Manager, использующего NetBEUI.
L. Коммуникационный сервер, предоставляющий терминальный доступ кузлам TCP/IP.
M. Шлюз по умолчанию в Вашей сети.

**IP-адрес необходим всем сетевым компонентам, кроме H, I, J и K.**

Стр. 65 Сейчас определите, какой класс адресов необходим для указанной IP-сети. Затем назначьте IP-адреса каждому типу узлов (UNIX, рабочие станции Windows NT, серверы), чтобы облегчить их идентификацию. Все компьютеры — в одной подсети.

Какие классы адресов могут использоваться для этой сети?

**Классы A и B.**

Какой из перечисленных ниже IP-адресов может быть использован для данной сети?

A. 197.200.3.0
B. 11.0.0.0
C. 221.100.2.0
D. 131.107.0.0

**B и D.**

Стр. 65 Используя выбранный Вами идентификатор сети, назначьте диапазон идентификаторов узлов каждому типу компьютеров так, чтобы можно было легко отличить друг от друга серверы и рабочие станции под управлением Windows NT и рабочие станции под управлением UNIX.

| Тип TCP/IP узла | Диапазон IP-адресов |
|---|---|
| Сервер Windows NT | **Всем серверам назначайте большие номера, например 200—250** |
| Рабочая станция Windows NT | **Всем рабочим станциям Windows NT назначайте маленькие номера, например 150—200** |
| Рабочая станция UNIX | **Компьютерам UNIX назначайте номера, отличные от используемых серверами и рабочими станциями UNIX** |

Стр. 66 Определите, сколько идентификаторов узлов и сетей необходимо для сети, изображенной ниже.

Сколько идентификаторов сетей необходимо для данного сетевого окружения?

**2 локальные сети (E и F) + 3 глобальные (A, B и C) = 5**

Сколько идентификаторов узлов необходимо для данного сетевого окружения?

**50 (компьютеры Windows NT Server) + 200 (компьютеры Windows NT Workstation) + 50 (рабочие станции UNIX) + + 6 (сетевые интерфейсы маршрутизаторов) = 306**

Какой шлюз по умолчанию (интерфейс маршрутизатора) должен быть указан для рабочих станций с ОС Windows NT, которые связываются в основном только с рабочими станциями UNIX?

**Интерфейс E маршрутизатора.**

Стр. 69 Выполните логическую операцию «И» с перечисленными ниже IP-адресами и маской подсети и определите, принадлежит ли IP-адрес получателя к локальной или удаленной сети.

1. Получен ли одинаковый результат?

   **Нет.**

2. Принадлежит IP-адрес получателя к локальной или к удаленной сети?

   **К удаленной.**

Стр. 73

## Закрепление материала

1. Какие октеты представляют идентификатор сети и узла в адресах классов A, B и C?

   **Класс A. Первое число (октет) — идентификатор сети, остальные три числа — идентификатор узла.**

   **Класс B. Первые два числа — идентификатор сети, другие два числа — идентификатор узла.**

   **Класс C. Первые три числа — идентификатор сети, последнее число — идентификатор узла.**

2. Какие значения не могут быть использованы в качестве идентификатоов сетей и почему? Какие значения не могут быть использованы в качестве идентификаторов узлов и почему?

   **В качестве идентификатора сети не может использоваться число 127, зарезервированое для локальной заглушки.**

   **В качестве идентификаторов сетей и узлов можно использовать любые числа, кроме «все 1» (255) и «все 0» (0). «Все 1» используется для широковещания. «Все 0» обозначает локальную сеть или «только эта сеть».**

3. Когда необходим уникальный идентификатор сети?

   **Разные идентификаторы сети необходимы для разных физических сетей и для соединения через два маршрутизатора в глобальной сети.**

4. Каким компонентам сетевого окружения TCP/IP, кроме компьютеров, необходим идентификатор узла?

   **Каждый узел, использующий TCP/IP, должен иметь идентификатор узла, который в совокупности с идентификатором сети уникален. Это касается и маршрутизаторов.**

## Ответы к упражнениям

Стр. 73 Изучите следующую иллюстрацию, перечислите все проблемы IP-адресации и объясните, как каждая из них может повлиять на сетевые соединения. Правильно ли выбраны IP-адреса и шлюзы по умолчанию в каждом из следующих случаев?

**Узлу B задан неверный адрес шлюза по умолчанию, поэтому связь будет ограничена только локальной сетью.**

**Узлу D не назначен шлюз по умолчанию, поэтому связь будет ограничена только локальной сетью.**

**Узлы F и I имеют одинаковые IP-адреса. Это может вызвать проблемы, если какой-нибудь узел попытается обратиться по IP-адресу 147.103.0.1.**

Стр. 74 Изучите следующую иллюстрацию, перечислите все проблемы IP-адресации и объясните, как каждая из них может повлиять на сетевые соединения. Правильно ли выбраны IP-адреса и шлюзы по умолчанию в каждом из следующих случаев?

**Узлы C и E имеют одинаковые IP-адреса (109.128.5.35). Windows NT обнаружит повторное использование адреса и произойдет сбой при инициализации TCP/IP. Если одинаковые IP-адреса имеют узлы другого типа, но использующие TCP/IP (например, LAN Manager), то узлы C и E не смогут взаимодействовать друг с другом, перестанут отвечать, и другие узлы не получат к ним доступа.**

**Для узла B задан идентификатор сети, отличный от других узлов. Поэтому он не сможет взаимодействовать ни с одним локальным узлом. Он не сумеет связаться с удаленными узлами, поскольку идентификатор сети шлюза по умолчанию тоже отличается идентификатора сети этого узла.**

**Узел F имеет тот же IP-адрес, что и его шлюз по умолчанию Он не сможет взаимодействовать ни с локальными, ни с удаленными узлами.**

# Глава 5. Подсети

## Ответы к упражнениям

Стр. 83

Определите необходимую маску подсети для различных ситуаций. Помните, что деление на подсети применяется не всегда.

1. Адрес класса A в локальной сети.
   **255.0.0.0**
2. Адрес класса B в локальной сети, состоящей из 4 000 узлов.
   **255.255.0.0**
3. Адрес класса C в локальной сети, состоящей из 254 узлов.
   **255.255.255.0**
4. Адрес класса A в сети, содержащей 6 подсетей.
   **255.224.0.0**
5. Адрес класса B в сети, содержащей 126 подсетей.
   **255.255.254.0**
6. Адрес класса A, если в настоящее время сеть содержит 30 подсетей, в следующем году планируется увеличить их число до 65, причем в каждой подсети будет более 50 000 узлов?
   **Используя 7 разрядов = 255.254.0.0**
   **Используя 8 разрядов = 255.255.0.0**
7. Какой запас на случай будущего расширения сети обеспечивает маска подсети из предыдущего задания?
   **Использование 7 разрядов обеспечивает до 126 подсетей и 131 070 узлов в каждой подсети.**
   **Использование 8 разрядов обеспечивает до 254 подсетей и 65 534 узла в каждой подсети.**
8. Адрес класса B, если в настоящее время сеть содержит 14 подсетей, в течение следующих двух лет размер каждой подсети может увеличиться вдвое, причем в каждой подсети будет не более 1500 узлов.
   **Используя 5 разрядов = 255.255.248.0**
9. Какой запас на случай будущего расширения сети обеспечивает маска подсети из предыдущего задания?
   **Использование 5 разрядов обеспечивает до 30 подсетей и 2 046 узлов в каждой подсети.**

Стр. 84 Рассмотрите две некорректно заданные маски подсети и определите, что произойдет при попытке установить соединение с узлом из локальной или удаленной сети.

Используя приведенную ниже информацию, преобразуйте IP-адреса двух Ваших компьютеров в двоичный формат. Применив логическое «И», сложите их с маской подсети и определите, почему она задана неправильно.

| | | |
|---|---|---|
| Ваш IP-адрес | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.255.248 | 11111111 11111111 11111111 11111000 |
| Результат | | |
| IP-адрес получателя | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.255.248 | 11111111 11111111 11111111 11111000 |
| Результат | | |

Можно ли по результату выполнения операции сказать, принадлежат адреса отправителя и получателя к одной сети или к разным?

**К разным.**

Почему Вы не смогли бы успешно выполнить Ping шлюза по умолчанию?

