MCSA/MCSE

Training Kit

Exam 70-291

Implementing, Managing, and Maintaining

a Microsoft®

Windows Server™ 2003 Network Infrastructure

J. C. Mackin and Ian McLean

Microsoft® Press

УДК 004
ББК 32.973.26-018.2
М15

Дж. С. Макин, Йен Маклин

М15 Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. Учебный курс MCSA/MCSE / Пер. с англ. - М. : Издательско-торговый дом «Русская Редакция», 2004. — 624 стр. : ил.

ISBN 5-7502-0227-5

Этот учебный курс посвящен созданию инфраструктуры сетей Windows Server 2003. Вы узнаете, как развертывать и конфигурировать протокол TCP/IP, использовать DHCP для управления IP-адресацией, настраивать DNS-клиенты, серверы и зоны. Также вы научитесь обеспечивать безопасность сети, организовывать маршрутизацию и удаленный доступ, в том числе на основе виртуальных частных сетей (VPN). Кроме того, вы узнаете, как выполнять мониторинг трафика, устранять неполадки сетевых подключений и служб, в том числе проблемы TCP/IP, DNS и DHCP.

Данный курс предназначен ИТ-специалистам, занимающимся развертыванием, администрированием и поддержкой сетей Windows Server 2003 и сопутствующих технологий, а также всем, кто хочет получить исчерпывающие знания в области сетей Windows Server 2003. Помимо теоретического материала курс содержит лабораторные работы, практикумы и контрольные вопросы для самопроверки. Он поможет вам подготовиться к сдаче экзамена по программам сертификации Microsoft (MCSA/MCSE) № 70-291: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure.

Издание состоит из 12 глав и предметного указателя. На прилагаемом компакт-диске находятся демонстрационная версия теста, учебные материалы для подготовки к экзамену, приложение, словарь терминов и другие справочные материалы.

УДК 004
ББК 32.973.26-018.2

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

ISBN **0-7356-1439-3** (англ.)
ISBN **5-7502-0227-5**

Об этой книге

Мы рады представить вам учебный курс MCSA/MCSE «Внедрение, управление и поддержка сетевой инфраструктуры Windows Server 2003». Он позволит вам подготовиться к сдаче экзамена 70-291: *Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*. Вы узнаете, как конфигурировать, управлять и устранять неполадки самых разных частей сетей Windows Server 2003, а имеющиеся в каждой главе лабораторные работы позволять вам на практике научиться развертывать и управлять различными компонентами сетей, в том числе сетевой адресацией, разрешением имен, маршрутизацией, удаленным доступом и безопасностью. После прочтения книги вы ответите на вопросы по темам и выполните практические упражнения, чтобы закрепить полученные знания об основных компонентах сетей Windows Server 2003.

Примечание Подробно о программе сертификации Microsoft Certified Professional (MCM) см. в разделе «Программа сертификации специалистов Microsoft».

Кому адресована эта книга

Данный курс предназначен ИТ-Специалистам, занимающимся развертыванием, администрированием и поддержкой сетей Windows Server 2003 и сопутствующих технологий, а также всем, кто хочет сдать сертификационный экзамен 70-291: *Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure*.

Примечание Конкретное содержание любого экзамена определяется компанией Microsoft и может быть изменено без предварительного уведомления.

Предварительные требования

Для изучения данного курса необходимо:

- минимум полтора года практического опыта администрирования сетевой среды Windows;
- знание принципов работы сетей на уровне, необходимом для получения сертификата CompTIA Network+.

Содержимое компакт-диска

На прилагаемом компакт-диске содержится ряд вспомогательных средств, которые помогут вам в изучении курса.

- **Электронные книги.** На компакт-диске записана полная электронная версия этой книги на английском языке, книги *Microsoft Encyclopedia of Networking, Second Edition* и *Microsoft Encyclopedia of Security,* а также избранные главы из книг издательства Microsoft Press по Windows Server 2003.
- **Материалы, необходимые для работы над лабораторными работами глав.**
- **Примерные экзаменационные вопросы** в системе Microsoft Press Readiness Review Suite, поддерживающей разные режимы тестирования. Они дадут вам представление о сертификационном экзамене, а также позволят выяснить, насколько полно вы усвоили материал этого курса
- **Подготовка к экзамену.** Изучив материал этого раздела, вы познакомитесь с основными типами вопросов, которые могут встретиться на экзамене, а задания по программе экзамена и примерные вопросы помогут понять, какие темы усвоены недостаточно и нуждаются в повторении.

  Примечание Полный список экзаменов с программами курсов см. по адресу *http://www.microsoft.com/traincert/mcp*.

  Содержимое этого раздела упорядочено по темам экзамена. Каждая глава освещает важную группу тем, составляющую раздел программы, и содержит перечень проверяемых на экзамене навыков и список дополнительной литературы.
  Раздел объединяет логически связанные темы экзамена, по каждой из которых вам будут предложены примерные вопросы с указанием верных и неверных ответов с пояснениями.

  Примечание Эти вопросы входят в состав пробного экзамена, который также находится на прилагаемом компакт-диске.

- **Программное обеспечение и другие материалы** для **сервисов Software Update Services (SUS),** в том числе SUS Server 1.0 с Service Pack 1 (SP1), агент автоматического обновления (для SUS Server 1.0 с SP1), SUS Server с SP1 и другие.

Дополнительные сведения о данном курсе и прилагаемом компакт-диске (включая ответы на типичные вопросы об установке и использовании) см. на Web-сайте технической поддержки издательства Microsoft Press по адресу *http://www.microsoft.com/mspress/support*. Вы также можете связаться с издательством Microsoft Press по электронной *(tkinput@microsoft.com)* или обычной почте (Microsoft Press Technical Support, One Microsoft Way, Redmond, WA 98052-6399).

Структура книги

Для повышения эффективности обучения главы этой книги разбиты на разделы:

- каждая глава начинается с раздела «Темы экзамена», где перечисляются освещаемые в ней разделы программы экзамена, за ним идет раздел «В этой главе» с кратким обзором содержания главы; следующий раздел «Прежде всего» поможет подготовиться к изучению главы;

- главы делятся на занятия, посвященные отдельным темам. Каждое занятие включает теоретическую часть и лабораторную работу, которая позволит вам закрепить полученные знания и поэкспериментировать с приложениями, о которых шла речь в занятии;
- занятия завершаются разделами «Закрепление материала». Вопросы этого раздела помогут проверить, насколько твердо вы усвоили материал. Ответы на вопросы приводятся в конце главы;
- в разделах «Пример из практики» и «Практикум по устранению неполадок» в конце главы вам будет предложено проанализировать реальную ситуацию и найти способ устранения тех или иных неполадок, чтобы научиться решать проблемы, возникающие в реальных сетях;
- каждое занятие завершается разделом «Резюме», где подводятся краткие итоги занятия, а каждая глава — разделом «Резюме главы», в нем формулируются основные выводы с указанием основных терминов и понятий, необходимых для сдачи экзамена.

Примечания

В книге встречаются различные виды примечаний.

- **Совет** — подсказывает более быстрый или нетривиальный способ решения задач, а также содержит полезные советы других специалистов.
- **Внимание!** — содержит сведения, критические для выполнения поставленной задачи, или предупреждение о возможной потере данных и повреждении системы.
- **Примечание** — содержит дополнительную информацию.
- **Подготовка к экзамену** — отмечает моменты, важные для подготовки к экзамену.
- На заметку — практический совет, как эффективно применить навыки, полученные на занятии.

Обозначения

- Названия элементов интерфейса Windows, с которыми работают при помощи мыши или клавиатуры, набраны буквами **полужирного** начертания, первыми приводятся названия из русскоязычной версии Windows 2003 Server, а за ними в скобках — названия тех же элементов из англоязычной версии этой ОС; пример: кнопка **Пуск (Start).**
- *Курсив* в операторах указывает, что в этом месте следует подставить собственные значения; новые понятия и термины; названия служб и инструментов также напечатаны *курсивом*.
- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры напечатаны ПРОПИСНЫМИ БУКВАМИ.
- Примеры кода, текста, выводимого на экран, а также вводимого в командной строке и различных полях выделены моноширинным шрифтом.
- В квадратные скобки, [ ], заключаются необязательные элементы. Например, наличие в синтаксисе команды элемента *[filename]* показывает, что здесь можно ввести имя файла. Сами скобки вводить не надо.
- В фигурные скобки, {}, заключаются обязательные элементы. Так, наличие в синтаксисе команды элемента *{filename}* показывает, что здесь необходимо ввести имя файла, сами скобки вводить не надо.

Сочетания клавиш

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что, удерживая нажатой клавишу Alt, нужно нажать Tab.
- Запятая, между названиями клавиш означает их последовательное нажатие. Например, выражение «Нажмите Alt, F, X» означает, что надо последовательно нажать и отпустить указанные клавиши. Если же указано «Нажмите Alt+W, L», то сначала следует нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.

Начало работы

Учебный курс содержит упражнения, которые помогут вам научиться развертывать, поддерживать и устранять неполадки сетевой инфраструктуры Windows Server 2003. Используйте этот раздел для подготовки своей учебной среды.
Для выполнения большинства упражнений необходимы два компьютера под управлением Windows Server 2003, объединенных в сеть.

Примечание Упражнения, равно как и изменения на тестовом компьютере, могут иметь нежелательные последствия, если они подключены к более крупной сети. Перед выполнением лабораторных работ и упражнений проконсультируйтесь с администратором сети.

Аппаратное обеспечение

Тестовый компьютер должен соответствовать приведенной ниже минимальной конфигурации. Желательно, чтобы все аппаратное обеспечение соответствовало списку устройств, совместимых с Microsoft Windows Server 2003; см. *список совместимых устройств* (Hardware Compatibility List, HCL) по адресу *http://www.microsoft.com/windowsserver2003/evaluation/sysreqs/default.mspx*.

- Процессор с частотой минимум 133 МГц (рекомендуется 733 МГц) для компьютеров семейства Intel Pentium/Celeron или AMD K6/Athlon/Duron.
- Не менее 128 Мб оперативной памяти (рекомендуется 256 Мб).
- 2 Гб свободного пространства на жестком диске.
- Монитор, с разрешением 800*600 или выше.
- Привод CD-ROM или DVD-ROM.
- Мышь Microsoft или другое совместимое устройство.

Программное обеспечение

Для выполнения упражнений вам потребуется Windows Server 2003 Enterprise Edition.

Подготовка компьютера к выполнению практических занятий

При выполнении упражнений, где требуется подключение к сети, необходимо позаботиться, чтобы компьютеры могли обмениваться информацией. После организации физических подключений установите на обоих компьютерах Windows Server 2003. Серверы сконфигурируйте следующим образом.

Страница Мастера установки Windows (Windows Setup Wizard)	Конфигурация первого компьютера	Конфигурация второго компьютера
Язык и региональные стандарты (Regional And Language Options)	По умолчанию (Россия) [Default (English)]	По умолчанию (Россия) [Default (English)]
Настройка принадлежности программ (Personalize Your Software)	Укажите свое имя и организацию	Укажите свое имя и организацию
Ключ продукта (Your Product Key)	Введите ключ устанавливаемой копии Windows Server 2003	Введите ключ устанавливаемой копии Windows Server 2003
Режимы лицензирования (Licensing Modes)	По умолчанию	По умолчанию
Имя компьютера и пароль администратора (Computer Name And Administrator Password)	Имя компьютера: Computerl Пароль администратора: (задайте надежный пароль)	Имя компьютера: Computerl Пароль администратора: (задайте надежный пароль)
Сведения о модеме (Modem Dialing Information)	По умолчанию	По умолчанию
Настройка времени и даты (Date and Time Settings)	Задайте текущее время, дату и часовой пояс	Задайте текущее время, дату и часовой пояс
Сетевые параметры (Networking Settings)	По умолчанию (стандартные параметры)	По умолчанию (стандартные параметры)
Рабочая группа или домен (Workgroup Or Computer Domain)	По умолчанию (рабочая группа WORKGROUP).	По умолчанию (рабочая группа WORKGROUP)

Внимание! Если компьютер подключен к большой сети, *непременно* согласуйте с ее администратором имя компьютера, домена и другие параметры, чтобы избежать конфликтов в сети.

Вопросы пробного экзамена

На компакт-диске находится пробный экзамен из 300 вопросов, а также 125 дополнительных вопросов для повторения основных тем. Используйте для закрепления материала и выявления тем, которые желательно повторить.

Чтобы установить на жесткий диск вопросы пробного экзамена, выполните следующие действия.

1. Вставьте прилагаемый компакт-диск в привод CD-ROM.

   Примечание Если на вашем компьютере отключена функция автозапуска, следуйте указаниям из файла Readme.txt на компакт-диске.

2. В открывшемся меню щелкните Readiness Review Suite и следуйте указаниям программы

Электронные книги

На прилагаемом компакт-диске вы найдете электронную версию этой книги на английском языке, а также *Microsoft Encyclopedia of Security* и *Microsoft Encyclopedia of Networking, Second Edition* в формате PDF, для просмотра электронных книг пользуйтесь программой Adobe Acrobat Reader.

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить ваши знания современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации, Microsoft разработала современные методы тестирования. Как и любой другой тест или экзамен, сертификация Microsoft служит критерием определенного уровня знаний специалиста, что важно при как трудоустройстве, так и для карьерного роста в организации.

Примечание Полный список преимуществ сертифицированных специалистов см. по адресу *http://www.microsoft.com/traincert/start/itpro.asp*.

Типы сертификации

Программа сертификации специалистов предлагает несколько типов сертификации по разным специальностям.

- *Сертифицированный специалист Microsoft (Microsoft Certified Professional, MCP)* — предполагает доскональное знание, по крайней мере, одной ОС из семейства Windows или ключевой платформы Microsoft. Такой специалист обладает навыками внедрения продукта или технологии Microsoft как части бизнес-системы предприятия.
- *Сертифицированный разработчик программных решений Microsoft (Microsoft Certified Solution Developer, MCSD)* — проектирование и разработка решений для бизнеса с использованием средств разработки, платформ и технологий корпорации Microsoft, включая Microsoft NET Framework.
- *Сертифицированный разработчик приложений Microsoft* (Microsoft Certified Application Developer, MCAD) для платформы Microsoft .NET — способен создавать, тестировать, развертывать и поддерживать мощные приложения с использованием средств и технологий от Microsoft, включая Visual Studio .NET и Web-сервисы XML.
- *Сертифицированный системный инженер Microsoft (Microsoft Certified System Engineer, MCSE)* — предполагает умение эффективно анализировать бизнес-требования, а также проектировать и развертывать инфраструктуры для бизнес-решений на базе Windows Server 2003 и других ОС корпорации Microsoft.
- *Сертифицированный системный администратор Microsoft (Microsoft Certified System Administrator, MCSA)* — занимается вопросами управления и устранения неполадок в существующих сетях и системах на основе Windows Server 2003 и других версий Windows.

- Сертифицированный администратор баз данных Microsoft (Microsoft Certified Database Administrator, MCDBA) — разработка, реализация и администрирование БД Microsoft SQL Server.
- *Сертифицированный преподаватель Microsoft (Microsoft Certified Trainer, MCT)* — теоретическая и практическая подготовка для ведения соответствующих курсов с использованием учебных материалов Microsoft Official Curriculum (MOC) в *сертифицированных центрах технического обучения Microsoft* (Microsoft Certified Technical Education Centers, CTECs).

Требования к соискателям

Требования, к соискателям определяются специализацией, а также служебными функциями и задачами сотрудника.

Соискатель сертификата Microsoft должен сдать экзамен, подтверждающий его глубокие знания в области программных продуктов Microsoft. Экзаменационные вопросы, подготовленные с участием ведущих специалистов компьютерной отрасли, отражают реалии применения программных продуктов Microsoft.

- На звание *Сертифицированного специалиста Microsoft* сдают экзамен по работе с одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с другими продуктами, инструментальными средствами или прикладными программами Microsoft.
- На звание *Сертифицированного разработчика программных решений на основе Microsoft* сдают три базовых экзамена и один по выбору (соискатели сертификата MCSD для Microsoft .NET сдают четыре ключевых экзамена и один по выбору).
- На звание *Сертифицированного разработчика приложений* сдают два базовых экзамена и один по выбору.
- На звание *Сертифицированного системного инженера Microsoft* сдают семь экзаменов: пять базовых и два по выбору.
- На звание *Сертифицированного системного администратора Microsoft* сдают три базовых экзамена и один по выбору.
- На звание *Сертифицированного администратора баз данных Microsoft* сдают три базовых экзамена и один по выбору.
- На звание *Сертифицированного преподавателя Microsoft* надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft. Участие в программе требует соответствия требованиям, предъявляемым при ежегодном обновлении статуса сертифицированного преподавателя. Более подробные сведения о сертификации по этой программе можно получить на сайте *http://www.microsoft.com/traincert/mcp/mct шт* в местном отделении компании Microsoft.

Техническая поддержка

Мы постарались сделать все от нас зависящее^ чтобы и учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Издательство Microsoft Press публикует постоянно обновляемый список исправлений и дополнений к своим книгам по адресу *http:// mspress. m icrosoft. com/support*.

Если все же у вас возникнут вопросы, или вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из указанных ниже адресов:

Электронная почта: TKINPUT@MICROSOFT.COM

Почтовый адрес:

Microsoft Press

Attn: *MCSE Self-Paced Training Kit (Exam 70-291):* Series Editor

One Microsoft Way

Redmond, WA 98052-6399

Дополнительные сведения о данном курсе и прилагаемом компакт-диске (включая ответы на типичные вопросы об установке и использовании) см. на Web-узле технической поддержки издательства Microsoft Press по адресу *http://www.microsoft.com/mspress/support*. Самостоятельно найти ответы на свои вопросы можно в базе знаний Microsoft Press Knowledge Base на сайте *http://www.microsoft.com/mspress/support/search.asp*. Консультацию по вопросам, связанных с поддержкой программных продуктов Microsoft, можно получить по адресу *http://support.microsoft.com*.

Содержание

ГЛАВА 1

Основные сведения о сетях Windows Server 2003

Темы экзамена

- Диагностика и устранение неполадок APIPA (Automatic Private IP Addressing).

В этой главе

Прочитав эту главу, вы узнаете об основных элементах инфраструктуры сети, которые присутствуют в любой офисной сети. Также здесь рассказывается о разнице в разрешении имен в доменах Windows NT и Windows Server 2003, что позволяет успешно устранять соответствующие неполадки в смешанном сетевом окружении. Подробно описано, как адресация связана с инфраструктурой сети, как сетевым подключениям назначаются службы, протоколы и клиенты, как изменяется порядок привязки подключений, протоколов и сетевых служб и каковы низкоуровневые различия между рабочими группами и доменами.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- два компьютера, физически объединенных в сеть;
- установленная на обоих компьютерах с параметрами по умолчанию ОС Windows Server 2003. Компьютерам следует присвоить имена Computer! и Computer2. [Инструкции по установке средствами *Мастера установки Windows* (Windows Setup Wizard) — в разделе «Об этой книге».];
- надежный пароль учетной записи *Администратор* (Administrators) на обоих компьютерах;
- локальная учетная запись, не обладающая привилегиями администратора.

Внимание! Вообще, вход в систему под учетной записью *Администратор* (Administrator) должен выполняться лишь на короткое время и только для выполнения административных задач. Другой способ выполнения административных операций — использование в командной строке команды *Runas* или *Run As.* После входа в систему под учетной записью *Администратор* компьютер ни в коем случае нельзя оставлять без надзора, особенно если он подключен к Интернету. Для предупреждения атак и распространения вирусов по окончании выполнения упражнений нужно завершать сеанс администратора или выключать компьютер.

Занятие 1. Основные сведения об инфраструктуре сети

Под инфраструктурой сети понимают множество взаимосвязанных технологий и систем, которые администраторы должны досконально знать, чтобы успешно поддерживать работу сети и устранять неполадки.

Примечание В настоящем курсе под семейством Windows Server 2003 подразумеваются Microsoft Windows Server 2003 Standard Edition, Enterprise Edition и Qatacenter Edition. Конкретные версии семейства Windows Server 2003 указываются при необходимости. (Хотя формально Microsoft Windows Server 2003 Web Edition также относится к семейству Windows Server 2003, эта версия поддерживает не все нужные для данного курса функции.)

Изучив материал этого занятия, вы сможете:

- объяснить разницу между физической и логической инфраструктурой сети;
- описать некоторые элементы инфраструктуры сети Windows Server 2003.

Продолжительность занятия — около 20 минут.

Определение инфраструктуры сети

Инфраструктура сети — это набор физических и логических компонентов, которые обеспечивают связь, безопасность, маршрутизацию, управление, доступ и другие обязательные свойства сети.

Чаще всего инфраструктура сети определяется проектом, но многое определяют внешние обстоятельства и «наследственность». Например, подключение к Интернету требует обеспечить поддержку соответствующих технологий, в частности протокола TCP/IP. Другие же параметры сети, например физическая компоновка основных элементов, определяются при проектировании, а затем уже наследуются позднейшими версиями сети.

Физическая инфраструктура

Под *физической инфраструктурой* сети подразумевают ее *топологию,* то есть физическое строение сети со всем ее оборудованием: кабелями, маршрутизаторами, коммутаторами, мостами, концентраторами, серверами и узлами. К физической инфраструктуре также относятся транспортные технологии: Ethernet, 802.11b, коммутируемая телефонная сеть общего пользования (PSTN), ATM — в совокупности они определяют, как осуществляется связь на уровне физических подключений. Предполагается, что вы знакомы с основами физической инфраструктуры сети, и эта тема в настоящей книге не рассматривается.

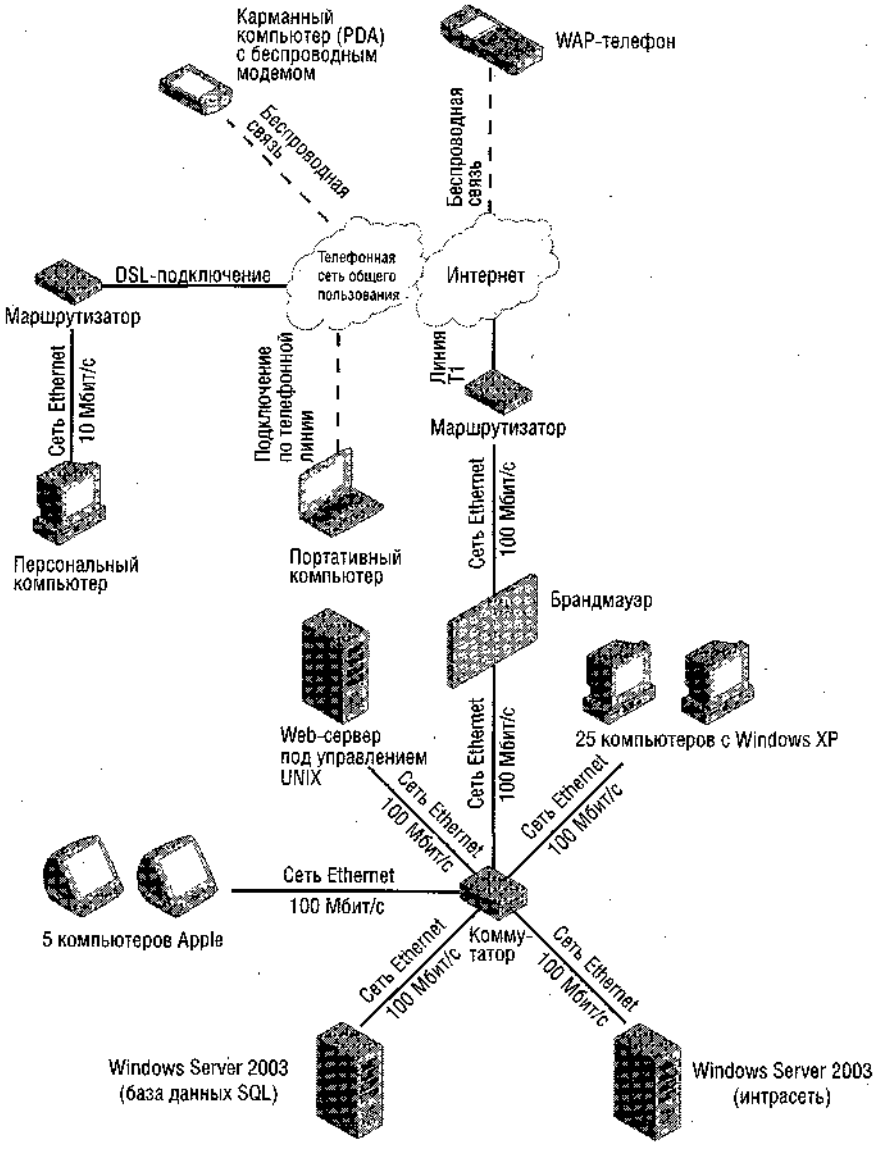


Рис. 1-1. Пример физической инфраструктуры сети

Логическая инфраструктура

Логическая инфраструктура сети состоит из всего множества программных элементов, служащих для связи, управления и безопасности узлов сети, и обеспечивает связь между компьютерами с использованием коммуникационных каналов, определенных в физической топологии. Примеры элементов логической инфраструктуры сети: *система доменных имен* (Domain Name System, DNS), сетевые протоколы, например TCP/IP, сетевые клиенты, например *Клиент для сетей NetWare* (Client Service for NetWare), а также сетевые службы, например *Планировщик пакетов качества службы (QoS)* [Quality of Service (QoS) Packet Scheduler].

Сопровождение, администрирование и управление логической инфраструктурой существующей сети требует глубокого знания многих сетевых технологий. Администратор сети даже в небольшой организации должен уметь создавать различные типы сетевых подключений, устанавливать и конфигурировать необходимые сетевые протоколы, знать методы ручной и автоматической адресации и методы разрешения имен и, наконец, устранять неполадки связи, адресации, доступа, безопасности и разрешения имен.

В средних и крупных сетях у администраторов более сложные задачи: настройка удаленного доступа по телефонной линии и виртуальных частных сетей (VPN); создание, настройка и устранение неполадок интерфейсов и таблиц маршрутизации; создание, поддержка и устранение неполадок подсистемы безопасности на основе открытых ключей; обслуживание смешанных сетей с разными ОС, в том числе Microsoft Windows, UNIX и Nowell NetWare.

На рис. 1-2 показан пример логической инфраструктуры сети.

Анализ сетей Windows Server 2003

Далее описывается большинство логических элементов сетей Windows Server 2003.

Сетевые подключения

В Microsoft Windows *сетевыми подключениями* называют логические интерфейсы между программными (например протоколами) и аппаратными средствами (такими как модемы или сетевые адаптеры). В окне **Сетевые подключения (Network Connections),** показанном на рис. 1-3, отображаются все сетевые подключения, перечисленные в соответствии с приоритетом и сконфигурированные для поддержки различных протоколов, служб и клиентов.

Сетевые протоколы — это языки взаимодействия компьютеров в сети. Например, взаимодействие сетей Windows и UNIX, а также связь в Интернете обеспечивается сетевым протоколом TCP/IP.

В сетях Windows подключения обеспечивают связь с другими узлами только по протоколам, которые установлены на локальном компьютере и привязаны к данным подключениям. По умолчанию протокол TCP/IP (версия 4) устанавливается и привязывается ко всем подключениям, а установка, настройка и привязка NWLink, необходимого для совместимости с сетями Nowell NetWare, выполняется вручную. (NWLink — это созданная Microsoft реализация протокола IPX/SPX, используемого в сетях NetWare.) AppleTalk также устанавливается вручную и привязывается к подключениям, которым нужна совместимость с сетями Apple, где не поддерживается TCP/IP.

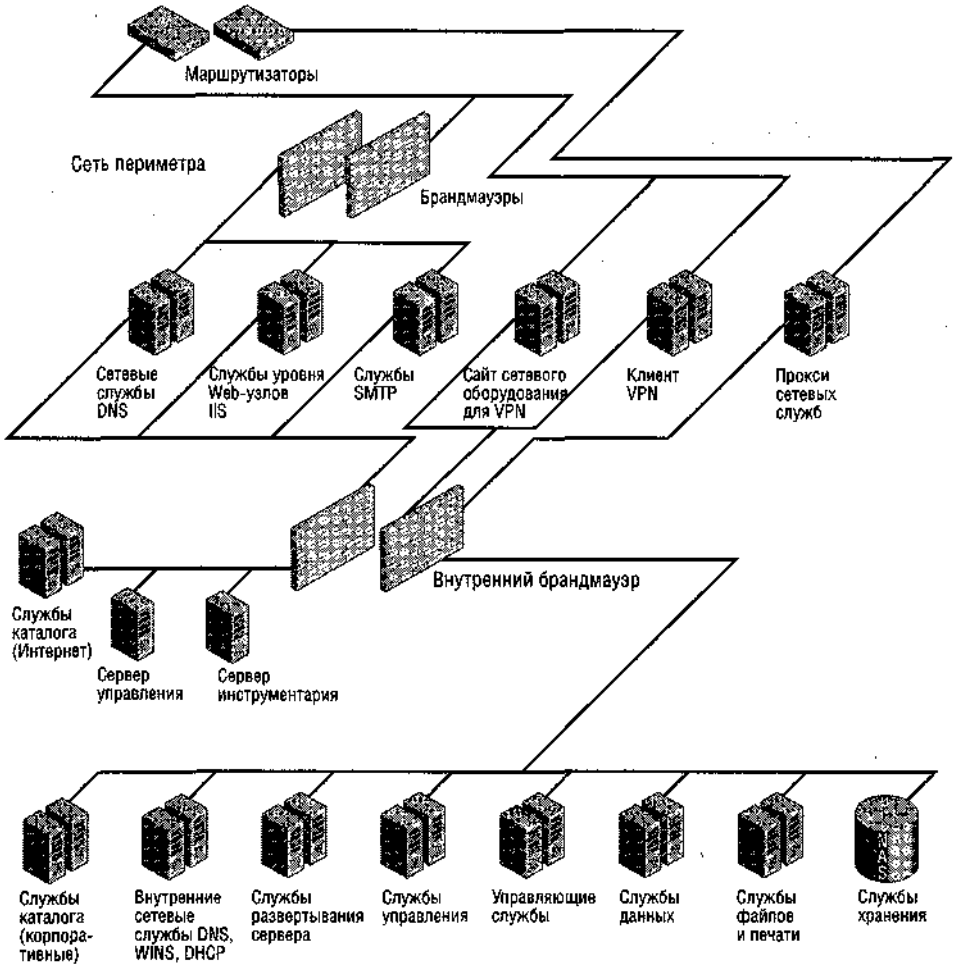


Рис. 1-2. Пример логической инфраструктуры сети

Примечание TCP/IP — это стек, или набор, протоколов, в числе которых APR, IP, TCP, UDP, DNS, HTTP и др.

На рис. 1-4 перечислены все протоколы, которые можно устанавливать и привязывать к подключению. Для подключения к сетям, где используется протокол, не указанный в перечне, придется самостоятельно разработать или приобрести поддерживающий его программный компонент.

Сетевые службы — это программы, предоставляющие определенные функции (например качество сервиса) узлам или протоколам в сети. На рис. 1-5 показаны сетевые службы, доступные для установки и привязки к сетевым подключениям. Дополнительные службы устанавливаются с установочного диска Windows Server 2003 или из другого источника.

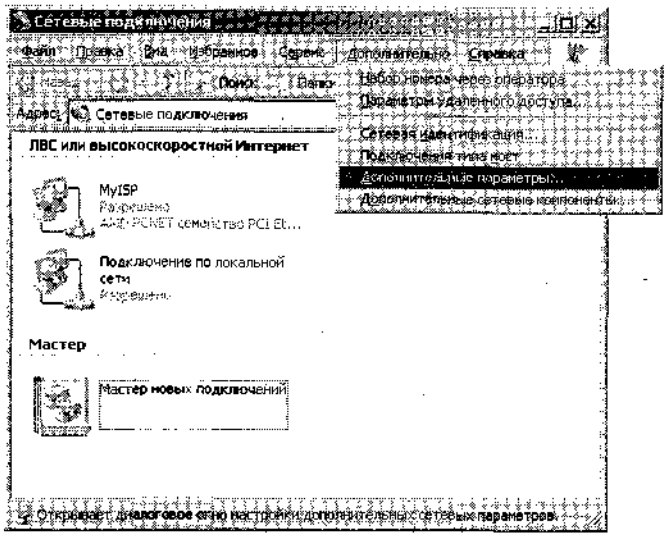


Рис. 1-3. Окно Сетевые подключения

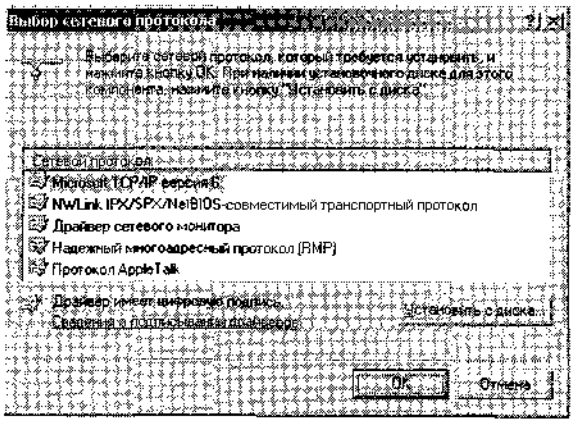


Рис. 1-4. Протоколы, поддерживаемые Windows Server 2003

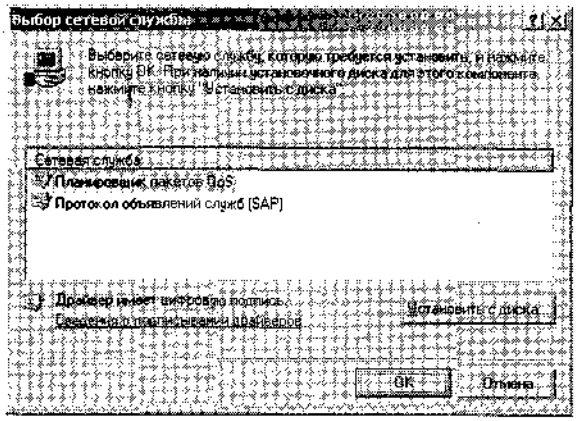


Рис. 1-5. Службы, доступные для установки в Windows Server 2003

Сетевые клиенты — в Windows это программы, позволяющие компьютеру подключаться к сетевой ОС. Например, установив *Клиент для сетей NetWare* (Client Service for NetWare) и создав привязку этого клиента к конкретному подключению, можно подключаться к сетям NetWare.

Адресация

Адресация — это согласованная система сетевых адресов, позволяющая компьютерам «общаться» друг с другом.

Обычно в сети узлы идентифицируются по специальному сетевому адресу. Например, в протоколе IP версии 4 каждому компьютеру присваивается 4-байтный адрес. Первая часть адреса (сетевой идентификатор) совпадает у всех компьютеров в локальной сети, или *подсети*. Для обеспечения взаимодействия таких компьютеров с узлами других подсетей нужно соединить подсети с помощью маршрутизаторов [например, с использованием службы *Маршрутизация и удаленный доступ* (Routing and Remote Access) в Windows Server 2003].

Адреса настраиваются вручную, распределяются автоматически DHCP-сервером или задаются ПО самого компьютера.

Разрешение имен

В большинстве сетей используются системы имен, позволяющие пользователям обращаться к компьютерам по именам, а не по адресам. *Разрешение имен* (name resolution) — это процесс прямого (имя компьютера => адрес) или обратного (адрес => имя компьютера) преобразования имен.

Традиционно Windows поддерживает две системы имен — NetBIOS и DNS. Первая использовалась в сетях Windows предыдущих версий и в настоящее время поддерживается в основном для совместимости. DNS — система имен Интернета и применяется, начиная с Windows 2000.

Разрешение NetBIOS-имен в сетях Microsoft выполняется путем рассылки широковещательного запроса всем системам в локальном сегменте сети или запроса на WINS-сервер. Разрешение имен DNS в сетях Microsoft выполняется DNS-серверами по протоколу DNS.

Группы компьютеров в сети

В Windows компьютеры объединяются в рабочие группы или домены.

- *Рабочая группа* (workgroup) — это простое объединение ресурсов, призванное облегчить пользователям поиск ресурсов, например принтеров или общих файлов. По умолчанию для адресации компьютеров в рабочих группах Windows используется система NetBIOS. Она же применяется в сопутствующих протоколах, таких как общий протокол доступа к интернет-файлам CIFS (расширенная версия протокола SMB), и обеспечивает совместное использование файлов, безопасность, общий доступ и поиск в сети. Однако NetBIOS не обеспечивает централизованной безопасности и управления.
- *Домен* (domain) — это определенное администратором сети подмножество компьютеров, которые совместно используют общий каталог, политики безопасности и отношения с другими доменами. Информация о безопасности и составе каталога хранится на контроллерах домена.

Служба каталогов Active Directory

В сетях Windows Server 2003 домены создаются и поддерживаются службой каталогов Active Directory. Это распределенная база данных и служба каталогов, которая реплицируется на все контроллеры домена в сети. В базе данных Active Directory хранится информация о сетевых объектах, в том числе о доменах, компьютерах, пользователях и других объектах. Распределенная природа Active Directory позволяет пользователям получать доступ к ресурсам, расположенным в любой точке сети, на основе одного входа в систему и обеспечивает единую политику администрирования для всех объектов сети.

Термин *домен* используется как для обозначения группы компьютеров в Active Directory, так и для задания суффиксов в именах DNS (например microsoft.com), определяющих иерархию доменов. Не следует забывать, что домены Active Directory и домены DNS — существенно разные объекты и управляются различными системами. Однако в целях упрощения администрирования домены Active Directory и компьютеры, принадлежащие этим доменам, обычно называют именами, совпадающими с DNS-именами, поэтому пространства имен Active Directory и DNS обычно перекрываются (рис. 1-6).