**Протокол IP определит, что шлюз по умолчанию находится в удаленной сети, а доступного шлюза нет.**

Используя приведенную ниже информацию, преобразуйте IP-адрес Вашего компьютера и IP-адрес удаленного узла в двоичный формат. Применив логическое «И», сложите их с маской подсети и определите, почему она задана неправильно.

| | | |
|---|---|---|
| Ваш IP-адрес | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.0.0 | 11111111 11111111 00000000 00000000 |
| Результат | | |
| IP-адрес получателя | 131.107.y.z | 10000011 01101011 |
| Маска подсети | 255.255.0.0 | 11111111 11111111 00000000 00000000 |
| Результат | | |

Свидетельствует результат выполнения операции о том, что IP-адрес получателя и маска подсети принадлежат удаленной сети или локальной сети?

**Локальной.**

Почему Вы не смогли бы успешно выполнить Ping удаленного узла?

**Протокол IP попытается отправить пакеты к узлу в локальной сети, хотя на самом деле он находится в удаленной сети.**

Сравните результаты, полученные из-за применения неправильной маски подсети. Попытайтесь понять различие в поведении TCP/IP в случаях, если маска подсети относится к локальной или удаленной сети. Какие выводы можно сделать о том, как TCP/IP использует маску подсети?

**Маска подсети используется для того, чтобы определить находится IP-адрес в локальной сети или в удаленной. Если IP-адрес получателя находится в локальной сети, то датаграмма посылается прямо на этот узел. Если же IP-адрес получателя находится в удаленной сети, то узел-отправитель посылает датаграмму своему шлюзу по умолчанию.**

Стр. 85

Для каких узлов маска подсети задана неправильно?

**D и E.**

Как неправильное значение маски подсети влияет на работу этих узлов?

**Они не смогут взаимодействовать с другими узлами, у которых второй октет IP-адреса отличается от их собственного.**

Каково правильное значение маски подсети?

**255.0.0.0**

Что неправильно в этой маске подсети?

**Маска подсети определяет, что оба узла находятся в одной сети.**

Как это влияет на соединения?

**Пакеты, посланные одним узлом другому, не попадут в другую сеть, следовательно, эти два узла не смогут взаимодействовать друг с другом.**

Каково правильное значение маски подсети?

**Правильной маской подсети будет 255.255.255.0. Другие правильные маски подсети:**

**255.255.254.0**

**255.255.252.0**

**255.255.248.0**

**255.255.240.0**

**255.255.224.0**

Стр. 89 Определите маску подсети, соответствующую указанному диапазону IP-адресов.

1. Диапазон адресов от 128.71.1.1 до 128.71.254.254.

   **255.255.0.0**

   **Только используя все разряды октета можно получить идентификатор сети, равный 254, в данном случае это третий октет.**

2. Диапазон адресов от 61.8.0.1 до 61.15.255.254.

   **255.248.0.0**

   **Маска подсети 248 определяет приращение, равное 8.**

3. Диапазон адресов от 172.88.32.1 до 172.88.63.254.

   **255.255.224.0**

   **Приращение 32 определяет маску подсети 224.**

4. Диапазон адресов от 111.224.0.1 до 111.239.255.254.

   **255.240.0.0**

   **Диапазон сетей 224—239 использует приращение 16.**

5. Диапазон адресов от 3.64.0.1 до 3.127.255.254.

   **255.192.0.0**

   **Диапазон сетей 64—127 имеет приращение 64, используя в маске подсети только 2 разряда.**

Стр. 92 Определите идентификаторы подсетей для объединенной сети, состоящей из двух сетей, используя 2 бита маски подсети класса B.

1. Выпишите все возможные битовые комбинации для указанной ниже маски подсети. Переведите их в десятичный формат, чтобы определить начальное значение идентификаторов узлов для каждой подсети.

| 255 | 255 | | 192 | 0 |
|---|---|---|---|---|
| 11111111 | 11111111 | | 11000000 | 00000000 |
| Не используется | 00000000 | = | 0 | |
| Подсеть 1 | **01000000** | = | **64** | |
| Подсеть 2 | **10000000** | = | **128** | |
| Не используется | 11000000 | = | 192 (маска подсети) | |

2. Выпишите диапазон идентификаторов узлов для каждой подсети

| Подсеть | Начальное значение | Конечное значение |
|---|---|---|
| Подсеть 1 | w.x.**64.1** | w.x.**127.254** |
| Подсеть 2 | w.x.**128.1** | w.x.**191.254** |

Стр. 92 Определите диапазон идентификаторов сетей для объединенной сети, состоящей из 14 подсетей, используя для этого 4 бита маски подсети класса B.

1. Выпишите все возможные битовые комбинации для указанной ниже маски подсети. Переведите их в десятичный формат, чтобы определить начальное значение идентификаторов узлов для каждой подсети.

| 255 | 255 | | 240 | 0 |
|---|---|---|---|---|
| 11111111 | 11111111 | | 11110000 | 00000000 |
| Не используется | 00000000 | = | 0 | |
| Подсеть 1 | **00010000** | = | **16** | |
| Подсеть 2 | **00100000** | = | **32** | |
| Подсеть 3 | **00110000** | = | **48** | |
| Подсеть 4 | **01000000** | = | **64** | |
| Подсеть 5 | **01010000** | = | **80** | |
| Подсеть 6 | **01100000** | = | **96** | |
| Подсеть 7 | **01110000** | = | **112** | |
| Подсеть 8 | **10000000** | = | **128** | |
| Подсеть 9 | **10010000** | = | **144** | |
| Подсеть 10 | **10100000** | = | **160** | |
| Подсеть 11 | **10110000** | = | **176** | |
| Подсеть 12 | **11000000** | = | **192** | |
| Подсеть 13 | **11010000** | = | **208** | |
| Подсеть 14 | **11100000** | = | **224** | |
| Не используется | 11110000 | = | 240 (маска подсети) | |

2. Выпишите диапазон идентификаторов узлов для каждой подсети.

| Подсеть | Начальное значение | Конечное значение |
|---|---|---|
| Подсеть 1 | w.x.**16.1** | w.x.**31.254** |
| Подсеть 2 | w.x.**32.1** | w.x.**47.254** |
| Подсеть 3 | w.x.**48.1** | w.x.**63.254** |
| Подсеть 4 | w.x.**64.1** | w.x.**79.254** |
| Подсеть 5 | w.x.**80.1** | w.x.**95.254** |
| Подсеть 6 | w.x.**96.1** | w.x.**111.254** |
| Подсеть 7 | w.x.**112.1** | w.x.**127.254** |

*(продолжение)*

| Подсеть | Начальное значение | Конечное значение |
|---|---|---|
| Подсеть 8 | w.x.**128.1** | w.x.**143.254** |
| Подсеть 9 | w.x.**144.1** | w.x.**159.254** |
| Подсеть 10 | w.x.**160.1** | w.x.**175.254** |
| Подсеть 11 | w.x.**176.1** | w.x.**191.254** |
| Подсеть 12 | w.x.**192.1** | w.x.**207.254** |
| Подсеть 13 | w.x.**208.1** | w.x.**223.254** |
| Подсеть 14 | w.x.**224.1** | w.x.**239.254** |

Стр. 93 Используйте быстрый метод для определения диапазона идентификаторов сетей для 14 сетей. Сравните результаты с полученными в предыдущем задании. Они должны совпадать. Первый пункт этого упражнения уже выполнен.

1. Запишите двоичными единицами количество бит, используемых для маски подсети, дополнив его справа нулями до одного байта.

| 255 | 255 | 240 | 0 |
|---|---|---|---|
| 11111111 | 11111111 | 11110000 | 00000000 |

2. Укажите десятичное значение самого младшего бита из установленных в 1.

   **16**

3. Запишите двоичными единицами количество бит, используемых для маски подсети, переведите полученную запись в десятичный формат и вычтите 1. Вы получите возможное количество подсетей.

   **00001111 = 15 (8+4+2+1)**

   **15 – 1 = 14 (возможных подсетей)**

4. Начиная с нуля, добавляйте приращение, полученное в п. 2, столько раз, сколько возможно различных битовых комбинаций (вычислено в пункте 3).

   **Результаты должны совпасть со значениями, полученными в предыдущем задании.**

Стр. 95 Определите диапазон идентификаторов узлов для каждой из перечисленных подсетей.

1. Идентификатор сети — 75.0.0.0, маска подсети 255.255.0.0, две подсети.