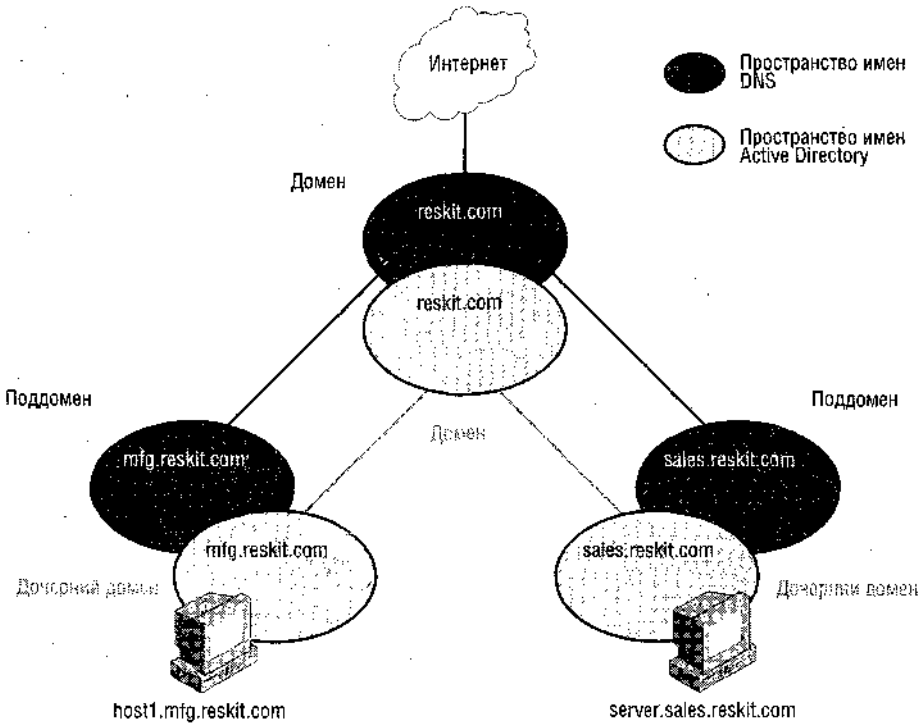


Рис. 1-6. Пространства имен DNS и Active Directory

Удаленный доступ

Для пользователей, подключающихся к сетям Windows с узлов, отличных от локальных, надо настроить подключения удаленного доступа. Есть два основных метода удаленного доступа: прямой удаленный доступ по телефонной линии к сетевому компьютеру и *виртуальные частные сети* (virtual private network, VPN). В первом случае нужно не только

сконфигурировать сервер для ответа на входящие звонки, но также настроить аутентификацию, разрешения доступа и требования к шифрованию. Виртуальные частные сети позволяют создавать частные и закрытые каналы связи, проходящие через открытые сети (например Интернет). VPN особым образом конфигурируются для обеспечения аутентификации, шифрования и безопасности.

Преобразование сетевых адресов

NAT (Network Address Translation) — это протокол преобразования сетевых адресов, позволяющий внутренним компьютерам сети, обладающим частными адресами, взаимодействовать с компьютерами в Интернете. NAT требует определенных изменений в схеме адресации. Общее подключение к Интернету (ICS) — это простая реализация NAT, присутствующая в последних версиях ОС Windows.

Инфраструктура сертификатов

Сертификаты (certificates) используются в инфраструктуре открытых ключей, важном элементе безопасности сетей Windows Server 2003. Сертификаты и открытые ключи применяются, например, в протоколах SSL и IPSec, смарт-картах и *шифрованной файловой системе* (Encryption File System, EFS), обеспечивающей безопасность файлов в сети. Инфраструктура сертификатов, поддерживаемая сетями Windows Server 2003, интегрируется с *инфраструктурой открытого ключа* (Public Key Infrastructure, PKI) — системой цифровых сертификатов, центров сертификации и других регистрационных центров для аутентификации каждой из сторон, участвующих в электронном обмене.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы администратор сети компании, в которой есть компьютеры под управлением Windows Server 2003 и Microsoft Windows XP Professional и сервер с Nowell NetWare. На сервере настроен только сетевой протокол IPX/SPX. Какие протоколы нужно установить на компьютерах сети, чтобы все они получили доступ к сетям NetWare и Windows Server 2003 и Интернету?
2. Работа какого из перечисленных компонентов не основывается на сертификатах и открытых ключах?
   a. SSL.
   b. EFS.
   c. IPSec.
   d. Безопасность рабочих групп.
3. Какой протокол обеспечивает именование и разрешение имен в рабочих группах Windows?
   a. NetBIOS.
   b. CIFS.
   c. DNS.
   d. Kerberos.

Резюме

- Физическая инфраструктура — это топология, физическое строение сети с ее оборудованием: кабелями, маршрутизаторами, коммутаторами, мостами, концентраторами, серверами и узлами. К физической инфраструктуре также относятся технологии, определяющие способ взаимодействия через конкретные типы физических подключений.
- Логическая инфраструктура сети состоит из многих программных элементов, обеспечивающих связь, управление и безопасность узлов.
- В среде Windows сетевые подключения — это логические интерфейсы между программами (например протоколами) и оборудованием (например модемами или сетевыми адаптерами). Подключения отличаются приоритетами и обычно конфигурируются для поддержки различных типов протоколов, служб и клиентов.
- Протоколы — это сетевые языки, используемые для взаимодействия между компьютерами.
- Адресация — согласованная система адресов в сети, служащая для идентификации компьютеров.
- В большинстве сетей используются системы имен, которые позволяют пользователям обращаться к компьютерам по именам, а не по адресам. Разрешение имен — это процесс прямого или обратного преобразования имен в адреса.

Занятие 2. Создание сетей Windows на основе стандартных компонентов

Если компьютеры под управлением Windows Server 2003 (или любой версии, начиная с Microsoft Windows 98) физически соединены посредством сетевых адаптеров, обычно сеть создается без дополнительного конфигурирования параметров. Windows Server 2003 автоматически обнаруживает подключения к локальной вычислительной сети (ЛВС) и обеспечивает основные виды взаимодействия между всеми узлами сети Windows. Не устанавливая никаких дополнительных компонентов, можно также конфигурировать новые сетевые подключения, например подключения удаленного доступа по телефонной линии.

Изучив материал этого занятия, вы сможете:

V описать возможности создания сетей на основе компонентов, предоставляемых Windows Server 2003, установленной с параметрами по умолчанию.

Продолжительность занятия — около 20 минут.

Сетевые подключения

В сетях Windows *подключение* (connection) — это логический интерфейс между физической сетью и сетевым адаптером или модемом. Подключения, сконфигурированные на компьютере, просматривают с помощью утилиты **Сетевые подключения** (Network Connections) в *Панели управления*.

Конфигурирование подключений

Windows Server 2003 автоматически обнаруживает и настраивает подключения сетевых адаптеров, установленных на локальном компьютере. Эти подключения отображаются в окне **Сетевые подключения (Network Connections)** вместе со всеми сконфигурированными вручную подключениями и значком *Мастера новых подключений* (New Connection Wizard), который служит для настройки новых подключений, в том числе подключений удаленного доступа.

Компоненты по умолчанию

Сами по себе подключения не в состоянии обеспечить взаимодействие узлов сети. Связь по сети в любом конкретном подключении обеспечивается привязанными к нему сетевыми клиентами, службами и протоколами. На вкладке **Общие (General)** диалогового окна свойств подключения отображаются его сетевые компоненты: сетевые клиенты, службы и протоколы.

На рис. 1-7 показаны компоненты, назначенные по умолчанию сетевому подключению. Привязка компонента к подключению отмечается флажком. В данном примере служба **Балансировка нагрузки сети (Network Load Balancing)** установлена на локальном компьютере, но не привязана к подключению.

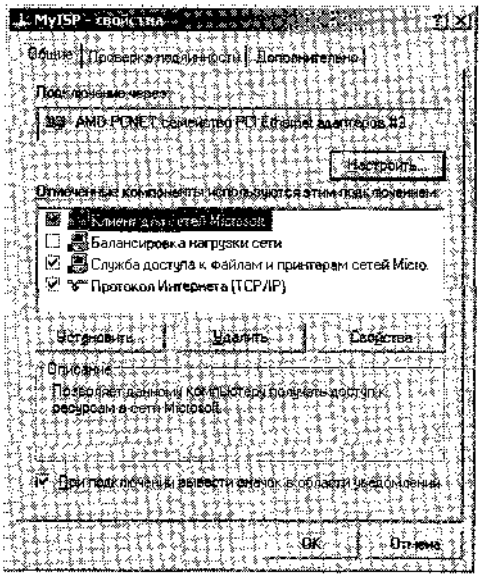


Рис. 1-7. Компоненты по умолчанию для подключения

Сетевые клиенты — это программные компоненты [например *Клиент для сетей NetWare* (Client Service for NetWare) или *Клиент для сетей Microsoft* (Client for Microsoft Networks)], обеспечивающие связь локального компьютера с сетью под управлением соответствующей ОС. По умолчанию *Клиент для сетей Microsoft* привязывается ко всем локальным подключениям и позволяет поддерживает выполнение задач в сети на основе протокола CIFS, например получение доступа к совместно используемым файлам.

Сетевые службы — это программные компоненты [например *Служба доступа к файлам и принтерам сетей Microsoft* (File and Printer Sharing for Microsoft Networks), *Балан-*

сировка нагрузки сети (Network Load Balancing) и *Планировщик пакетов QoS* (QoS Packet Scheduler)], обеспечивающие дополнительные возможности сетевых подключений. *Служба доступа к файлам и принтерам сетей Microsoft,* обеспечивающая доступ к общим файлам, по умолчанию устанавливается и привязывается к локальным подключениям.

Сетевые протоколы — это базовые программные компоненты (например TCP/IP или AppleTalk), которые обеспечивают взаимодействие с другими компьютерами. Сетевые клиенты и службы располагаются на более высоком уровне, чем сетевые протоколы. По умолчанию протокол TCP/IP привязывается ко всем подключениям.

Дополнительные параметры подключения

Дополнительные параметры подключения отображаются при выборе в окне **Сетевые подключения (Network Communicatons)** команды **Дополнительные параметры (Advanced Settings)** в меню **Дополнительно (Advanced).**

В диалоговом окне **Дополнительные параметры (Advanced Settings),** показанном на рис. 1-8, подключения отображаются в порядке их приоритета. Компьютер пытается связаться по сети с использованием доступных подключений в определенном здесь порядке. Можно также настроить порядок привязки служб к каждому из подключений.

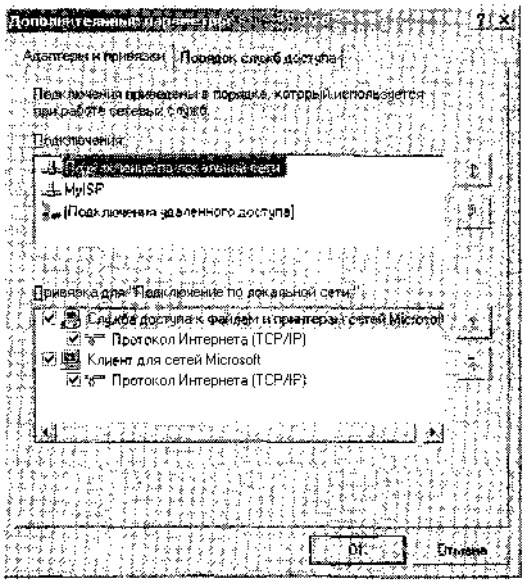


Рис. 1-8. Диалоговое окно *Дополнительные параметры*

На вкладке **Порядок служб доступа (Provider Order)** отображается порядок, в котором осуществляются попытки доступа к различным сетевым службам, в числе которых **Сеть NetWare или совместимая (NetWare Network), Сеть Microsoft Windows (Microsoft Windows Network)** и **Службы терминалов (Microsoft Terminal Services)** (рис. 1-9). Порядок сетевых служб не связан с подключениями. Если компьютер настроен на доступ сначала к сетям NetWare, а после — к сетям Windows, такой порядок будет соблюдаться во всех подключениях.

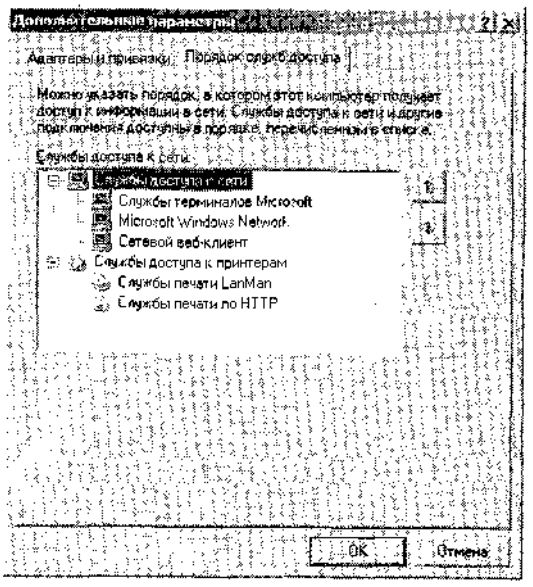


Рис. 1-9. Вкладка Порядок служб доступа

При установке в конфигурации по умолчанию *Службы терминалов* получают приоритет перед Microsoft Windows Network, поскольку в процессе работы замещает собой другие подключения. Также по умолчанию подключение к сети Web-клиента выполняется лишь после неудачи при подключении к первым двум службам.

На вкладке **Порядок служб доступа (Provider Order)** также показан порядок доступа к службам печати. По умолчанию **Службы печати LanMan (LanMan Print Services)** (стандартный провайдер печати в сетях Windows) приоритетнее **Служб печати по HTTP (HTTP Print Services).**

Стандартные параметры протокола TCP/IP

Параметры подключения TCP/IP можно увидеть в окне **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties]** (рис. 1-10). Для этого откройте диалоговое окно свойств подключения, выберите **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]** в списке сетевых компонентов и щелкните **Свойства (Properties).**

IP-адрес присваивается компьютеру автоматически в процессе установки Windows в конфигурации по умолчанию. Для нового компьютера или в сети, в которой не сконфигурирован DHCP-сервер, IP-адрес назначается автоматически из диапазона 169.254.0.1—169.254.255.254. Для этого используется механизм APIPA (Automatic Private IP Addressing).

Автоматическое назначение частных IP-адресов

APIPA — система адресации в простых сетях из одного сетевого сегмента. Если компьютер с Windows Server 2003 настроен на автоматическое получение IP-адреса и не применяется DHCP-сервер или альтернативная конфигурация, частный IP-адрес из диапазона 169.254.0.1—169.254.255.254 назначается автоматически по протоколу APIPA.

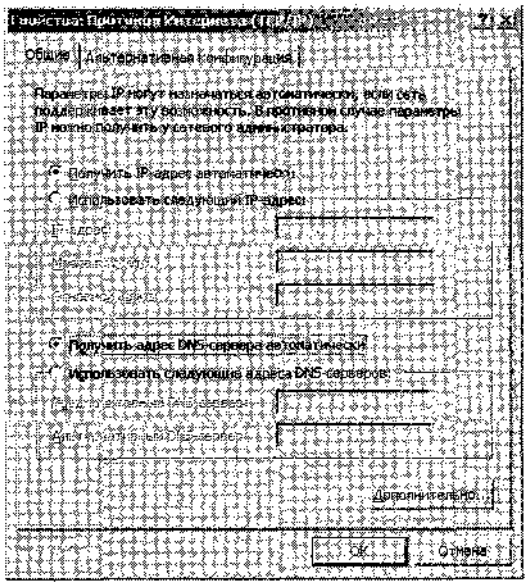


Рис. 1-10. Стандартные параметры TCP/IP

Для определения состояния APIPA (активен или нет) из командной строки выполните ipconf ig /all. Эта утилита предоставляет информацию об IP-адресе и других сетевых параметрах компьютера. Если в строке **Автонастройка включена (Antoconfiguration Enabled)** стоит Да (Yes), а IP-адрес относится к диапазону 169.254.0.1—169.254.255.254, то APIPA включен.

Эта функция автоматической адресации работает, только если получить IP-адрес другими средствами не удается. Если после присвоения APIPA-адреса становится доступным DHCP-сервер, IP-адрес меняется на полученный от DHCP-сервера. Компьютеры с APIPA-адресами могут взаимодействовать только с другими компьютерами с APIPA-адресами из того же сегмента сети; они недоступны напрямую из Интернета. Также APIPA не задает адрес DNS-сервера, шлюза по умолчанию или WINS-сервера. Если надо, чтобы в отсутствие DHCP-сервера автоматически назначались адрес, шлюз по умолчанию, DNS-сервер и/или WINS-сервер, придется воспользоваться альтернативной конфигурацией.

APIPA-адресация доступна на любых компьютерах под управлением Windows 98/Me/2000/XP или Windows Server 2003.

Отключение APIPA

APIPA отключают либо настройкой альтернативный конфигурации в свойствах IP-подключения, либо прямо запрещая автоматическую адресацию путем редактирования системного реестра. Имейте в виду, что при отключении APIPA на одном или всех адаптерах редактируют разные разделы реестра.

Отмена APIPA на одном адаптере осуществляется так.

1. В редакторе реестра Regedit в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\<Код_адаптера > добавьте параметр IPAutoconfigurationEnabled типа REG_DWORD со значением 0.
2. Перезагрузите компьютер.

На всех адаптерах APIPA отключается так.

1. В редакторе реестра Regedit в разделе HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters добавьте параметр IPAutoconfiguration-Enabled типа REG_DWORD со значением 0.
2. Перезагрузите компьютер.

Подготовка к экзамену Запомните разделы системного реестра, относящиеся к APIPA.

Устранение неполадок APIPA

На компьютерах под управлением любой версии, начиная с Windows 98, по умолчанию назначаются APIPA-адреса. Иначе говоря, такие адреса присваиваются узлам, если конфигурация сети остается неизменной с момента установки ОС. В небольших сетях можно оставить эти адреса без изменения — это избавляет от лишней работы по обеспечению сетевого взаимодействия и администрированию. В этом случае проверка, попадают ли адреса локальных соединений на каждом компьютере в диапазон 169.254.0.1—169.254.255.254 выполняется командой ipconfig /all.

Если при выполнении команды APIPA-адрес не обнаруживается, возвращается один из трех возможных ответов: пустой адрес с сообщением об ошибке или без него, адрес, состоящий из одних нулей, или ненулевой IP-адрес, не попадающий в диапазон APIPA.

Когда узлу не присваивается IP-адрес, в сообщении об ошибке иногда указывается конкретная причина, например отсоединение сетевого кабеля. В данном случае нужно проверить присоединение сетевого кабеля, а затем выполнить команду Ipconf ig /renew, чтобы APIPA назначил новый IP-адрес. Если таким образом не удастся назначить узлу IP-адрес, следует продолжить проверку исправности оборудования: кабелей, концентраторов и коммутаторов.

Иногда сообщение утилиты Ipconfig не раскрывает явно причину неполучения IP-адреса. В таком случае проверяют правильность установки сетевого адаптера, а также наличие последней версии соответствующего драйвера. Затем командой Ipconfig /renew повторяют попытку получить IP-адрес. Если неполадка не исчезает', продолжают диагностику оборудования.

Устранение неполадок без применения сложных инструментов

При первых признаках неполадок сетевого оборудования системные администраторы вроде бы должны хвататься за осциллографы и тестеры. Однако на самом деле многие администраторы, особенно в небольших компаниях, не знают, как пользоваться этими приборами, и находят свои способы устранения неполадок. Например, при остановке сетевого трафика можно просто начать с перезапуска концентратора или коммутатора. Если это не поможет, стоит обработать пылесосом порты концентраторов и адаптеров, а также разъемы сетевых кабелей: часто в нарушении связи виновата именно пыль.

Даже после исключения легко устранимых неисправностей можно продолжить выяснение причины нарушения связи без использования специальных инструментов. Например, если не удается получить APIPA-адрес, просто замените кабель заведомо рабочим. Если команда Ipconfig /renew позволит присвоить компьютеру APIPA-адрес, неполадки можно смело приписать неисправности кабеля.

Если неисправность не исчезает, можно воспользоваться специальным кабелем-кроссовером, чтобы обойти концентратор и присоединиться к другому компьютеру напрямую. Если это решит проблему, ясно, что причиной был концентратор. Если все же какой-либо из компьютеров не сможет получить APIPA-адрес, замените на нем сетевую карту.

Другие ошибки, связанные с APIPA, не порождают подозрительных сообщений в выводе утилиты Ipconfig. Например, если команда Ipconf ig /a11 обнаруживает IP-адрес из одних нулей, возможно IP-адрес был удален командой Ipconfig /release и больше не обновлялся. Новый адрес получают командой Ipconfig /renew. Если адрес остается нулевым, проверьте соответствующие элементы системного реестра, чтобы убедиться, что режим APIPA не отключен.

Если, выполнив команду Ipconfig /a11, вы увидите, что компьютер получил ненулевой IP-адрес вне APIPA-диапазона, нужно выполнить команду Ipconfig /renew: возможно «неправильный» адрес сохранился от прежней (или текущей) конфигурации. Если ошибочный адрес остается, проверьте параметры IP-подключения и убедитесь, что компьютер сконфигурирован на автоматическое получение адреса. Затем перейдите на вкладку **Альтернативная конфигурация (Alternate Configuration)** и проверьте, установлен ли переключатель **Автоматический частный IP-адрес (Automatic private IP address) (рис. 1-11).**

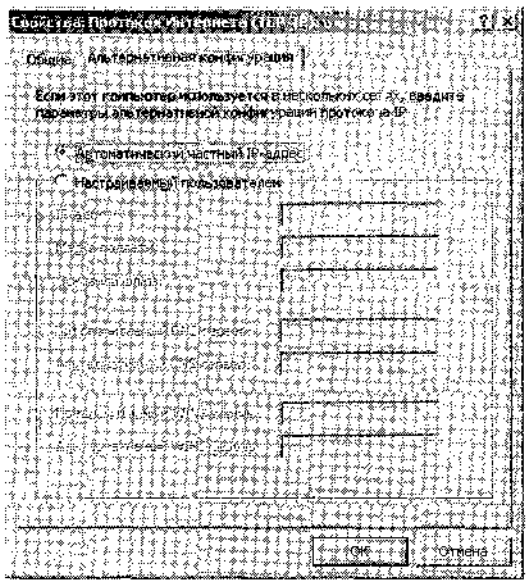


Рис. 1-11. Настройка APIPA

На заметку На практике APIPA-адрес — это только временный адрес, позволяющий компьютеру «общаться» с другими машинами, пока ему не присвоили «настоящий» адрес. Возможно, вам никогда не придется увидеть сеть компании на основе APIPA-адресов, поскольку эти адреса несовместимы с общим доступом к Интернету, подсетями и централизованным управлением, а для поддержки этих функций необходим DHCP-сервер.

Стандартные сети и рабочие группы

Физически соединенные компьютеры под управлением Windows Server 2003 объединяются по умолчанию в единственную рабочую группу WORKGROUP. Имена компьютеров — это NetBIOS-имена, разрешаемые с использованием широковещательных NetBT-запросов в локальном сегменте сети. Сама рабочая группа — это просто название совокупности компьютеров, и она не обеспечивает никаких возможностей централизованной безопасности или управления. Совместное использование файлов, сетевая безопасность, просмотр сети и печать в пределах рабочей группы управляются по протоколу CIFS. В такой ситуации ни Active Directory, ни DNS недоступны.

Маршрутизация и инфраструктура сети Windows Server 2003

Установленная в стандартной конфигурации Windows Server 2003 содержит службу *Маршрутизация и удаленный доступ* (Routing and Remote Access), но в неактивном состоянии. Консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access) позволяет активизировать эту службу и настроить маршрутизацию: удаленный доступ, маршрутизацию в локальной сети и преобразование сетевых адресов (NAT).

Имейте в виду, что включить маршрутизацию в Windows Server 2003 можно только на компьютере с двумя или более сетевыми адаптерами. Такие компьютеры могут выполнять роль маршрутизаторов между сетями, к которым подключены их сетевые адаптеры.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Windows Server 2003 установлена на компьютере ServerOOl с несколькими сетевыми адаптерами. Адаптер А подключен к крупной сети, где 80% NetWare-серверов, а остальные 20% работают под управлением Windows Server 2003. Адаптер В подключен к крупной сети, где 80% управляются Windows Server 2003, а 20% — NetWare. Согласно журналам сервера, через адаптер В проходит больший трафик, чем через А. Как надо настроить порядок служб доступа на ServerOOl в целом и порядок привязки служб на адаптерах А и В?
2. Какие из перечисленных компонентов конфигурируются в Windows Server 2003 автоматически?
   a. Локальные подключения.
   b. Удаленный доступ.
   c. Таблицы маршрутизации.
3. Какие из указанных компонентов привязываются к подключениям автоматически?
   a. *Клиент для сетей NetWare* (Client Service for NetWare).
   b. *Драйвер сетевого монитора* (Network Monitor Driver).
   c. *Клиент для сетей Microsoft* (Client for Microsoft Networks).
4. Какие из перечисленных функций не могут конфигурироваться из консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access)?
   a. Удаленный доступ.
   b. Фильтрация пакетов.

c. Общий доступ к Интернету.

d. Active Directory.

5. Какие из перечисленных компонентов необходимы для создания сетей в среде Windows Server 2003?

   a. DHCP.

   b. Сетевой протокол.

   c. WINS.

Резюме

- Копия Windows, установленная с параметрами по умолчанию, обеспечивает немедленную поддержку сети, состоящей из одного сегмента физически соединенных компьютеров под управлением любых версий, начиная с Windows 98.
- По умолчанию и в отсутствие DHCP-сервера Windows Server 2003 присваивает обнаруженным подключениям IP-адреса из диапазона 169.254.0.1—169.254.255.254.
- Подключения, сконфигурированные на компьютере, отображаются в окне **Сетевые подключения (Network Connections).** При необходимости можно настроить новые подключения (например подключения удаленного доступа) с помощью *Мастера новых подключений* (New Connection Wisard).
- Чтобы увидеть сетевые компоненты, привязанные к конкретному подключению, откройте окно свойств. По умолчанию к каждому подключению привязываются: *Клиент для сетей Microsoft* (Client for Microsoft Networks), *Служба доступа к файлам и принтерам сетей Microsoft* (File and Printer Sharing for Microsoft Networks) и протокол TCP/IP.
- В диалоговом окне **Дополнительные параметры (Advanced Settings),** открываемом из окна **Сетевые подключения (Network Connections),** отображается порядок привязки к подключению сетевых протоколов и служб, а также общий порядок служб доступа в сеть и печати. Этот порядок можно изменять.

Занятие 3. Расширение инфраструктуры сетей Windows Server 2003

Хотя Windows Server 2003 сразу после установки обеспечивает поддержку простой инфраструктуры сети, возможности этой инфраструктуры можно значительно расширить, устанавливая и конфигурируя дополнительные сетевые компоненты. При наличии полномочий учетной записи *Администратор* (Administrator) на локальном компьютере можно установить для сетевого подключения новые клиенты, службы и протоколы или настроить компьютер с Windows Server 2003 на выполнение дополнительных задач в сети, устанавливая компоненты Windows или добавляя роли сервера [например централизованные сетевые службы адресации (DHCP) и разрешения имен (WINS, DNS)].

Изучив материал этого занятия, вы сможете:

- *V* находить и устанавливать сетевые компоненты Windows;
- *V* описать работу различных сетевых подкомпонентов Wndows.

Продолжительность занятия — около 15 минут.

Добавление компонентов к подключению

Стандартная инфраструктура сети Windows Server 2003 состоит из набора IP-адресов из диапазона 169.254.0.1—169.254.255.254 и единственной рабочей группы, объединяющей локальный и другие компьютеры под управлением Windows. Разрешение имен выполняется с применением широковещательных NetBT-запросов в сегменте сети. Совместное использование файлов, безопасность, просмотр сети и печать обеспечиваются и управляются по протоколу CIFS. Сетевым подключениям автоматически назначаются» компоненты *Клиент для сетей Microsoft* (Client for Microsoft Networks), *Служба доступа к файлам и принтерам сетей Microsoft* (File and Printer Sharing for Microsoft Networks) и протокол TCP/IP.

К локальному подключению можно привязать дополнительные клиенты, службы и протоколы: откройте диалоговое окно свойств подключения, щелкните **Установить (Install)** и в окне **Выбор типа сетевого компонента (Select Network Component Type)** выберите нужный компонент (рис. 1-12).

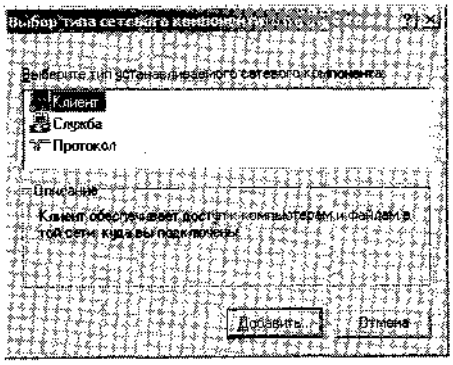


Рис. 1-12. Привязка сетевого компонента к подключению

Создавать привязку с новым сетевым компонентом следует только при условии, что он действительно нужен. Это позволяет сократить число протоколов и клиентов и за счет этого повысить производительность сети и сократить объем трафика.

Новый сетевой компонент добавляется так.

1. Откройте окно **Сетевые подключения (Network Connections).**
2. Щелкните подключение, к которому предполагается добавить сетевой компонент, правой кнопкой и выберите **Свойства (Properties).**
   - Если это локальное подключение, щелкните **Установить (Install).**
   - Если это подключение по телефонной линии, к виртуальной частной сети или входящее подключение, перейдите на вкладку **Сеть (Networking)** и щелкните кнопку **Установить (Install).**
3. В открывшемся окне **Выбор типа сетевого компонента (Select Network Component Type)** выберите **Клиент (Client), Служба (Service)** или **Протокол (Protocol)** и щелкните **Добавить (Add).**
   a Если это стандартный компонент Windows, выберите соответствующий клиент, службу или протокол и щелкните OK.
   a Если компонент устанавливается с диска, щелкните **Установить с диска (Have Disk),** вставьте установочный диск в дисковод и щелкните OK.

Установка службы *Клиент для сетей NetWare*

Для установки службы *Клиент для сетей NetWare* (Client Service for NetWare) откройте окно свойств подключения, щелкните **Установить (Install),** выберите **Клиент (Client)** и **Клиент для сетей NetWare (Client Service for NetWare)** и щелкните OK. При необходимости перезагрузите компьютер. Помимо самого сетевого клиента автоматически устанавливается протокол NWLink (IPX), необходимый для взаимодействия с сетями NetWare. После установки клиент автоматически привязывается ко всем сетевым адаптерам, поэтому для некоторых из них (которым он не нужен), привязку придется отключить.

Типы кадров и протокол NWLink (IPX)

Типы кадров **IPX** определяют метод инкапсуляции данных в IPX-пакеты. Хотя в протоколе NWLink обычно используется режим автоматического определения типа кадра, он не поддерживает потоки кадров нескольких типов. Эта ситуация возникает, когда в сети есть серверы под управлением Novell NetWare 3.11 (тип кадра - 802.3) и более поздних версий NetWare (тип кадра - 802.2). В этом случае придется редактировать системный реестр, чтобы разрешить разные типы кадров.

Установка сетевых компонентов Windows

Утилита *Установка и удаление программ* (Add or Remove Programs) позволяет расширить сетевые возможности Windows Server 2003. В окне **Установка и удаление программ** щелкните **Установка компонентов Windows (Add/Remove Windows Components)** - откроется окно **Мастер компонентов Windows (Windows Component Wizard)** (рис. 1-13).

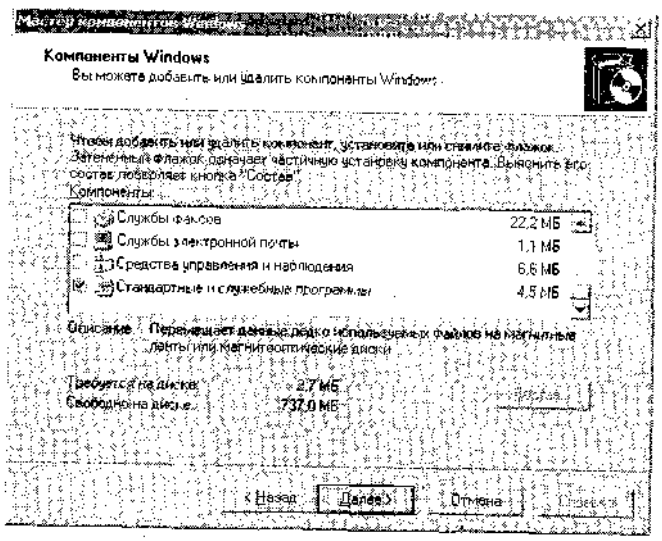


Рис. 1-13. Окно *Мастер компонентов Windows*

Здесь показаны все доступные для установки компоненты Windows Server 2003 (также они доступны для выбора в процессе установки).

Примечание Windows Server 2003 предоставляет упрощенный способ добавления новых компонентов — утилиту *Управление данным сервером* (Manage Your Server), которая позволяет добавлять роли сервера, допустим, превращать его в сервер печати, почтовый сервер, DNS- или DHCP-сервер. При добавлении роли сервера автоматически устанавливаются необходимые компоненты Windows.

Четыре из не устанавливаемых по умолчанию компонентов Windows Sever 2003 содержат подкомпоненты, относящиеся к инфраструктуре сети: *Средства управления и наблюдения* (Management and Monitoring Tools), *Сетевые службы* (Networking Services), *Другие службы доступа к файлам и принтерам сети* (Other Network File and Print Sevices) и *Службы сертификации* (Certificate Services).

Совет Быстро получить доступ к сетевым компонентам Windows можно, открыв папку **Сетевые подключения (Network Connections)** и выбрав в меню **Дополнительно (Advanced)** команду **Дополнительные сетевые компоненты (Optional Networking Components).** Откроется окно **Мастер дополнительных сетевых компонентов Windows (Windows Optional Networking Components Wizard),** который предлагает три компонента: **Средства управления и наблюдения (Management and Monitoring Tools), Сетевые службы (Networking Services), Другие службы доступа к файлам и принтерам сети (Other Network File and Print Sevices).** Этот способ непригоден для установки *Служб сертификации* (Certificate Services).

Компонент *Средства управления и наблюдения*

Этот компонент предоставляет средства администрирования, мониторинга и управления работой сети, среди которых *Сетевой монитор* (Network Monitor), обеспечивающий сбор и анализ кадров в сети, и протокол SNMP (Simple Network Management Protocol) для управления и мониторинга устройств в сетях TCP/IP. В табл. 1-1 описаны подкомпоненты *Средств управления и наблюдения* (Management and Monitoring Tools) в Windows Server 2003.

Табл. 1-1. Подкомпоненты *Средств управления и наблюдения*

Подкомпонент	Описание
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Средство разработки нестандартных подключений для удаленных пользователей
Службы точек подключений (Connection Point Services)	*Служба телефонной книги* (Phone Book Service), обеспечивающая поддержку телефонных книг для профиля *Диспетчер подключений* (Connection Manager). Для работы этой службы необходим сервер IIS
Средства сетевого монитора (Network Monitor Tools)	Анализирует пакеты данных, передаваемые в сети
Протокол SNMP (Simple Network Management Protocol)	Содержит агенты, осуществляющие мониторинг активности сетевых устройств и передающие отчеты на сетевую консоль рабочей станции
WMI поставщик SNMP {WMI SNMP Provider)	Позволяет клиентским приложениям получать доступ к статическим и динамическим SNMP-данным с помощью инструментальных средств управления средой Windows (WMI)

Компонент *Сетевые службы*

Этот компонент значительно расширяет сетевые возможности, предоставляя различные специализированные службы и протоколы. В табл. 1-2 описаны подкомпоненты *Сетевые службы* (Networking Services) в Windows Server 2003.

Табл. 1-2. Подкомпоненты компонента *Сетевые службы*

Подкомпонент	Описание
Domain Name System (DNS)	DNS-сервер отвечает на запросы на разрешение имен и обновляет базу данных DNS-имен
Dynamic Host Configuration Protocol (DHCP)	DHCP-сервер автоматически присваивает временные IP-адреса клиентским компьютерам сети
Служба проверки подлинности в Интернете (Internet Authentification Service)	Обеспечивает аутентификацию, авторизацию и создание учетных записей для пользователей доступа по телефонной линии и VPN. Поддерживает протокол RADIUS
RPC через HTTP-прокси (RPC over HTTP Proxy)	Обеспечивает удаленный вызов процедур (RPC) в DCOM по протоколу HTTP через IIS
Простые службы TCP/IP (Simple TCP/IP Services)	Поддерживает следующие службы TCP/IP: Character Generator, Daytime, Discard, Echo и Quote of the Day
WINS (Windows Internet Name Service)	WINS-сервер поддерживает базу данных NetBIOS-имен и разрешает NetBIOS-имена для клиентов

Компонент *Другие службы доступа к файлам и принтерам сети*

Этот компонент (табл. 1-3) обеспечивает службы доступа к файлам и принтерам ОС Macintosh, а также UNIX.

Табл. 1-3. Подкомпоненты *Других служб доступа к файлам и принтерам сети*

Подкомпонент	Описание
Файловые службы Macintosh (File Services For Macintosh)	Позволяет пользователям Macintosh хранить и получать доступ к файлам на сервере под управлением Microsoft Windows
Службы печати для Macintosh (Print Services For Macintosh)	Позволяет пользователям Macintosh отправлять задания диспетчеру печати на сервере под управлением Microsoft Windows
Службы печати для UNIX (Print Services For Unix)	Позволяет UNK-клиентам печатать на любом принтере, доступном на локальном компьютере

Подготовка к экзамену Выучите функции подкомпонентов *Другие службы доступа к файлам и принтерам сети* (Other Network File and Print Services) — это понадобится на экзамене.

Компонент *Службы сертификации*

Этот компонент (табл. 1-4) содержит службы выдачи и управления сертификатами в рамках системы защиты данных на основе технологий открытого ключа. Помимо про-

чего сертификаты используются для проверки подлинности электронной почты, достоверности отправителя и получателя сообщений, аутентификации Web-клиентов и серверов, идентификации смарт-карт и шифрования файлов.