   **Сеть A: 75.x.0.1 — 75.x.255.254**

**Сеть B: 75.y.0.1 — 75.y.255.254**

**(где x и y — любые числа от 1 до 254, но отличные друг от друга).**

2. Идентификатор сети — 150.17.0.0, маска подсети 255.255.255.0, четыре подсети.

   **Сеть A: 150.17.w.1 — 150.17.w.254**

   **Сеть B: 150.17.x.1 — 150.17.x.254**

   **Сеть C: 150.17.y.1 — 150.17.y.254**

   **Сеть D: 150.17.z.1 — 150.17.z.254**

   **(где w, x, y и z — любые числа от 1 до 254, попарно различные).**

3. Идентификаторы сетей — 107.16.0.0 и 107.32.0.0, маска подсети 255.240.0.0, две подсети.

   **Сеть A: 107.16.0.1 — 107.31.255.254**

   **Сеть B: 107.32.0.1 — 107.47.255.254**

   **Маска подсети со значением 240 допускает не более 14 подсетей, при этом идентификаторы сетей имеют значения с шагом 16.**

4. Идентификаторы сетей — 190.1.16.0, 190.1.32.0, 190.1.48.0, 190.1.64.0, маска подсети 255.255.248.0, четыре подсети.

   **Сеть A: 190.1.16.1 — 190.1.23.254**

   **Сеть B: 190.1.32.1 — 190.1.39.254**

   **Сеть C: 190.1.48.1 — 190.1.55.254**

   **Сеть D: 190.1.64.1 — 190.1.71.254**

   **Маска подсети со значением 248 допускает не более 30 подсетей, каждый идентификатор сети увеличивается на 8.**

5. Идентификаторы сетей — 154.233.32.0, 154.233.96.0 и 154.233.160.0, маска подсети 255.255.224.0, три подсети.

   **Сеть A: 154.233.32.1 — 154.233.63.254**

   **Сеть B: 154.233.96.1 — 154.233.127.254**

   **Сеть C: 154.233.160.1 — 154.233.191.254**

   **Маска подсети со значением 224 допускает не более 6 подсетей, каждый идентификатор сети увеличивается на 32.**

Стр. 98

## Закрепление материала

1. Каково назначение маски подсети?

   **Для маскирования части IP-адреса, чтобы службы IP могли отличать идентификатор сети и идентификатор узла.**

2. Когда необходима маска подсети?

   **Необходимо задать для каждого узла в TCP/IP-сети.**

3. Когда используется маска подсети по умолчанию?

   **Маска подсети по умолчанию используется в том случае, если TCP/IP-узел не является частью подсети.**

4. Когда необходимо задать специальную маску подсети?

   **Когда Вы делите Вашу сеть на подсети.**

## Ответы к упражнениям

Стр. 98 InterNIC выделил Вам один адрес сети класса B: 131.107.0.0. Интрасеть Вашей организации в настоящий момент состоит из 5 подсетей, в каждой из которых около 300 узлов. В течение следующего года число подсетей увеличится в 3 раза. В трех подсетях число узлов может достигнуть 1 000.

1. Сколько бит Вы использовали для маски подсети?
2. Какой запас на случай появления дополнительных сетей Вы оставили?
3. Какой запас на случай увеличения числа узлов Вы оставили?

   **Использование 5 бит позволит создать до 30 подсетей по 2046 узлов каждая.**

   **Использование 6 бит позволит создать до 62 подсетей по 1022 узлов каждая.**

Стр. 99 InterNIC выделил Вам один адрес сети класса A: 124.0.0.0. Изолированная сеть Вашей организации в настоящий момент состоит из 5 подсетей. В каждой из подсетей около 500 000 узлов. В ближайшем будущем Вы планируете разделить эти 5 подсетей на 25 меньших, чтобы облегчить управление ими. Число узлов в каждой из них может достичь 300 000.

1. Сколько бит Вы использовали для маски подсети?
2. Какой запас на случай появления дополнительных сетей Вы оставили?
3. Какой запас на случай увеличения числа узлов Вы оставили?

   **Использование 5 разрядов позволит создать до 30 подсетей по 524 286 узлов каждая.**

Стр. 99 В Вашей сети 5 подсетей, в каждой из которых около 300 узлов. В течение полугода количество подсетей превысит 100. Число узлов в каждой из них вряд ли станет больше 2 000. Вы не собираетесь подключать свою сеть к Интернету.

1. Какой класс адресов Вы использовали?
2. Сколько бит Вы использовали для маски подсети?
3. Какой запас на случай появления дополнительных сетей Вы оставили?
4. Какой запас на случай увеличения числа узлов Вы оставили?

**Здесь не обязательно разбивать сеть на подсети. Вы можете для каждой сети использовать IP-адреса принадлежащие различным сетям класса A или класса B. Адреса класса C использоваться не могут, поскольку они допускают не более 254 узлов в одной сети.**

Стр. 100 Поставщик услуг Интернета получил диапазон из 2 048 адресов сетей класса C, начиная с 192.24.0.0 до 192.31.255.0.

1. Какой IP-адрес должен использоваться в таблице маршрутизации для направления пакетов в объединенную сеть этого провайдера?

   **192.24.0.0**

2. Какая маска подсети должна использоваться для объединения всех этих сетей?

   **255.248.0.0**

   Клиенты этого провайдера предъявляют следующие требования:

   - клиент 1 собирается иметь не более 2 023 узлов;
   - клиент 2 собирается иметь не более 4 047 узлов;
   - клиент 3 собирается иметь не более 1 011 узлов;
   - клиент 4 собирается иметь не более 500 узлов.

Стр. 100 Определите значения недостающих параметров для каждого клиента.

1. Клиент 1

| | |
|---|---|
| Начальный IP-адрес | 192.24.0.1 |
| Конечный IP-адрес | 192.24.7.8 |
| Маска подсети | **255.255.248.0** |

2. Клиент 2

| | |
|---|---|
| Начальный IP-адрес | **192.24.16.1** |
| Конечный IP-адрес | 192.24.31.254 |
| Маска подсети | 255.255.240.0 |

3. Клиент 3

| | |
|---|---|
| Начальный IP-адрес | 192.24.8.1 |
| Конечный IP-адрес | **192.24.11.254** |
| Маска подсети | 255.255.252.0 |

4. Клиент 4

| | |
|---|---|
| Начальный IP-адрес | 192.24.14.1 |
| Конечный IP-адрес | 192.24.15.254 |
| Маска подсети | **255.255.254.0** |

# Глава 6. Реализация IP-маршрутизации

## Ответы к упражнениям

► **Просмотр таблицы маршрутизации**

Стр. 108 Какие адреса, отличные от Вашего IP-адреса и адреса заглушки отображены в поле **Gateway Address**? Если Вы работаете с компьютером, не подключенным к сети, то адрес шлюза не появится.

**Адрес шлюза по умолчанию для сети 0.0.0.0.**

► **Просмотр таблицы маршрутизации**

Стр. 109 Показан ли адрес шлюза по умолчанию в поле **Gateway Address**?

**Нет.**

► **Проверка сетевого соединения**

Стр. 109 • Выполните Ping IP-адреса Вашего второго компьютера или компьютера Вашей локальной сети.

Была ли попытка успешной?

**Да.**

Возможен ли Ping IP-адреса удаленного узла, если не указан адрес шлюза в таблице маршрутизации?

**Нет. Вы получите сообщение об ошибке, в котором сказано, что узел-получатель недоступен.**

► **Добавление записи маршрута**

Стр. 110 3. Если бы Вы указали адрес узла из другой сети, то был бы Ping успешным? Почему?

**Нет. Не заданы маршруты, ведущие в другую сеть, и не задан шлюз по умолчанию.**

Стр. 118

## Закрепление материала

1. Как осуществляется поддержка IP-маршрутизации?

   **Добавляют несколько плат сетевых адаптеров или назначают компьютеру несколько IP-адресов, а затем устанавливают флажок *Enable IP Forwarding*.**

2. Обязательно ли нужна таблица маршрутизации на компьютере с несколькими сетевыми интерфейсами, подключенном к корпоративной сети с двумя подсетями?

   **Нет, поскольку компьютер уже имеет интерфейсы для обеих.**

3. Когда надо создать статическую таблицу маршрутизации?

   **Когда компьютер с несколькими интерфейсами не поддерживает RIP и не имеет интерфейса к подсети.**

4. Какая информация нужна для таблицы маршрутизации?