Табл. 1-4. Подкомпоненты *Службы сертификации*

Подкомпонент	Описание
ЦС служб сертификации (Certificate Services CA)	Центр сертификации (ЦС), отвечающий за выдачу и управление цифровыми сертификатами
Служба подачи заявок на сертификат через Интернет (Certificate Services Web Enrollment Support)	Разрешает на сервере публикацию Web-страниц для получения запросов на сертификаты и отзыва сертификатов, из ЦС

Установка Active Directory в сети Windows

Чтобы установить в сети Active Directory, нужно просто повысить роль сервера до контроллера домена, добавив эту роль в окне **Управление данным сервером (Manage Your Server).**

Установка Active Directory значительно изменяет логическую инфраструктуру сети Windows. Например, если раньше в сети не было DNS-сервера, то после установки Active Directory для разрешения имен используется не NetBIOS, а DNS. Также обеспечивается безопасность на сетевом уровне и аутентификация на основе протокола Kerberos. Наконец, Active Directory привносит массу возможностей, связанных с самой службой каталогов, в том числе глобальный каталог, содержащий информацию о всех объектах каталога, и службу репликации, отвечающую за распространение данных каталога по сети.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какие подкомпоненты нужно установить, чтобы пользователи Macintosh смогли хранить и получать доступ к файлам в сети Windows Server 2003?
2. Какие компоненты Windows надо установить для обеспечения функциональности DHCP, DNS и WINS?
   a. *Средства управления и наблюдения* (Management and Monitoring Tools).
   b. *Сетевые службы* (Networking Services).
   c. *Другие службы доступа к файлам и принтерам сети* (Other File and Print Services).
3. Компьютер с Windows Server 2003 должен взаимодействовать с сетью NetWare, в которой есть серверы под управлением NetWare 3.11 и NetWare 4.1. Как в такой ситуации следует настроить протокол NWLink?
   a. Оставить протокол в режиме Auto Detect.
   b. Задать тип кадра 802.2.
   c. Задать тип кадра 802.3.
   d. Изменить системный реестр, обеспечив разрешение обоих типов кадров (802.2 и 802.3).

4. Для работы каких из перечисленных сетевых компонентов не обязательна инфраструктура открытого ключа?
   a. IPSec.
   b. Совместное использование файлов.
   c. SSl.
5. Как обычно осуществляется разрешение имен в собственных доменах Windows Server 2003 и Windows 2000?
6. Какие подкомпоненты Windows содержат агенты мониторинга и управления серверами Windows, UNIX и сетевым оборудованием?

Резюме

- Привязка дополнительных клиентов, служб и протоколов к сетевому подключению выполняется в окне свойств подключения: для этого необходимо выбрать компонент и щелкнуть кнопку **Установить (Install).**
- Службы DHCP и разрешения имен (WINS, DNS) не устанавливаются по умолчанию, и их нужно устанавливать утилитой *Установка и удаление программ* (Add or Remove Programs).
- По умолчанию в NWLink используется режим автоматического определения типа кадров, но он не работает в сети, где есть разные типы кадров.
- Чтобы установить в сети Active Directory, нужно просто повысить роль компьютера до контроллера домена, добавив соответствующую роль сервера. Active Directory значительно изменяет логическую инфраструктуру сети Windows.

Лабораторная работа

Приведенные далее упражнения помогут вам освоить решение задач, возникающих в реальных ситуациях, а также научиться быстро и эффективно устранять неполадки.

Анализ ситуации

После физического объединения 15 компьютеров в небольшую сеть компании Contoso, вы выполняете на каждом компьютере команду Ipconfig /all, которая на большинстве узлов показывает наличие APIPA-адреса, но есть исключения.

Узел CS-7 возвращает такую информацию:

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows IP Configuration

        Host Name. . . . . . . . . . . . : CS-7
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Mixed
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
```

```
Ethernet adapter Local Area Connection:

        Media State. . . . . .  .: Media disconnected
        Description. . . . . .  .: Intel(R) PRO/100 P Mobile Combo Adapter
        Physical Address. . . . . .: 00-00-59-80-B7-F6
```

1. Что нужно предпринять в первую-очередь?
2. Узел CS-8 никак не реагирует на команду Ipconfig /all. Вы убедились, что сетевой адаптер на узле установлен. Что предпринять далее?
3. Узел CS-10 возвращает IP-адрес 0.0.0.0. После выполнения команды Ipconf ig /renew адрес не изменяется. Что делать, если компьютеру надо присвоить APIPA-адрес?

Резюме главы -

- По умолчанию компьютеры сети объединяются в единственную рабочую группу с названием WORKGROUP. Базовым в сети является набор протоколов TCP/IP. Компьютеры получают NetBIOS-имена, а разрешение имен выполняется путем широковещательных рассылок NetBT в локальном сегменте сети. Безопасность настраивается локально на каждом компьютере; централизованная система безопасности не поддерживается.

я В отсутствие DHCP-сервера компьютеры автоматически получают APIPA-адреса из диапазона 169.254.0.1—169.254.255.254. Такая стандартная адресация обеспечивает базовую связь по сети, но не поддерживает общее подключение к Интернету, подсети и централизованное управление адресацией.

- Стандартную сетевую инфраструктуру Windows Server 2003 можно значительно расширить, устанавливая и конфигурируя дополнительные сетевые компоненты или добавляя роли сервера.
- В Windows Server 2003 можно установить службы централизованного управления адресацией (DHCP) и разрешения HMeH-(WINS, DNS).

а Полномочия учетной записи *Администратор* (Administrator) на локальном компьютере позволяют устанавливать новые клиенты, службы и протоколы, привязывая их к конкретным сетевым подключениям.

и Для расширения функциональности сервера Windows Server 2003, а также обеспечения доступа из других узлов сети на сервере можно настроить службы *Маршрутизация и удаленный доступ* (Routing and Remote Access) или *Службы сертификации* (Certificate Services).

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Следует помнить диапазон APIPA-адресов, так как на экзамене часто придется ис пользовать их как признак недоступности или неправильной работы DHCP-серверг
- Неспособность узла автоматически получить APIPA-адрес в отсутствие DHCP-сер вера обычно свидетельствует о неполадках оборудования.
- Запомните разделы системного реестра, используемые для отмены режима APIPA н всех или отдельных адаптерах.
- Помните типы кадров NetWare и не забывайте, когда режим автоматического опре деления приводит к ошибкам.
- Запомните устанавливаемые сетевые компоненты и подкомпоненты Windows, в то] числе *Файловые службы Macintosh* (File Services for Macintosh), *Службы печати дл Macintosh* (Print Services for Macintosh) и *Службы печати для UNIX* (Print Services fc UNIX).

Основные термины

APIPA — функция протокола TCP/IP в Windows XP и в семействе Windows Server 2003 предусматривающая автоматическое назначение уникального IP-адреса, когда TCP IP настроен на динамическую адресацию, а DHCP-сервер недоступен. IP-адреса вы бираются случайным образом из диапазона 169.254.0.1—169.254.255.254 и получаю маску подсети 255.255.0.0. Диапазон APIPA-адресов зарезервирован Агентством п выделению имен и уникальных параметров протоколов Интернета (IANA), и 1P-ад реса данного диапазона не используются в Интернете.

NetBT [сокращение от *NetBIOS поверх TCP/IP* (NetBIOS over TCP/IP)} — протокол, ле жащий в основе высокоуровневой связи в сетях Microsoft, в том числе по протоко лам SMB и CIFS.

CIFS — расширение протокола SMB, служащее для совместного использования файло: и других функций в сетях Microsoft. Одно из преимуществ CIFS перед SMB — спо собность работать прямо через DNS, минуя NetBIOS.

NWLink — реализация Microsoft протокола IPX/SPX, используемого в сетях NetWare NWLink обеспечивает связь между компьютерами под управлением Windows и сетя ми NetWare с протоколом IPX/SPX.

? Вопросы и ответы

Занятие 1. Закрепление материала

1. Вы администратор сети компании, в которой есть компьютеры под управление* Windows Server 2003 и Microsoft Windows XP Professional и сервер с Nowell NetWare На сервере настроен только сетевой протокол IPX/SPX. Какие протоколы нужно ус тановить на компьютерах сети, чтобы все они получили доступ к сетям NetWare i Windows Server 2003 и Интернету?

   Правильный ответ: NWLink и TCP/IP

2. Работа какого из перечисленных компонентов не основывается на сертификатах \ открытых ключах?

a. SSL.
b. EFS.
c. IPSec.
d. Безопасность рабочих групп.

Правильный ответ: d.

3. Какой протокол обеспечивает именование и разрешение имен в рабочих группах Windows?
   a. NetBIOS.
   b. CIFS.
   c. DNS.
   d. Kerberos.

   Правильный ответ: a.

Занятие 2. Закрепление материала

1. Windows Server 2003 установлена на компьютере ServerOOl с несколькими сетевыми адаптерами. Адаптер А подключен к крупной сети, где 80% NetWare-серверов, а остальные 20% работают под управлением Windows Server 2003. Адаптер В подключен к крупной сети, где 80% управляются Windows Server 2003, а 20% — NetWare. Согласно журналам сервера, через адаптер В проходит больший трафик, чем через А. Как надо настроить порядок служб доступа на ServerOOl в целом и порядок привязки служб на адаптерах А и В?

   Правильный ответ: в списке сетевых провайдеров Microsoft Windows Network должен предшествовать NetWare. На адаптере А *Клиент для сетей NetWare* (Client Service for NetWare) должен предшествовать *Клиенту для сетей Microsoft* (Client for Microsoft Networks), а на адаптере В порядок должен быть обратным.

2. Какие из перечисленных компонентов конфигурируются в Windows Server 2003. автоматически?
   a. Локальные подключения.
   b. Удаленный доступ.
   c. Таблицы маршрутизации.

   Правильный ответ: a.

3. Какие из указанных компонентов привязываются к подключениям автоматически?
   a. *Клиент для сетей NetWare* (Client Service for NetWare).
   b. *Драйвер сетевого монитора* (Network Monitor Driver).
   c. *Клиент для сетей Microsoft* (Client for Microsoft Networks).

   Правильный ответ: c.

4. Какие из перечисленных функций не могут конфигурироваться из консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access)?
   a. Удаленный доступ.
   b. Фильтрация пакетов.
   c. Общий доступ к Интернету.
   d. Active Directory.

   Правильный ответ: d.

5. Какие из перечисленных компонентов необходимы для создания сетей в среде Windows Server 2003?
   a. DHCP.
   b. Сетевой протокол,
   c. WINS.
   Правильный ответ: b,

Занятие 3, Закрепление материала

1. Какие подкомпоненты нужно установить, чтобы пользователи Macintosh смогли хранить и получать доступ к файлам в сети Windows Server 2003?
   Правильный ответ: Файловые службы Macintosh (File Services for Macintosh).
2. Какие компоненты Windows надо установить для обеспечения функциональности DHCP, DNS и WINS?
   a. *Средства управления и наблюдения* (Management and Monitoring Tools).
   b. *Сетевые службы* (Networking Services).
   c. *Другие службы доступа к файлам и принтерам сети* (Other Network File and Print Sevices).
   Правильный ответ: b.
3. Компьютер с Windows Server 2003 должен взаимодействовать с сетью NetWare, в которой есть серверы под управлением NetWare 3.11 и NetWare 4.1. Как в такой ситуации следует настроить протокол NWLink?
   a. Оставить протокол в режиме автоматического определения типа кадров.
   b. Задать тип кадра 802.2.
   c. Задать тип кадра 802.3.
   d. Изменить системный реестр, обеспечив разрешение обоих типов кадров (802.2 и 802.3).
   Правильный ответ: d.
4. Для работы каких из перечисленных сетевых компонентов не обязательна инфраструктура открытого ключа?
   a. IPSec.
   b. Совместное использование файлов.
   c. **SSI.**
   Правильный ответ: b.
5. Как обычно осуществляется разрешение имен в собственных доменах Windows Server 2003 и Windows 2000?
   Правильный ответ: посредством DNS.
6. Какие подкомпоненты Windows содержат агенты мониторинга и управления серверами Windows, UNIX и сетевым оборудованием?
   Правильный ответ: протокол SNMP.

Занятие 3. Лабораторная работа. Анализ ситуации

1. .Что нужно предпринять в первую очередь?
   Правильный ответ: проверьте правильность и надежность подключения Ethernet-кабеля к сетевому адаптеру и концентратору или коммутатору.

2. Узел CS-8 никак не реагирует на команду Ipconfig /all. Вы убедились, что сетевой адаптер на узле установлен. Что предпринять далее?
   Правильный ответ: воспользуйтесь утилитой Диспетчер устройств (Device Manager), чтобы проверить, установлена ли самая последняя версия драйвера сетевого адаптера и убедиться в корректной работе адаптера.
3. Узел CS-10 возвращает IP-адрес 0.0.0.0. После выполнения команды Ipconfig /renew адрес не изменяется. Что делать, если компьютеру надо присвоить APIPA-адрес?
   Правильный ответ: удалите следующие параметры реестра (если они определены):

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPAutoconfigurationEnabled

   и

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\</cofl_aflanrepa>\IPAutoconfigurationEnabled/

ГЛАВА 2

Общие сведения о TCP/IP

Темы экзамена

- Настройка адресации TCP/IP на сервере.
- Устранение неполадок адресации TCP/IP.
  - Диагностика и устранение неполадок, обусловленных некорректной конфигурацией.

В этой главе

Здесь описаны основные понятия и концепции TCP/IP, понимание которых необходимо для успешного устранения неполадок, связанных с некорректной конфигурацией подсетей IP, основных шлюзов, масок подсетей или адресов, а также рассказывается, как проверять конфигурацию диапазонов адресов, используя знания о необходимом количестве битов для идентификаторов подсети и узла. И наконец, вы узнаете, как и в каких случаях применять ручную, автоматическую и альтернативную конфигурацию IP в сети.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- два физически объединенных в сеть компьютера;
- установленная на обоих компьютерах с параметрами по умолчанию Windows Server 2003. Компьютерам следует присвоить имена Computer1 и Computer2. (Инструкции по установке средствами мастера Windows Setup Wizard — в разделе «Об этой книге».);
- надежный пароль учетной записи *Администратор* (Administrator) на обоих компьютерах;
- локальная учетная запись, не обладающая привилегиями администратора. Всю работу на компьютере (кроме упражнений из этой книги) следует выполнять от ее имени.

Занятие 1. Что такое TCP/IP

TCP/IP — это набор протоколов, лежащий в основе сетей Windows и Интернета. Стек протоколов TCP/IP состоит из четырех уровней: сетевого интерфейса, межсетевого, транспортного и прикладного.

Основными в сервисах TCP/IP являются межсетевой и транспортный уровни. В частности, такие протоколы, как ARP (Address Resolution Protocol), IP (Internet Protocol), TCP (Transmission Control Protocol), UDP (User Datagram Protocol) и ICMP (Internet Control Message Protocol) используются во всех вариантах TCP/IP.

Изучив материал этого занятия, вы сможете:

- *S* рассказать о четырех уровнях модели TCP/IP;
- *S* привести примеры протоколов каждого из уровней стека TCP/IP;
- *S* описать основные функции ARP, IP, ICMP, TCP и UDP.

Продолжительность занятия — около 10 минут.

Уровни в модели TCP/IP

Сквозные подключения на основе TCP/IP состоят из четырех уровней (рис. 2-1).

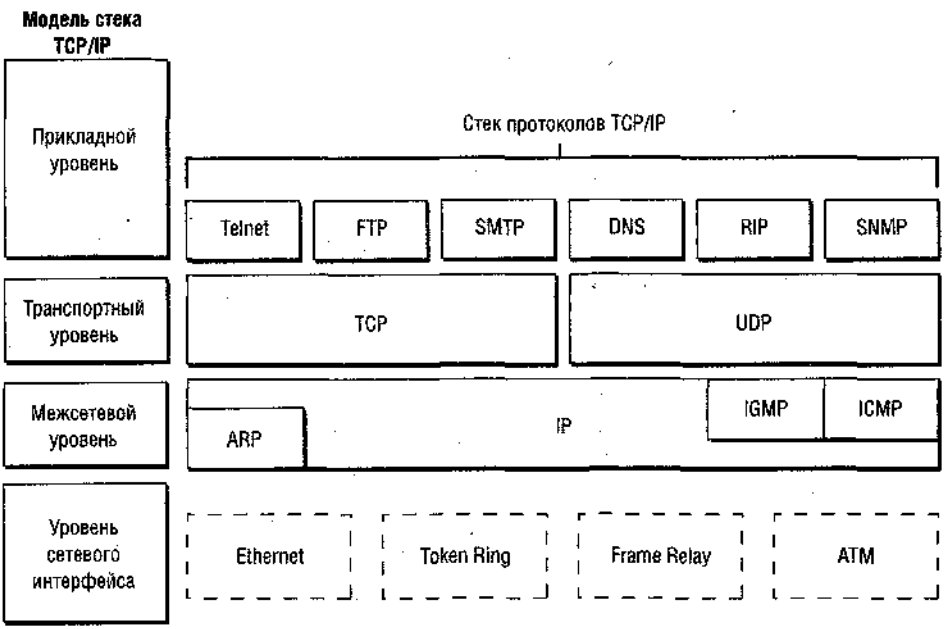


Рис. 2-1. Четырехуровневая модель TCP/IP и стек протоколов

Уровень сетевого интерфейса

Этот уровень определяет стандарты физической среды и передачи электрических сигналов. К стандартам этого уровня относятся; Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), X.25, Frame Relay, RS-232 и V.35.

Межсетевой уровень

Это этап процесса передачи информации, на котором данные упаковываются, снабжаются адресом и переправляются в нужную точку сети. Примеры протоколов этого уровня: ARP, IP и ICMP.

- **ARP (Address Resolution Protocol)** — протокол IP переправляет пакеты по логическим адресам, которые часто находятся на расстоянии сотен сегментов сетей, а ARP служит для нахождения в каждом из сегментов физических компьютеров, которым предназначаются IP-пакеты. После обнаружения с помощью ARP физических адресов устройств создается сопоставление IP- и MAC-адресов, и эта информация сохраняется в локальном кэше ARP. Для просмотра кэша служит команда arp -a, а для очистки — arp -d.

  На заметку С точки зрения экзаменов на звание MCSE, команда arp -d призвана экономить массу времени в условиях, когда невозможно подключиться к компьютеру, чью сетевую карту только что заменили. Логика такова: вместе с новым адаптером компьютер получит новый физический адрес, соответствующая запись в таблице сопоставления IP- и MAC-адресов окажется недействительной, а ваш компьютер будет, пытаться связаться с несуществующей сетевой картой. Так все выглядит в теории (т. е. такова логика составителей экзаменационных вопросов).
  В реальности же почти все записи ARP — динамические, т. е. попадают в кэш и удаляются из него по необходимости. Время жизни динамической ARP-записи — всего 2 минуты. Так что если предположить, что сопоставление сохранено в кэше, а затем кто-то выключил компьютер, заменил сетевую карту и снова включил, умудрившись при этом уложиться в 120 секунд, и слишком нетерпелив, чтобы дождаться момента повторной команды ping, тогда команда arp -d действительно поможет. В других обстоятельствах она бесполезна.

в IP (Internet Protocol) отвечает за адресацию и маршрутизацию пакетов между узлами. IP-пакет может теряться, доставляться в-неправильной очередности, дублироваться или откладываться — как в любых других протоколах. Однако IP не предусматривает исправление этих ошибок. За распознавание входящих пакетов, сохранение их очередности и восстановление потерянных пакетов отвечают протоколы более высокого уровня, такие как TCP.

- **ICMP (Internet Control** Message **Protocol)** позволяет IP-узлам и маршрутизаторам сообщать об ошибках и обмениваться (в определенных рамках) управляющей информацией и сведениями о состоянии. Команда ping служит для отправки эхо-запроса и получении эхо-ответа, который позволяет выявлять отсутствие связи и устранять стандартные неполадки TCP/IP.

ICMP и брандмауэры

Каждый уважающий себя администратор обязан настроить ICMP-сообщения на брандмауэре, защищающем доступ в Интернет. Большинство брандмауэров, в том числе и Basic Firewall из состава Windows Server 2003 (его еще называют Internet Connection Firewall), позволяют указывать ICMP-запросы, на которьхе должен отвечать брандмауэр. Например, чтобы посылать эхо-запросы брандмауэру, его следует сконфигурировать на обслуживание таких запросов.

Транспортный уровень

Транспортный уровень модели TCP/IP — это этап процесса передачи информации, на котором определяются стандарты передачи данных. Примеры из семейства **TCP/IP:** TCP и UDP.

- **TCP** (Transmission **Control Protocol)** принимает данные с прикладного уровня и обрабатывает их в виде потока байт, которые группируются в сегменты. TCP нумерует сегменты и ставит в очередь на доставку на узел сети. Получая поток данных от узла в сети, TCP переправляет эти данные приложению-адресату.

  Порты TCP позволяют различным приложениям и программам использовать сервисы TCP на одном узле (рис. 2-2). Каждая использующая TCP-порты программа прослушивает собственный порт (или порты) на предмет входящих сообщений. Данные, отправленные на определенный TCP-порт передаются прослушивающему его приложению.

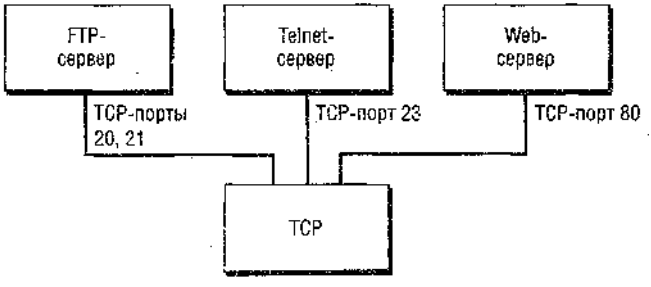


Рис. 2-2. TCP-порты

Подготовка к экзамену Фильтрация пакетов на маршрутизаторе позволяет блокировать или разрешать TCP- или UDP-трафик на основании номера порта. Для ответа на некоторые вопросы экзамена надо знать, какие порты открыть для доступа по протоколам File Transfer Protocol (FTP; TCP-порты 20 и 21), Hypertext Transfer Protocol (HTTP; TCP-порт80), Hypertext Transfer Protocol Secure/Secure Sockets Layer (HTTPS/SSL; TCP-порт 443), Pomt-to-Point Tunneling Protocol (PPTP; TCP-порт 1723) и L2TP/IPSec (UDP-порты 500, 1701 и 4500). Запомните номера этих портов!

UDP (User Datagram **Protocol)** — большинство сетевых сервисов (например DNS) используют в качестве транспортного протокола не TCP, а UDP, который обеспечивает быструю передачу дейтаграмм за счет отказа от присутствующих в TCP функций обеспечения надежности, таких как гарантированная доставка и проверка очередности пакетов. В отличие от TCP, UDP — это сервис *без установления соединения,* обеспечивающий лишь доставку дейтаграмм узлу сети. Если требуется надежная связь, следует использовать TCP или специальную программу с собственными функциями распознавания пакетов и сохранения их очередности.

Подготовка к зкззмеку Для экзамена надо знать, что не создающие соединений TCP/IP-сервисы используют в качестве транспорта UDP.

Прикладной уровень

На этом этапе данные конечного пользователя обрабатываются, упаковываются и пересылаются (или принимаются) на порты транспортного уровня. Протоколы прикладного уровня часто определяют понятный пользователю способ представления, именования, передачи или получения данных. К наиболее популярным прикладным протоколам TCP/IP относятся: HTTP, Telnet, FTP, TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), DNS (Domain Name System), POP3 (Post Office Protocol 3), SMTP (Simple Mail Transfer Protocol), NNTP (Network News Transfer Protocol).

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какой из уровней модели TCP/IP не содержит TCP/1P-протоколов?
   a. Уровень сетевого интерфейса.
   b. Межсетевой уровень.
   c. Транспортный уровень.
   d. Прикладной уровень.
2. Какой из перечисленных TCP/IP-протоколов не работает на межсетевом уровне?
   a. IP.
   b. ARP.
   c. TCP.
   d. ICMP.
3. Какой из перечисленных протоколов относится к транспортному уровню?
   a. IGMP.
   b. UDP.
   c. DNS.
   d. Ethernet.
4. Какие из перечисленных сервисов подключаются к UDP-портам? (Выберите все подходящие варианты.)
   a. NetBIOS.
   b. DNS.
   c. Ethernet.
   d. Telnet.

Резюме

- Набор протоколов TCP/IP состоит из четырех уровней: сетевого интерфейса, межсетевого, транспортного и прикладного.
- Протокол IP переправляет пакеты по логическим адресам, которые часто находятся на расстоянии сотен сегментов сетей, а ARP служит для нахождения в каждом из сегментов компьютеров, которым предназначаются IP-пакеты.
- TCP — это обязательный стандарт TCP/IP, обеспечивающий надежный сервис доставки пакетов с установлением логических соединений. UDP обеспечивает обмен

дейтаграммами, но не создает соединения и в отличие от TCP не гарантирует доставку или проверку их очередности. Как TCP, так и UDP предоставляет порты, по которым приложения взаимодействуют с сервисами транспортного уровня.

Занятие 2. **IP-адресация**

Чтобы успешно обмениваться данными в частной TCP/IP-сети или через Интернет, каждый сетевой узел должен обладать уникальным 32-битным IP-адресом. IP-адреса делятся на *общие* и *частные*. Первые уникальны в глобальном масштабе и используются для адресации в Интернете. Вторые ограничены диапазонами, которые обычно используются в частной сети, но не видны из Интернета.

Администратор сети Windows Server 2003 должен разбираться в механизме IP-адресации, в том числе в общей и частной адресации, шестнадцатеричной и двоичной нотации, классах адресов, масках подсетей и основных шлюзов.

Изучив материал этого занятия, вы сможете:

- *S* описать различные типы TCP/IP-адресации, поддерживаемые Windows Server 2003;
- *S* преобразовывать IP-адреса из точечно-десятичного в двоичное представление и наоборот;
- *S* различать идентификатор сети по умолчанию и идентификатор узла в любом IP-адресе;
- *У* рассказать о функциях маски подсети и основного шлюза.

Продолжительность занятия — около 45 минут.

Общие IP-адреса

Каждый IP-адрес в Интернете уникален. Для обеспечения такой уникальности адресов сетей в Интернете организация IANA (Internet Assigned Numbers Authority) разделила незанятую часть пространства IP-адресов и делегировала полномочия по их распределению региональным реестрам, среди которых Asia-Pacific Network Information Center (APNIC), American Registry for Internet Numbers (ARIN) и Reseaux IP Europeens (RIPE NCC). Региональные регистраторы выделяют блоки адресов небольшому количеству крупных поставщиков интернет-услуг (ISP), которые затем выдают более мелкие блоки своим клиентам и менее крупным провайдерам.

Как правило интернет-провайдер выдает по одному общему IP-адресу на каждый напрямую подключенный к провайдеру компьютер. Этот IP-адрес может назначаться динамически в момент подключения компьютера к ISP или статически закрепляться за выделенной линией или модемным подключением.

Частные IP-адреса

Часть IP-адресов никогда не используется в Интернете. Они называются *частными* и используются для организации адресации в сетях, которые «не видны» в общей сети. Например, пользователю, объединяющему компьютеры в домашнюю TCP/IP-сеть, не надо назначать общие IP-адреса каждому узлу — он использует частные адреса (табл. 2-1).

Табл. 2-1. Диапазоны частных адресов

Начальный адрес	Конечный адрес
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Узлы с частными IP-адресами могут подключаться к Интернету через прокси-сервер или компьютер с Windows Server 2003, сконфигурированный в качестве NAT-сервера (Network Address Translation). Windows Server 2003 также поддерживает *сервис общего доступа к Интернету* (Internet Connection Sharing, ICS), предоставляющий клиентам частной сети упрощенные сервисы NAT.

Методы IP-адресации

IP-адреса могут назначаться вручную, динамически (DHCP-сервером) или автоматически [например, с помощью APIPA (Automatic Private IP Addressing)].

Ручная IP-адресация

Назначение IP-адресов вручную используется нечасто, но иногда без него не обойтись. Например, ручное конфигурирование потребуется в сети, состоящей из нескольких сегментов, при отсутствии DHCP-сервера, или если IP-адрес DHCP-сервера также назначается вручную. Наконец, важным сетевым серверам, например DNS- или WINS-серверу или контроллеру домена, обычно назначают статические IP-адреса. Статические IP-адреса можно выделить по механизму резервирования DHCP-адресов, но большинство администраторов предпочитает не перепоручать это дело DHCP-серверу и назначают их вручную.

Во всех остальных случаях ручное конфигурирование рекомендуется, только если невозможно использовать DHCP. Администрирование назначенных вручную IP-адресов отнимает много времени и чревато ошибками, особенно в средних и крупных сетях.

Протокол DHCP

DHCP-сервер автоматически выделяет DHCP-клиентам IP-адреса из заданных администратором диапазонов. DHCP-сервер можно настроить на конфигурирование других параметров TCP/IP, например адресов DNS- и WINS-серверов, основных шлюзов и т. п.

Автоматическое назначение частных IP-адресов

APIPA (Automatic Private IP Addressing) служит для автоматического назначения адресов и применяется в простых односегментных сетях без DHCP-сервера (см. главу 1).

Альтернативная конфигурация

Подобно APIPA, альтернативная конфигурация позволяет назначить IP-адрес компьютерам, которым недоступен DHCP-сервер. Однако в отсутствие такого сервера компьютер с альтернативной конфигурацией не сможет использовать APIPA, даже если этот протокол будет доступен в сети.

Эта функция полезна, когда компьютер работает в нескольких сетях, в одной из которых нет DHCP-сервера. Например, портативный компьютер, используемый для работы в офисе и дома. В обеих сетях используется один и тот же адаптер и локальное

подключение, настроенное на автоматическое получение IP-адреса. При подключении к корпоративной сети параметры TCP/IP настраиваются DHCP-сервером. Дома DHCP-сервера нет, поэтому используется определенная альтернативная конфигурация: IP-адрес, маска подсети и основной шлюз для домашней сети.

Структура IP-адреса

IP-адреса привычно представляется в форме четырех чисел, разделенных точкой, например 192.168.100.22. Однако это лишь одна из форм IP-адреса, которая называется *десятично-точечной нотацией* и используется для удобства запоминания адреса. В компьютере применяется двоичная нотация, в которой все числа представлены только цифрами 1 и 0. Это «родная» форма IP-адреса.

Логика IP-адресации становится понятной при рассмотрении двоичной версии IP-адреса. Для конфигурирования, управления и устранения неполадок IP-адресации надо уметь работать с IP-адресами в двоичной форме, а также переводить их из двоичного в десятичное представление и обратно.

Преобразование нотации вручную

В эпоху компьютеров и инженерных калькуляторов ручное преобразование чисел в другую систему исчисления может показаться устаревшим и крайне нудным способом решения арифметических задачек. По правде говоря, администраторы сети в своей работе редко сталкиваются с необходимостью подобных вычислений, но уж если придется, они скорее схватятся за калькуляторы, чем за перо и бумагу. И даже во время экзамена вам скорее всего не потребуются ручные вычисления, поскольку в большинстве центров тестирования в пользовательском интерфейсе программы экзамена предусмотрен инженерный калькулятор (а уж обыкновенный калькулятор есть в любом центре тестирования).

Возникает законный вопрос: зачем утомлять себя ручными вычислениями, если можно просто взять калькулятор? Ответ прост: научившись выполнять эти действия вручную, вы получите более четкое представление о форме IP-адреса и сможете быстрее выявлять и устранять неполадки конфигурации. Этот навык особенно ценен в сетях с многими подсетями, где схемы IP-адресапии могут сбить с толку любого.

Помимо сугубо практического применения, умение преобразовывать представление IP-адреса показывает высокий класс администратора, подобно тому, как современный бухгалтер, использующий в повседневной работе бухгалтерское ПО, должен уметь рисовать «самолетики» с оборотами по дебету и кредиту счетов. Если и эта аналогия кажется неубедительной, просто считайте, что этот навык пригодиться, если в критической ситуации под рукой не окажется калькулятора. Кроме того, вы сможете блеснуть подобным «высшим пилотажем» перед коллегами.

Преобразование двоичного и десятичного представлений

Привыкшие к десятичным системам счисления люди с большой неохотой относятся к двоичным числам. В десятично-точечной нотации каждое 32-битное число IP-адреса представляется в виде четырех десятичных групп, значение каждой из которых лежит в диапазоне 0—255, например 192.168.0.225. Эти числа представляют четыре 8-битных зна-

чения, составляющих 32-битный адрес. В любой нотации каждая из четырех групп называется *октет*. Но только двоичная форма позволяет наглядно увидеть значение каждого бита. Например, IP-адрес 192.168.0.225 в двоичной форме выглядит так:

11000000 10101000 00000000 11100001

В IP-адресах октеты и биты считаются слева направо. Первый октет соответствует первому слева, а биты с 1 по 8 соответствуют первым восьми битам, начиная с самого левого. Второй октет— это следующие восемь битов (9—16), затем идет третий октет (биты 17—24), а замыкает последовательность четвертый октет (биты 25—32). В десятично-точечной нотации октеты отделяются точками, а в двоичной — пробелами.

В табл. 2-2 показаны экспоненциальное и десятичное представление битов в двоичном октете. Обратите внимание: если смотреть слева направо, то первый бит дает значение 128, а каждый последующий бит — половину значения предыдущего. И наоборот, в направлении справа налево, начиная с восьмого бита (значение 1), «цена» каждого последующего бита в два раза больше, чем предыдущего.

Табл. 2-2. Возможные значения в бинарном октете

Октет	**Первый бит**	**Второй бит**	**Третий бит**	**Четвертый бит**	**Пятый бит**	**Шестой бит**	**Седьмой бит**	**Восьмой бит**
Экспоненциальное представление	**27**	**26**	**25**	**24**	**23**	**22**	**21**	**20**
Десятичное представление	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Пример	**1**	**0**	**1**	**0**	**1**	**1**	**0**	**0**

Обратите внимание, что вклад бита в общую сумму ненулевой, только если он содержит 1. Например, если первый бит — 1, ему соответствует десятичное значений 128. Если же его значение — 0, то и десятичное значение равно нулю. Октету со всеми битами; равными 1, соответствует десятичное значение 255. Если все биты содержат 0, десятичное значение октета равно 0.

Пример перевода из двоичной нотации в десятичную. Пусть первый октет IP-адреса в двоичном представлении выглядит так:

1010100

Первый, третий, пятый и шестой биты содержат 1, а остальные — 0. Для упрощения решения нарисуем таблицу перевода, в которой отобразим возможные «веса» битов октета:

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
1	**0**	**1**	**0**	**1**	**1**	**0**	**0**

сложим десятичные эквиваленты каждого бита и найдем десятичную сумму октета:
1-й бит (128) + 3-й бит (32) + 5-й бит (8) + 6-й бит (4) = сумма.октета (172)

Поскольку сумма составляет 172, первый октет нашего IP-адреса в десятичной форме равен 172.

Применив этот же метод, можно преобразовать полный IP-адрес вида

10101100 00010001 00000111 00011011

в десятично-точечное представление: 172.17.7.27.

Пример перевода из десятичной нотации в двоичную. Перевод октета из десятичной формы в двоичную осуществляется записью 1 или 0 в соответствующий бит октета слева направо, пока не будет получено искомое десятичное число. Если запись 1 в очередной бит приводит к тому, что полученная сумма превосходит десятичное число, просто запишите в этот бит 0 и перейдите к следующему.

Допустим, надо перевести IP-адрес 172.31.230.218 в двоичный вид. Первым делом запишите последовательность возможных весов битов в таблицу:

128	64	32	16	8	4	2	1
							—.

Начнем с первого числа — 128. Поскольку 128 меньше 172, запишем 1 в первый бит, а наша промежуточная сумма будет 128. Затем посмотрим вес второго бита — 64. Так как 128 + 64 больше 172, второй бит установим в 0. Затем перейдем к третьему биту, вес которого — 32. 128 и 32 в сумме дают меньше 172, поэтому запишем в этот бит 1. Промежуточная сумма становится 128 + 0 + 32=160. Перейдем к четвертому биту, его вес — 16. 160 и 16 в сумме дают больше 172, поэтому пишем 0. Вес пятого бита — 8. Сумма 160 + 8 меньше 172, пишем в пятый бит 1, а промежуточная сумма становится 128 + 0 + 32 + 0 + 8 = 168. И наконец вес шестого бита — 4, сумма 168 и 4 равна 172, т. е. искомому числу. Поэтому пишем 1 в шестой бит, а оставшиеся седьмой и восьмой биты заполняем нулями.

Таким образом, первый октет в двоичной форме выглядит так:

```
10101100
```

Выполнив аналогичные операции с остальными октетами получим двоичное представление адреса 172.31.230.218:

```
10101100 00011111 11100110 11011010
```

Перевод между системами счисления с помощью калькулятора. При помощи *Калькулятора* (Calculator) эта операция выполняется намного быстрее. Чтобы воспользоваться функцией перевода между системами счисления, в меню **Вид** (View) выберите **Инженерный (Scientific)** и установите переключатель в положение **Dec** или Bin (в зависимости от того, из какой системы счисления необходимо перевести число). Например, для перевода двоичного числа 11001100 в десятичное представление, отметьте Bin, введите двоичное число (рис. 2-3). Рекомендуем по возможности использовать копирование и вставку.

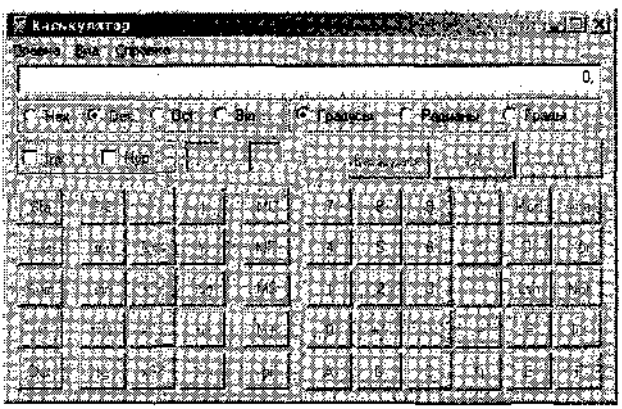


Рис. 2-3. Ввод двоичных чисел в калькуляторе

После ввода двоичного числа просто установите Dec и получите число в десятичном представлении.

Примечание Как и в десятичной нотации, калькулятор отбрасывает крайние левые нули, октет 00001110 отображается как 1110. Поэтому необходимо контролировать число отображаемых в окошке калькулятора битов, чтобы не перепутать значения. Например, легко спутать двоичное число 1100001 (десятичное 97) с 11000001 (десятичное значение 193). Если число бит меньше 8, для представления октета IP-адреса надо добавить необходимое количество нулей слева. Можно также использовать функцию группировки цифр, но она, к сожалению, не доступна на экзамене.

Идентификаторы сети и узла

Маршрутизаторы, переправляющие пакеты данных между TCP/IP-сетями не обязаны знать, какому именно узлу предназначен тот или иной IP-пакет. Вместо этого маршрутизатор считывает из IP-пакета только адрес сети, в которой находится узел — приемник пакета, а затем на основе своей таблицы маршрутизации определяет, каким образом доставить пакет в сеть, в которой расположен адресат. Точное местоположение узла определяется только после доставки пакета в нужный сегмент сети.

Такой механизм маршрутизации возможен благодаря делению IP-адреса на два компонента:

- *идентификатор сети* (network ID) — первая часть IP-адреса, представляющая конкретную сеть в более крупной TCP/IP-сети (например в Интернете);
- *идентификатор узла* (host ID) — вторая часть IP-адреса, определяющая узел TCP/IP (рабочую станцию, сервер, маршрутизатор или любое другое TCPДР-устройство).

На рис. 2-4 показано разбиение IP-адреса (131.107.16.200) на идентификаторы сети (пеивые два октета — 131.107) и узла (последние два октета — 16.200). • •

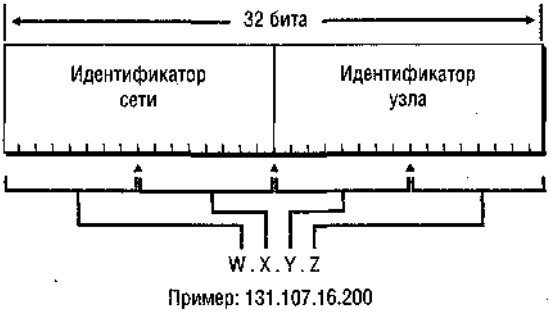


Рис. 2-4. Идентификаторы сети и узла

Идентификаторы сетям и узлам назначают по определенным правилам:

- нельзя присваивать всем битам идентификаторов сети и узла значение 1, поскольку такие адреса считаются широковещательными;
- нельзя присваивать всем битам идентификаторов сети и узла значение 0, поскольку такой адрес интерпретируется как «только эта сеть»;
- идентификатор узла должен быть уникален в пределах локальной сети.

Классы IP-адресов

Класс IP-адреса определяется по значению первого октета и показывает, какие из 32 битов представляют идентификатор сети по умолчанию. Класс IP-адреса также определяет максимально возможное количество узлов в сети. Определено пять классов адресов, из которых для адресации TCP/IP-узлов используются только классы A, B и C.

В табл. 2-3 октеты IP-адреса обозначаются как *w.x.y.z*- В ней показано:

- как значение первого октета (w) определяет класс IP-адреса;
- как октеты адреса подразделяются на идентификаторы сети и узла;
- максимальное число сетей и узлов в сети данного класса.

Табл. 2-3. Классы IP-адресов

Класс	Значение *w*	Значения первых битов	Идентификатор сети	Идентификатор узла	Количество сетей в классе	Количество узлов в сети (по умолчанию)
A	1-126	0	*w*	*x.y.z*	126	16777214
B	128-191	10	*w.x*	*y-z* .	16384	65534
C	192-223	ПО	*w.x.y*	*Z*	2097152	254
D	224-239	1110	Зарезервирован для многоадресной рассылки	Нет	•Нет	Нет
E	240-254	1111	Зарезервирован для экспериментального использования	Нет	Нет	Нет

Рис. 2-5 демонстрирует различие между адресами классов A, B и C.

Маска подсети

Еще один необходимый для нормальной работы TCP/IP параметр — *маска подсети* (subnet mask), которая служит для определения, в какой сети находится приемник пакета — локальной или внешней. Маска подсети — это 32-битный адрес, представляющий собой последовательность битов со значением 1, который используется для выделения, или *маскировки,* идентификатора сети адреса назначения пакета и отделения идентификаторов сети и узла. Каждому узлу сети TCP/IP нужна маска подсети (если сеть не разбита.на подсети, т. е. состоит из одной подсети) или маска по умолчанию (в случае разбиения сети на подсети).

Например, такое 32-битное число представляет маску подсети по умолчанию для узлов с адресами класса B (например 172.20.16.200):

```
11111111 11111111 00000000 00000000 (255.255.0.0)
```

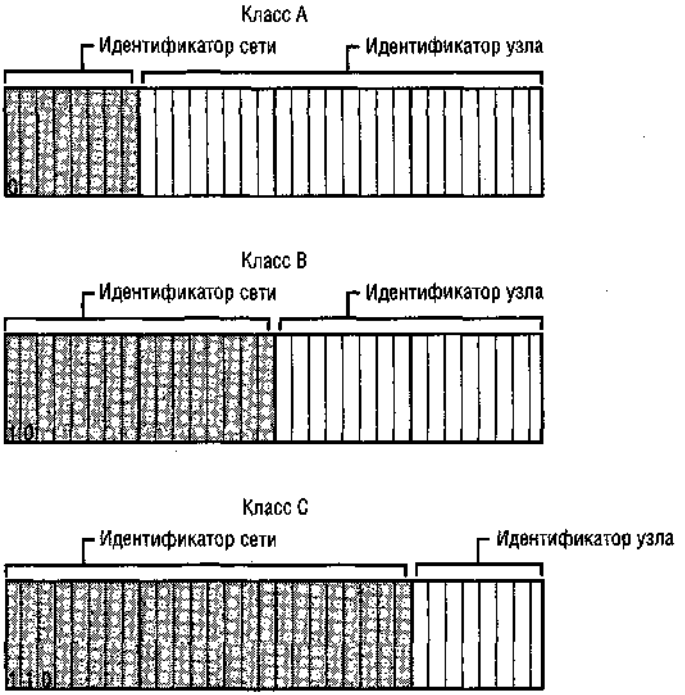


Рис. 2-5. Классы IP-адресов

Когда TCP/IP-узел с адресом 172.20.16.200 отправляет пакет по адресу 172.21.17.201, он сначала выполняет побитовую операцию «И» по отношению к локальным адресу и маске подсети. Поскольку эта логическая операция в результате дает 0 во всех битах кроме тех, в который в обоих операндах стояли 1, то