   **Адрес сети назначения, маска подсети для этого адреса и адрес маршрутизатора, через который доступна сеть назначения. Можно использовать имена, но только если в файлах Networks и Hosts есть соответствующие записи.**

5. Почему протокол RIP обычно не используется в большой сети?

   **Потому что он производит слишком много широковещательных сообщений. Кроме того, дублирование информация от RIP на всех маршрутизаторах может занять много времени.**

# Глава 7. Протокол DHCP

## Ответы к упражнениям

► **Определение адреса сетевого адаптера**

Стр. 134

• В командной строке наберите *ipconfig /all*, и нажмите ENTER.

Существует как минимум два способа выяснения адреса Вашей платы сетевого адаптера. Назовите их.

**Перейдите в окно командной строки и введите *net config server*[redacted]**

**или**

**щелкните кнопку Start, выберите Programs, укажит[redacted] Administrative Tools, а затем щелкните Windows NT Diagnostic[redacted] Щелкните вкладку Network, а потом — Transports.**

► **Создание диапазона действия протокола DHCP**

Стр. 136 2. Дважды щелкните пиктограмму **Services**. Каковы имена сервисов протокола DHCP?

**Microsoft DHCP Server и DHCP Client.**

► **Проверка информации протокола TCP/IP, назначенной протоколом DHCP**

Стр. 143 2. Какой IP-адрес был назначен компьютеру клиента сервером протокола DHCP?

**Зарезервированный адрес клиента.**

3. Каков адрес шлюза по умолчанию?

**131.107.2.1 (назначен при помощи DHCP).**

► **Обновление аренды протокола DHCP**

Стр. 144 2. Когда истекает срок аренды?

**Ответ может быть разным, но примерно — спустя 24 часа с настоящего момента.**

5. Когда истекает срок аренды?

**Ответ может быть разным, но примерно — спустя 24 часа с настоящего момента.**

Стр. 152 ## Закрепление материала

1. Из каких этапов состоит аренда протокола DHCP?

**Клиент, использующий DHCP, посылает широковещательный запрос (DHCPDISCOVER) чтобы получить IP-адрес.**

**Все DHCP-серверы посылают предложения (DHCPOFFER).**

**DHCP-клиент выбирает предложение (DHCPREQUEST) от первого DHCP-сервера.**

**DHCP-сервер подтверждает его (DHCPACK) и выделяет IP-адрес для клиента.**

2. Когда клиенты протокола DHCP обновляют аренду?

**Сначала, по истечении половины времени аренды, осуществляется первая попытка обновить аренду на DHCP-сервере выделившем IP-адрес. Потом, по истечении 87,5% времени аренды — на любом DHCP-сервере.**

3. Как надо сконфигурировать сервер протокола DHCP для получения аренды клиентом протокола DHCP?

**На DHCP-сервере надо задать диапазон имющихся IP-адресов и маску подсети.**

4. В каких ситуациях нужно более одного сервера протокола DHCP в объединенной сети?

   **Когда ни один маршрутизатор не поддерживает RFC 1542.**

5. Как надо настроить DHCP-серверы, чтобы они «подстраховывали» друг друга?

   **В диапазоне доступных IP-адресов каждого сервера 75% составляют адреса в локальной сети и 25% — в удаленной.**

6. В каких случаях необходимо резервировать конкретный IP-адрес для клиента?

   **Когда в сети есть серверы, которые работают с клиентами, не использующими WINS. Для разрешения NetBIOS-имен узлов в удаленных сетях, эти клиенты должны использовать файл LMHOSTS. Если IP-адрес сервера не будет зарезервирован, то он может измениться, и клиент не сумеет разрешить его имя средствами файла LMHOSTS.**

# Глава 8. NetBIOS поверх TCP/IP

## Ответы к упражнениям

► **Настройка файла LMHOSTS**

Стр. 170 8. В окне **Path** наберите *\\Server2* и щелкните **OK**.

Каков ответ?

**Появится список совместно используемых ресурсов на \\Server2.**

Стр. 171 Добавьте необходимые записи в приведенные ниже файлы LMHOSTS так, чтобы узлы в обеих сетях могли взаимодействовать друг с другом.

**Файл LMHOSTS для узлов сети A**

| IP-адрес | Имя |
|---|---|
| **131.107.24.27** | **LMU** |
| **131.107.24.28** | **Workstation1** |
| **131.107.24.29** | **LMserver** |

**Файл LMHOSTS для узлов сети B**

| IP-адрес | Имя |
|---|---|
| **131.107.8.28** | **Workgroup1** |
| **131.107.8.29** | **Workgroup2** |

Стр. 172 **Закрепление материала**

1. Какие методы применяются для разрешения имен NetBIOS?

   **Локальное широковещание, файл LMHOSTS, сервер имен NetBIOS (например, WINS), файл HOSTS и DNS.**

2. Каково назначение файла LMHOSTS?

   **Разрешать NetBIOS-имена узлов удаленных сетей.**

# Глава 9. Windows Internet Name Service (WINS)

## Ответы к упражнениям

► **Использование службы WINS для разрешения имен**

Стр. 192 3. Запустите Windows NT Explorer и попытайтесь соединиться с другим компьютером в локальной сети.

   Была ли попытка успешной?

   **Да, просмотр локальных узлов возможен.**

   Установится ли соединение с удаленным узлом?

   **Нет, просмотр удаленных узлов не будет возможен.**

► **Просмотр содержимого базы данных WINS**

Стр. 201 6. Какие NetBIOS-имена клиент регистрирует на сервере WINS?

   **Все NetBIOS-имена, зарегистрированные сервером WINS, имя пользователя (если оно уникально) и WORKGROUP (возможно несколько раз).**

7. Как долго существуют такие имена?

   **Не меньше 6 дней.**

8. Есть ли записи для удаленных узлов на сервере WINS?

   **Нет.**

Стр. 206 **Закрепление материала**

1. Каковы основные преимущества службы WINS?

   **Автоматическая регистрация и освобождение NetBIOS-имен. Предоставляет возможности межсетевого и междоменного обзора. Отпадает необходимость в локальном файле LMHOSTS.**

2. Какими двумя способами можно установить поддержку WINS на клиентском компьютере?

   **Вручную или автоматически при помощи DHCP.**

3. Сколько серверов WINS необходимо в сети, состоящей из 12 подсетей?

   **Один. Но для надежности рекомендуется иметь несколько.**

4. Какими способами не WINS-клиенты могут разрешать имена NetBIOS?

   **Кэш имен NetBIOS, широковещание, локальный файл LMHOSTS, централизованный файл(ы) LMHOSTS, локальный файл HOSTS, DNS или прокси-агент WINS (WINS Proxy Agent).**

5. Когда необходимо использовать прокси-агент WINS?

   **Когда в подсетях есть не WINS-клиенты. Прокси-агент WINS перенаправляет серверу WINS широковещательные сообщения о регистрации и освобождении имен.**

6. Как часто происходит резервное копирование базы данных WINS после установки WINS с параметрами по умолчанию?

   **Никогда. Вам надо задать каталог для резервного копирования, после этого автоматическое резервное копирование будет осуществляться каждые 24 часа.**

7. Какие типы имен хранятся в базе данных WINS?

   **Уникальные и групповые имена NetBIOS.**

8. Как надо настроить репликацию WINS в глобальной сети с низкоскоростной связью и ограниченной полосой пропускания?

   **Для оптимального использования полосы пропускания репликация должна производится в период малой загруженности сети.**

9. Как надо настроить репликацию WINS в локальной сети, не перегружая сетевой трафик?

   **Чтобы лучше синхронизировать серверы, репликация должна происходить после небольшого числа изменений в базе данных.**

10. Когда служба WINS использует групповую адресацию?

    **Когда сообщает о себе другим WINS-серверам и, возможно, автоматически конфигурируется как партнер по репликации.**

# Глава 10. Просмотр сетевых ресурсов и функции доменов

## Ответы к упражнениям

Стр. 219

1. Какие компьютеры используют файл LMHOSTS для поддержки обзора объединенной сети? Записи для каких компьютеров необходимо занести в файл LMHOSTS?

   **Компьютеру C необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров G и H.**

   **Компьютеру G необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров C и H.**

   **Компьютеру H необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров C и G.**

2. Какие компьютеры используют файл LMHOSTS для подтверждения регистрации? Записи для каких компьютеров необходимо занести в файл LMHOSTS?

   **Ни одному компьютеру не нужен файл LMHOSTS, поскольку в каждой подсети есть контроллер домена. Если же локальный контроллер домена выйдет из строя, то указанным компьютерам нужен файл LMHOSTS.**

   **Компьютерам A и B нужен файл LMHOSTS, в котором указаны IP-адреса и NetBIOS-имена компьютеров G и H.**

   **Компьютерам D, E и F нужен файл LMHOSTS, в котором указаны IP-адреса и NetBIOS-имена компьютеров C и H.**

   **Компьютеру I нужен файл LMHOSTS, в котором указаны IP-адреса и NetBIOS-имена компьютеров C и G.**

3. Какие компьютеры используют файл LMHOSTS для поддержки синхронизации учетных записей домена? Записи для каких компьютеров необходимо занести в файл LMHOSTS?

   **Компьютеру C необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров G и H.**

   **Компьютеру G необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров C и H.**

   **Компьютеру H необходим файл LMHOSTS, в котором записаны IP-адреса и NetBIOS-имена компьютеров C и G.**

4. Если сервер WINS установлен в подсети Y и все компьютеры настроены для использования WINS, каким из них понадобится файл LMHOSTS?

   **Никаким.**

Стр. 220

### Закрепление материала

1. Почему возникают проблемы при обзоре ресурсов корпоративной IP-сети?

   **По умолчанию IP-маршрутизаторы не распространяют пакеты объявления узлов, доменов или рабочих групп.**

2. Каким образом главный броузер в подсети определяет IP-адрес главного броузера домена, если домен охватывает несколько подсетей?

   **Если главный броузер является WINS-клиентом, то он пытается разрешить NetBIOS-имя. Иначе, ищет в файле LMHOSTS запись с префиксом #DOM, соответствующую этому домену.**

3. Чем помогает сервис WINS при сборе информации о доменах и рабочих группах?

   **Главный броузер домена запрашивает у службы WINS список имен, которым дополняет свой список доменов и рабочих групп.**

4. Что необходимо сделать на контроллерах домена, не являющихся клиентами WINS, чтобы обеспечить синхронизацию учетных записей, когда домен охватывает несколько подсетей?

   **В файле LMHOSTS на каждом контроллере домена должны быть записи для всех остальных контроллеров домена.**

# Глава 11. Разрешение имен узлов

## Ответы к упражнениям

► **Ping имени локального узла**

Стр. 230

1. Введите *ping Server1* (где *Server1* — это имя Вашего компьютера) и нажмите ENTER.

   Каков результат?

   **Четыре подтверждения «Reply from IP address».**

2. Введите *ping Server2* (где *Server2* — Ваш второй компьютер) и нажмите ENTER.

   Каков результат теперь?

   **Четыре подтверждения «Reply from IP address».**

► **Ping имени компьютера в локальной сети**

Стр. 230 • Введите *ping computertwo* (*computertwo* — имя компьютера) и нажмите ENTER.

Каков результат?

**«Bad IP address computertwo».**

► **Использование файла HOSTS для разрешения имен**

Стр. 231 • Введите *ping computertwo* и нажмите ENTER.

Каков результат?

**Четыре подтверждения «Reply from IP address».**

Стр. 231 ### Закрепление материала

1. Что такое имя узла?

   **Псевдоним, назначенный TCP/IP-узлу для облегчения доступа к нему.**

2. Для чего используется имя узла?

   **Для упрощения ссылок на этот узел. Имена узлов используются программой Ping и другими утилитами TCP/IP.**

3. Из чего состоят записи файла HOSTS?

   **Из имени или имен узлов и соответствующего IP-адреса.**

4. Что происходит раньше: разрешение IP-адреса или разрешение имени узла?

   **Разрешение имени узла.**

# Глава 12. Доменная система имен

## Ответы к упражнениям

### Сценарий 1

Стр. 250 1. Сколько доменов Вам понадобится?

   **Один (или ни одного, если сервером имен управляет поставщик услуг Интернета).**

2. Сколько поддоменов Вам понадобится?

   **Ни одного.**

3. Сколько зон Вам понадобится?

   **Одну (или ни одной, если сервером имен управляет поставщик услуг Интернета).**

4. Сколько основных DNS-серверов Вам понадобится?

   **Один (или ни одного, если сервером имен управляет поставщик услуг Интернета).**

5. Сколько резервных DNS-серверов Вам понадобится?
   **Один (или ни одного, если сервером имен управляет поставщик услуг Интернета).**
6. Сколько кэширующих DNS-серверов Вам понадобится?
   **Ни одного.**

**Сценарий 2**

Стр. 253

1. Сколько доменов Вам понадобится?
   **1**
2. Сколько поддоменов Вам понадобится?
   **3**
3. Сколько зон Вам понадобится?
   **4**
4. Сколько основных DNS-серверов Вам понадобится?
   **4**
5. Сколько резервных DNS-серверов Вам понадобится?
   **4**
6. Сколько кэширующих DNS-серверов Вам понадобится?
   **10**
7. Используя приведенную ниже таблицу расстояний (в милях), распределите филиалы по зонам. Филиал должен находиться в той же зоне, что и ближайший к нему главный узел.

| Портланд, шт. Орегон | Бостон | Чикаго | Атланта |
|---|---|---|---|
| Лос-Анджелес | Монреаль | Денвер | Даллас |
| Солт-Лейк-Сити | Вашингтон, округ Колумбия | Канзас-Сити | Майами |
| Сан-Франциско | — | — | Новый Орлеан |

**Сценарий 3**

Стр. 255

1. Сколько доменов Вам понадобится?
   **Ни одного (домен этой компании находится в Женеве, Швейцария).**
2. Сколько поддоменов Вам понадобится?
   **11**
3. Сколько зон Вам понадобится?
   **11**

4. Сколько основных DNS-серверов Вам понадобится?
   **11**
5. Сколько резервных DNS-серверов Вам понадобится?
   **11**
6. Сколько кэширующих DNS-серверов Вам понадобится?
   **3 или более.**

Стр. 256

## Закрепление материала

1. Назовите три основных компонента DNS.
   **Пространство доменных имен, серверы имен и DNS-клиенты.**
2. Объясните различие между основным, резервным и главным серверами имен.
   **Основной сервер имен содержит зональную информацию в локальном файле зоны. Резервный сервер имен получает зональную информацию от своего главного сервера имен. Главный сервер имен является источником зональной информации для резервного сервера имен (он сам может быть как основным, так и резервным сервером имен).**
3. Перечислите три причины, по которым надо создавать резервный сервер имен.
   **(1) Они играют роль «страхующих» серверов имен (Необходимо не менее одного «страхующего» сервера имен в каждой зоне). (2) Если у Вас есть удаленные клиенты находящиеся на большом удалении, то наличие резервного сервера имен позволит избежать связи по низкоскоростным линиям. (3) Уменьшается нагрузка на основной сервер имен.**
4. Опишите различие между доменом и зоной.
   **Домен — это «ветвь» в пространстве имен DNS. Зона — это часть домена, которая существует в виде отдельного файла на диске и содержит ресурсные записи.**
5. Чем отличаются рекурсивные и итеративные запросы?
   **Ответом на рекурсивный запорс может быть либо запрашиваемая информация, либо сообщение об ошибке, если она не найдена. На итеративный запрос DNS-сервер дает ответ, лучший в данный момент; обычно это ссылка на другой сервер имен, который может разрешить запрос.**
6. Перечислите файлы, необходимые для реализации DNS в ОС Windows NT.
   **Файл базы данных, кэш-файл и файл обратного просмотра.**

7. Каково назначение загрузочного файла?

   **Загрузочный файл используется реализацией BIND для запуска и настройки DNS-сервера.**

# Глава 13. Внедрение DNS

## Ответы к упражнениям

► **Осмотр установленного по умолчанию DNS-сервера**

Стр. 264 9. Дважды щелкните каждую из зон обратного просмотра. Какие типы записей они содержат?

**NS и SOA.**

► **Добавление зоны**

Стр. 267 6. Щелкните каждую ресурсную запись. Какие типы записей содержит каждая из них?

**NS и SOA.**

► **Задание зоны обратного просмотра на основном DNS-сервере**

Стр. 268 1. Определите, какое имя надо дать зоне обратного просмотра на основном DNS-сервере. Для этого воспользуйтесь одним из перечисленных правил.