```
172.20.16.200 И 255.255.0.0 = 172.20.0.0
```

Затем узел повторяет эту операцию, но вместо адреса отправителя подставляет адрес получателя. В результате получается 172.21.0.0. Затем TCP/IP сравнивает результаты этих операций. Если они совпадают, получатель расположен в этой же подсети. Иначе приемник и получатель расположены в разных подсетях.

Длина префикса сети в маске подсети

Поскольку биты идентификатора сети всегда идут последовательно и начинаются с самого левого, самый простой способ показать маску подсети — это указать количество битов идентификатора сети в виде *префикса сети*. Таким образом, маска подсети выражается в виде «IP-адрес/префикс сети». Например, IP-адрес 131.107.16.200 и маску подсети 255.255.0.0 можно записать в виде 131.107.16.200/16. Число 16 после слеша обозначает количество единичных битов в маске подсети. Точно так же, /24 обозначает маску подсети 255.255.255.0 для адреса класса C, например 206.73.118.23/24.

Примечание Нотация с префиксом сети также известна как *бесклассовая междоменная маршрутизация* (Classless Interdomain Routing, CIDR).

В табл. 2-4 показаны маски подсети по умолчанию для классов адресов Интернета.

Табл. 2-4. Маски подсети

Класс адреса	Маска подсети по умолчанию в двоичном виде	Префикс сети и десятичный эквивалент
Класс A	11111111 00000000 00000000 00000000	/8 = 255.0.0.0
Класс B	11111111 1111111100000000 00000000	/16 = 255.255.0.0
Класс C	11111111 11111111 11111111 00000000	/24 =-255.255.255.0

Основной шлюз

Связь между TCP/IP-узлами разных сетей как правило выполняется через маршрутизаторы. *Маршрутизатор* — это устройство с несколькими интерфейсами, подключенными к разным сетям, а *маршрутизация* — процесс приема IP-пакетов на одном интерфейсе и пересылка их на другой интерфейс в направлении адресата. С точки зрения узла сети TCP/IP, *основной шлюз* — это IP-адрес маршрутизатора, сконфигурированного на пересылку IP-трафика в другие сети.

Пытаясь передать информацию другому узлу IP-сети, компьютер определяет тип узла (локальный или удаленный) по маске подсети. Если узел-получатель расположен в локальном сегменте сети, пакет направляется в локальную сеть по методу широковещания. В противном случае компьютер пересылает пакет в основной шлюз, определенный в параметрах TCP/IP. Обязанность дальнейшей пересылки пакета в нужную сеть возлагается на маршрутизатор, адрес которого указан в качестве основного шлюза.

Лабораторная работа. **Октеты**

Вы будете вручную переводить числа из десятичной нотации в двоичную и обратно, а также преобразовывать маски подсети.

Упражнение 1. Перевод числа из десятичного представления в двоичное вручную

Переведите число, указанное над таблицей. Для перевода используйте таблицу, затем воспользуйтесь калькулятором и сравните результаты.

Число в десятичном представлении: 159

128	64	32	16	8	4	2	1

Число в двоичном представлении:_____

Число в десятичном представлении: 65

128	64	32	16	8	4	2	1

Число в двоичном представлении:_____

Число в двоичном представлении: 1001010

128	64	32	16	8	4	2	1

Число в десятичном представлении:_____

Число в двоичном представлении: 01110011

128	64	32	16	8	4	2	1

Число в десятичном представлении:_____

Упражнение 2. Преобразование маски подсети из десятично-точечной формы в форму с префиксом сети и обратно

Преобразуйте нестандартную маску подсети из десятично-точечной формы в форму с префиксом сети и наоборот. Помните, что это нестандартные маски подсетей (см. занятие 3). При выполнении задания воспользуйтесь калькулятором и табл. 2-4.

1. 255.255.255.192.
2. 255.255.252.0.
3. /27.
4. /21.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Что используется для определения идентификатора сети назначения пакета?
   a. IP-заголовок.
   b. Маска подсети.
   c. Класс адреса.
2. Выяснилось, что идентификатор сети назначения пакета совпадает с идентификатором сети узла. Что узел должен сделать с пакетом?
   a. Отправить широковещательный ARP-запрос, чтобы определить MAC-адрес узла назначения, и передать пакет в локальную сеть.
   b. Отправить пакет серверу, который выполнить его широковещание в локальной сети.
   c. Отправить пакет основному шлюзу с тем, чтобы тот доставил его получателю.
3. Какое из перечисленных далее десятично-точечных значений соответствует двоичному адресу 11001100 00001010 11001000 00000100? Сначала переведите число вручную, а затем проверьте ответ с помощью калькулятора.
   a. 204.18.200.3.
   b. 204.34.202.4.
   c. 204.10.200.44.
   d. 202.10.200.4.

4. Какое из перечисленных далее двоичных значений соответствует адресу 207.209.68.100? Сначала переведите число вручную, а затем проверьте ответ с помощью калькулятора.
   a. 1100111Г 11010001 01000100 01100100.
   b. 11000111110100010100100 01100100.
   c. 11001111110100010100100 01101100.
   d. 11001111 11010001 11001101 01100100.
5. Определите двоично-десятичный эквивалент приведенного далее адреса. Используйте нотацию CIDR для определения маски подсети по умолчанию. Сначала выполните преобразование вручную, а потом проверьте его с помощью калькулятора.

   10010010 01101011 00100111 10001001

Резюме

- Общие IP-адреса используются в Интернете и являются уникальными. Частные IP-адреса ограничены определенными диапазонами и могут использоваться для адресации в локальных сетях.
- В отсутствие DHCP-сервера альтернативная конфигурация позволяет автоматически конфигурировать компьютер для использования указанного IP-адреса вместо APIPA.
- В TCP/IP основной шлюз — это маршрутизатор, соединяющий подсеть с другими сетями.
- Маска подсети служит для сравнения идентификатора сети локального узла и идентификаторов сети каждого отправляемого IP-пакета. При совпадении идентификаторов сетей узла и адресата пакет пересылается по локальной сети. В противном случае пакет направляется на основной шлюз.
- Класс IP-адреса определяет маску подсети по умолчанию.

Занятие 3. Разбиение IP-сетей на подсети и создание надсетей

Маски подсети позволяют настраивать адресное пространство в соответствии с требованиями к сети. Разбиение на подсети позволяет организовать иерархическую структуру сетей, а надсети и CIDR позволяют объединить разные сети в едином адресном пространстве.

Изучив материал этого занятия, вы сможете:

- *S* применять маски подсети в соответствии с требованиями и ограничениями сетей;
- *S* на основании сетевого адреса и маски подсети определять количество доступных подсетей и узлов;
- *S* определять диапазон IP-адресов для каждой подсети по заданному сетевому адресу и маске подсети;
- *S* применять маски подсети для настройки адресного пространства подсетей;
- *S* конфигурировать маски подсети переменной длины для подсетей различного размера.

Разбиение на подсети

Маски подсети помогают определить, как IP-адрес разбивается на идентификаторы сети и узла. В адресах классов A, B и C применяются стандартные маски подсети, занимающие соответственно первые 8, 16 и 24 бита 32-битового адреса. *Подсетью* называется логическая сеть, определяемая маской подсети.

Стандартные маски годятся для сетей, которые не предполагается разбивать. Например, в сети из 100 компьютеров, соединенных с помощью карт гигабитного Ethernet, кабелей и коммутаторов, все узлы могут обмениваться информацией по локальной сети. Сеть не нуждается в маршрутизаторах для защиты от чрезмерного широковещания или для связи с узлами, расположенными в отдельных физических сегментах. В таком простом случае вполне достаточно идентификатора сети класса C (рис. 2-6).

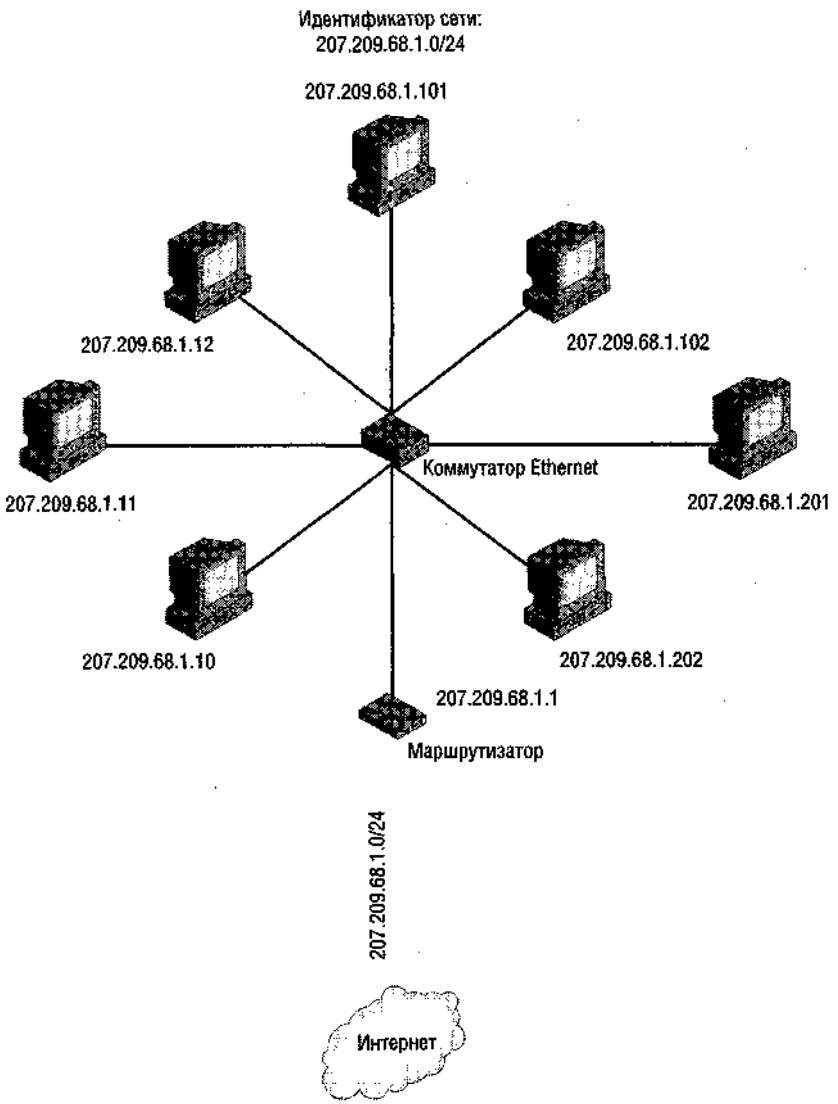


Рис. 2-6. Сеть, состоящая из одной подсети

Механизм разбиения на подсети

Разбиение на подсети (subnetting) — это логическое разделение адресного пространства сети путем установки в 1 дополнительных битов маски подсети. Такое расширение позволяет создавать многие подсети в адресном пространстве сети.

Например, если маска подсети по умолчанию 255.255.0.0 используется для узлов сети класса B 131.107.0.0, IP-адреса 131.107.1.11 и 131.107.2.11 находятся в одной подсети и поддерживают взаимодействие посредством широковещания. Но если расширить маску подсети до 255.255.255.0, то эти адреса окажутся в разных подсетях и для обмена данными соответствующим узлам придется пересылать пакеты на основной шлюз, который перенаправит дейтаграммы в нужную подсеть. Внешние по отношению к сети узлы попрежнему используют маску подсети по умолчанию для взаимодействия с узлами внутри сети. Обе версии показаны на рис. 2-7 и 2-8.

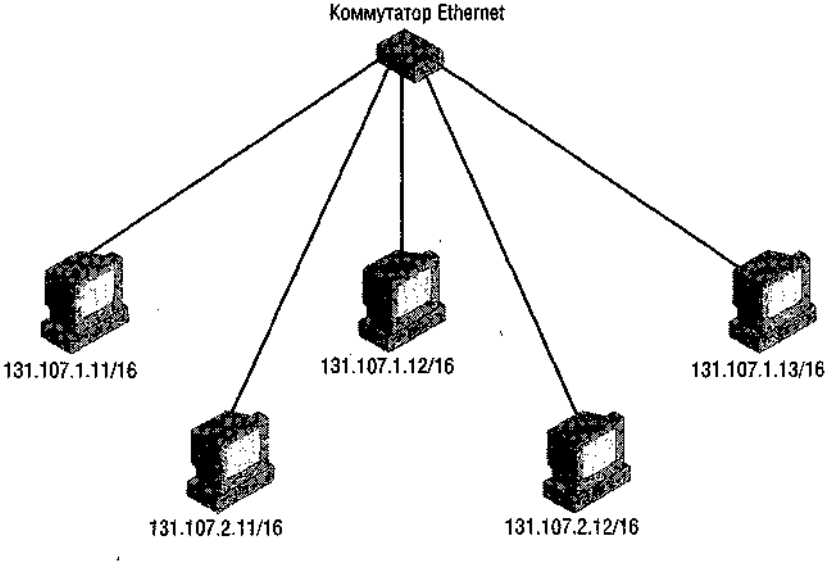


Рис. 2-7. Не разбитое на подсети адресное пространство класса B

Показанное на рис. 2-7 исходное адресное пространство класса B, состоящее из единственной подсети, может содержать максимум 65 534 узлов, а новая маска подсети (рис. 2-8) позволяет разделить адресное пространство на 256 подсетей, в каждой из которых можно разместить до 254 узлов.

Преимущества разбиения на подсети

Разбиение на подсети часто используют для обеспечения соответствия физической и логической топологии сети или Для ограничения широковещательного трафика. Другие несомненные преимущества: более высокий уровень защиты (благодаря ограничению неавторизованного трафика маршрутизаторами) и упрощение администрирования (благодаря передаче управления подсетями другим отделам или администраторам).

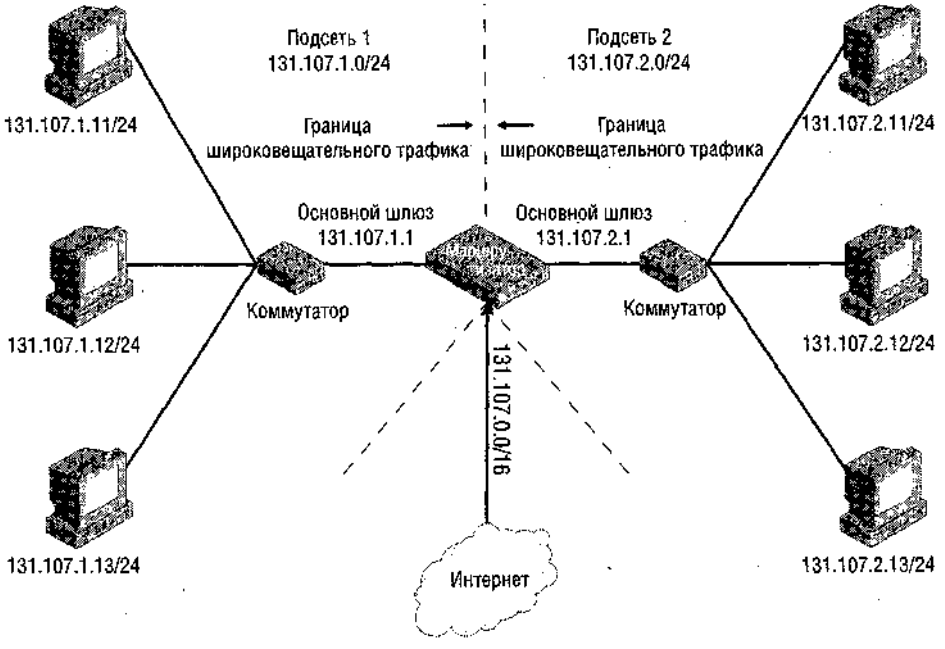


Рис. 2-8. Разбитое на подсети адресное пространство класса B

Соответствие физической топологии. Допустим, вам поручили спроектировать университетскую сеть, состоящую из 200 узлов, распределенных в четырех зданиях — Voter Hall, Twilight Hall, Monroe Hall и Sunderland Hall. В каждом здании планируется разместить по 50 узлов. Если интернет-провайдер выделил адрес 208.147.66.0 класса C, вам доступны адреса 208.147.66—208.147.66.254. Однако из-за размещения в четырех физически отделенных зданиях, узлы не могут обмениваться данными по локальной сети. Расширив маску подсети на 2 бита (т. е. позаимствовав их у идентификатора узла), сеть" разбивают на четыре логические подсети, а для связи устанавливается маршрутизатор (рис. 2-9).

Ограничение широковещательного трафика. Широковещание — рассылка сообщений с одного компьютера на все расположенные в локальном сегменте устройства. Широковещание существенно нагружает ресурсы, поскольку занимает полосу пропускания и требует участия всех сетевых адаптеров и процессоров логического сегмента сети.

Маршрутизаторы блокируют широковещание и защищают сети от излишнего трафика. Поскольку маршрутизаторы также определяют логические ограничения подсетей, разбиение на подсети позволяет косвенно ограничивать широковещательный трафик в сети.

Определение максимального количества узлов в сети

Зная сетевой адрес, определить максимальное количество узлов в сети просто: надо возвести 2 в степень, равную количеству битов в идентификаторе узла и вычесть 2. Например, в сетевом адресе 192.168.0.0/24 под идентификатор узла отведено 8 бит, поэтому возможное максимальное число узлов $2^8 - 2 = 254$.

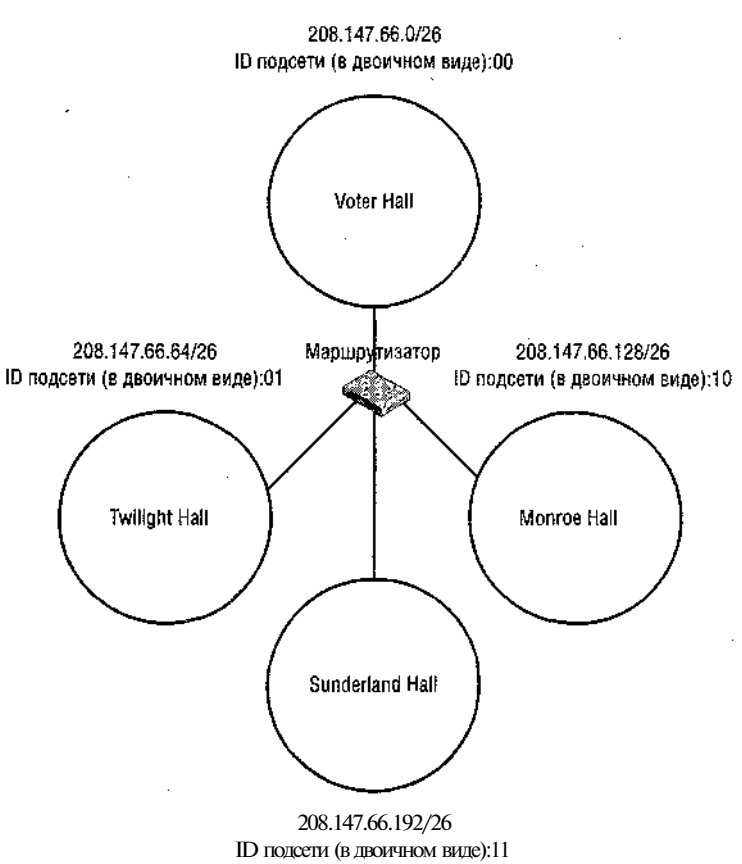


Рис. 2-9. Разбиение на подсети в соответствии с физической топологией

Совет В *Калькуляторе* степень двойки вычисляют с помощью кнопки x^y. Эта функция доступна только в инженерном режиме.

Исключение идентификаторов узла, состоящих из одних нулей или одних единиц. Значение 2^x показывает общее количество комбинаций значений битов двоичного числа *x,* включая комбинации из одних нулей и одних единиц. Например, *V* дает 8, т. е. количество различных комбинаций из 3 битов *(dec.* означает десятичную систему счисления):

000 = 0 (дес.)
001 = 1 (дес.)
010 = 2 (дес.)
011 = 3 (дес.)
100 = 4 (дес.)
101 = 5 (дес.)
110 = .6 (дес.)
111 = 7 (дес.)

Однако узлам нельзя назначать адреса, состоящие из одних только нулей или единиц, поскольку они зарезервированы для других целей. Идентификатор узла, состоящий из одних нулей, на самом деле определяет сеть без указания конкретного узла. Идентификатор узла из одних единиц зарезервирован в протоколе IP для широковещания (передачи сообщения всем узлам сети). При подсчете максимального количества узлов в сети эти варианты надо исключить из рассмотрения (т. е. вычесть из него 2).

Определение емкости подсети

При увеличении количества битов в маске подсети для создания подсетей в адресном пространстве идентификатор узла укорачивается, и создается новое адресное пространство для идентификатора подсети (рис. 2-10 и 2-11).

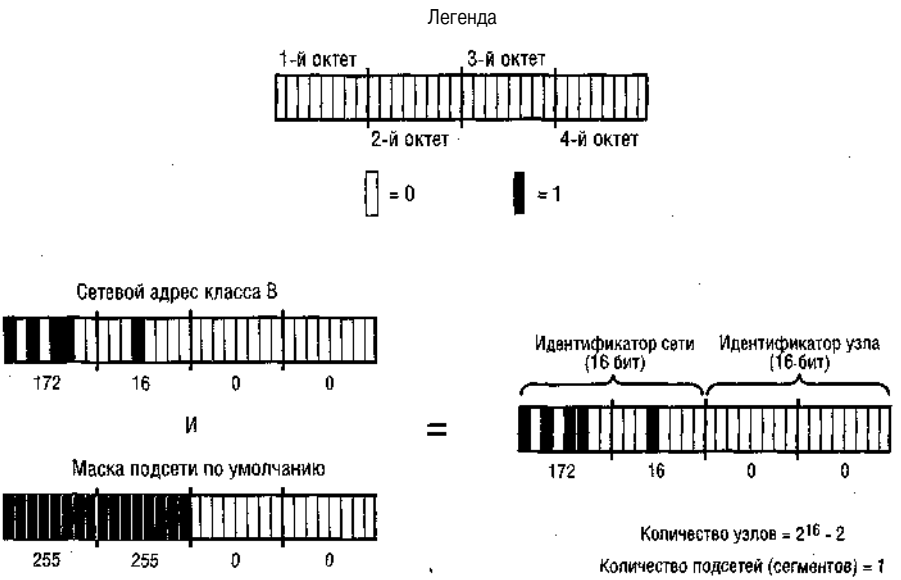


Рис. 2-10. Адресное пространство класса B по умолчанию

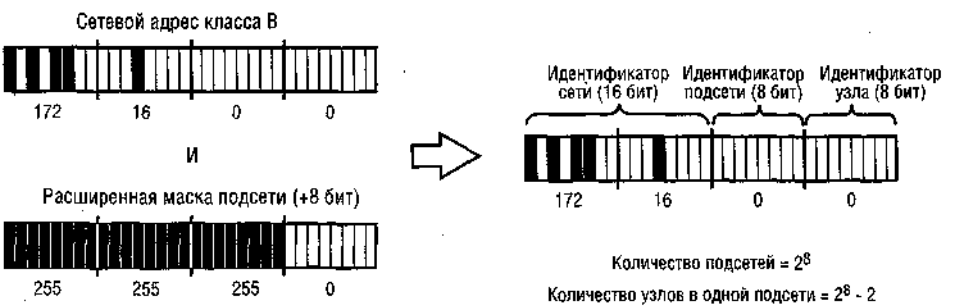


Рис. 2-11. Адресное пространство с идентификатором подсети

Чтобы определить количество доступных в адресном пространстве подсетей, просто возведите 2 в степень *y*, где *y* — количество бит в идентификаторе подсети. Например, если в адресном пространстве 172.16.0.0/16 выделить 8 бит на адрес подсети (т. е. привести к виду 172.16.0.0/24), количество доступных подсетей станет 2^8, или 256. Из него не

надо вычитать 2, поскольку большинство современных маршрутизаторов [включая сервис *Маршрутизация и удаленный доступ* (Routing and Remote Access) в Microsoft Windows NT Server, Microsoft Windows 2000 Server и Windows Server 2003] принимают идентификаторы подсетей только из единиц или нулей.

Планируя адресное пространство и маски подсети убедитесь, что отведенных на идентификатор подсети бит достаточно для размещения всех подсетей, а также обеспечен резерв для расширения сети в будущем. Помните, что любую физическую сеть надо рассматривать как подсеть.

Совет Калькулятор позволяет быстро определить необходимое число бит для идентификатора подсети. Вычтите 1 из требуемого количества подсетей в десятичном формате, переведите результат в двоичный вид и посчитайте количество бит в нем. Например, если нужна 31 подсеть, введите 30 и установите переключатель **Bin.** Полученное число НПО говорит, что под идентификатор подсети нужно зарезервировать 5 бит.

Количество узлов в подсети. Количество идентификаторов узлов в подсети определяется так же, как и узлов в сети — оно равно $2^x - 2$, где x — количество бит в идентификаторе узла. Например, в адресе 172.16.0.0/24 резервируется 8 бит под идентификатор узла, поэтому число узлов в подсети равно $2^8 - 2$, т. е. 254. Для вычисления количества узлов во всей сети умножают полученный результат на количество подсетей. В нашем примере адресное пространство 172.16.0.0/24 дает 254 сетей x 256 узлов = 65 024.

Конфигурируя адресное пространство и маски подсети в соответствии с требованиями сети убедитесь, что отвели на идентификатор узла достаточно бит с учетом возможного увеличения количества узлов в подсети в будущем.

Совет *Калькулятор* позволяет быстро определить необходимое количество бит для идентификатора узла. Прибавьте 1 к требуемому количеству узлов в подсети в десятичном формате, переведите результат в двоичный вид и посчитайте количество бит в нем. Например, если нужно 33 узла в подсети, введите 34 и установите переключатель **Bin.** Результат 100010 говорит о том, что нужно зарезервировать 6 бит под идентификатор подсети.

Примеры подсетей

В предыдущем примере мы расширили маску подсети для адресного пространства 172.16.0.0/16 до 255.255.255.0, увеличив ее на целый октет. На практике маску расширяют более мелкими порциями, вплоть до отдельных битов.

Например, на рис. 2-12 показано адресное пространство 10.0.0.0/12. Поскольку адрес относится к классу A, количество единичных битов в маске подсети по умолчанию равно 8. Мы расширили его на 4 бита, т. е. 4 бита отдано под идентификатор подсети, а оставшиеся 20 служат идентификатором узла. В такой сети диапазон адресов первой подсети (идентификатор 000) 10.0.0.1-10.15.255.254.

На рис. 2-13 адресу класса B 172.20.0.0 назначена нестандартная маска подсети 255.255.248.0, расширяющая маску по умолчанию на 5 бит. В такой сети диапазон адресов первой подсети (идентификатор 00000) 172.20.0.1-172.20.7.254.

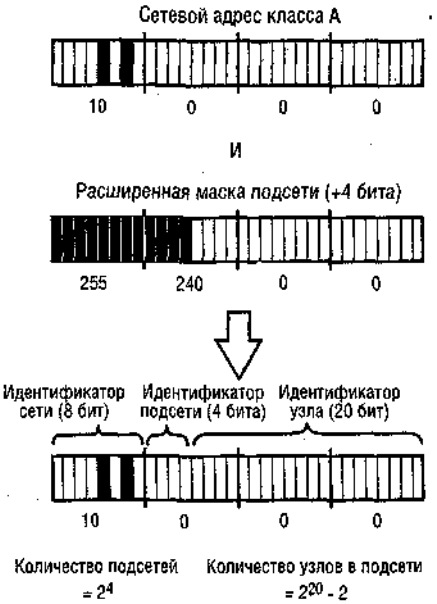


Рис. 2-12. Разделение на подсети адресного пространства класса A

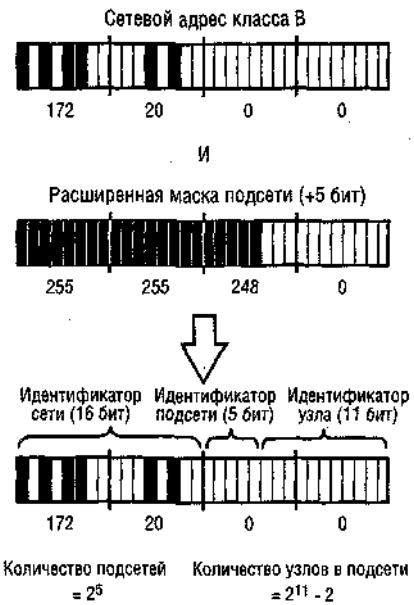


Рис. 2-13. Разделение на подсети адресного пространства класса B

На рис. 2-14 показан адрес класса C 192.168.0.0/26. В этом примере 2 бита зарезервированы для идентификатора подсети и 6 — под идентификатор узла. В такой сети диапазон адресов первой подсети (идентификатор 00) 192.168.0.1—192.168.0.62.

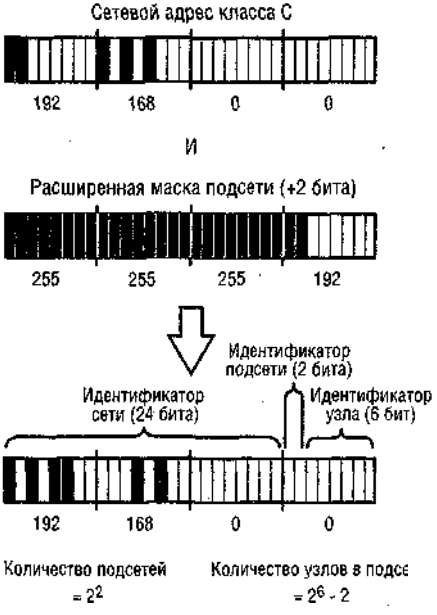


Рис. 2-14. Разбитое на подсети адресное пространство класса С

Определение диапазонов адресов подсети

Десятично-точечная форма маски подсети позволяет определить диапазоны IP-адресов в каждой подсети простым вычитанием из 256 числа в соответствующем октете маски. Например, в сети класса С с адресом 207.209.68.0 с маской подсети 255.255.255.192 вычитание 192 из 256 даст 64. Таким образом, новый диапазон начинается после каждого 64 адреса: 207.209.68.0-207.209.68.63, 207.209.68.64-207.209.68.127 и т.д. В сети класса В 131.107.0.0 с маской подсети 255.255.240.0 вычитание 240 из 256 дает 16. Следовательно, диапазоны адресов подсетей группируются по 16 в третьем октете, а четвертый октет принимает значения из диапазона 0—255: 131.107.0.0—131.107.15.255, 131.107.16.0—131.107.31.255 и т. д.

Помните, что узлам нельзя назначать идентификаторы из одних нулей или единиц, так что исключаются первый и последний адрес каждого диапазона.

Сложение маршрутов путем создания надсетей

Чтобы предотвратить истощение доступных идентификаторов сетей старших классов, организации, ответственные за адресацию в Интернете, предложили схему, называемую *созданием надсетей* (supernetting), согласно которой несколько сетей (маршрутов) можно объединить (или сложить) в единую более крупную сеть. Надсети позволяют эффективнее управлять выделением участков адресного пространства.

Допустим, организации нужно объединить в сеть 2000 узлов. Это слишком много для одной сети класса С, которая поддерживает не более 254 узлов. Сеть класса В поддерживает 65 534 узла, но таких сетей возможно всего 16 383 и количество свободных стремительно сокращается. Интернет-провайдеру нет смысла (да и возможности) выделять сети класса В клиентам, которые будет использовать только 3% диапазона адресов.

Надсети позволяют интернет-провайдеру выделить клиенту блок адресов класса C, который будет рассматриваться как единая сеть, представляющая собой нечто среднее между классами C и B. В нашем примере блок из 8 идентификаторов сети класса C даст возможность организации объединить в сеть до 2032 узлов.

Как работают надсети

Надсети отличаются от подсетей тем, что заимствуют биты идентификатора сети и маскируют их как идентификатор узла. Допустим, интернет-провайдер выделил блок из 8 адресов сети: 207.46.168.0—207.46.175.0. Если определить на маршрутизаторах провайдера и всех узлов сети маску подсети /21 (вместо /24 по умолчанию), все сети будут казаться единственной сетью из-за того, что их идентификаторы (урезанные до 21 бита) будут выглядеть одинаково (рис. 2-15).

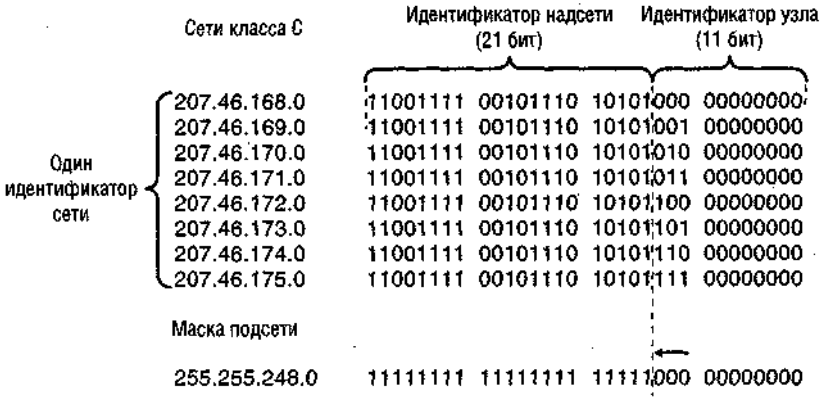


Рис. 2-15. Надсеть на основе блока адресов класса C

Использование бесклассовой междоменной маршрутизации

CIDR — это эффективный метод поддержки надсетей с помощью таблиц маршрутизации. Не будь CIDR, в таблицах маршрутизации следовало бы размещать отдельные записи для каждой сети в надсети, а так вся надсеть представляется одной записью (рис. 2-16).

Примечание Выделенные региональными регистраторами Интернета или интернет-провайдерами блоки адресов надсети часто называют CIDR-блоками, а термин CIDR часто используется для обозначения самих надсетей.

Примечание CIDR не совместим с устаревшим протоколом RIP (Routing Information Protocol) версии 1, который применялся в старых маршрутизаторах, и требует, чтобы маршрутизатор использовал бесклассовый протокол маршрутизации, такой как RIP версии 2 или OSPF (Open Shortest Path First). Подробнее о протоколах маршрутизации — в занятии 4 главы 9.

До применения CIDR

Таблица маршрутизации маршрутизатора B

207.46.168.0	255.255.255.0	207.46.168.1
207.46.169.0	255.255.255.0	207.46.168.1
207.46.170.0	255.255.255.0	207.46.168.1
207.46.171.0	255.255.255.0	207.46.168.1
207.46.172.0	255.255.255.0	207.46.168.1
207.46.173.0	255.255.255.0	207.46.168.1
207.46.174.0	255.255.255.0	207.46.168.1
207.46.175.0	255.255.255.0	207.46.168.1

После применения CIDR

Таблица маршрутизации маршрутизатора B

207.46.168.0	255.255.248.0	207.46.168.1

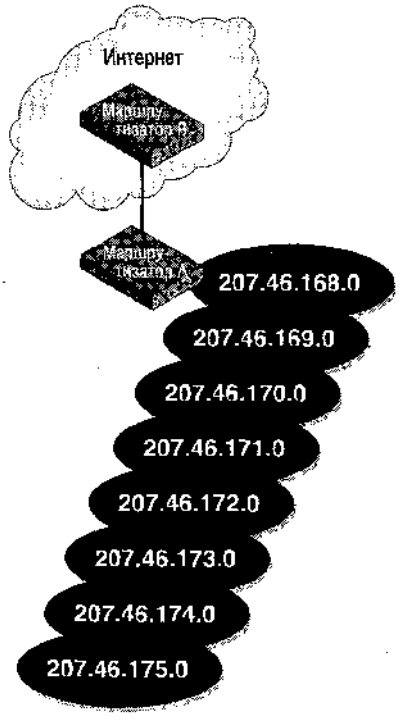


Рис. 2-16. Использование CIDR для упрощения создания надсетей

Будущее адресного пространства

Использование CIDR для выделения адресов дает новую жизнь идентификаторам сети. CIDR-блок из предыдущего примера (131.107.0.0, 255.255.248.0) можно рассматривать двояко:

- как блок 8 адресов сетей класса C;
- как адресное пространство, в котором зафиксирован 21 бит, а 11 битов доступны для изменения.

Во втором случае идентификаторы сети освобождаются от «классовой наследственности» и становятся частью бесклассового пространства IP-адресов. Каждый идентификатор сети независимо от длины представляет адресное пространство, в котом биты идентификатора сети зафиксированы, а биты узла можно менять. Биты узла можно использовать в качестве идентификаторов узлов или в других целях (допустим, для организации подсетей) и таким образом наилучшим образом удовлетворить потребности организации в поддержке сетей.

Маски подсети переменной длины

Традиционно все узлы и маршрутизаторы организации используют одну маску подсети. В этом случае сеть может разбиваться на подсети, в которых максимальное количество идентификаторов узлов одинаковое.

Однако поддержка *масок подсети переменной длины* (variable-length subnet mask, VLSM) позволяет маршрутизаторам обслуживать разные маски. Чаще всего VLSM при-

меняют для разбиения на подсети самих подсетей. Допустим, большой организации принадлежит большое адресное пространство 131.107.0.0/16. Внешние маршрутизаторы для определения идентификатора сети используют первые 16 бит адреса и в соответствии с этим осуществляют маршрутизацию. При получении данных из Интернета маршрутизаторы организации используют маску подсети /22 для перенаправления трафика в любой из 64 региональных отделений организации. А маршрутизаторы региональных офисов в свою очередь используют маску подсети /25 для маршрутизации трафика в 8 отделов в рамках отделения.

Примечание Как и **CIDR,** работа масок подсетей переменной длины основана на бесклассовых протоколах маршрутизации, таких как **RIP** версии **2** и **OSPF. VRLM** несовместим с более старыми протоколами маршрутизации (например с RIP версии 1).

Использование VLSM для поддержки подсетей разного размера

VLSM также позволяет разбивать сеть на подсети разных размеров на одном уровне иерархии и более эффективно использовать адресное пространство.

Например, если одна подсеть должна объединять 100 компьютеров, вторая — 50, а третья — 20, то не удастся обойтись традиционной маской по умолчанию для единственного идентификатора сети класса С. Как видно.из табл. 2-5, никакая из масок подсети по умолчанию не обеспечивает одновременно достаточное число подсетей и узлов в подсети.

Табл. 2-5. Параметры маски подсети класса С (статические)

Сетевой адрес	**Число подсетей**	**Число узлов в подсети**
208.147.66.0/24	1	254
208.147.66.0/25	2	126
208.147.66.0/26	4	62
208.147.66.0/27	8	30

В таких ситуациях проблему решает VLSM. При этом не надо обращаться к интернет-провайдеру за новым диапазоном адресов.

При разбиении на подсети различного размера нужно использовать специальный шаблон с завершающими нулями; сеть класса С поддерживает до семи подсетей. Завершающие нули нужны для предотвращения пересечения адресных пространств подсетей. Если идентификатор подсети с маской переменной длины соответствует шаблону из табл. 2-6, подсети не пересекутся и адреса будут интерпретироваться однозначно.

Табл. 2-6. **Идентификаторы подсети на основе VLSM**

Номер подсети	**Идентификатор подсети (двоичный)**	**Маска подсети**	**Количество узлов**	**Пример адреса подсети**
1	0	255.255.255.128	126	208.147.66.0.0/25
2	10	255.255.255.192	62	208.147.66.0.128/26
3	110	255.255.255.224	**30**	208.147.66.0.192/27
4	1110	255.255.255.240	14	208.147.66.0.224/28
5	11110	255.255.255.248	**6**	208.147.66.0.240/29
6	111110	255.255.255.252	**2**	208.147.66.0.248/30
7	НИИ	255.255.255.252	**2**	208.147.66.0.252/30

На рис. 2-17 показано, как с помощью VLSM построить 3 сети с 100, 50 и 20 узлами соответственно.

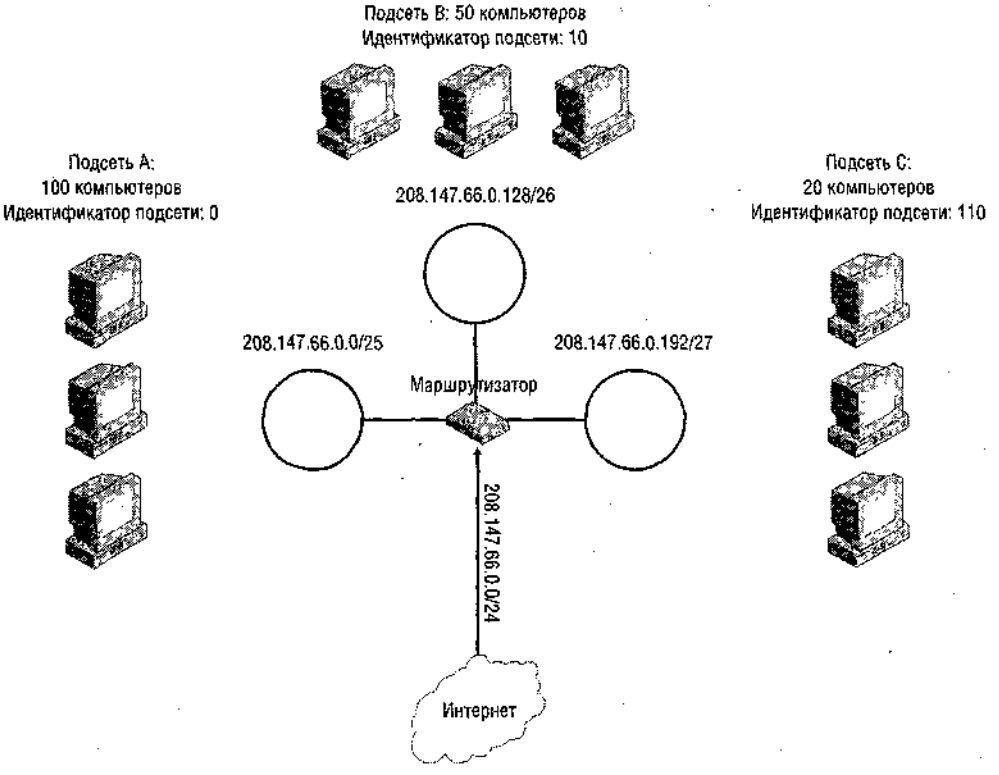


Рис. 2-17. VLSM дает дополнительную гибкость при разбиении на подсети

Увеличение количества доступных узлов средствами VLSM. Обратите внимание, что в табл. 2-6 седьмая (и последняя) подсеть имеет такое же количество узлов, как и шестая, отличаются только идентификаторы подсети, да и то всего одним битом (в идентификаторе 7-й сети в отличие от остальных отсутствует завершающий нуль). Можно не использовать все семь подсетей — достаточно определить состоящий из одних единиц идентификатор подсети на любом уровне, который заменит все перечисленные в следующих строках таблицы подсети. Например, определить идентификатор подсети 1111, который заменит подсети 5—7 (см. табл. 2-6). Благодаря этому вы получите еще одну подсеть с 14 узлами вместо 3 подсетей, вместе содержащих только 10 узлов. Это позволит максимизировать количество узлов, которые вмещает сеть, состоящая из 5 подсетей.

Совет Если сеть класса C разбита на 3, 5, 6 или 7 подсетей, VLSM позволяет максимизировать количество доступных узлов.

Лабораторная работа. Подсети и маски подсети

Вы используете калькулятор и советы занятия 3 для вычисления недостающей информации о подсети.

Упражнение 1. Вычисление масок подсети

Допустим, интернет-провайдер выделил вам адрес сети 206.73.118.0/24. Заполните таблицы, указав количество бит, необходимое для идентификаторов подсети или узла, число бит, оставшееся на идентификатор узла или подсети, маску подсети в виде префикса сети и маску подсети в десятично-точечном виде. При заполнении отталкивайтесь от требований, указанных над таблицей.

Образец: **Требование: 6 подсетей**

Количество бит, необходимое для идентификатора подсети	(Ответ: 3)
Оставшееся на идентификатор узла количество бит	(Ответ: 5)
Маска подсети (в виде префикса сети)	(Ответ: /27)
Маска подсети (в десятично^точечном виде)	(Ответ: 255.255.255.224)

Требование: 9 подсетей

Количество бит, необходимое для идентификатора подсети	
Оставшееся на идентификатор узла количество бит	
Маска подсети (в виде префикса сети)	
Маска подсети (в десятично-точечном виде)	

Требование: 3 подсети

Количество бит, необходимое для идентификатора подсети	
Оставшееся на идентификатор узла количество бит	
Маска подсети (в виде префикса сети)	
Маска подсети (в десятично-точечном виде)	

Требование: 20 узлов на подсеть

Количество бит, необходимое для идентификатора узла	
Оставшееся на идентификатор подсети количество бит	
Маска подсети (в виде префикса сети)	
Маска подсети (в десятично-точечном виде)	

Упражнение 2. Вычисление различных параметров подсети

Определите класс сети и маску подсети по умолчанию для каждого приведенного в таблице идентификатора сети. Затем с помощью калькулятора вычислите действительную маску подсети, назначенную адресу, доступное количество подсетей и количество узлов в каждой подсети.

Идентификатор сети	Класс сети	Маска подсети по умолчанию	Заданная маска подсети (в точечно-десятичном виде)	Доступное количество подсетей	Доступное количество узлов в подсети
207.209.68.0/27					
131.107.0.0/20					
10.0.0.0/13					
208.147.66.0/25					

На заметку Для успешной сдачи экзамена надо уметь выполнять эти вычисления, однако в реальной жизни администраторы редко делают это вручную. Для получения связанной с подсетями информации используют специальные утилиты — *калькуляторы подсетей* и *калькуляторы сетей*. Большинство из них распространяется бесплатно, а некоторые доступны прямо на Web-страницах. Типичный калькулятор подсети принимает определенную информацию об адресации, например адрес сети и количество узлов в подсети, и автоматически вычисляет всю остальную связанную с адресацией информацию, в том числе подходящую маску подсети, количество подсетей, адрес в двоичной форме и широковещательный адрес сети.

Упражнение 3. Вычисление диапазонов адресов подсети

В этом упражнении нужно вычислить диапазоны адресов подсети, определив диапазоны первых трех подсетей сети. Для каждого адреса сети и маски подсети (столбец A), вычтите из 256 значение соответствующего октета маски подсети. Запишите полученное значение в колонку B. Затем впишите в колонку C первые четыре кратные единицы (начните с 0) этого значения. С помощью этих значений заполните колонки D и E, как показано в примере.

(A) Адрес сети и маска подсети	(B) Число групп	(C) Первые четыре кратные единицы B (включая 0)	(D) Начальный адрес диапазонов адресов первых трех подсетей	(E) Конечный адрес диапазонов адресов первых трех подсетей
10.0.0.0 255.240.0.0	256 - 240 = 16	0, 16, 32, 48	10.0.0.0, 10.16.0.0, 10.32.0.0	10.15.255.255, 10.31.255.255, 10.47.255.255
172.16.0.0 255.255.224.0				
172.18.0.0 255.255.248.0		-		
192.168.1.0 255.255.255.192				

Упражнение 4. Проверка двух адресов на принадлежность одной подсети

С помощью логической функции «И» калькулятора можно определить, принадлежат ли два адреса одной и той же логической подсети. Необходимо просто выполнить две операции «И» над соответствующими октетами маски подсети и октетами заданного IP-адреса. Если результаты совпадут, адреса принадлежат одной логической подсети.

Например, при маске подсети 255.255.255.240 и IP-адресах 192.168.0.220 и 192.168.0.192, выражение «240 И 220» дает 208, а «240 И 220» — 176. Результаты записываются в соответствующие колонки. Они отличаются, поэтому адреса принадлежат разным логическим подсетям.

Маска подсети	Адрес №1	Результат первой операции логического «И»	Адрес №2	Результат второй операции логического «И»	Адреса в одной подсети? (да/нет)
255.255.255.192	192.168.1.116		192.168.1.124		
255.255.255.224	192.168.0.180		192.168.0.192		
255.255.252.0	172.16.100.23 4		172.16.98.234		
255.255.240.0	172.16.64.10		172.16.72.200		

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Вы администрируете сеть филадельфийского офиса крупной компании. Находящийся в штаб-квартире в Нью-Йорке ИТ-отдел выделил на всю сеть филиала диапазон адресов 172.16.0.0/21. Сеть филиала разбита на 4 подсети, в каждой из которых 40 узлов, адреса подсетей уже назначены: 172.16.0.0/24, 172.16.1.0/24, 172.16.2.0/24 и 172.16.3.0/24. Все маршрутизаторы поддерживают CIDR и VLSM.

   Сколько еще подсетей можно создать в филиале, если воспользоваться существующей схемой адресации и не менять маску подсети?
2. Вы администрируете сеть крупной компании. Сети назначен адрес 131.107.0.0/16. Какую маску подсети надо назначить, если надо предусмотреть 25 подсетей до 2000 узлов в каждой. Ответ нужно выразить в нотации CIDR (с префиксом сети) и десятично-точечной.
3. Интернет-провайдер выделил для сети из 400 узлов два адреса класса С: 131.107.10:0 и 131.107.11.0. Какие из перечисленных ниже адресов сети и масок подсети (с префиксом сети) можно назначить адресному пространству, чтобы ваши маршрутизаторы и узлы «видели» эти две сети как одну?
   a. 131.107.10.0/23.
   b. 131.107.11.0/24.
   c. 131.107.10.0/22.
   d. 131.107.11.0/22.

4. Вы администратор сети с адресом 131.107.0.0/24. Вы еще не разбили сеть на подсети, но хотите объединить 8 узлов отдела дизайна и выделить их в отдельную подсеть. Как средствами VLSM выполнить это требование и при этом максимизировать общее доступное количество узлов в сети? Ответы впишите в таблицу. Используйте столько строк, сколько необходимо для перечисления всех подсетей.

Номер подсети	Идентификатор подсети (двоичный)	Маска подсети (десятичная)	Количество узлов в подсети	Адрес сети (с префиксом сети)
1				
2				
3				
4				
5				
6				
7				

Резюме

- Сеть можно разбивать на подсети, увеличив длину строки битов со значением 1 в. маске подсети по умолчанию. Это позволит создать новые логические сети в рамках исходной сети, состоящей из одной подсети.
- Разбиение на подсети часто используют для обеспечения соответствия физической и логической топологии сети или для ограничения широковещательного трафика. Другими несомненными преимуществами разбиения являются более высокий уровень защиты (благодаря ограничению неавторизованного трафика маршрутизаторами) и упрощение администрирования {за счет уменьшения сегментов сети).

м Для любого адреса сети максимальное количество узлов, которое она способна содержать, вычисляется по формуле 2^x— 2, где x — количество бит в идентификаторе узла. Максимальное количество подсетей для адресного пространства определяется по формуле 2^y, где у — количество бит маски подсети.

- Создание надсетей отличается от создания подсетей тем, что при этом заимствуются биты идентификатора сети и маскируются как идентификатор узла. Так группируют несколько сетей в одну. Эффективным способом поддержки надсетей в таблицах маршрутизации является CIDR.
- VLSM позволяет маршрутизаторам внутри организации обрабатывать маски подсети различного размера. VLSM чаще всего используются для разбиения самих подсетей на более мелкие подсети. Также VLSM применяется для разделения сети на подсети различного размера на одном уровне иерархии, за счет чего достигается более эффективное использование адресного пространства сети.

Занятие 4. Установка и конфигурирование TCP/IP

По умолчанию установщик Windows Server 2003 настраивает протокол TCP/IP на автоматическую адресацию. Но после установки все параметры TCP/IP можно изменить.

Изучив материал этого занятия, вы сможете:

- Устанавливать TCP/IP на компьютере с Windows Server 2003;
- Сконфигурировать автоматическое назначение адреса в Windows Server 2003;
- Задать альтернативный статический адрес в Windows Server 2003;
- Настроить статический адрес в Windows Server 2003 вручную;
- Использовать команды Ipconfig и Ping для проверки состояния узлов TCP/IP.

Продолжительность занятия — около 30 минут.

Установка TCP/IP

TCP/IP устанавливается при выборе варианта **Обычные параметры (Typical Settings)** в процессе установки Windows Server 2003. Поэтому TCP/IP редко приходится устанавливать отдельно. Однако если TCP/IP удалялся или не выбран при установке Windows Server 2003, придется установить его отдельно.

Примечание Установка TCP/IP выполняется с привилегиями группы *Администраторы* (Administrators). На сетевом компьютере установке могут помешать политики.

1. В окне **Сетевые подключения (Network Connections)** щелкните правой кнопкой подключение, для которого надо установить и разрешить TCP/IP, и выберите **Свойства (Properties).**
2. Если на вкладке **Общие (General)** (для локальных соединений) или **Сеть (Networking)** (для всех остальных) в списке установленных компонентов отсутствует **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)],** сделайте следующее.
   a. Щелкните кнопку **Установить (Install).**
   b. Выберите **Протокол (Protocol)** и щелкните **Добавить (Add).**
   c. В окне **Выбор сетевого протокола (Select Network Protocol)** щелкните **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)],** а затем OK.
3. Убедитесь, что **Протокол Интернета (TCP/IP)** отмечен флажком, и щелкните **Закрыть (Close).**

Способы конфигурирования TCP/IP

Если TCP/IP уже установлен, можно настроить IP-адресацию и прочие функции в окне **Свойства протокола Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties].** Откройте папку **Сетевые подключения (Network Connections),** щелкните правой кнопкой нужное подключение и выберите **Свойства (Properties).** В появившемся окне выберите в списке компонентов **Протокол Интернета (TCP/IP)** и щелкните **Свойства (Properties).**

При настройке IP-адресации в первую очередь надо решить, как будет настраиваться IP-адрес: автоматически (этот режим используется по умолчанию при установке Windows Server 2003) или вручную. На рис. 2-18 и 2-19 показана вкладка **Общие** окна **Свойства протокола Интернета (TCP/IP),** на которой определяется способ определения IP-адреса. Обратите внимание, что, если установлен переключатель **Получить IP-адрес автоматически (Obtain an IP address automatically),** отображается вкладка **Альтернативная конфигурация (Alternate Configuration).**

Примечание Для конфигурирования свойств TCP/IP необходимо войти в систему под учетной записью члена группы *Администраторы*.

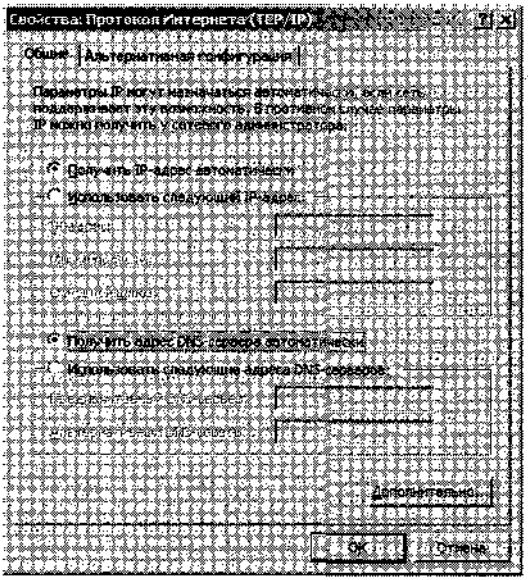


Рис. 2-18. Автоматическая настройка IP-адреса

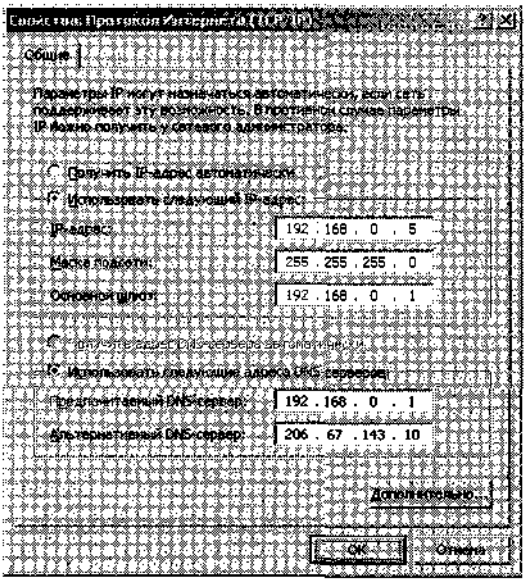


Рис. 2-19. Ручная настройка IP-адреса

Автоматическая настройка

Если оставить свойства TCP/IP без изменений (в том числе выбранную по умолчанию автоматическую настройку), то при наличии DHCP-сервера адрес будет назначать именно он. Если же DHCP-сервер недоступен, можно задать параметры альтернативной (статической) конфигурации на вкладке **Альтернативная конфигурация.** Если не определять статическую альтернативную конфигурацию, адрес определяется средствами APIPA.

Настройка TCP/IP на динамическую адресацию с применением DHCP-сервера выполняется так.

1. В окне **Сетевые подключения** щелкните правой кнопкой нужное подключение и выберите **Свойства.**
2. На вкладке **Общие** (для локальных соединений), или **Сеть** (для всех остальных) выберите **Протокол Интернета (TCP/IP)** и щелкните **Свойства.**
3. Установите переключатель **Получить IP-адрес автоматически (Obtain an IP address automatically)** и щелкните **OK.**

Примечание Предполагается, что узлу, на котором выполняются эти операции, доступен DHCP-сервер.

Вкладка **Альтернативная конфигурация (Alternate Configuration)** содержит IP-адрес узла, используемый при недоступности DHCP-сервера. Как показано на рис. 2-20 и 2-21, можно назначить узлу адрес средствами APIPA или вручную задать альтернативный адрес.

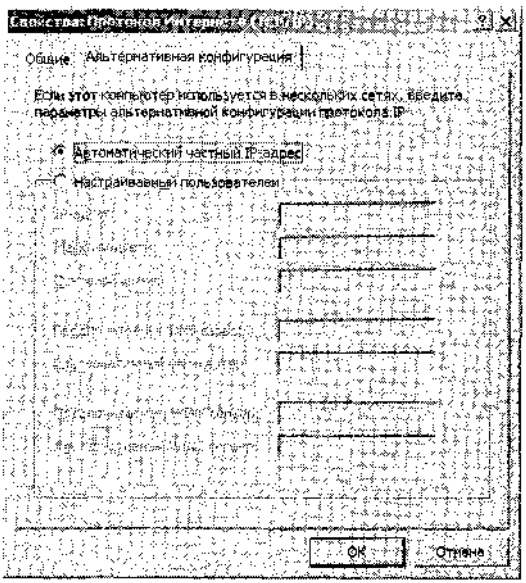


Рис. 2-20. Альтернативный APIPA-адрес

Локальное TCP/IP-подключение настраивается на использование APIPA так.

1. В окне **Сетевые подключения** щелкните правой кнопкой нужное подключение и выберите **Свойства.**
2. На вкладке **Общие** выберите **Протокол Интернета (TCP/IP)** и щелкните **Свойства.** Откроется окно свойств TCP/IP.

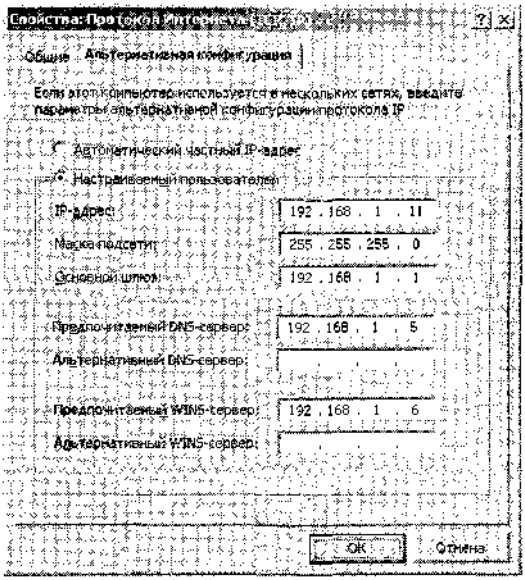


Рис. 2-21. Настройка альтернативного статического адреса

3. На вкладке **Общие** выберите **Получить IP-адрес автоматически.**
4. На вкладке **Альтернативная конфигурация** выберите **Автоматический частный IP-адрес (Automatic Private IP Address)** и щелкните **OK.**

Примечание Предполагается, что DHCP-сервер недоступен. Нельзя настроить узел так, чтобы он игнорировал назначенный DHCP-сервером адрес и использовал APIPA-адрес.

Примечание APIPA не позволяет задать такие параметры по умолчанию, как основной шлюз, DNS- или WINS-серверы. Этот протокол предназначен для сетей, состоящих из одного сегмента и не подключенных к Интернету.

Настройка альтернативной статической конфигурации для локального TCP/1P-подключения выполняется так.

1. В окне **Сетевые подключения** щелкните правой кнопкой нужное подключение и выберите **Свойства.**
2. На вкладке **Общие** выберите **Протокол Интернета (TCP/IP)** и щелкните **Свойства.** Откроется окно свойств TCP/IP.
3. На вкладке **Общие** выберите **Получить IP-адрес автоматически (Obtain an IP address automatically).**
4. На вкладке **Альтернативная конфигурация** выберите **Настраиваемый пользователем (User Configured)** и введите соответствующие значения в следующие текстовые поля:
   - **IP-адрес (IP address);**
   - ***a*** **Маска подсети (Subnet mask);**
   - **a** **Основной шлюз (Default gateway)** (при необходимости);
   - **a** **Предпочитаемый DNS-сервер (Preferred DNS Server)** (при необходимости);
   - **Альтернативный DNS-сервер (Alternate DNS Server)** (при необходимости);

а **Предпочитаемый WINS-сервер (Preferred WINS Server)** (при необходимости);

- **Альтернативный WINS-сервер (Alternate WINS Server)** (при необходимости).

Настройка вручную

При ручном конфигурировании свойств протокола TCP/IP в окне свойств сетевого подключения задают статические IP-адрес, маску подсети, основной шлюз, адреса DNS- и WINS-серверов. Эти же параметры можно задать в мастере установки Windows Server 2003, если в окне **Сетевые подключения (Networking Settings)** вместо **Обычные параметры (Typical Settings)** выбрать **Настраиваемые параметры (Custom Settings).**

Настройка статической адресации для TCP/IP-подключения вручную выполняется так.

1. В окне **Сетевые** подключения щелкните правой кнопкой нужное подключение и выберите **Свойства.**
2. На вкладке Общие (для локальных соединений) или **Сеть** (для всех остальных) выберите **Протокол Интернета (TCP/IP)** и щелкните **Свойства.**
3. **В** открывшемся окне свойств выберите вариант **Использовать следующий IP-адрес (Use the following IP address)** и выполните одно из действий:
   - для локального подключения назначьте IP-адрес, маску подсети и основной шлюз;
   - для всех остальных назначьте IP-адрес.
4. (При необходимости.) В текстовые поля **Предпочитаемый DNS-сервер (Preferred DNS Server)** и **Альтернативный DNS-сервер (Alternate DNS Server)** введите адреса основного и дополнительного DNS-серверов.
5. (При необходимости.) Чтобы настроить WINS-сервер, щелкните **Дополнительно (Advanced),** перейдите на вкладку **WINS** и, щелкнув кнопку **Добавить (Add),** задайте адрес WINS-сервера.

Лабораторная работа. **Настройка TCP/IP-адресов**

Вы сконфигурируете статический IP-адрес на Computerl и альтернативный адрес для Computer2. До этого момента вашим компьютерам были назначены APIPA-адреса.

Примечание Предполагается, что на компьютерах Computerl и Computer2 установлена Windows Server 2003 с параметрами по умолчанию и они физически объединены в сеть. Также предполагается, что в сети нет других компьютеров.

Упражнение 1. Проверка существующего IP-адреса

При выполнении этого упражнения вы проверите существующую конфигурацию IP на Computerl.

1. Войдите в систему Computerl под учетной записью *Администратор.*
2. Из командной строки исполните ipconf ig. Эта команда служит для просмотра конфигурации протокола IP и выводит на экран информацию о сетевых подключениях. Напротив строки **IP-адрес автонастройки (Autoconflguration IP Address)** указывается текущий адрес в форме *169.254.y.z,* где *y* и *z* соответствуют текущему идентификатору узла Computerl, назначенному APIPA. Маска подсети по умолчанию — 255.255.0.0. APIPA назначила компьютеру Computerl адрес потому, что установка Windows Server 2003 с параметрами по умолчанию подразумевает автоматическое назначение IP-адреса. APIPA используется при недоступности DHCP-сервера.

Упражнение 2. Ручная настройка адреса

В этом упражнении надо назначить статический IP-адрес компьютеру Computerl. Статический IP-адрес необходим компьютерам, на которых устанавливаются важные сетевые сервисы, например DNS или DHCP.

1. В окне **Сетевые подключения** щелкните правой кнопкой **Подключение по локальной сети (Local Area Connection)** и выберите **Свойства** (операции выполняются под учетной записью *Администратор)*.
2. **В** списке **Отмеченные компоненты используются этим подключением (This connection uses the following items)** диалогового окна **Подключение по локальной сети — свойства (Local Area Connection Properties)** выберите **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]** и щелкните **Свойства.**
3. На вкладке **Общие** окна свойств TCP/IP установите переключатель **Использовать следующий IP-адрес (Use the following IP address).**
4. **В** поле **IP-адрес (IP Address)** введите 192.168.0.1.
5. Поместите курсор в поле **Маска подсети (Subnet Mask). В** нем появится значение маски подсети — 255.255.255.0. Щелкните **OK.**
6. Закройте окно **Подключение по локальной сети — свойства.**
7. Выйдите из системы Computerl.

Упражнение 3. Настройка альтернативного статического адреса

В этом упражнении вы измените конфигурацию компьютера Computer2 так, чтобы при отсутствии DHCP-сервера ему присваивался заданный адрес.

1. Войдите в систему Computer2 под учетной записью *Администратор.* В окне **Сетевые подключения** щелкните правой кнопкой **Подключение по локальной сети** и выберите **Свойства.**

   В списке **Компоненты, используемые этим подключением (This connection uses the following items)** отображаются компоненты подключения к локальной сети: **Клиент для сетей Microsoft (Client for microsoft networks), Служба доступа к файлам и принтерам сетей Microsoft (File and printer sharing for Microsoft networks)** и **Протокол Интернета (TCP/ IP) [Internet Protocol (TCP/ IP)].**
2. Выберите **Протокол Интернета (TCP/ IP)** и щелкните **Свойства.**

   Убедитесь, что на вкладке **Общие** установлены переключатели **Получить IP-адрес автоматически (Obtain an IP address automatically)** и **Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically).**
3. Перейдите на вкладку **Альтернативная конфигурация.** На ней установлен переключатель **Автоматический частный IP-адрес (Automatic Private IP Address).** Поскольку DHCP-сервер недоступен, на компьютере Computer2 используется APIPA.
4. Установите переключатель **Настраиваемый пользователем (User Configured).**
5. **В** поле **IP-адрес** введите 192.168.0.2.
6. Поместите курсор в поле **Маска подсети. В** нем появится значение маски подсети по умолчанию — 255.255.255.0. Оставьте его без изменений и щелкните **OK.**

   Заданный на Computer2 альтернативный IP-адрес 192.168.0.2 будет использоваться, пока недоступен DHCP-сервер.
7. Закройте окно **Подключение по локальной сети — свойства.**

Упражнение 4. Проверка подключения

В этом упражнении вы проверите действие нового IP-адреса и способность компьютеров взаимодействовать между собой.

1. Откройте окно командной строки на Computer2 (операции выполняются под учетной записью *Администратор)*.
2. Исполните команду ipconfig.

   На экране появится результат команды. В строке **IP-адрес (IP Address)** должен отображаться только что назначенный IP-адрес — 192.168.0.2.
3. Выполните команду ping Computer"!. Она используется для проверки наличия TCP/IP-соединения между двумя узлами.

   Выведенный на экран результат подтвердит, что Computerl и Computer2 взаимодействуют по TCP/IP, а также что адрес компьютера Computerl изменился на 192.168.0.1.
4. Выйдите из системы Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какое из приведенных далее высказываний больше всего подходит для компьютера с IP-адресом 169.254.130.13?
   a. Адрес назначен вручную.
   b. Маска подсети этого адреса—255.255.255.0.
   c. В сети нет DHCP-сервера.
2. Компьютеру назначен альтернативный статический IP-адрес 192.168.0.1, но, запустив утилиту Ipconfig, вы обнаружили, ,что адрес другой. Какая наиболее вероятная причина неполадки?
   a. Адрес назначен DHCP-сервером.
   b. Другой назначенный вручную адрес обладает преимуществом перед альтернативным адресом.
   c. Адрес назначен средствами APIPA.
3. Как определяется IP-адрес локального узла при установке Windows Server 2003 с параметрами по умолчанию?
4. Каковы отличия между параметрами конфигурации адресации TCP/IP для локальных и всех остальных подключений (допустим, по телефонной линии)?

Резюме

- Адреса TCP/IP конфигурируются автоматически или вручную. По умолчанию используется автоматическая адресация, которая предполагает назначение адресов DHCP-сервером.
- В отсутствие DHCP-серверов узел автоматически получает альтернативный адрес, указанный на вкладке **Альтернативная конфигурация (Alternate Configuration)** окна свойств TCP/IP.

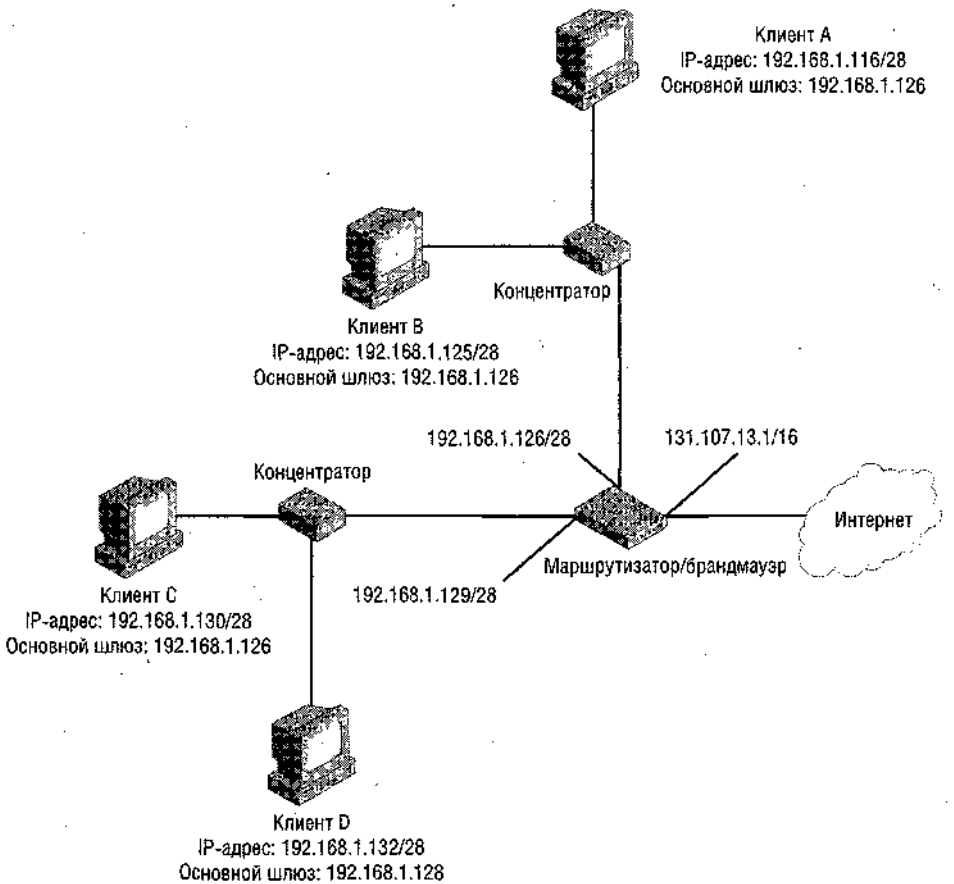
в В отсутствие DHCP-серверов и заданного статического альтернативного IP-адреса узел автоматически получает адрес из диапазона 169.254.0.1—169.254.255.254 с применением APIPA.

- Настроить адрес вручную можно как в процессе установки Windows Server 2003, так и позднее. При настройке IP-адреса вручную задают статический IP-адрес и маску подсети локального узла, а также указывают основные шлюзы, DNS- или WINS-серверы.

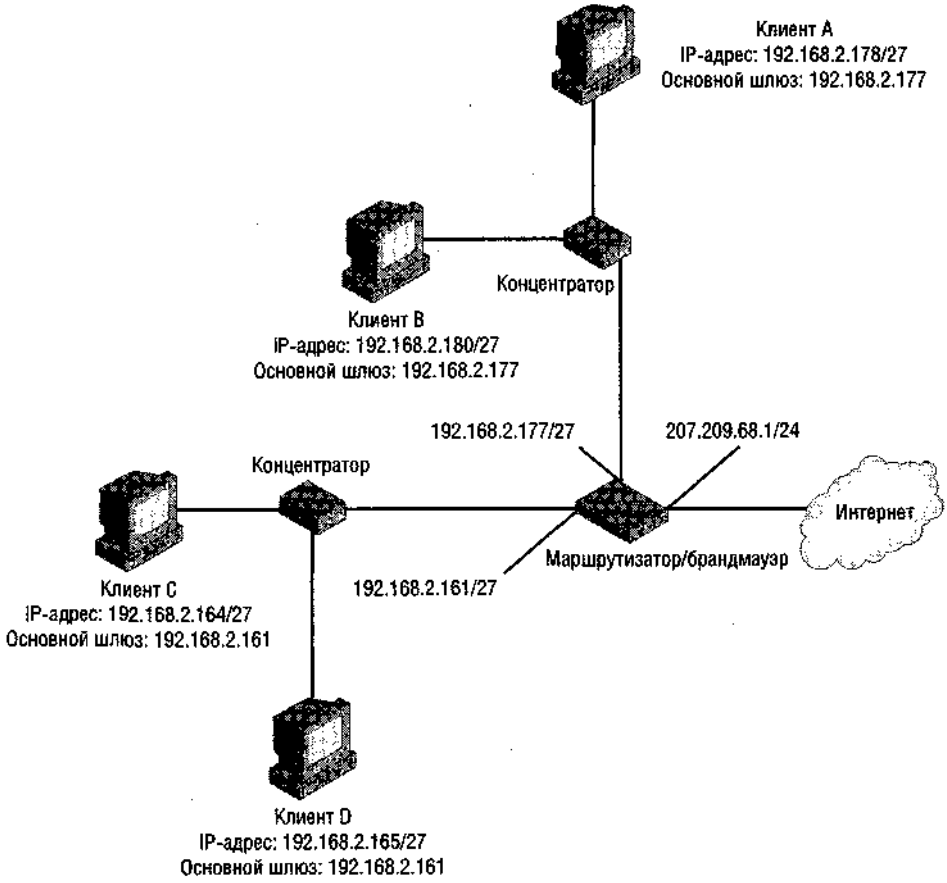
Пример из практики

Вы консультант по компьютерным сетям, предоставляющий свои услуги трем компаниям по устранению неполадок в их сетях. Посетив каждую из компаний, вы нарисовали схемы соответствующих частей сети. Используя схемы, найдите ошибки в конфигурации IP, которые вызывают сбои в сетях компаний.

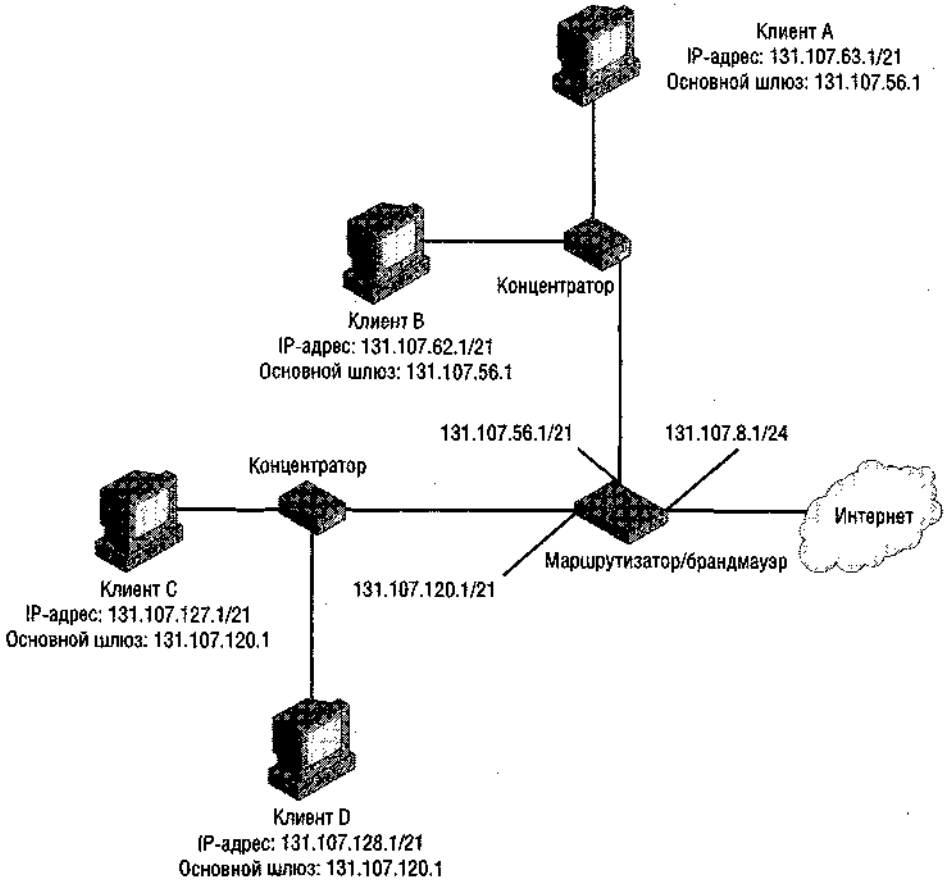
1. Где ошибка в конфигурации?



2. Где ошибка в конфигурации?



3. Где ошибка в конфигурации?



Резюме главы

- TCP/IP лежит в основе сетей Windows и Интернета и включает протоколы межсетевого уровня ARP, IP и ICMP, а также протоколы транспортного уровня TCP и UDP.
- IP-адрес узла должен быть уникальным в пределах IP-сети.
- IP-адрес делится на адрес, или идентификатор, сети и адрес, или идентификатор, узла.
- Маска подсети локального узла — это 32-битный адрес, используемый для сравнения идентификатора сети локального узла и идентификатора сети IP-пакетов, которые узел отправляет в сеть.
- При совпадении идентификатора сети локального узла совпадает с идентификатором сети получателя IP-пакета, пакет передается в локальную сеть. В противном случае пакет передается на основной шлюз.
- Разбить сеть на логические подсети можно, удлинив строку битов со значением 1 в маске подсети по умолчанию.

- При отсутствии доступных DHCP-серверов узлу автоматически назначается альтернативный адрес, указанный на вкладке **Альтернативная конфигурация (Alternate Configuration)** окна свойств TCP/IP.
- В отсутствие DHCP-серверов и статического альтернативного IP-адресе узел автоматически получает адрес из диапазона 169.254.0.1—169.254.255.254 по протоколу APIPA.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

Необходимо:

- уметь определять, какие октеты заданного IP-адреса относятся к идентификаторам сети и узла.
- уметь решать следующие задачи с помощью калькулятора:
  - переводить адрес из десятичной в двоичную форму и наоборот;
  - a переводить маску подсети из формы с префиксом сети в десятично-точечную и наоборот;
  - a с помощью операции логического «И» определять, принадлежат ли два IP-адреса одной подсети;
  - a определять, сколько бит необходимо зарезервировать под идентификатор подсети и идентификатор узла согласно требованиям к сети, а затем получать на основании этой информации маску подсети;
- уметь вычислять диапазоны адресов подсети по десятично-точечной форме маски подсети;
- понимать принцип образования CIDR-блоков с тем, чтобы распознавать и правильно интерпретировать их при ответе на вопросы экзамена;
- уметь обнаруживать такие ошибки конфигурации, как некорректно заданный основной шлюз или несовместимые IP-адреса.

Основные термины

ARP (Address Resolution Protocol) — один из протоколов TCP/IP, для сопоставления IP-адресов MAC-адресам сетевых карт в котором используется широковещательный трафик локальной сети.

ICMP (Internet Control Message Protocol) — обязательный вспомогательный протокол в семействе TCP/IP, служащий для информирования об ошибках и обеспечения упрощенной связи. ICMP применяется в утилите Ping для выявления неполадок TCP/IP.

CIDR (Classless Interdomain Routing) — способ управления IP-адресами и маршрутизацией, который позволяет выделять IP-адреса так, чтобы сократить число маршрутов на отдельных маршрутизаторах и одновременно увеличить количество доступных IP-адресов.

VLSM (Variable-Length Subnet Mask) — использование разных масок подсетей на маршрутизаторах одной сети. Эта методика позволяет гибче определять диапазоны адресов подсетей по сравнению со статическими масками подсети.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Какой из уровней модели TCP/IP не содержит TCPДР-протоколов?
   a. Уровень сетевого интерфейса.
   b. Межсетевой уровень.
   c. Транспортный уровень.
   d. Прикладной уровень.

   Правильный ответ: a.
2. Какой из перечисленных TCPДР-протоколов не работает на межсетевом уровне?
   a. IP.
   b. ARE
   c. TCP.
   d. ICMP.

   Правильный ответ: c.
3. Какой из перечисленных протоколов относится к транспортному уровню?
   a. IGMP.
   b. UDP.
   c. DNS.
   d. Ethernet.

   Правильный ответ: Ь.
4. Какие из перечисленных сервисов подключаются к UDP-портам? (Выберите все подходящие варианты.)
   a. NetBIOS.
   b. DNS. "
   c. Ethernet.
   d. Telnet.

   Правильный ответ: a и b.

Занятие 1. Упражнение 1

Переведите число, указанное над таблицей. Для перевода используйте таблицу, затем воспользуйтесь калькулятором и сравните результаты.

Число в десятичном представлении: 159

128	64	32	16	8	4	2	1

Число в двоичном представлении: **10011111**
Число в десятичном представлении: 65

128	64	32	16	8	4	2	1

Число в двоичном представлении: **01000001**

Число в двоичной нотации: 1001010

128	64	32	16	8	4	2	1

Число в десятичном представлении: 74
Число в двоичном представлении:01110011

128	64	32	16	8	4	2	1

Число в десятичном представлении: **125**

Занятие 1. Упражнение 2

1. 255.255.255.192
   Правильный ответ: /26.
2. 255.255.252.0
   Правильный ответ: /22.
3. **/27**
   Правильный ответ: 255.255.255.224.
4. /21
   Правильный ответ: 255.255.248.0.

Занятие 2. Закрепление материала

1. Что используется для определения идентификатора сети назначения пакета?
   a. IP-заголовок.
   b. Маска подсети.
   c. Класс адреса.
   Правильный ответ: Ь.
2. Выяснилось, что идентификатор сети назначения пакета совпадает с идентификатором сети узла. Что узел должен сделать с этим пакетом?
   a. Отправить широковещательный ARP-запрос, чтобы определить MAC-адрес узла назначения, и передать пакет в локальную сеть.
   b. Отправить пакет серверу, который выполнить его широковещание в локальной сети.
   c. Отправить пакет основному шлюзу с тем, чтобы тот доставил его получателю.
   Правильный ответ: a.
3. Какое из перечисленных далее десятично-точечных значений соответствует двоичному адресу 11001100 00001010 11001000 00000100? Сначала переведите число вручную, а затем проверьте ответ с помощью калькулятора.
   a. 204.18.200.3.
   b. 204.34.202.4.
   c. 204.10.200.44.
   d. 202.10.200.4.
   Правильный ответ: c.

4. Какое из перечисленных далее двоичных значений соответствует десятично-точечному адресу 207.209.68.100? Сначала переведите число вручную, а затем проверьте ответ с помощью калькулятора.
   a. 11001111111010001010001000 01100100.
   b. 11000111111010001010001000 01100100.
   c. 11001111111010001010001000 01101100.
   d. 11001111111010001110011010 1100100.

   Правильный ответ: a.

5. Определите двоично-десятичный эквивалент приведенного далее адреса. Используйте нотацию CIDR для определения маски подсети по умолчанию. Сначала выполните преобразование вручную, а потом проверьте с помощью калькулятора.
   10010010 01101011001001111 10001001

   Правильный ответ: 146.107.39.137/16.

Занятие 2. Упражнение 1

Пример: Требование: 6 подсетей

Количество бит, необходимых для идентификатора подсети	(Ответ: 3)
Оставшееся на идентификатор узла количество бит	(Ответ: 5)
Маска подсети (в виде префикса сети)	(Ответ: /27)
Маска подсети (в точечно-десятичном виде)	(Ответ: 255.255.255.224)

Требование: 9 подсетей

Количество бит, необходимых для идентификатора подсети	4
Оставшееся на идентификатор узла количество бит	4
Маска подсети (в виде префикса сети)	/28
Маска подсети (в точечно-десятичном виде)	**255.255.255.240**

Требование: 3 подсети

Количество бит, необходимых для идентификатора подсети	2
Оставшееся на идентификатор узла количество бит	6
Маска подсети (в виде префикса сети)	**/26**
Маска подсети (в точечно-десятичном виде)	**255.255.255.192**

Требование: 20 узлов на подсеть

Количество бит, необходимых для идентификатора узла	5
Оставшееся на идентификатор подсети количество бит	3
Маска подсети (в виде префикса сети)	**27**
Маска подсети (в точечно-десятичном виде)	**255.255.255.224**

Занятие 2. Упражнение 2

Идентификатор сети	Класс сети	Маска подсети по умолчанию	Заданная маска подсети (в точечно-десятичном виде)	Доступное количество подсетей	Доступное количество узлов в подсети
207.209.68.0/27	**C**	**/24 или 255.255.255.0**	**255.255.255.224**	**8**	**30**
131.107.0.0/20	**B**	**/16 или 255.255.0.0**	**255.255.240.0**	**16**	**4094**
10.0.0.0/13	**A**	**/8 или 255.0.0.0**	**255.248.0.0**	**32**	**524,286**
208.147.66.0/25	**C**	**/24 или 255.255.255.0**	**255.255.255.128**	**2**	**126**

Занятие 2. Упражнение 3

(A) Адрес сети и маска подсети	(B) Число групп	(C) Первые четыре кратные единицы B (включая 0)	**0»** Начальный адрес диапазонов адресов первых трех подсетей	(E) Конечный адрес диапазонов адресов первых трех подсетей
10.0.0.0 255.240.0.0	256 - 240 = 16	0, 16, 32, 48	10.0.0.0, 10.16.0.0, 10.32.0.0	10.15.255.255, 10.31.255.255, 10.47.255.255
172.16.0.0 255.255.224.0	256 - 224 = 32	0, 32, 64, 96	172.16.0.0, 172.16.32.0, 172.16.64.0	172.16.31.255, 172.16.63.255, 172.16.95.255
172.18.0.0 255.255.248.0	256 - 248 = 8	0, 8, 16, 24	172.18.0.0, 172.18.8.0, 172.18.16.0	172.18.7.255, 172.18.15.255, 172.18.23.255
192.168.1.0 255.255.255.192	256 - 192 = 64	0, 64, 128, 192	192.168.1.0, 192.168.1.64, 192.168.1.128	192.168.1.63, 192.168.1.127, 192.168.1.191

Занятие 2. Упражнение 4

Маска подсети	Адрес №1	Результат первой операции логического «И»	Адрес №2	Результат второй операции логического «И»	Адреса в одной подсети? (да/нет)
255.255.255.192	192.168.1.116	**64**	192.168.1.124	**64**	**Да**
255.255.255.224	192.168.0.180	**160**	192.168.0.192	**192**	**Нет**
255.255.252.0	172.16.100.23 4	**100**	172.16.98.234	**96**	**Нет**
255.255.240.0	172.16.64.10	**64**	172.16.72.200	**64**	**Да**

Занятие 3. Закрепление материала

1. Вы администрируете сеть филадельфийского офиса крупной компании. Находящийся в штаб-квартире в Нью-Йорке ИТ-отдел выделил на всю сеть филиала диапазон адресов 172.16.0.0/21. Сеть филиала разбита на 4 подсети, в каждой из которых 40 узлов, адреса подсетей уже назначены: 172.16.0.0/24, 172.16.1.0/24, 172.16.2.0/24 и 172.16.3.0/24. Все маршрутизаторы поддерживают CIDR и VLSM.

   Сколько еще подсетей можно создать в филиале, если воспользоваться существующей схемой адресации и не менять маску подсети?

   Правильный ответ: 4.

2. Вы администрируете сеть крупной компании. Сети назначен адрес 131.107.0.0/16. Какую маску подсети надо назначить, если надо предусмотреть 25 подсетей до 2000 узлов в каждой. Ответ нужно выразить в нотации CIDR (с префиксом сети) и десятично-точечной.

   Правильный ответ: 21 или /255.255.248.0.

3. Интернет-провайдер выделил для сети из 400 узлов два адреса класса С: 131.107.10.0 и 131.107.11.0. Какие из перечисленных ниже адресов сети и масок подсети (с префиксом сети) можно назначить адресному пространству, чтобы ваши маршрутизаторы и узлы «видели» эти две сети как одну?

   a. 131.107.10.0/23.

   b. 131.107.11.0/24.

   c. 131.107.10.0/22.

   d. 131.107.11.0/22.

   Правильный ответ: a.

4. Выадминистратор сети с адресом 131.107.0.0/24. Вы еще не разбили сеть на подсети, но хотите объединить 8 узлов отдела дизайна и выделить их в отдельную подсеть. Как средствами VLSM выполнить это требование и при этом максимизировать общее доступное количество узлов в сети? Ответы впишите в таблицу. Используйте столько строк, сколько необходимо для перечисления всех подсетей.

Номер подсети	Идентификатор	Маска подсети (десятичная)	Количество узлов в подсети	Адрес сети (с префиксом сети)
1	0	255.255.255.128	126	131.107.0.0/25
2	10	255.255.255.192	62	131.107.0.128/26
3	110	255.255.255.224	30	131.107.0.192/27
4	1110	255.255.255.240	14	131.107.0.224/28
5	1111	255.255.255.240	14	131.107.0.240/28

Занятие 4. Закрепление материала

1. Какое из приведенных далее высказываний больше всего подходит для компьютера с IP-адресом 169.254.130.13?

   a. Адрес назначен вручную.

   b. Маска подсети этого адреса — 255.255.255.0.

   c. В сети нет DHCP-сервера.

   Правильный ответ: c.

2. Вы-назначили компьютеру альтернативный статический IP-адрес 192.168.0.1, но, запустив утилиту Ipconfig, обнаружили, что адрес другой. Какая из причин наиболее вероятна?
   a. Адрес назначен DHCP-сервером.
   b. Другой назначенный вручную адрес обладает преимуществом перед альтернативным адресом.
   c. Адрес назначен средствами APIPA.

   Правильный ответ: a.
3. Как определяется IP-адрес локального узла при установке Windows Server 2003 с параметрами по умолчанию?

   Правильный ответ: после установки Windows Server 2003 с параметрами по умолчанию IP-адрес локального узла назначается DHCP-сервером (если он доступен). В противном случае узел получает альтернативный адрес, который определен на вкладке Альтернативная конфигурация окна свойств TCP/IP. Если DHCP-сервер недоступен и не задан статический альтернативный адрес, узел получает адрес с помощью APIPA из диапазона 169.254.0.1-169.254.255.254.
4. Каковы отличия между параметрами конфигурации адресации TCP/IP для локальных и всех остальных подключений (допустим, по телефонной линии)?

   Правильный ответ: для нелокальных соединений нельзя настроить альтернативный статический IP-адрес и APIPA-адрес.

Пример из практики

1. Где ошибка в конфигурации?

   Правильный ответ: на клиенте C некорректно настроен основной шлюз. Адрес основного шлюза должен быть 192.168.1.129.
2. Где ошибка в конфигурации?

   Правильный ответ: в сети назначена некорректная маска подсети. Правильное значение: 255.255.255.240 или /28.
3. Где ошибка в конфигурации?

   Правильный ответ: в IP-адресе компьютера Клиент D неправильно указана логическая подсеть. Значение третьего октета должно быть в диапазоне 120—127.

Примечание *Кадр* (frame) — это инкапсулированный пакет данных сетевого уровня (или уровня 2). Говоря, что *Сетевой монитор* перехватывает кадры, мы подразумеваем, что он считывает и отображает информацию об инкапсуляции, которая включает как данные сетевого (типа данных Ethernet), так более высоких уровней — таких протоколов, как ARP (Address Resolution Protocol), IP (Internet Protocol), TCP (Transmission Control Protocol) и DNS (Domain Name System). С технической точки зрения кадр отличается от *пакета* (packet) уровнем инкапсуляции: подразумевается, что последний относится к межсетевому уровню (или уровню 3). Тем не менее, под этими терминами часто подразумевают одно и то же.

Есть две версии *Сетевого монитора*. В составе Windows Server 2003 поставляется базовая версия, а полная входит в Microsoft Systems Management Server (см. табл. 3-1).

На заметку В принципе, существует огромное различие между версиями *Сетевого монитора:* базовая версия собирает лишь информацию о трафике на локальном компьютере, а полная в состоянии перехватывать трафик любых компьютеров сетевого сегмента. К сожалению, это верно только в сетях, где нет коммутаторов, а только концентраторы. Но в действительности в большинстве современных сетей используются коммутаторы, которые пересылают кадры прямо на компьютер-адресат. Они сильно ограничивают возможности анализаторов протоколов (в том числе *Сетевого монитора),* скрывая весь трафик, который не создается или не предназначен компьютеру, на котором работает анализатор. Поэтому, если связь узлов в сети обеспечивают коммутаторы, вы не сможете воспользоваться преимуществами полной версии.

Табл. 3-1. Версии *Сетевого монитора*

Функция	Базовая версия	Полная версия
Перехват локального трафика	Только входящий и исходящий трафик локального компьютера	Трафик всех устройств сетевого сегмента
Перехват удаленного трафика	Нет	Да
Определение пользователя, занимающего наибольшую долю пропускной способности сети	Нет	Да
Определение протокола, занимающего наибольшую долю пропускной способности сети	Нет	Да
Обнаружение маршрутизаторов	Нет	Да
Разрешение имен устройств в MAC-адреса	Нет	Да
Редактирование и ретрансляция сетевого трафика	Нет	Да

Компоненты *Сетевого монитора*

Сетевой монитор состоит из инструмента администрирования *Сетевой монитор* (Network Monitor) *и агента. Драйвер сетевого монитора* (Network Monitor Driver). Оба необходимы для перехвата, отображения и анализа сетевых кадров.

Сетевой монитор из состава Windows Server 2003 копирует в буфер кадры, исходящие или входящие на локальный компьютер, этот процесс называется *записью данных* (data capture).

Объем информации, собираемой *Сетевым монитором,* ограничен лишь объемом памяти, однако обычно нужно собирать только небольшую часть всего потока кадров. Подмножество собираемых кадров задается фильтрами, работа которых напоминает запрос базы данных, — они выделяют из общего потока лишь нужную информацию. Фильтровать кадры можно на основе адресов источника и целевого узла, уровня протоколов: сетевого интерфейса, межсетевого и транспортного, а также на основе свойств протокола и при отклонении структуры кадров от заданного шаблона.

Интерфейс *Сетевого монитора*

При первом запуске *Сетевого монитора* открывается окно **Выбор сети (Select a network)** (рис. 3-1), где предлагается выбрать сетевой адаптер, трафик которого будет анализироваться. Он становится адаптером по умолчанию, информация о котором автоматически отображается при следующих запусках *Сетевого монитора*. Чтобы вернуться в это окно и выбрать другую сеть, в меню **Запись (Capture)** выберите **Сети (Networks).**

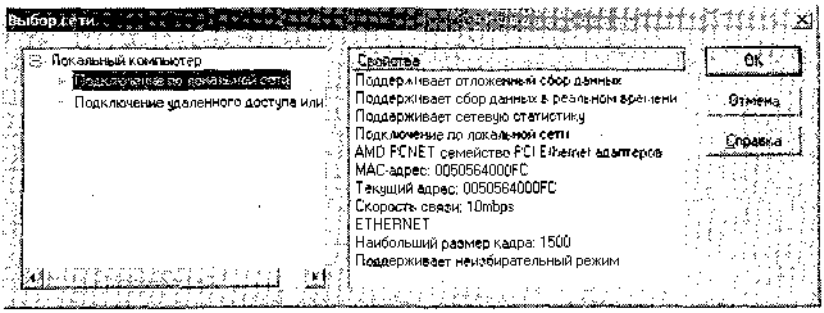


Рис. 3-1. Окно *Выбор* сети

После выбора сети открывается окно записи данных — основное окно *Сетевого монитора,* предоставляющее самые разнообразные статистические данные для анализа поведения сети. Здесь находятся панели **Диаграмма (Graph), Статистика сеанса (Session statistics), Статистика станции (Station statistics)** и **Общая статистика (Total statistics)** (рис. 3-2, табл. 3-2).

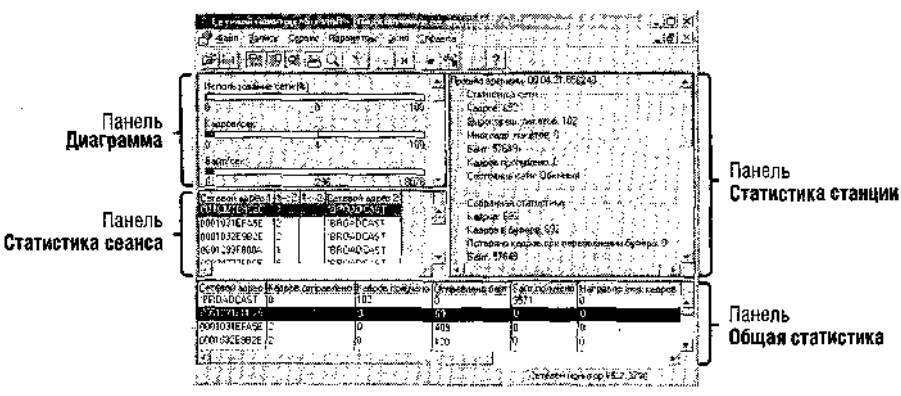


Рис. 3-2. Окно записи данных

Табл. 3-2. Окно записи данных

Панель	Описание
Диаграмма (Graph)	**В** процессе записи в графическом виде отображается информация следующих счетчиков: **Использование сети (%) [% of Network Utilization], Кадров/сек (Frames Per Second), Байт/сек (Bytes Per Second), Широковещ. пакетов/сек (Broadcasts Per Second)** и **Многоадр. пакетов/сек (Multicasts Per Second)**
Статистика сеанса (Session statistics)	Сводка обмена двумя узлами и информация об узлах, инициирующих широковещание и многоадресные рассылки
Статистика станции (Station statistics)	Сводка общего числа кадров, отправленных узлом, число отправленных и полученных кадров и байт, а также число отправленных широковещательных кадров и кадров многоадресных рассылок
Общая статистика (Total statistics)	Общая статистика сетевого трафика и записанных кадров, в среднем за секунду и сетевого адаптера

Запись данных средствами *Сетевого монитора*

Запись данных запускается выбором команды **Запустить (Start)** из меню **Запись (Capture).** Есть и другие варианты: нажать F10 или щелкнуть кнопку **Начать запись данных (Start Capture)** на панели инструментов (рис. 3-3).

В процессе записи новые данные отображаются в панелях окна **Запись.** Запись останавливается выбором команды **Остановить (Stop)** в меню **Запись.** Другие варианты: нажать F11 или щелкнуть кнопку **Закончить запись данных (Stop Capture)** на панели инструментов (рис. 3-3).

Чтобы просмотреть записанные данные, в меню **Запись** выберите **Отобразить записанные данные (Display Captured Data),** нажмите F12 или на панели инструментов щелкните кнопку **Отобразить записанные данные (Display Captured Data)** с изображением очков (рис. 3-3).

Остановить запись и просмотреть данные можно и одной операцией — в меню **Запись** выбрать команду **Остановить и просмотреть (Stop and View),** нажать Shift+F11 или на панели инструментов щелкнуть кнопку **Закончить запись и просмотреть данные (Stop and View Capture)** с изображением очков и символа остановки (рис. 3-3).

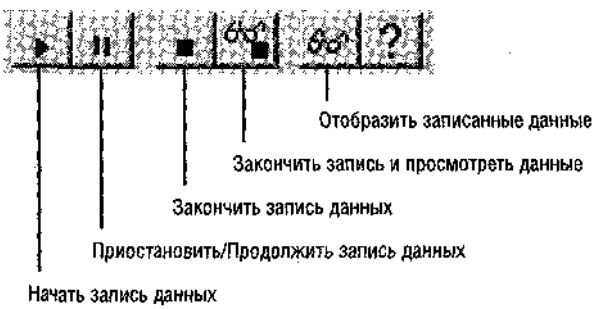


Рис. 3-3. Панель инструментов *Сетевого монитора*

Подготовка к экзамену Консоль **Сетевой монитор (Network Monitor)** позволяет узнать такие параметры, как MAC-адрес сетевой платы, глобально уникальный идентификатор (GUID) компьютера пользователя или используемый протоколом порт.

Анализ записанных данных

При включении просмотра собранных данных открывается окно просмотра кадров со сводной информацией о кадрах в порядке их поступления (рис. 3-4).

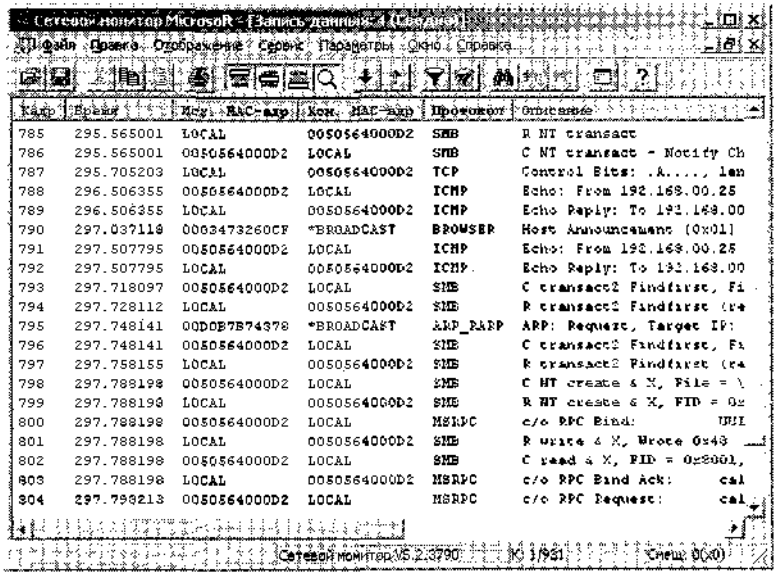


Рис. 3-4. Панель со сводкой данных

Двойной щелчок переключает режим отображения между исходным представлением со сводкой и представлением с тремя панелями: **Сводка (Summary), Сведения (Details)** и **Шестнадцатеричный (Hexadecimal)** (рис. 3-5).

Панель Сводка

Она содержит перечень всех кадров, отображаемых в текущем представлении. При выборе кадра информация о нем отображается в панелях подробностей и шестнадцатеричного представления.

В сводной панели щелчком можно сортировать, перемещать и изменять размеры следующих девяти столбцов.

- **Кадр (Frame).** Все кадры одного сеанса нумеруются в порядке их записи. В этом столбце отображаются номера кадров, начиная с 1. Следует помнить, что порядок получения кадров совсем не обязательно совпадает с порядком их отправки источником.
- **Время (Time).** Содержит сведения о времени записи кадра с момента начала записи. Здесь может отображаться точное время записи кадра или время, прошедшее с момента записи предыдущего кадра.
- **Исх. MAC-адр (Src MAC Addr).** Содержит аппаратный адрес компьютера, отправившего кадр или маршрутизатора, с которого поступил кадр.
- **Кон. MAC-адр (Dst MAC Addr).** Содержит аппаратный адрес компьютера-адресата.

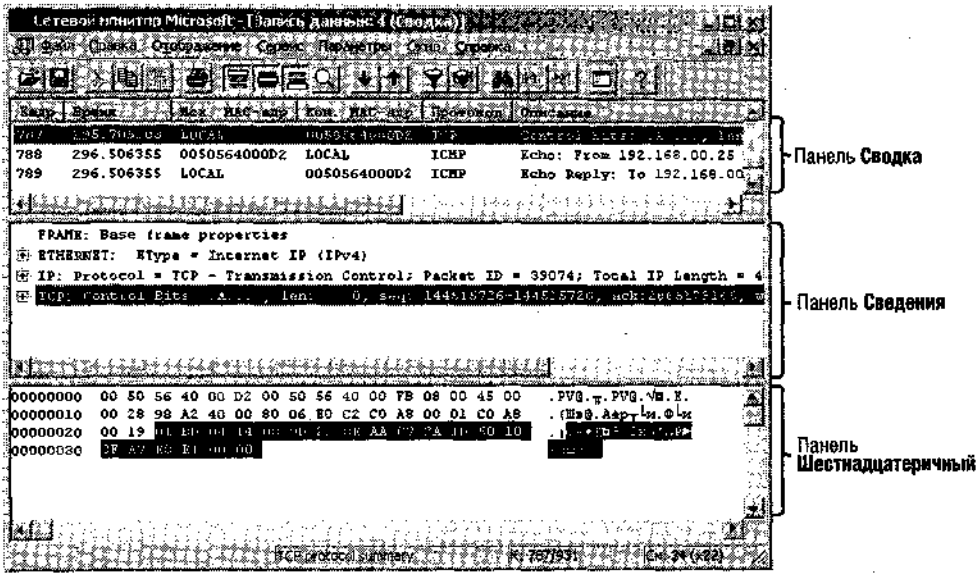


Рис. 3-5. Три панели окна отображения кадров

- **Протокол (Protocol).** Содержит протокол самого высокого уровня, который удалось распознать *Сетевому монитору* в кадре.
- **Описание (Description).** Содержит описательную информацию о кадре, например первый и последний протокол, использованный при создании кадра.
- **Исх. иной адр (Src Other Addr).** Дополнительный идентификационный адрес создателя кадра, отличный от MAC-адреса. Это может быть IP- или IPX-адрес.
- **Кон. иной адр (Dst Other Addr).** Содержит ту же информацию, что и **Исх. иной адр,** но не источника, а адресата.
- **Ввод иного адр (Type Other Addr).** Определяет, адрес какого типа отображается в предыдущих двух столбцах (например, возможно отображение IP- или IPX-адреса).

Панель Сведения

Эта панель содержит информацию о протоколе кадра, выбранного в панели **Сводка (Summary).** Когда кадр содержит инкапсуляцию протоколов нескольких уровней, здесь отображаются сведения о самой внешней оболочке. При выборе протокола в панели **Сводка** в панели **Шестнадцатеричный** отображаются соответствующие шестнадцатеричные строки.

Панель Шестнадцатеричный

Здесь в шестнадцатеричном формате отображается содержимое выбранного кадра. Представленные в этой панели сведения полезны разработчикам, нуждающимся в максимально точной информации об используемых в создаваемом приложении сетевых протоколах.

Анализ кадров

В окне записи кадров в обратном порядке указаны содержащиеся в кадре протоколы: вверху— протокол самого низкого уровня (например протокол сетевого интерфейса Ethernet), а внизу — протокол самого высокого уровня (например прикладной протокол DNS). Именно так *Сетевой монитор* получает данные из сети.

Вот информация о кадре службы *Обозреватель компьютеров* (Computer Browser) в окне записи:

```
+ Frame: Base frame properties
+ ETHERNET: EType = Internet IP (IPv4)
+ IP: Protocol = UDP - User Datagram; Packet ID = 1576;
    Total IP Length = 236; Options = No Options
+ UDP: Src Port: NETBIOS Datagram Servi ce (138);
    Dst Port: NETBIOS Datagram Service (138); Length = 216 (0xD8)
+ NBT: DS: Type = 17 (DIRECT GROUP)
+ SMB: C transact, File = \MAILSLOT\BR0 WSE
+ Browser: Workgroup Announcement [0x0c ] WORKGROUP
```

Каждый протокол представлен в сводной (свернутой) форме, а чтобы получить полную информацию, надо развернуть соответствующий узел. Первый уровень (Frame) добавлен *Сетевым монитором* в качестве описания кадра, которое содержит сведения об общей длине кадра и времени изменения с момента записи предыдущего кадра. Следующий уровень, Ethernet, является самым «внешним» протоколом кадра и соответствует уровню сетевого интерфейса в модели TCP/IP. За межсетевым уровнем следует протокол IP. В рассматриваемом наборе протоколов в качестве транспортного используется протокол UDP.

Сетевой монитор и модель OSI. Последние три протокола являются протоколами сети Microsoft, которые не входят в стандартный набор протоколов TCP/IP. Поскольку эти протоколы не были с самого начала предусмотрены стандартом TCP/IP, на них ссылаются по их положению в рамках более общей модели OSI (Open Systems Interconnection). На рис. 3-6 приводится сравнение сетевых моделей OSI и TCP/IP.

Рис. 3-6. Сетевые модели OSI и TCP/IP

Описание протокола по его положению в модели OSI демонстрирует и следующий протокол в кадре — NetBT, относящийся к сеансовому уровню. NetBIOS поверх TCP/IP, или NetBT (NBT в *Сетевом мониторе),* предназначен для связи протоколов тран-

спортного уровня TCP/IP — TCP и UDP — с высокоуровневым сетевым ПО, таким как *Клиент сетей Microsoft* (Client for Microsoft Networks).

Подготовка к экзамену Надо твердо помнить, что NetBT — это интерфейс сеансового уровня.

Следующий протокол в кадре — SMB (Server Message Block) — традиционно базируется на NetBIOS и обеспечивает общий доступ к файлам и папкам в сетях Microsoft. [Хотя этот протокол после расширения был официально переименован в CIFS (Common Internet File System), *Сетевой монитор* его по-прежнему распознает как SMB.] Последний протокол в кадре обозначен как Browser и представляет службу *Обозреватель компьютеров* (Computer Browser), которая выполняется поверх SMB и позволяет пользователям просматривать сетевые элементы в Windows.

Добавление парсеров *Сетевого монитора*

Процесс чтения, анализа и описания содержимого кадров называется *разбором* (parsing) и выполняется специальными модулями, или *парсерами* (parser). В *Сетевом мониторе* это DLL-файлы, отвечающие за разбор и чтение сообщений различных протоколов. По умолчанию сетевой монитор содержит более 20 парсеров, обеспечивающих разбор свыше 90 протоколов.

Функциональность *Сетевого монитора* можно расширять за счет подключения новых парсеров. Если в компании используется частный протокол, рекомендуется создать специальную DLL-библиотеку, позволяющую *Сетевому монитору* анализировать такой протокол. Файл нового парсера размещается в папке для парсеров *Сетевого монитора* — *WINDOWS\System32\Netmon\Parsers*. Кроме того, нужно добавить информацию о новом парсере и протоколе в файл *Parser.ini*. Это файл с описанием всех парсеров и протоколов, поддерживаемых сетевым монитором, а размещается он в папке *WINDOWS\$ystem32\Netmon*.

На заметку Добавление записей в файл *Parser.ini* может показаться сложным, пока не узнаешь, что все записи одинаковы. Во-первых, в разделе [parsers] надо добавить следующую запись:

<имя_парсера>.611 = 0: *<имя_протокола>*

Затем найти разделы, соответствующие отдельным протоколам, скопировать один из них в конец файла и заменить название и описание, чтобы они соответствовали протоколу, поддерживаемому новым парсером.

Подготовка к экзамену Надо помнить обе операции определения нового парсера в *Сетевом мониторе*. Кроме того, нужно знать точные названия и местоположение файла *Parser.ini* и папки *Parsers*. Запомните: файл *Parser.ini* находится в папке *\System32\Netmon*, которая является родительской по отношению к папке *Parsers*.

Лабораторная работа. **Использование сетевого монитора**

На этой лабораторной работе вы установите *Сетевой монитор,* выполните запись сетевого трафика и сохраните собранные данные.

Упражнение 1. Установка *Сетевого монитора*

Вы установите компоненты Windows, необходимые для работы *Сетевого монитора*.

1. Войдите в систему Computerl как *Администратор* (Administrator).
2. Вставьте установочный компакт-диск Windows Server 2003 в дисковод.
3. Из *Панели управления* (Control Panel) откройте окно утилиты *Установка и удаление программ* (Add or Remove Programs) и щелкните **Установка компонентов Windows (Add/ Remove Windows Components).**
4. На первой странице *Мастера компонентов Windows* (Windows Components Wizard) выберите **Средства управления и наблюдения (Management and Monitoring Tools)** и щелкните **Состав (Details).**
5. **В** окне **Средства управления и наблюдения (Management and Monitoring Tools)** отметьте флажком **Средства сетевого монитора (Network Monitor Tools)** и щелкните OK.
6. На странице **Компоненты Windows (Windows Components)** *Мастера компонентов Windows* щелкните кнопку **Далее** (Next).
7. Щелкните кнопку **Готово (Finish).**
8. Закройте окно **Установка и удаление программ.**

Упражнение 2. Запись данных средствами сетевого монитора

Вы запишете и просмотрите информацию о трафике с помощью *Сетевого монитора*.

1. Войдите в систему Computerl как *Администратор* (Administrator) и выберите **Пуск (Start)/Администрирование (Administrative Toos) /Сетевой монитор (Network Monitor).** Откроется окно **Сетевой монитор (Network Monitor)** с сообщением о необходимости выбрать сеть. Щелкните OK.
2. Разверните узел **Локальный компьютер (Local Computer)** в левой панели окна **Выбор сети (Select a network),** чтобы открыть список сетевых адаптеров на локальном компьютере. Подключения по телефонной линии объединены в узел **Подключение удаленного доступа или VPN (Dial-up Connection or VPN).**
3. Выберите **Подключение к локальной сети (Local Area Connection)** и щелкните OK. Откроется окно *Сетевого монитора* с окном **Запись (Capture)** для выбранного сетевого адаптера.
4. На панели инструментов окна **Запись** щелкните кнопку **Начать запись данных (Start Capture).**
5. Из командной строки исполните следующую команду:

   ```
   ping computer2
   ```

   Это нужно для проверки сетевых подключений. Вы должны увидеть четыре строки (рис. 3-7), подтверждающие наличие связи между Computerl и Computer2.
6. По завершении работы команды Ping на панели инструментов щелкните кнопку **Закончить запись и просмотреть данные (Stop and View Capture)** или нажмите Shift+Fll. Откроется окно записи данных с заголовком **Запись данных: 1 (Capture: 1). В** скобках отображается слово **Сводка (Summary),** указывающее на то, что панель сводных данных является активной и единственной видимой панелью окна. Здесь перечисляются все записанные кадры.
7. Дважды щелкните любой из кадров, указанных в панели **Сводка.** В окне записи данных откроются две дополнительных панели: **Сведения (Details)** и **Шестнадцатеричный (Hexadecimal),** содержащие подробную информацию о выбранном кадре.

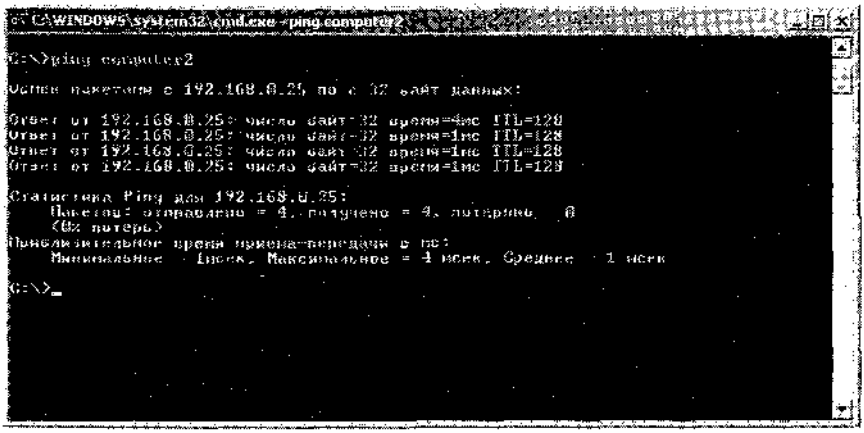


Рис. 3-7. Результат работы команды Ping

8. Снова дважды щелкните кадр в панели **Сводка.** Панели **Сведения** и **Шестнадцатеричный** закроются — так переключаются между двумя представлениями окна **Запись.**
9. Выберите **Файл (File)/СохраНИТЬ как (Save** As), чтобы открыть окно **Сохранить как (Save As).**
10. В поле **Имя файла (File Name)** введите Ping Capture и щелкните **Сохранить (Save).** Файл *Ping Capture'.cap* сохранится в папке *\Рабочий стол\Мои документы\Мои записи (\Desktop\My Documents\My Captures).*
11. Выберите **Файл (File)/ЗаКрЬт> (Close).** Окно записи данных закроется, а в консоли *Сетевой монитор* снова появится окно **Запись.**

Упражнение 3. Сохранение кадров в текстовом файле

Вы скопируете информацию пакета в текстовый файл. Задание выполняется в окне **Сетевой монитор (Network Monitor)** под учетной записью *Администратор* (Administrator).

1. Выберите **Файл (РНе)/Открыть (Open).** Откроется окно **Открыть (Open)** с файлом *Ping Capture.cap* в папке **Мои записи (My Captures).**
2. Выберите файл *Ping Capture.cap* и щелкните **Открыть (Open),** чтобы открыть его в окне записи данных.
3. В панели **Сводка (Summary),** найдите и выберите кадр со словом «ICMP» в столбце **Протокол (Protocol).**
4. Нажмите Ctrl+C, чтобы скопировать кадр.
5. Откройте *Блокнот* (Notepad) и нажмите Ctrl+V, чтобы вставить информацию о кадре в новый текстовый файл.

   В текстовый файл вставляются все данные записанного кадра. Обратите внимание: первая строка содержит все поля и в той же последовательности, что и в панели **Сводка** окна сбора данных. Кроме того, большая часть данных — около 40 строк — соответствуют информации, отображаемой в панели **Сведения (Details).** Но здесь информация представлена в развернутом виде. В конце текста размещены шестнадцатеричные значения из панели **Шестнадцатеричный (Hexadecimal).**
6. **В** *Блокноте* нажмите Ctrl+S, чтобы сохранить файл. Откроется окно **Сохранить как** (Save As). Выберите папку *\Рабочий стол\Мои документы\Мои записи (\Desktop\My Documents\My Captures),* но пока не сохраняйте файл.

7. В поле со списком **Кодировка (Encoding)** выберите **Юникод (Unicode).**
8. **В** поле **Имя файла (File Name)** замените введите ICMP frame и щелкните **Сохранить (Save).**
9. Закройте окно **ICMP Frame.txt - Блокнот (ICMP Frame.txt - Notepad).**
10. Закройте окно **Сетевой монитор,** выбрав **Файл (МеДВыход (Exit).** На предложение сохранить адрес в базе данных вответьте **Нет** (No).
11. Выйдите из системы Computer *Y.*

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Что из перечисленного не обязательно для записи кадров с сетевого адаптера удаленного компьютера?
   a. Установка компонента *Драйвер сетевого монитора* (Network Monitor Driver) на удаленном компьютере.
   b. Установка компонента *Драйвер сетевого монитора* на локальном компьютере.
   c. Установка полной версии *Сетевого монитора* (Network Monitor) на локальном компьютере.
   d. Установка полной версии *Сетевого монитора* на удаленном компьютере.
2. Какой интерфейс сеансового уровня используется для обеспечения доступа *Клиента сетей Microsoft* (Client for Microsoft Networks) к протоколу TCP/IP?
   a. SMB.
   b. NetBIOS.
   c NetBT.
   d. Обозреватель.
3. Вы сетевой администратор крупной компании со штаб-квартирой в Бостоне и пятью отделениями на территории Северной Америки. В корпоративной сети недавно развернули новое сетевое приложение, использующее особый протокол XTXA, специально разработанный программистами компании. В состав приложения входит файл парсера Xtxa.dll, позволяющего *Сетевому монитору* анализировать этот частный протокол. Надо обеспечить запись и анализ трафика этого протокола, чтобы успешно устранять неполадки, которые могут возникнуть при работе нового приложения. Как обеспечить запись и разбор трафик XTXA с помощью *Сетевого монитора!* (Выберите два варианта.)
   a. Скопировать файл Xtxa.dll в папку *\System32\Netmon.*
   b. Скопировать файл Xtxa.dll в папку *\System32\Netmon \Parsers.*
   c. Добавить запись о Xtxa.dll в файл *\System32\Netmon\Parser.ini.*
   d. Добавить запись о Xtxa.dll в файл *\System32\Netmon\Parsers\Parser.ini.*

Резюме

- *Сетевой монитор* (Network Monitor) — это анализатор протокола, поддерживающий запись и анализ сетевого трафика.

- Компонент *Сетевой монитор* входит в состав компонента *Средства управления и наблюдения* (Management and Monitoring Tools). При установке *Сетевого монитора* необходимый для его работы драйвер устанавливается на компьютере автоматически.
- Существуют две версии *Сетевого монитора:* базовая входит в состав Windows Server 2003, а полная — в Systems Management Server. Первая поддерживает запись кадров только на локальном компьютере, а вторая позволяет записывать трафик других компьютеров в локальном сегменте сети.
- По умолчанию сетевой монитор поддерживает анализ более 90 протоколов. Его возможности расширяют, добавляя новые парсеры. Чтобы добавить парсер в *Сетевой монитор* надо: разместить DLL-библиотеку парсера в папке *WINDOWS\System32\Netmon\Parsers,* где хранятся файлы всех парсеров, и добавить запись о новом парсере и анализируемом им протоколе в файле Parser.ini.

Занятие 2. Устранение неполадок подключений TCP/IP

Основной метод устранения проблем сетевой связи заключается в точной локализации неполадки, а затем проверки работы низких уровней сети.

При сбоях сетевого подключения определенного узла начинают с проверки базовой конфигурации IP. Если IP-адрес, маска подсети, адрес шлюза или другие параметры конфигурации IP в порядке, с помощью различных утилит выясняют, на каком уровне наблюдается неполадка: выше, ниже или на межсетевом уровне TCP/IP.

Изучив материал этого занятия, вы сможете:

- использовать утилиту Ipconfig, сетевую диагностику и Netdiag для устранения неполадок сетевой конфигурации;
- применять утилиты Ping, PathPing, Tracert и Arp для устранения неполадок сетевых подключений.

Продолжительность занятия — около 45 минут.

Неполадки конфигурации TCP/IP

Устраняя неполадки сетей TCP/IP, начните с проверки конфигурации TCP/IP на сбойном компьютере.

Ipconfig применяется для получения базовой информации о конфигурации узла: IP-адреса, маски подсети и основного шлюза. При запуске с параметром /all эта утилита предоставляет более подробные сведения о конфигурации всех сетевых интерфейсов (рис. 3-8).

Результат работы Ipconfig внимательно изучается на предмет ошибок конфигурации. Например, у компьютера, который получил дубликат уже существующего в сети IP-адреса, в поле маски подсети содержится 0.0.0.0.

Рис. 3-8. Результат выполнения команды Ipconfig /all

Диагностика сети

Диагностика сети (Network Diagnostics) — графический инструмент устранения неполадок из состава Windows Server 2003, предоставляющий подробную информацию о сетевой конфигурации локального компьютера. Чтобы открыть окно **Диагностика сети** выберите **Пуск (Start)/СпраВКа и поддержка (Help and Support). В** окне **Центр справки и поддержки (Help and Support Center)** в панели **Задачи поддержки (Support Tasks) выберите Служебные программы (Tools),** в панели **Средства (Tools)** разверните узел **Средства центра справки и поддержки (Help and Support Center Tools)** и **выберите Диагностика сети (Network Diagnostics)** (рис. 3-9).

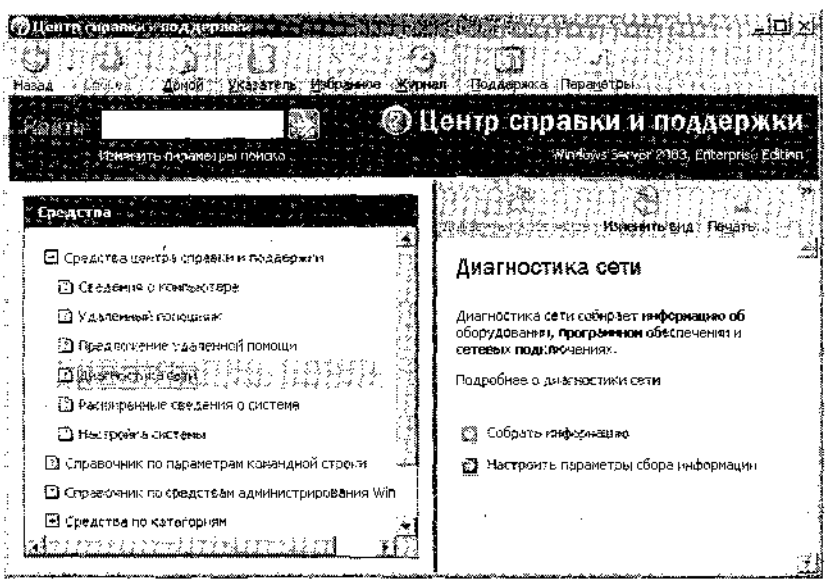


Рис. 3-9. Окно *Диагностика сети*

Если щелкнуть **Собрать информацию (Scan Your System)** утилита выполнит ряд проверок, собирая информацию о среде локального компьютера (рис. 3-10).

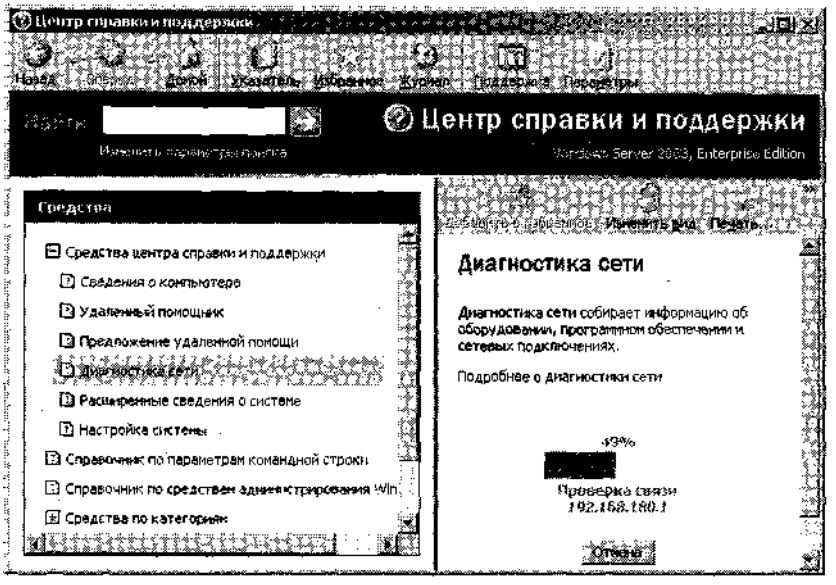


Рис. 3-10. Диагностика сети в **процессе сбора** данных

Собранная информация разбивается на ряд категорий. В каждой категории данные свернуты в узлах дерева, которые раскрываются щелчком соответствующего значка «плюс».

По умолчанию утилита собирает информацию только трех категорий: *Службы Интернета* (Internet Service) — сведения о Microsoft Outlook Express Mail, Microsoft Outlook Express News и Internet Explorer Web Proxy; *Информация о компьютере* (Computer Information) — данные о из реестра о системе, ОС и ее версии; *Модемы и сетевые адаптеры* (Modems and Network Adapters) — информация о параметрах реестра, соответствующих модемам, сетевым адаптерам и сетевым клиентам.

Щелкнув кнопку **Настроить параметры сбора информации (Set Scanning Options),** можно изменять состав категорий собираемых данных и выполняемые проверки (рис. 3-11).

Сохранение информации в файл

В общем случае диагностика и устранение неполадок клиентского компьютера намного эффективнее, если выполняется по сети, а не локально. Но это не всегда возможно, допустим, из-за неполадок сетевого подключения, которые не позволяют применить средства диагностики. Когда серьезная неполадка случается в удаленном месте, например служащий в другом филиале компании испытывает трудности с подключением к сети, приходится прибегать с сложным расспросам и процедурам, чтобы собрать достаточно информации для решения проблемы.

Диагностика сети поддерживает функцию *Сохранить в файл* (Save to file), предоставляющую еще один способ диагностики удаленных клиентов, к которым нельзя подключиться по сети. Можно не заставлять пользователей выполнять в командной строке утилиты Ipconfig, Ping и другие, а просто попросить выполнить диагностику сети, сохранить файл на диске и переслать его по электронной почте с другого компьютере.

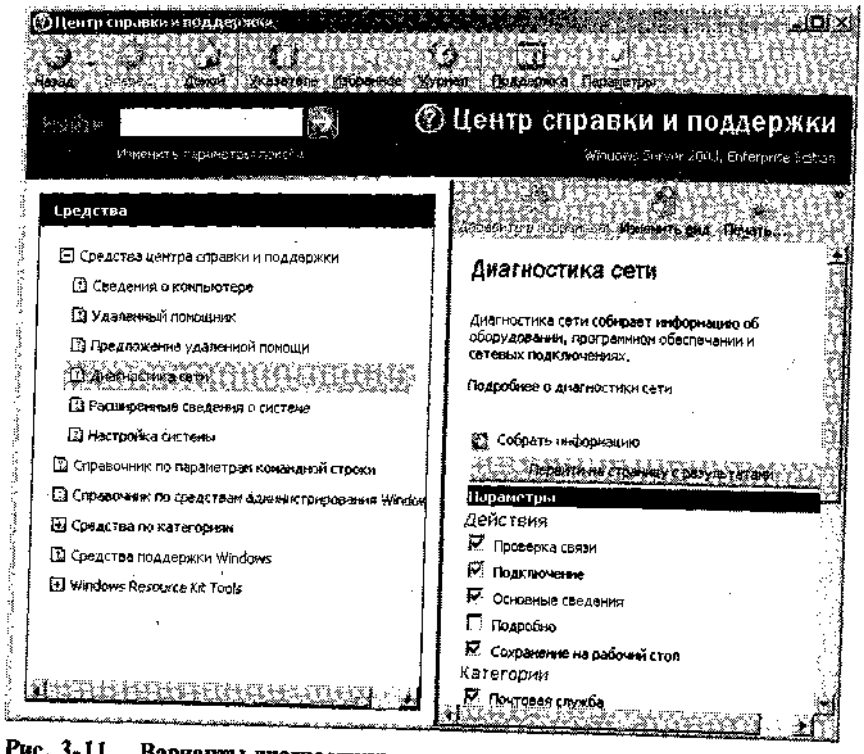


Рис. 3-11. Варианты диагностики сети

Утилита Netdiag

Эта утилита командной строки входит в набор *Средства поддержки Windows* (Windows Support Tools) и устанавливается вручную запуском файла Soptools.msi из папки *\Support\Tools* на установочном диске Windows Server 2003. Запускается Netdiag из папки, указанной в процессе установки.

Как и *Диагностика сети,* Netdiag выполняет проверки локального компьютера и отображает их результаты, в которых и следует искать сообщения об ошибках.

В табл. 3-3 перечислена часть проверок, выполняемых Netdiag по умолчанию.

Табл. 3-3. Проверки, выполняемые Netdiag

Проверка	Описание
Опрос сетевого адаптера	Собирается подробная информация о конфигурации сетевого адаптера, в том числе имя, IP-адрес и основной шлюз. Если адаптер не отвечает, остальные проверки не выполняются
Проверка принадлежности к домену	Собираются сведения об основном домене, в том числе роль компьютера, имя и GUID домена. Выясняется, работает ли служба *Сетевой вход в систему* (Netlogon), основной домен добавляется в список доменов и запрашивается идентификатор безопасности (SID) основного домена
Проверка NetBT-имен	Проверяется, совпадает ли имя сервиса рабочей станции <00> с именем компьютера, есть ли имя службы сообщений <03> и службы сервера <20> на всех интерфейсах, нет ли между ними конфликта. Аналогична команде nbtstat -n

Табл. 3-3. *(окончание)*

Проверка	Описание
Проверка WINS	Запросы на разрешение NetBT-имен направляются на все определенные WINS-серверы
Проверка DNS	Проверяется работоспособность службы кэширования DNS и правильность регистрации локального компьютера на определенных DNS-серверах. Если компьютер является контроллером домена, проверяется, все ли записи DNS в Netlogon.dns зарегистрированы на DNS-сервере. Если записи некорректны и присутствует параметр /fix, выполняется попытка повторной регистрации записи контроллера домена на DNS-сервере
Проверка привязок	Перечисляются все привязки, в том числе имя интерфейса, имя ниже- и вышестоящего модуля, состояние (активизирована/отключена) и владелец
Проверка конфигурации WAN	Перечисляются параметры и состояние текущих активных подключений удаленного доступа
Проверка IP-безопасности (IP Security)	Проверяется, активизирован ли протокол IPSec и отображается список активных политик IPSec

Если эти проверки не позволяют найти источник неполадок, обычно дальше пытаются выяснить места нарушения связи по протоколу TCP/IP.

Устранение неполадок с помощью Ping и PathPing

Ping служит для проверки связи на уровне IP, а PathPing позволяет обнаружить потерю пакетов на маршруте со многими переходами. Команда Ping направляет эхо-запрос узла или IP-адреса по протоколу ICMP. Используйте Ping для проверки возможности узла передавать IP-пакеты другому узлу-адресату. Также эта команда применяется для устранения неполадок оборудования и несовместимости конфигурации.

Устранение неполадок сетевой связи с помощью команды Ping рекомендуется выполнять в такой последовательности.

Примечание Информация, получаемая в пп. 1 и 2, также предоставляется командой Ipconflg /all и Netdiag. *(Диагностика сети* автоматически выполняет только п. 2. Если эта утилита сообщает о неудаче самопроверки, можно выполнить п. 1 вручную.)

1. Проверьте с помощью Ping *адрес замыкания на себя* (loopback address), чтобы убедиться в наличии и корректности настройки TCP/IP на локальном компьютере. Для этого в командной строке выполните команду:

   ping 127.0.0.1.

   Отсутствие реакции говорит о неполадках стека IP: порче драйверов TCP, неработоспособности сетевого адаптера или конфликта IP с другой службой.
2. Проверьте корректность IP-адреса локального компьютера командой:

   ping *<1P-адрес локального узла>*
3. Проверьте доступность IP-адреса основного шлюза:

   ping *<1P-адрес основного шлюза>*

Это позволяет убедиться в доступности основного шлюза и способности локального компьютера связываться с другими узлами сети.

4. Проверьте доступность удаленного узла, расположенного за основным шлюзом:

   ping *<1P-адрес удаленного узла>*

   Это проверка связи с узлами других сетевых сегментов

Примечание Для более быстрого выполнения последней проверки можно воспользоваться командой Tracert утилиты PathPing. Tracert находит сбойные места сети, но не предоставляет статистики об эффективности маршрутизатора.

Ping использует разрешение имен узлов для определения IP-адреса на основании имени компьютера, поэтому если при указании адреса проверка утилитой Ping проходит успешно, а при указании имени — нет, то проблема в механизме разрешения имен, а не сетевых подключениях.

Если проверка с помощью Ping вообще не дает результатов, надо удостовериться:

- правильно ли определен IP-адрес и маска подсети локального компьютера;
- определен ли основной шлюз и есть ли связь между узлом и основным шлюзом. При устранении неполадок обязательно определять не более одного основного шлюза.

Примечание Если на пути к удаленной системе, проверяемой эхо-запросом Ping, находится отрезок, характеризующийся большими задержками, например линия спутниковой связи, на получение эхо-ответов может понадобиться больше времени. Для увеличения тайм-аута служит параметр –w, например команда