- Для адресов класса A, добавьте первое число IP-адреса к *.in-addr.arpa* (например, для IP-адреса класса A 29.122.15.88 зона обратного просмотра должна иметь имя *29.in-addr.arpa*).
- Для адресов класса B, добавьте первые два числа IP-адреса в обратном порядке к *.in-addr.arpa* (например, для IP-адреса класса B 129.122.15.88 зона обратного просмотра должна иметь имя *122.129.in-addr.arpa*).
- Для адресов класса C, добавьте первые три числа IP-адреса в обратном порядке к *.in-addr.arpa* (например, для IP-адреса класса C 219.122.15.88 зона обратного просмотра должна иметь имя *15.122.219.in-addr.arpa*).

Какое имя имеет Ваша зона обратного просмотра?

**107.131.in-addr.arpa**

Стр. 276 ## Закрепление материала

1. Для чего необходимо задавать имя узла и имя домена в диалоговом окне настройки параметров DNS протокола TCP/IP *перед* установкой службы Microsoft DNS Server?

   **Служба DNS Server использует имя узла и имя домена для создания записей типа SOA и NS во время установки.**

2. Каковы функции утилиты Nslookup?

   **Утилита Nslookup может работать из командной строки или в интерактивном режиме как DNS-клиент (resolver) и используется для тестирования DNS-серверов.**

3. Опишите процесс использования WINS.

   **Служба Microsoft DNS Server получает DNS-запрос, который не удается разрешить. Тогда, имя узла преобразуется в NetBIOS-имя и посылается для разрешения указанному WINS-серверу.**

4. Опишите ситуацию, когда полезно использовать WINS.

   **Когда клиентам, не использующим Microsoft TCP/IP, необходимо обращение к ресурсам, расположенным на компьютерах, получающих IP-адреса с помощью DHCP и зарегистрированных в службе WINS, например Internet Information Server.**

# Глава 14. Взаимодействие в гетерогенных средах

## Ответы к упражнениям

► **Запуск сеанса FTP**

Стр. 287 Какой TCP-порт использует FTP со стороны сервера?

**Порт 21.**

Стр. 295 ## Закрепление материала

1. Что необходимо компьютеру под управлением Windows NT для соединения с другим узлом?

   **Транспорт TCP/IP и соответствующие службы и утилиты TCP/IP.**

2. Что необходимо компьютеру под управлением Windows NT для соединения и взаимодействия с RFC-совместимым NetBIOS-узлом, например LAN Manager for UNIX.

   **Наличие хотя бы одного общего для обоих узлов транспортного протокола и наличие SMB-сервера на NetBIOS-совместимом узле.**

   **Общий идентификатор области видимости для NetBIOS.**

3. Опишите два отличия в обращении к ресурсам TCP/IP-узлов посредством команд Windows NT или утилит TCP/IP.

   **Windows NT: Используются NetBIOS-имена и стандартные команды.**

**Утилиты TCP/IP: Используются команды, специфичные для этих утилит. Можно использовать IP-адрес или имя узла.**

4. Какие утилиты TCP/IP используют для копирования файлов?

   **FTP, TFTP и RCP.**

5. Какие утилиты TCP/IP позволяют исполнять команды на удаленных узлах?

   **Telnet, RSH и REXEC.**

6. Какие функции обеспечивает поддержка сетевой печати по протоколу TCP/IP?

   **Поддержка принтера, оснащенного сетевым интерфейсом.**

   **Доступ к принтерам, подключенным к UNIX-узлам.**

# Глава 15. Использование SNMP-сервисов

## Ответы к упражнениям

► **Просмотр новых объектов в Performance Monitor**

Стр. 312 4. Перечислите относящиеся к TCP/IP объекты.

**ICMP, IP, TCP, UDP и сетевой интерфейс.**

► **Наблюдение за датаграммами IP с помощью Performance Monitor**

Стр. 312 12. Вернитесь в **Performance Monitor**, и Вы сможете наблюдать активность, вызванную выполнением Ping.

Какая активность отмечена в результате выполнения Ping?

**Сообщения ICMP и IP-датаграммы.**

Сколько сообщений ICMP в секунду было записано?

**2 (1.997)**

Сколько IP-датаграмм в секунду было послано?

**1 (0.999)**

Почему сообщений ICMP послано в два раза больше чем IP-датаграмм?

**На каждую отправленную IP-датаграмму в ответ приходит два сообщения ICMP — эхо-запрос (echo request) и эхо-ответ (echo reply).**

► **Просмотр данных SNMP**

3. С помощью утилиты Snmputil.exe определите относящиеся к DHCP SNMP-объекты. Введите следующую команду в одной строке и затем нажмите ENTER: (*host_id* замените нужным значением).

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.3.2.1.1.1
```

Сколько адресов было арендовано?

**Должен быть выделен один IP-адрес.**

4. Примените утилиту Snmputil.exe к объекту WINS 1.3.6.1.4.1.311.1.2.1.17. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.2.1.17
```

Сколько успешно разрешенных запросов было обработано WINS-сервером?

**Ответы могут быть разными.**

5. Примените утилиту Snmputil.exe к объекту WINS 1.3.6.1.4.1.311.1.2.1.18. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.311.1.2.1.18
```

Сколько неудачных запросов было обработано WINS-сервером?

**Ответы могут быть разными.**

7. Примените утилиту Snmputil.exe к объекту LAN Manager 1.3.6.1.4.1.77.1.1.1. Наберите:

```
snmputil getnext 131.107.2.host_id
public.1.3.6.1.4.1.77.1.1.1
```

Какая версия Windows NT Server работает на компьютере?

**Версия 4.0; в первой строке возвращается значение 4, во второй — 0.**

Стр. 315 **Закрепление материала**

1. Какие четыре операции SNMP Вы знаете?

   ***get, get-next, set*** и ***trap***

2. Какие операции SNMP инициируются системой управления? Какие инициируются агентом?

   **Системы управления выполняют операции *get*, *get-next* и *set*.**

   **Агенты выполняют операции *trap*.**

3. Какие виды MIB поддерживаются ОС Windows NT 4.0?

   **Internet MIB II, LAN Manager MIB II, Microsoft DHCP MIB и Microsoft WINS MIB.**

4. Какие методы разрешения имен узлов использует SNMP?

   **Файл HOSTS, DNS, сервер имен NetBIOS, широковещание и файл LMHOSTS.**

5. Для чего используется имя сообщества?

   **Чтобы обеспечить простейшую безопасность и проверку контекста для агентов, посылающих сообщения *trap* и для управляющих систем, принимающих сообщения *trap*.**

# Глава 16. Поиск и устранение неисправностей Microsoft TCP/IP

Стр. 322 **Закрепление материала**

1. Какие три утилиты Windows NT используются при диагностике проблем, связанных с TCP/IP?

   **Ping, Nbtstat, Arp и Netstat.**

2. Какие утилиты TCP/IP используются для проверки связей от уровня сетевого интерфейса до уровня Интернета?

   **Ping.**

3. Какие две процедуры диагностики IP-сети Вы знаете?

   **Успешный Ping и установка соединения.**

# Предметный указатель

## E



## F



## G



## H



## I

## J



## L



## M

## N

## O



## P



## R



## S

## T

## U



## W



## Z

## Н



## О



## П



## Р



## С

## Т



## У



## Ш



## Э

Microsoft Corporation

# Microsoft TCP/IP
## Учебный курс MCSE

3-е издание, исправленное

од с английского под общей редакцией **О. О. Миха**

Редакторы **Ю. П. Леонова, С. В. Дергачев**
Технический редактор **Н. Г. Тимченко**

Верстальщик **Е. Р. Данилов**
Дизайнер обложки **Е. В. Козлова**



Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

Главный редактор **А. И. Козлов**

Подготовлено к печати издательско-торговым домом
«Русская Редакция»


Лицензия ЛР № 066 422 от 19.03.99 г.
Подписано в печать 23.01.2001 г. Формат 60×90 1/16. Тираж 2000 экз.
Заказ № 1799

Отпечатано в ОАО «Типография "Новости"»
107005, Москва, ул. Фр. Энгельса, 46

# ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ MICROSOFT

прилагаемый к книге компакт-диск

ЭТО ВАЖНО -- ПРОЧИТАЙТЕ ВНИМАТЕЛЬНО. Настоящее лицензионное соглашение (далее «Соглашение») является юридическим документом, оно заключается между Вами (физическим или юридическим лицом) и Microsoft Corporation (далее «корпорация Microsoft») на указанный выше продукт Microsoft, который включает программное обеспечение и может включать сопутствующие мультимедийные и печатные материалы, а также электронную документацию (далее «Программный Продукт»). Любой компонент, входящий в Программный Продукт, который сопровождается отдельным Соглашением, подпадает под действие именно того Соглашения, а не условий, изложенных ниже. Установка, копирование или иное использование данного Программного Продукта означает принятие Вами данного Соглашения. Если Вы не принимаете его условия, то не имеете права устанавливать, копировать или как-то иначе использовать этот Программный Продукт.

## ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ

Программный Продукт защищен законами Соединенных Штатов по авторскому праву и международными договорами по авторскому праву, а также другими законами и договорами по правам на интеллектуальную собственность.

1. **ОБЪЕМ ЛИЦЕНЗИИ.** Настоящее Соглашение дает Вам право:
   - **a)** **Программный продукт.** Вы можете установить и использовать одну копию Программного Продукта на одном компьютере. Основной пользователь компьютера, на котором установлен данный Программный Продукт, может сделать только для себя вторую копию и использовать ее на портативном компьютере.
   - **b)** **Хранение или использование в сети.** Вы можете также скопировать или установить экземпляр Программного Продукта на устройстве хранения, например на сетевом сервере, исключительно для установки или запуска данного Программного Продукта на других компьютерах в своей внутренней сети, но тогда Вы должны приобрести лицензии на каждый такой компьютер. Лицензию на данный Программный продукт нельзя использовать совместно или одновременно на других компьютерах.
   - **c)** **License Pak.** Если Вы купили эту лицензию в составе Microsoft License Pak, можете сделать ряд дополнительных копий программного обеспечения, входящего в данный Программный Продукт, и использовать каждую копию так, как было описано выше. Кроме того, Вы получаете право сделать соответствующее число вторичных копий для портативного компьютера в целях, также оговоренных выше.
   - **d)** **Примеры кода.** Это относится исключительно к отдельным частям Программного Продукта, заявленным как примеры кода (далее «Примеры»), если таковые входят в состав Программного Продукта.
     - i) **Использование и модификация.** Microsoft дает Вам право использовать и модифицировать исходный код Примеров при условии соблюдения пункта (d)(iii) ниже. Вы не имеете права распространять в виде исходного кода ни Примеры, ни их модифицированную версию.
     - ii) **Распространяемые файлы.** При соблюдении пункта (d)(iii) Microsoft дает Вам право на свободное от отчислений копирование и распространение в виде объектного кода Примеров или их модифицированной версии, кроме тех частей (или их модифицированных версий), которые оговорены в файле Readme, относящемся к данному Программному Продукту, как не подлежащие распространению.
     - iii) **Требования к распространению файлов.** Вы можете распространять файлы, разрешенные к распространению, при условии, что: а) распространяете их в виде объектного кода только в сочетании со своим приложением и как его часть; б) не используете название, эмблему или товарные знаки Microsoft для продвижения своего приложения; в) включаете имеющуюся в Программном Продукте ссылку на авторские права в состав этикетки и заставки своего приложения; г) согласны освободить от ответственности и взять на себя защиту корпорации Microsoft от любых претензий или преследований по закону, включая судебные издержки, если таковые возникнут в результате использования или распространения Вашего приложения; и д) не допускаете дальнейшего распространения конечным пользователем своего приложения. По поводу отчислений и других условий лицензии применительно к иным видам использования или распространения распространяемых файлов обращайтесь в Microsoft.

2. **ПРОЧИЕ ПРАВА И ОГРАНИЧЕНИЯ**

- **Ограничения на реконструкцию, декомпиляцию и дизассемблирование.** Вы не имеете права реконструировать, декомпилировать или дизассемблировать данный Программный Продукт, кроме того случая, когда такая деятельность (только в той мере, которая необходима) явно разрешается соответствующим законом, несмотря на это ограничение.
- **Разделение компонентов.** Данный Программный Продукт лицензируется как единый продукт. Его компоненты нельзя отделять друг от друга для использования более чем на одном компьютере.
- **Аренда.** Данный Программный Продукт нельзя сдавать в прокат, передавать во временное пользование или уступать для использования в иных целях.
- **Услуги по технической поддержке.** Microsoft может (но не обязана) предоставить Вам услуги по технической поддержке данного Программного Продукта (далее «Услуги»). Предоставление Услуг регулируется соответствующими правилами и программами Microsoft, описанными в руководстве пользователя, электронной документации и/или других материалах, публикуемых Microsoft. Любой дополнительный программный код, предоставленный в рамках Услуг, следует считать частью данного Программного Продукта и подпадающим под действие настоящего Соглашения. Что касается технической информации, предоставляемой Вами корпорации Microsoft при использовании ее Услуг, то Microsoft может задействовать эту информацию в деловых целях, в том числе для технической поддержки продукта и разработки. Используя такую техническую информацию, Microsoft не будет ссылаться на Вас.
- **Передача прав на программное обеспечение.** Вы можете безвозвратно уступить все права, регулируемые настоящим Соглашением, при условии, что не оставите себе никаких копий, передадите все составные части данного Программного Продукта (включая компоненты, мультимедийные и печатные материалы, любые обновления, Соглашение и сертификат подлинности, если таковой имеется) и принимающая сторона согласится с условиями настоящего Соглашения.
- **Прекращение действия Соглашения.** Без ущерба для любых других прав Microsoft может прекратить действие настоящего Соглашения, если Вы нарушите его условия. В этом случае Вы должны будете уничтожить все копии данного Программного Продукта вместе со всеми его компонентами.

3. **АВТОРСКОЕ ПРАВО.** Все авторские права и право собственности на Программный Продукт (в том числе любые изображения, фотографии, анимации, видео, аудио, музыку, текст, примеры кода, распространяемые файлы и апплеты, включенные в состав Программного Продукта) и любые его копии принадлежат корпорации Microsoft или ее поставщикам. Программный Продукт охраняется законодательством об авторских правах и положениями международных договоров. Таким образом, Вы должны обращаться с данным Программным Продуктом, как с любым другим материалом, охраняемым авторскими правами, **с тем исключением**, что Вы можете установить Программный Продукт на один компьютер при условии, что храните оригинал исключительно как резервную или архивную копию. Копирование печатных материалов, поставляемых вместе с Программным Продуктом, запрещается.

**ОГРАНИЧЕНИЕ ГАРАНТИИ**

ДАННЫЙ ПРОГРАММНЫЙ ПРОДУКТ (ВКЛЮЧАЯ ИНСТРУКЦИИ ПО ЕГО ИСПОЛЬЗОВАНИЮ) ПРЕДОСТАВЛЯЕТСЯ БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ. КОРПОРАЦИЯ MICROSOFT СНИМАЕТ С СЕБЯ ЛЮБУЮ ВОЗМОЖНУЮ ОТВЕТСТВЕННОСТЬ, В ТОМ ЧИСЛЕ ОТВЕТСТВЕННОСТЬ ЗА КОММЕРЧЕСКУЮ ЦЕННОСТЬ ИЛИ СООТВЕТСТВИЕ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ВЕСЬ РИСК ПО ИСПОЛЬЗОВАНИЮ ИЛИ РАБОТЕ С ПРОГРАММНЫМ ПРОДУКТОМ ЛОЖИТСЯ НА ВАС.
НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОРПОРАЦИЯ MICROSOFT, ЕЕ РАЗРАБОТЧИКИ, А ТАКЖЕ ВСЕ, ЗАНЯТЫЕ В СОЗДАНИИ, ПРОИЗВОДСТВЕ И РАСПРОСТРАНЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО УЩЕРБ (ВКЛЮЧАЯ ВСЕ, БЕЗ ИСКЛЮЧЕНИЯ, СЛУЧАИ УПУЩЕННОЙ ВЫГОДЫ, НАРУШЕНИЯ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРИ ИНФОРМАЦИИ ИЛИ ДРУГИХ УБЫТКОВ) ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ MICROSOFT БЫЛА ИЗВЕЩЕНА О ВОЗМОЖНОСТИ ТАКИХ ПОТЕРЬ. ТАК КАК В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ИСКЛЮЧЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ, УКАЗАННОЕ ОГРАНИЧЕНИЕ МОЖЕТ ВАС НЕ КОСНУТЬСЯ.

**РАЗНОЕ**

Настоящее Соглашение регулируется законодательством штата Вашингтон (США), кроме случаев (и лишь в той мере, насколько это необходимо) исключительной юрисдикции того государства, на территории которого используется Программный Продукт.
Если у Вас возникли какие-либо вопросы, касающиеся настоящего Соглашения, или если Вы желаете связаться с Microsoft по любой другой причине, пожалуйста, обращайтесь в местное представительство Microsoft или пишите по адресу: Microsoft Sales Information Center, One Microsoft Way, Redmond, WA 98052-6399.

# Книги Microsoft Press на русском языке по программам сертификации Microsoft

| Сертификационный экзамен | Издания, необходимые для подготовки к экзамену | Примечание |
|---|---|---|
| ***бязательный экзамен MCSD*** | | |
| **ᵍ 70-100**<br>ıalyzing Requirements and Defining<br>ɔlution Architectures | **Принципы проектирования и разработки программного обеспечения. Учебный курс MCSD** | ISBN 5-7502-0125-2<br>608 стр., + CD, 2001 г. |
| ***бязательные экзамены MCSE 2000*** | | |
| **ᵍ 70-210**<br>ıstalling, Configuring, and<br>dministering Microsoft Windows<br>000 Professional | **Microsoft Windows 2000 Professional. Учебный курс MCSE** 2-е изд. | ISBN 5-7502-0183-X<br>672 стр., 2001 г. |
| **ᵍ 70-215**<br>stalling, Configuring, and<br>dministering Microsoft Windows<br>000 Server | **Microsoft Windows 2000 Server. Учебный курс MCSE** 2-е изд. | ISBN 5-7502-0182-1<br>912 стр., 2001 г. |
| **ᵍ 70-216**<br>ıplementing and Administering<br>ıicrosoft Windows 2000<br>etwork Services Infrastructure | **Администрирование сети на основе Microsoft Windows 2000. Учебный курс MCSE** | ISBN 5-7502-0164-3<br>512 стр., 2001 г. |
| **ᵍ 70-217**<br>ıplementing and Administering<br>ıicrosoft Windows 2000<br>irectory Services Infrastructure | **Microsoft Windows 2000 Active Directory Services. Учебный курс MCSE** | ISBN 5-7502-0139-2<br>800 стр., 2001 г. |
| **ᵍ 70-210,**<br>**ᵍ 70-215,**<br>**ᵍ 70-216,**<br>**ᵍ 70-217** | **MCSE Windows 2000. Компакт-диск:**<br>*учебные материалы для подготовки к сертифицированным экзаменам №№ 70-210, 70-215, 70-216, 70-217* 2-е изд. | ISBN 5-7502-0197-X<br>16 стр., + CD, 2001 г. |
| ***бязательные экзамены MCSE 2000 по выбору*** | | |
| **ᵍ 70-220**<br>esigning Microsoft Windows<br>000 Network Security | **Безопасность сети на основе Microsoft Windows 2000. Учебный курс MCSE** | ISBN 5-7502-0176-7<br>912 стр., + CD, 2001 г. |
| **ᵍ 70-221**<br>esigning a Microsoft Windows<br>000 Network Infrastructure | **Инфраструктура сети на основе *Microsoft Windows 2000*. Учебный курс MCSE** | ISBN 5-7502-0192-9<br>**готовится к изданию** |
| **ᵍ 70-226**<br>esigning Highly Available Web<br>ɔlutions with Microsoft Windows<br>000 Server | ***Web-разработка на платформе* Microsoft Windows 2000 Server. Учебный курс MCSE** | ISBN 5-7502-0196-1<br>**готовится к изданию** |

# Книги Microsoft Press на русском языке по программам сертификации Microsoft

| Сертификационный экзамен | Издания, необходимые для подготовки к экзамену | Примечание |
|---|---|---|
| ***Экзамены по выбору*** | | |
| **№ 70-016** Designing and Implementing Desktop Applications with Microsoft Visual C++ 6.0 | **Разработка приложений на Microsoft Visual C++ 6.0. Учебный курс** 2-е изд. | ISBN 5-7502-0185-6 704 стр., + CD, 2001 г. |
| **№ 70-029** Designing and Implementing Database with Microsoft SQL Server 7.0 | **Реализация баз данных Microsoft SQL Server 7.0. Учебный курс** | ISBN 5-7502-0116-3 528 стр., + CD, 2000 г. |
| **№ 70-059** Internetworking with Microsoft TCP/IP on Microsoft Windows NT 4.0 | **Microsoft TCP/IP. Учебный курс** 3-е изд. | ISBN 5-7502-0171-6 400 стр., + CD, 2001 г. |
| **№ 70-086** Implementing and Supporting Microsoft Systems Management Server 2.0 | **Microsoft Systems Management Server 2.0. Учебный курс** | ISBN 5-7502-0121-X 576 стр., + CD, 2000 г. |
| **№ 70-175** Distributed Apllications for Microsoft Visual Basic 6.0. | **Разработка распределенных приложений на Microsoft Visual Basic 6.0. Учебный курс** | ISBN 5-7502-0133-3 400 стр., + CD, 2000 г. |
| **№ 70-227** Microsoft Internet Security and Acceleration Server 2000 | **Microsoft Internet Security and Acceleration Server 2000. Учебный курс MCSE** | ISBN 5-7502-0191-0 **готовится к изданию** |
| **№ 70-228** Instailing Configuring, and Administering Microsoft SQL Server 2000 Enterprise Edition | **Администрирование Microsoft SQL Server 2000. Учебный курс MCSE** | ISBN 5-7502-0144-9 **готовится к изданию** |
| **№ 70-229** Designing and Implementing Databases with Microsoft SQL Server 2000 Enterprise Edition | **Реализация баз данных Microsoft SQL Server 2000. Учебный курс MCSE** | ISBN 5-7502-0149-X **готовится к изданию** |
| ***Экзамены CompTIA*** | | |
| **A+Certification** | **A+Сертификация. Учебный курс** | ISBN 5-7502-0115-5 496 стр., 2000 г. |
| **Network+ Certification** | **Network+ Сертификация. Учебный курс** | ISBN 5-7502-0190-2 **готовится к изданию** |


**издательство компьютерной литературы**

РУССКАЯ РЕДАКЦИЯ

**ПРОДАЖА КНИГ**

**оптом** тел.: (095) 142-0571, e-mail: alexg@rusedit.ru;
**интернет-магазин** http://www.ITbook.ru; тел.: (095) 145-45
**в розницу** магазин «КОМПЬЮТЕРНАЯ и ДЕЛОВАЯ КНИГА»
Москва, Ленинский пр-т, стр. 38, тел.: (095) 778-7269

MCSE Учебный курс

# Microsoft® TCP/IP

**Третье издание исправленное**

Сертификационный **экзамен 70-059**

**Освоив этот учебный курс, Вы приобретете теоретические знания и практические навыки в области проектирования и поддержки сетей на основе Microsoft® TCP/IP, а также подготовитесь к сдаче экзамена 70-059 по программе сертификации специалистов MCSE.**

## Вы научитесь:

- устанавливать и конфигурировать протокол Microsoft TCP/IP;
- назначать корректные параметры протокола TCP/IP узлам Вашей сети;
- использовать деление на подсети и объединение сетей;
- конфигурировать Windows NT Server для работы в качестве IP-маршрутизатора;
- устанавливать и настраивать агент ретрансляции DHCP и сервер DHCP;
- конфигурировать серверы DNS и WINS;
- устанавливать FTP-сервер, настраивать поддержку печати по протоколу TCP/IP и соединяться с удаленными узлами, например с UNIX;
- тестировать IP-сети и устранять обнаруженные неисправности.

**Прилагаемый компакт-диск** содержит учебные и демонстрационные материалы, а также Microsoft NT Server 4.0 Evaluation Edition и пакеты обновления Service Pack 6.

**Сертификация — ключ к успешной карьере**

Диплом сертифицированного системного инженера Microsoft (Microsoft Certified Systems Engineer, MCSE) — «визитная карточка» специалиста в области установки и обслуживания сетей под управлением Microsoft Windows.

ISBN 5-7502-0171-6


Web-узел издательства: **www.rusedit.ru**
Интернет-магазин: **www.ITbook.ru**