```
ping -w 2000 172.16.48.10
```

ожидает ответа 2 секунды (по умолчанию — 1 сек, или 1000 мс).

Устранение неполадок с помощью Tracert

Tracert отслеживает маршрут пакета на расстоянии до 30 переходов между маршрутизаторами. Tracert направляет эхо-запрос по протоколу ICMP на IP-адрес и увеличивает поле TTL в IP-заголовке, начиная с единицы, и анализирует возвращенные ошибки протокола ICMP. Tracert выводит упорядоченный список маршрутизаторов на пути пакета, которые возвратили сообщения об ошибках. В следующем примере Tracert применяется для проверки пути от локального компьютера к удаленному с адресом www.contoso.com.

```
C:\>tracert www.contoso.com
Tracing route to www.contoso.com [10.10 2.252.1]
over a maximum of 30 hops:
 1 300 ms 281 ms 280 ms roto.contoso.co m [10.181.164.100]
 2 300 ms 301 ms 310 ms sl-stk-1-S12- T1.contoso.com [10.228.192.65]
 3 300 ms 311 ms 320 ms sl-stk-5-FO/ O.contoso.com [10.228.40.5]
 4 380 ms 311 ms 340 ms icm-fix-w-H2/0- T3.contoso.com [10.228.10.22]
 5 310 ms 301 ms 320 ms arc-nas- gw.arc.contoso.com [10.203.230.3]
 6 300 ms 321 ms 320 ms n254-ed- cisco7010.contoso.com [10.102.64.254]
 7 360 ms 361 ms 371 ms www.contoso.com [10.102.252.1]
```

Подготовка к экзамену Надо четко понимать разницу между Tracert и PathPing. Tracert применяется для быстрого определения разрыва на пути к удаленному узлу, а PathPing полезнее в ситуациях, когда наблюдается эпизодическая потеря пакетов или длительные задержки. PathPing позволяет точно установить, где потерялся пакет.

Устранение неполадок с помощью утилиты ARP

Иногда сетевой трафик не проходит из-за того, что в ответ на ARP-запрос прокси маршрутизатора возвращает неправильный адрес. Если удается получить ответы на эхо-запросы Ping по адресу замыкания на себя и собственному IP-адресу компьютера, но Ping-запрос другого компьютера локальной подсети терпит неудачу, то далее следует проверить корректность информации в кэше ARP.

Команда ARP позволяет изучить содержимое кэша ARP. Если два узла одной подсети не в состоянии обменяться эхо-запросами, попытайтесь выполнить на обоих компьютерах команду ARP с параметром -a, это позволит выяснить корректность определения MAC-адресов компьютера-адресата. Для определения MAC-адреса можно воспользоваться командой Ipconf ig /a11 или Getmac. Затем надо выполнить команду ARP с параметром -d, чтобы удалить все неправильные записи; новые записи создаются с помощью параметра -s.

Если эхо-запрос Ping компьютера локальной подсети по IP-адресу безуспешен, а команда ARP -a говорит об отсутствии ошибок в MAC-адресах, надо проверить исправность физических устройств — сетевых карт, концентраторов и кабелей.

Лабораторная работа. **Диагностика сети и Netdiag**

Вы воспользуетесь утилитами *Диагностика сети* (Network Diagnostics) и Netdiag и сохраните результаты их работы в файлах.

Упражнение 1. Использование утилиты диагностики сети

Вы сохраните результаты, полученные с помощью утилиты *Диагностика сети,* в HTML-файле.

1. Войдите в систему Computerl *как Администратор* (Administrator).
2. Выберите **Пуск (Start)/СпраВКа и поддержка (Help and Support).** Откроется окно **Центр справки и поддержки (Help and Support Center).**
3. В панели **Задачи поддержки (Support Tasks)** выберите **Служебные программы (Tools).**
4. **В** панели **Средства (Tools)** разверните узел **Средства центра справки и поддержки (Help and Support Center Tools)** и выберите **Диагностика сети (Network Diagnostics).**
5. Щелкните кнопку **Собрать информацию (Scan Your System).** Несколько секунд потребуется на проверки, а затем появятся данные, разбитые на три раздела: **Службы Интернета (Internet Service), Информация о компьютере (Computer Information)** и **Модемы и сетевые адаптеры (Modems and Network Adapters).**
6. Разверните узлы всех категорий, щелчком соответствующих значков «плюс» — появится полная информация о только что выполненных проверках. Познакомьтесь с представленным сведениями.
7. Вернитесь в окно **Диагностика сети** и щелкните кнопку **Настроить параметры сбора информации (Set Scanning Options).** Под заголовком **Параметры (Options)** появятся списки **Действия (Actions)** и **Категории (Categories).**

8. В списке Действия установите флажок **Подробно (Verbose).**
9. **В** списке **Категории** сбросьте следующие флажки: **Почтовая служба (Mail Service), Служба новостей (News Service), Прокси-сервер (Internet Proxy Server), Информация о компьютере (Computer Information), Операционная система (Operating System)** и **Версия Windows (Windows Version).** Должны остаться только **Модемы (Modems), Сетевые Клиенты (Network Clients)** и **Сетевые адаптеры (Adapters).**
10. Щелкните кнопку **Собрать информацию.** По завершении проверок появится только информация категории **Модемы и сетевые адаптеры.**
11. Щелкните кнопку **Сохранить в файл (Save to file),** чтобы сохранить результаты в файл. Откроется информационное окно с сообщением о том, что файл сохранен на рабочем столе и в еще одной папке (она указана). Щелчком **OK** закройте окно.
12. Щелкните ссылку **Показать сохраненные файлы (Show Saved Files)** рядом с кнопкой **Сохранить в файл.** Откроется одна из папок, в которой сохранен новый файл.
13. На панели **Быстрый запуск (Quick Launch)** щелкните **Показать рабочий стол (Show Desktop).** На рабочем столе находится другая копия HTML-файла, созданного утилитой **Диагностика сети.**
14. Переместите этот документ в папку **Мои документы (My documents).**
15. Закройте ненужные окна.

Упражнение 2. Установка средств поддержки Windows

Перед выполнением упражнения вставьте установочный диск Windows Server 2003 в дисковод компьютера Computerl.

1. Войдите в систему Computerl как *Администратор* (Administrator) и на установочном-диске откройте папку *\Support\Tools*.
2. Дважды щелкните файл **Suptools.msi.** Откроется окно мастера *Windows Support Tools Setup Wizard*. Щелкните Next.
3. На странице лицензионного соглашения **End User License Agreement** выберите I **Agree** и щелкните **Next.**
4. На странице **User Information** в полях **Name** и **Organization** укажите свое имя и организацию и щелкните **Next.**
5. На странице **Destination Directory** оставьте заданный по умолчанию путь установки и щелкните **Install Now.**
6. По завершении установки щелкните кнопку **Finish.**

Упражнение 3. Использование Netdiag через сеть

Вы подключитесь к Computerl no Telnet и в командной строке Telnet выполните Netdiag.

1. Войдя в систему Computerl как *Администратор* (Administrator), откройте консоль *Службы* (Services), выбрав **Пуск (81ar1)/Администрирование (Administrative Too1в)/Службы (Services).**
2. **В** правой панели консоли *Службы* выберите в списке **Telnet.** Обратите внимание, что соответствующее поле **Состояние (Status)** пусто.

   Запустите службу Telnet: дважды щелкните значок **Telnet,** в открывшемся окне в поле со списком **Тип запуска (Startup Type)** выберите **Вручную (Manual)** и щелкните **Применить (Apply),** а затем — кнопки **Пуск (Start)** и **OK. В** поле **Состояние** службы Telnet должно появиться **Работает (Started).**
3. Закройте консоль *Службы*.

4. Войдите в систему Computer2 как *Администратор*. Из командной строки исполните команду:

   ```
   telnet computerl
   ```

5. Система предупредит о пересылке пароля на удаленный компьютер. Нажмите Y и Enter.

   Если пароли учетной записи *Администратор* на Computer2 и Computerl одинаковы, появится сообщение об успешном входе и приглашение сервера Telnet. Если на Computerl другой пароль, придется ввести реквизиты, чтобы успешно открыть приглашение Telnet.

6. В командной строке Telnet введите `netdiag` и нажмите Enter. Несколько секунд уйдет на сбор информации, а затем она отобразится в окне командной строки. Это результат выполнения утилиты Netdiag на компьютере Computerl. Ознакомьтесь с результатами.
7. В командной строке Telnet введите `cd мои документы` (в англоязычной версии — `cd my documents`) и нажмите Enter, чтобы перейти в соответствующую папку.
8. В командной строке Telnet введите:

   ```
   netdiag > NetdiagOutput.txt
   ```

   нажмите Enter. Копия результатов Netdiag будет сохранена в папке *Мои документы* (My Documents) на Computerl.

9. В командной строке Telnet выполните команду:

   ```
   netdiag /v > VerboseNetdiagOutput.txt
   ```

   В папке *Мои документы* будут сохранены подробные результаты работы Netdiag.

10. На Computerl откройте файлы *NetdiagOutput.txt* и *VerboseNetdiagOutput.txt* из папки *Мои документы* и сравните их.
11. Перейдите к папке *Netdiag* с сохраненным HTML-файлам результатов Netdiag, полученных с помощью утилиты *Диагностика сети* (Network Diagnostics). Сравните эту информацию с данными, полученными с применением Netdiag.
12. Закройте все открытые окна на Computerl и Computer2 и выйдите из систем этих компьютеров.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Компьютер в локальной подсети не отвечает за эхо-запрос Ping. Перезагрузка компьютера не решает проблему. Что предпринять далее?
   a. Проверить оборудование.
   b. Выполнить команду `I peon fig /all`.
   c. Выполнить диагностику сети в режиме *Подробно* (Verbose).
2. После замены сетевой платы компьютер перестал отвечать на эхо-запросы Ping с другого компьютера локальной подсети. Проверка конфигурации TCP/IP на обоих компьютерах не обнаружила ошибок. Запросы Ping замыкания на себя на обоих компьютерах проходят успешно. Наконец, убедились, что установлена самая последняя версия драйвера сетевого адаптера и *Диспетчер устройств* сообщает о корректной работе устройства. Что предпринять далее?

a. Проверить корректность информации в кэше ARP.
b. Понаблюдать за трафиком ближайшего маршрутизатора с помощью *Сетевого монитора*.
c. Выполнить команду I peon fig /a11.

3. С узла C1 не проходит запрос Ping на узел C2 той же подсети. Проверка IP-параметров обоих компьютеров ошибок конфигурации TCP/IP не обнаружила. Запросы Ping адреса замыкания на себя на обоих компьютерах проходят успешно, но только C2 в состоянии получать эхо-ответы Ping с других компьютеров. Также установлено отсутствие ошибок сопоставления IP- и MAC-адресов компьютеров. Что следует предпринять?
   a. Проверить оборудование на C1.
   b. Выполнить утилиту *Диагностика сети* (Network Diagnostics).
   c. Проверить корректность информации в кэше ARP.
   d. Проверить оборудование на C2.
4. При подключении к удаленному Web-сайту наблюдается задержка. Какой инструмент позволит точно установить, какой маршрутизатор(ы) повинен в этом?
   a. Netdiag.
   b. *Диагностика сети* (Network Diagnostics).
   c. Tracert.
   d. PathPing.

Резюме

- Команда Ipconfig применяется для получения базовой информации о конфигурации узла, в том числе сведений об IP-адресе, маске подсети и основном шлюзе. Параметр /a11 позволяет получить более детальную информацию о сетевых адаптерах.
- *Диагностика сети* (Network Diagnostics) — графический инструмент устранения неполадок, предоставляющий подробную информацию о конфигурации сети локального компьютера. *Диагностика сети* доступна из *Центра справки и поддержки* (Help And Support Center).
- Как и *Диагностика сети,* утилита командной строки Netdiag выполняет ряд проверок локального компьютера и отображает их результаты.
- Ping — инструмент проверки связи на уровне IP, а PathPing позволяет обнаруживать потери пакетов на маршрутах со многими переходами.
- При устранении неполадок подключения, прежде всего проверяют с помощью Ping адрес замыкания на себя, локальный IP-адрес, основной шлюз и лишь после этого — удаленный узел по его IP-адресу, а затем по имени узла. При задержках связи с удаленным узлом используйте PathPing.
- Tracert — утилита проверки маршрута, позволяющая отследить путь пакета на расстоянии до 30 переходов между маршрутизаторами. Ее применяют при полном отсутствии связи с узлом, так как Tracert позволяет обнаружить место, где пропадает связь.
- Если компьютер проходит проверку с помощью эхо-запроса Ping адреса замыкания на себя, собственного IP-адреса и основного шлюза, но не удается получить эхо-ответ от компьютера локальной подсети, прежде всего следует проверить правильность информации, хранящейся в кэше ARP.

- Если не удается получить эхо-ответ от компьютера локальной подсети при проверке с помощью Ping по его IP-адресу, а команда AR P - а не обнаруживает ошибок в сопоставлении аппаратных адресов, надо проверить исправность физических устройств: сетевых карт, концентраторов и соединительных кабелей.

Ц Пример из практики

Вы сетевой администратор в компании со штатом в 300 человек. У компании есть штаб-квартира в столице и два филиала в городах-сателлитах. ИТ-отдел находится в штаб-квартире, сеть которой состоит из трех подсетей, защищенных брандмауэром. Сеть каждого из филиалов состоит из одной подсети, защищенной брандмауэром. Три офиса компании объединены через Интернет. Карта корпоративной сети показана на рис. 3-12.

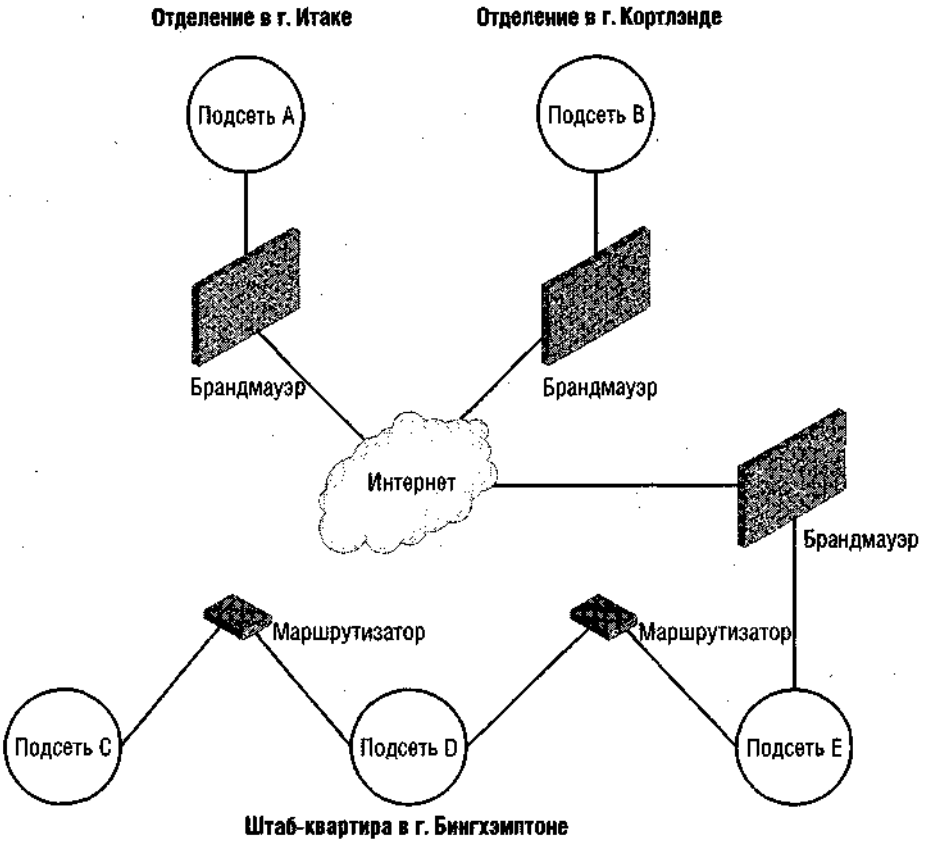


Рис. 3-12. Карта корпоративной сети

В ваши обязанности входит техническая поддержка по запросам служащих всех отделений. Обычно сотрудники описывают возникшую и них проблему, а вы предпринимаете решение, какой диагностический инструмент лучше всего подходит для выяснения причин и устранения неполадки.

Далее описываются запросы о неполадках, поступившие от шести различных сотрудников. Для каждого запроса определите, какие средства больше всего подходят для устранения неполадки— *Сетевой монитор* (Network Monitor), Ping, Tracert, PathPing, Netdiag *или Диагностика сети* (Network Diagnostics). Обоснуйте свой выбор.

1. У пользователя подсети Е нет доступа ни к каким сетевым ресурсам.
2. Пользователь подсети С не может получить доступ к ресурсами подсети Е.
3. Пользователю подсети С удается подключиться к ресурсами корпоративной экстрасети в обоих отделениях, но связь с отделением в г. Кортлэнде очень замедлена. Очень часто не удается дождаться загрузки изображений на Web-страницах экстрасети, которые размещены в этом отделении.
4. Пользователь подсети С сообщает, что иногда не удается получить доступ к сетевому ресурсу по его имени. Пользователь знает свой IP-адрес, и на всех пользовательских компьютерах подсети С работает служба Telnet.
5. Пользователь из Итаки сообщает о сбоях доступа к сети. Он не знает свой IP-адрес, кроме того, на пользовательских компьютерах отделения в Итаке не доступна служба Telnet.
6. Руководство поручило одному из сотрудников развернуть приложение обмена сообщениями между всеми тремя отделениями. Ответственный за приложение сотрудник обращается к вам, сообщая, что программа прекрасно работает в рамках отделения, но нет связи между разными отделениями. К сожалению, ему не известен номер порта TCP, который используется приложением.

Резюме главы

* *Сетевой монитор* (Network Monitor) — анализатор протоколов, служащий для записи и анализа сетевого трафика по более чем 90 протоколам.

• Чтобы расширить функциональность *Сетевого монитора* путем добавления нового парсера, надо скопировать DLL-библиотеку парсера в папку *WINDOWS\$system32\Netmon\Parsers* и внести запись о новом парсере и анализируемом им протоколе в файл *Parser.ini.*

ш Команда Ipconfig применяется для получения базовой информации о конфигурации узла, в том числе сведения об IP-адресе, маске подсети и основном шлюзе. Параметр /all служит для получения более детальной информации о сетевых адаптерах.

• При устранении неполадок подключения, прежде всего проверяют с помощью Ping адрес замыкания на себя, локальный IP-адрес, основной шлюз и лишь после этого — удаленный узел по его IP-адресу, а затем по имени узла. При задержках связи с удаленным узлом используйте PathPing.

• Tracert — утилита проверки маршрута, позволяющая отследить путь пакета на расстоянии до 30 переходов между маршрутизаторами. Ее применяют при полном отсутствии связи с узлом, так как Tracert позволяет обнаружить место, где пропадает связь.

• *Диагностика сети* (Network Diagnostics) — графический инструмент устранения неполадок, предоставляющий подробную информацию о конфигурации сети локального компьютера. *Диагностика сети* доступна из *Центра справки и поддержки* (Help And Support Center).

• Как и *Диагностика сети,* утилита командной строки Netdiag выполняет ряд проверок локального компьютера и отображает их результаты.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- *Сетевой монитор* (Network Monitor) применяется для получения определенной сетевой информации о компьютере, такой как сведения об MAC-адресе узла, GUID пользовательского компьютера, порт протокола.
- Запомните последовательность подключения нового парсера протокола к *Сетевому монитору*.
- Запомните последовательность проверок с помощью утилиты Ping при устранении неполадок подключения: адрес замыкания на себя, IP-адрес локального компьютера, основной шлюз, IP-адрес удаленного узла и, наконец, имя удаленного узла.
- Запомните, чем отличаются утилиты Tracert и PathPing: первая применяется для устранения неполадок связи с удаленными узлами, а вторая — для устранения задержек со связью.

Основные термины

Парсер ~ parser — *динамически загружаемая библиотека* (DLL), служащая для записи и анализа трафика определенного протокола.

PathPing — инструмент командной строки, позволяющий локализовать потерянные пакеты на маршрутах со многими переходами.

***Диагностика сети* (Network Diagnostics)** — графический инструмент устранения неполадок в Windows Server 2003, предоставляющий подробную информацию о сетевой конфигурации локального компьютера.

Netdiag — инструмент командной строки, который предоставляет подробную информацию о сетевой конфигурации локального компьютера. Netdiag входит в состав *Средств поддержки Windows* (Windows Support Tools), устанавливаемый с установочного компакт-диска Windows Server 2003.

Глобально уникальный идентификатор ~ Globally Unique Identifier, GUID— 1 байтовое значение, вычисляемое на основе уникального идентификатора устройства, текущей даты и времени и порядковом номере. GUID используется для идентификации устройств или компонентов.

Вопросы и ответы

Занятие 1. Закрепление материала

1. Что из перечисленного не обязательно для записи кадров с сетевого адаптера удаленного компьютера?
   a. Установка компонента *Драйвер сетевого монитора* (Network Monitor Driver) на удаленном компьютере.
   b. Установка компонента *Драйвер сетевого монитора* на локальном компьютере.

c. Установка полной версии *Сетевого монитора* (Network Monitor) на локальном компьютере.

d. Установка полной версии *Сетевого монитора* на удаленном компьютере.

Правильный ответ: d.

2. Какой интерфейс сеансового уровня используется для обеспечения доступа *Клиента сетей Microsoft* (Client for Microsoft Networks) к протоколу TCP/IP?

   a. SMB.

   b. NetBIOS,

   c NetBT.

   d. Обозреватель.

   Правильный ответ: с.

3. Высетевой администратор крупной компании со штаб-квартирой в Бостоне и пятью отделениями на территории Северной Америки. В корпоративной сети недавно развернули новое сетевое приложение, использующее особый протокол XTXA, специально разработанный программистами компании. В состав приложения входит файл парсераXtxa.dll, позволяющего *Сетевому монитору* анализировать этот частный протокол. Надо обеспечить запись и анализ трафика этого протокола, чтобы успешно устранять неполадки, которые могут возникнуть при работе нового приложения. Как обеспечить запись и разбор трафик XTXA с помощью *Сетевого монитора!* (Выберите два варианта.)

   a. Скопировать файл Xtxa.dll в папку *\System32\Netmon*.

   b. Скопировать файл Xtxa.dll в папку *\System32\Netmon\Parsers*.

   c. Добавить запись о Xtxa.dll в файл *\System32\Netmon\Parser.ini*.

   d. Добавить запись о Xtxa.dll в файл *\System32\Netmon\Parsers\Parser.ini*.

   Правильные ответы: Ь, с.

Занятие 2. Закрепление материала

1. Компьютер в локальной подсети не отвечает за эхо-запрос Ping. Перезагрузка компьютера не решает проблему. Что предпринять далее?

   a. Проверить оборудование.

   b. Выполнить команду Ipconfig /all.

   c. Выполнить диагностику сети в режиме *Подробно* (Verbose).

   Правильный ответ: Ь.

2. После замены сетевой платы компьютер перестал отвечать на эхо-запросы Ping с другого компьютера локальной подсети. Проверка конфигурации TCP/IP на обоих компьютерах не обнаружила ошибок. Запросы Ping замыкания на себя на обоих компьютерах проходят успешно. Наконец, убедились, что установлена самая последняя версия драйвера сетевого адаптера и *Диспетчер устройств* сообщает о корректной работе устройства. Что предпринять далее?

   a. Проверить корректность информации в кэше ARP.

   b. Понаблюдать за трафиком ближайшего маршрутизатора с помощью *Сетевого монитора.*

   c. Выполнить команду Ipconfig /all.

   Правильный ответ: а.

3. С узла C1 не проходит запрос ping на узел C2 той же подсети. Проверка IP-параметров обоих компьютеров ошибок конфигурации TCP/IP не обнаружила. Запросы Ping адреса замыкания на себя на обоих компьютерах проходят успешно, но только C2 в состоянии получать эхо-ответы Ping с других компьютеров. Также установлено отсутствие ошибок сопоставления IP- и MAC-адресов компьютеров. Что следует предпринять?
   a. Проверить оборудование на C1.
   b. Выполнить утилиту *Диагностика сети* (Network Diagnostics).
   c. Проверить корректность информации в кэше ARP.
   d. Проверить оборудование на C2.

   Правильный ответ: a.
4. При подключении к удаленному Web-сайту наблюдается задержка. Какой инструмент позволит точно установить, какой маршрутизатор(ы) повинен в этом?
   a. Netdiag.
   b. *Диагностика сети* (Network Diagnostics).
   c. Tracert.
   d. PathPing.

   Правильный ответ: d.

Пример из практики

1. У пользователя подсети E нет доступа ни к каким сетевым ресурсам.
   Правильный ответ: лучше всего использовать Ping, так как это базовая неполадка, и устранять ее придется на локальном компьютере.
2. Пользователь подсети C не может получить доступ к ресурсами подсети E.
   Правильный ответ: начать надо с Tracert, так как в данной ситуации подсети разделяют два маршрутизатора. Эта утилита позволит выяснить, в какой подсети или на каком маршрутизаторе происходит сбой.
3. Пользователю подсети C удается подключиться к ресурсами корпоративной экстрасети в обоих отделениях, но связь с отделением в г. Кортлэнде очень замедлена. Очень часто не удается дождаться загрузки изображений на Web-страницах экстрасети, которые размещены в этом отделении.

   Правильный ответ: рекомендуется использовать PathPing, так как связь нестабильна и медленна. Этот инструмент позволит определить, где происходят потери пакетов: на брандмауэре отделения в Кортлэнде или на другом маршрутизаторе.
4. Пользователь подсети C сообщает, что иногда не удается получить доступ к сетевому ресурсу по его имени. Пользователь знает свой IP-адрес, и на всех пользовательских компьютерах подсети C работает служба Telnet.

   Правильный ответ: в этом случае надо с помощью Telnet удаленно подключиться к ресурсу по его IP-адресу и выполнить диагностику с помощью Netdiag. Это позволит получить исчерпывающую информацию о IP-конфигурации компьютера, включая определенные на клиентах серверы имен.
5. Пользователь из Итаки сообщает о сбоях доступа к сети. Он не знает свой IP-адрес, кроме того, на пользовательских компьютерах отделения в Итаке не доступна служба Telnet.

Правильный ответ: под руководством администратора пользователь может выполнить диагностику с помощью средства Диагностика сети (Network Diagnostics), сохранить результаты в файл и переправить их по электронной почте. Поскольку неполадки сети наблюдаются эпизодически, скорее всего, потребуется проанализировать очень подробную информацию об IP-конфигурации (именно такие сведения предоставляет эта утилита).

6. Руководство поручило одному из сотрудников развернуть приложение обмена сообщениями между всеми тремя отделениями. Ответственный за приложение сотрудник обращается к вам, сообщая, что программа прекрасно работает в рамках отделения, но нет связи между разными отделениями. К сожалению, ему не известен номер порта TCP, который используется приложением.

Правильный ответ: с помощью Сетевого монитора можно выяснить номер порта, используемого приложением, а затем открыть его на брандмауэрах.

Настройка серверов и клиентов DNS

Темы экзамена

я Устранение неполадок TCP/IP-адресации.

• Установка и конфигурирование DNS-сервера.

м Управление параметрами записей DNS.

В этой главе

Данная глава начинается с описания базовых принципов разрешения имен в сетях Windows Server 2003 и, в частности, DNS. Далее описан процесс настройки DNS-серверов и DNS-клиентов в сети Windows Server 2003. Затем вы познакомитесь с важнейшими инструментами устранения неполадок разрешения имен в сети, в том числе с утилитами Nbtstat и Ipconfig '/flushdns.

Прежде всего

Для изучения материалов данной главы вам потребуется:

в два физически объединенных в сеть компьютера с именами Computer 1 и Computer^ под управлением Windows Server 2003. Компьютеру Computerl надо назначить статический адрес 192.168.0.1/24, а Cqmputer2 — 192.168.0.2/24. Computer2 также настраивается на автоматическое получение IP-адреса;

я телефонная линия и учетная запись интернет-провайдера (можно использовать и выделенную линию, но тогда придется внести коррективы в упражнения);

• на Computerl установить подкомпонент *Средства сетевого монитора* (Network Monitor Tools) компонента *Средства управления и наблюдения* (Management and Monitoring Tools);

я на Computerl установить *Средства поддержки Windows* (Windows Support Tools).

Занятие 1. Основные сведении о разрешении имен в Windows Server 2003

Практически в каждой сети требуется механизм, позволяющий разрешать имен компьютеров в IP-адреса и обратно. Это требование обусловлено тем, что пользователи и приложения обычно обращаются к компьютерам в сети по именам, и лишь службы нижнего уровня обращаются к сетевым узлам по IP-адресам. Исторически сложилось так, что в сетях Windows Server 2003 сосуществуют две системы имен — NetBIOS и DNS. Они не связаны между собой и используют разные механизмы разрешения имен в IP-адреса.

Изучив материал этого занятия, вы сможете;

- *S* рассказать о методах разрешения имен в сетях Windows Server 2003;
- *f* сравнить и описать различия между NetBIOS- и DNS-именами;
- *S* описать процедуры разрешения NetBIOS- и DNS-имен;
- *S* использовать команду Nbtstat для просмотра и очистки кэша NetBIOS-имен;
- *S* отключить поддержку NetBIOS-имен в сети.

Продолжительность занятия — около 30 минут.

Сравнение DNS и NetBIOS

Доменная система имен (Domain Name System, DNS) — это предпочтительная система имен в семействе Windows Server 2003, отличающаяся лучшей масштабируемостью, безопасностью и совместимостью с Интернетом, чем NetBIOS. Хотя до начала работы DNS надо обязательно должным образом настроить, она является неотъемлемым элементом доменов Active Directiory и поэтому используется в большинстве сетей Windows Server 2003. Тем не менее, NetBIOS все еще часто используется в качестве вспомогательного механизма разрешения имен, так как позволяет без дополнительной настройки обеспечить разрешение имен компьютеров одного сегмента сети. Кроме того, NetBIOS используется для совместимости с предыдущими версиями Windows, например при просмотре сети Windows с помощью компонента *Сетевое окружение* (My Network Places) или доступе к совместно используемым ресурсам по UNC-адресам, например, *\\computerl\sharel.*

Примечание По сути NetBIOS представляет собой не систему имен, а API-интерфейс, применяемый в ранних сетях Windows для обеспечения связи и взаимодействия компьютеров. Именование и разрешение имен — лишь два из множества сервисов, предлагаемых NetBIOS.

В сетях Windows Server 2003 разрешение имен по механизму DNS имеет приоритет перед NetBIOS. Приоритет обеспечивается службой DNS-клиента, которая принимает решение, куда направлять запросы на разрешение имен. DNS-клиент сначала пытается разрешить имя в DNS, а если это не удается, обращается к NetBIOS.

Примечание Службу DNS-клиента также называют *распознавателем* (resolver).

В табл. 4-2 сравниваются NetBIOS-имя компьютера и имя узла DNS.

	NetBIOS-имя компьютера	DNS-имя компьютера
Тип	Одноуровневое	Иерархическое
Ограничения по символам	Символы Unicode, цифры, пробелы, а также символы: ! @ # $ % ^ & ') (. - { } ~	A-Z, a-z, 0-9 и дефис (-); у точки (.) особое зарезервированное значение
Максимальная длина	15 символов	63 байта на одну метку; 255 байт на полное доменное имя
Службы разрешения имен	WINS. Широковещание NetBIOS. Файл *Lmhosts*	DNS. Файл *Hosts*

Сравнение процедур разрешения имен

В каждой из двух основных систем разрешения имен в Windows Server 2003 — DNS и NetBIOS — используются свои, особые методы. DNS поддерживает два метода:

- поиск имени в кэше DNS-клиента. Имена попадают в кэш при более ранних запросах или загружаются из файла *Hosts,* расположенного в папке *Windows\System32\Drivers\Etc;*
- запрос DNS-сервера.

В NetBIOS больше способов разрешения имен:

- поиск в кэше NetBIOS-имен;
- запрос WINS-сервера;
- широковещательные NetBIOS-запросы в локальной сети;
- поиск имени в файле *Lmhosts,* из папки *Windows\System32\Drivers\Etc.*

Подготовка к экзамену Запомните следующие команды, связанные с NetBIOS:

- Nbtstat -c (выводит список имен в кэше имен NetBIOS);
- Nbtstat -R (очищает локальный кэш имен NetBIOS).

Когда обязательна DNS

В сетях с доменами Windows 2000 или Windows Server 2003. Когда компьютеры являются членами доменов Windows 2000 или Windows Server 2003, нужно обязательно переконфигурировать DNS. Служба каталогов Active Directory тесно связана с DNS и использует ее в качестве службы локатора. (Служба локатора позволяет клиентам в доменах Windows 2000 и Windows Server 2003 находить в пределах данного домена узлы и службы, местоположение которых неизвестно.)

При доступе в Интернет или в интрасеть. DNS используется для связи с компьютерами в интрасети или Интернете по DNS-именам узлов.

Когда обязательна NetBIOS

В сетях Windows Server 2003 поддерживается протокол NetBT (NetBIOS поверх TCP/IP); это делается для обратной совместимости с более ранними версиями Windows и совместимости с NetBIOS-приложениями. Имена и протокол NetBIOS используются в доменах Microsoft Windows NT, а также в рабочих группах Microsoft Windows 95/98/Me/NT.

Разрешение имен NetBIOS также необходимо сетевым клиентам, использующим приложения или службы, нуждающиеся в разрешении NetBIOS-имен, например службу *Обозреватель компьютеров* (Computer Browser), активизируемую щелчком значка **Microsoft Windows Network** в *Проводнике*.

Наконец, разрешение имен NetBIOS требуется в сетях, где не завершена конфигурация системы DNS, например в рабочей группе, в которой нет DNS-сервера; в такой ситуации разрешение имен компьютеров выполняется с использованием широковещательных рассылок NetBIOS.

Просмотр сети без применения NetBIOS

Кроме NetBIOS, нет способа разрешения имей на основе широковещания, но некоторые безопасные альтернативные методы просмотра сети все же существуют. Во-первых, при добавлении общих ресурсов в глобальный каталог Active Directory пользователи легко обнаруживают эти ресурсы и подключаются к ним средствами *Проводника*. Кроме того, для построения легко просматриваемой структуры всех совместно используемых папок в сети можно использовать *распределенную файловую систему* (Distributed File System, DFS). Подключившись к корневому ресурсу DFS, пользователь получает возможность просматривать предоставленные в общий доступ ресурсы независимо от их размещения на том или ином сервере. Наконец, следует помнить, что хотя без NetBIOS *просмотр* сети невозможен, к сетевым ресурсам можно подключаться в окне Сетевое окружение (My Network Places) по их точным именам.

Отключение NetBIOS

NetBIOS включено по умолчанию для всех локальных подключений Windows Server 2003. Однако в сетях с DNS, где не нужна совместимость с версиями, предшествующими Windows 2000, можно отключить NetBIOS для всех сетевых подключений.

Основное преимущество отключения NetBIOS — значительное укрепление безопасности сети. NetBIOS хранит информацию о сетевых ресурсах и предоставляет ее любому узлу в ответ на широковещательный запрос. Таким образом, злоумышленнику ничего не стоит получить эту информацию и воспользоваться ею для атаки. Еще одно преимущество отмены NetBIOS заключается в упрощении процедур администрирования за счет сокращения числа систем именования, которые нужно конфигурировать и поддерживать.

Наиболее очевидное неудобство, вызванное отключением NetBIOS, заключается в невозможности просмотра сети утилитой Microsoft Windows Network. [Чтобы воспользоваться ею, в *Проводнике* раскройте **Сетевое окружение (My Network Places)** и дважды щелкните значок **Вся сеть (Entire Network)].** Просмотр сети возможен за счет использования списков просмотра, созданных службой *Обозреватель компьютеров* (Computer Browser), основанной на NetBIOS и протоколе NetBT. Другое неудобство, вызванное отключением NetBIOS, состоит в снижении отказоустойчивости. В неправильно сконфигурированной DNS разрешение имен вообще невозможно. Наконец, в некоторых сетях используются сторонние приложения, которым необходима NetBIOS. Перед отключением NetBIOS проверьте возможность этой операции в тестовой сети, чтобы убедиться, что отключение не нарушит работу ни одного из важных приложений.

Разрешение WINS/NetBIOS-имен выполняется так.

1. Откройте окно Сетевые подключения (Network Connections).
2. Щелкните Подключение по локальной сети (Local Area Connection) правой кнопкой и выберите Свойства (Properties). Откроется окно Подключение по локальной сети — свойства (Local Area Connection Properties).
3. В списке компонентов выберите Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)] и щелкните Свойства (Properties). Откроется окно Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties.
4. Щелкните кнопку Дополнительно (Advanced). Откроется окно Дополнительные, параметры TCP/IP (Advanced TCP/IP Settings).
5. На вкладке WINS установите переключатель Отключить NetBIOS через TCP/IP (Disable NetBIOS Over TCP/IP).
6. Два раза щелкните OK, а затем — Закрыть (Close).

На заметку Даже в сетях, где NetBIOS не нужна, отказаться от нее иногда довольно трудно, в том числе от привычки разрешения имен гутем широковещания (хотя бы в качестве подстраховки на случай отказа DNS), а также от просмотра сети в окне Microsoft Windows Network. На самом деле, хотя о NetBIOS часто говорят как об унаследованном протоколе, в большинстве современных сетей Windows он все еще используется — как подспорье или даже необходимый элемент. Тем не менее, настоятельно рекомендуем принести в жертву удобство и привычность NetBIOS и укрепить безопасность сети: доступность сетевой информации, предоставляемой NetBIOS, и делает данный API-интерфейс потенциально небезопасным.

Лабораторная работа. Запись **трафика** разрешения *имей*

На этой лабораторной работе вы зарегистрируете весь трафик, которым обмениваются узлы в процессе разрешения имен.

Упражнение 1. Запись трафика разрешения *штев*

Вы очистите оба кэша имен на Computer1, затем направите эхо-запрос Ping на Computer2, после чего изучите результат записи этого процесса средствами *Сетевого монитора* (Network Monitor).

1. Войдите'в систему Computed *как Администратор* (Administrator).
2. Откройте окно командной строки и очистите кэш DNS-клиента, исполнив команду ipconfig /flushdns.
3. Выполните команду nbtstat. -R, чтобы очистить кэш NetBIOS-имен на локальном компьютере.
4. Откройте окно **Сетевой монитор (Network Monitor)** и в меню **Запись (Capture)** выберите **Сети (Networks).**
5. **В** окне **Выбор сети (Select a Network)** настройте *Сетевой монитор* (Network Monitor) на регистрацию трафика локальной сети.
6. В окне **Сетевой монитор (Network Monitor)** запустите запись трафика.
7. Вернитесь в командную строку и выполните команду ping compute r2.
8. После получения четырех откликов от Computer2 вернитесь в **Сетевой монитор (Network Monitor)** и щелкните кнопку **Закончить запись и отобразить данные (Stop and**

View Capture)., Откроется окно **Запись данных (Capture)** с информацией о только что записанных кадрах.

9. Обратите внимание на протоколы, присутствующие в зафиксированных кадрах. В окне **Сетевой монитор (Network Monitor)** NBT обозначает протокол NetBT, а DNS — протокол DNS. На основе протоколов и описания записанных данных определите, какой из методов разрешения имен использован для разрешения имени Computer2 — DNS или NetBIOS. Почему использован именно этот метод, а не другой?
10. Сохраните результаты записи трафика в папке *Мои документы\Мои записи* (My Documents\My Captures) в файле *Name Resolution 1.*
11. Закройте окно **Сетевой монитор** и окно командной строки.
12. Выйдите из системы компьютера Computerl.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите материал занятия. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы администратор сети из 10 компьютеров с Windows Server 2003 и 200 компьютеров с Microsoft Windows XP Professional. В сети установлен DNS-сервер DNS1, обслуживающий зону *lucernepublishing.com.* Зона также настроена на возможность динамического обновления. DHCP-сервер отвечает за определение IP-конфигурации всех компьютеров под управлением Windows XP Professional. Один из этих компьютеров, *cl.lucernepublishing.com,* доступен только по IP-адресу, но не по имени. Как зарегистрировать этот компьютер в DNS (выберите из списка)?
   a. Выполнить команду Nbtscat -R.
   b. Выполнить команду Ipconfig /registerdns.
   c. Выключить и перезагрузить *cl.lucernepublishing.com.*
   d. Выполнить команду Nbtstat /registerdns.
2. Что из нижеперечисленного является корректным NetBIOS-именем компьютера?
   a. *hostl.microsoft.com.*
   b. hostl local.
   c. *hostlO_microsoft.*
   d. *host 1-microsoft.*
3. Какую команду применяют для очистки локального кэша NetBIOS-имен?

Резюме

- В сетях Windows Server 2003 обычно используются DNS- и NetBIOS-имена. Разные типы имен разрешаются в IP-адреса с применением разных механизмов.
- Имена и протокол NetBIOS необходимы в доменах Windows NT, рабочих группах с версиями Windows, предшествующими Windows 2000, а также для совместимости с некоторыми сетевыми службами, например службой *Обозреватель компьютеров* (Computer Browser).
- Имена и протокол DNS требуются для нормальной работы доменов Active Directory и для поддержки Интернета и интрасетей.
- При разрешении имен DNS-клиент Windows Server 2003 всегда пытается сначала разрешить имя средствами DNS и лишь затем прибегает к помощи NetBIOS.

- Как DNS-, так и NetBIOS-имена создаются на основе имени компьютера [оно отображается в окне **Свойства системы (System Properties)].** Если имя компьютера длиннее 15 символов, для NetBIOS это имя усекается до 15 символов.

Занятие 2. **DNS в сетях Windows Server 2003**

DNS позволяет находить компьютеры и другие ресурсы в IP-сетях по их именам. До появления DNS имена узлов в IP-сетях образовали плоское пространство имен и разрешались с помощью статических файлов *Hosts.* Появление иерархической структуры и автоматического кэширования и разрешения имен узлов в DNS позволило преодолеть многие административные и структурные сложности именования узлов в Интернете.

Изучив материал этого занятия, вы сможете:

- описать структуру пространств имен DNS;
- рассказать, как организовано и управляется пространство имен в Интернете;
- описать компоненты сетей DNS: серверы и клиенты DNS, распознаватели, серверы пересылок, зоны, корни и записи ресурсов;
- рассказать, как клиенты и серверы DNS обрабатывают запросы на разрешение имен;
- описать работу с файлом корневых ссылок.

Продолжительность занятия — около 50 минут.

Основы DNS

DNS позволяет пользователям и программам подключаться к IP-узлам по именам, *например ftp.lucernepublishing.com.* DNS обеспечивает механизмы как для именования узлов, так и для поиска IP-узлов по именам.

Пространство имен DNS

Система именования DNS представляет собой иерархическую и логическую древовидную структуру, которую называют *пространство имен DNS* (DNS namespace), где есть один корень, у которого может быть любое число поддоменов. У отдельных поддоменов в свою очередь могут быть дочерние поддомены. Например, в пространстве имен Интернета корень "" (пустая строка) объединяет множество нижележащих доменных имен верхнего уровня, одно из которых — *хот.* В домене *com* может быть поддомен компании Lucerne Publishing: *lucernepublishing.com,* который в свою очередь является родительским для дочернего домена следующего уровня, например домена производственного отдела: *mfg.lucernepublishing.com.* Организации вправе создавать частные сети и использовать собственные, недоступные из Интернета, пространства DNS-имен.

Доменные имена

Каждый узел в дереве DNS-домена идентифицируется по его полному доменному имени (FQDN) — имени домена DNS, которое однозначно определяет его расположение по отношению к корню дерева доменов. Например, FQDN сервера производственного отдела в домене *lucernepublishing.com* будет *mfgserver.lucemepublishing.com.* Оно представляет собой

объединение имени узла *(mfgserver)* основного суффикса DNS *(lucemepublishing.com)* и замыкающей точки (.). Замыкающая точка является стандартным разделителем доменной метки верхнего уровня и меткой пустой строки, соответствующей корню. (При повседневном использовании замыкающую точку часто опускают, но ее добавляет служба DNS-клиента при выполнении запросов.)

Пространство доменных имен Интернета

Корень (самый верхний уровень) пространства имен Интернета управляется ICANN (Internet Corporation for Assigned Names and Numbers). Эта организация координирует присвоение идентификаторов, которые должны быть уникальными во всем Интернете, в том числе доменных имен, IP-адресов, параметров протоколов и номеров портов.

Ниже корневого уровня располагаются домены верхнего уровня, также находящиеся в ведении ICANN. Существует три типа таких доменов.

- **Домены организаций** — в их имени присутствует трехбуквенный код, указывающий на основной род деятельности организаций данного DNS-домена. Некоторые домены организаций имеют глобальный характер, другие выделяются только организациями внутри США.
- **Географические домены** — в их имени присутствует двухбуквенный код страны или региона, как определено Международной организацией по стандартизации (ISO 3166), например *.ru* — Россия, *.uk*— Великобритания, *.it*— Италия. Эти домены выделяются организациями вне США, хотя это требование соблюдается не слишком жестко.
- **Домены с-обратными доменными адресами** — это специальные домены, имена которых принадлежат *in-addr.arpa.* Они используются для сопоставлений IP-адресов в имена (т. е. обратного просмотра).

В ноябре 2000 года ICANN объявила о создании семи дополнительных доменов верхнего уровня:

- *.aero;*
- *-bit,*
- *.coop;*
- *-info;*
- *.museum;*
- *.name;*
- *.pro.*

Примечание Самая свежая информация о доменах верхнего уровня есть на сайте *http:// www. icann. org/tlds.*

Ниже доменов верхнего уровня ICANN и другие уполномоченные органы, отвечающие за присвоение имен в Интернете, допустим, Network Solutions или Nominet (в Великобритании) передают домены различным организациям, например Microsoft *(microsoft.com)* или Carnegie Mellon University *(cmu.edu).* Эти организации подключаются к Интернету и присваивают имена узлам в пределах своих доменов. DNS -серверы служат для преобразования имен в IP-адреса в зоне действия пространства имен организации. Кроме того, организации предоставляют поддомены своим пользователям или клиентам. Например, интернет-провайдеры получают домен от ICANN и могут передавать поддомены в распоряжение своих клиентов.

Пространство частных доменных имен

Организации вправе организовать *частное пространство имен* (private namespace), т. е. пространство DNS-имен, в основе которого несколько корневых серверов, полностью независимых от пространства доменных имен Интернета. В рамках частного пространства имен можно назначать имена и создавать собственный корневой сервер или серверы и любые необходимые поддомены. Частные имена недоступны и не разрешаются в Интернете. Пример частного доменного имени: *my company.local.*

Компоненты DNS

Для нормальной работы DNS необходимо правильно сконфигурировать DNS-серверы, зоны, распознаватели и записи ресурсов.

DNS-серверы

DNS-сервер — это компьютер с ПО DNS-сервера, например служба DNS-сервера или BIND. DNS-серверы поддерживают базу данных DNS с информацией о части структуры доменного дерева DNS и обрабатывают запросы на разрешение имен, поступающие от DNS-клиентов. В ответ на запрос DNS-сервер предоставляет запрашиваемую информацию, дает ссылку на другой сервер, который может ответить на запрос, либо сообщает, что информация недоступна или не существует.

При размещении зоны на DNS-сервере он является *полномочным* (authoritative) (или удостоверяющим) для этой зоны, если выполняет роль основного или дополнительного DNS-сервера. Отвечая на запросы узлах внутри домена, полномочный сервер этого домена использует исключительно локальные записи ресурсов, а не информацию из кэша. Такие серверы определяют свою часть пространства DNS-имен.

Сервер может быть полномочным для одного или нескольких уровней доменной иерархии. Например, корневые DNS-серверы в Интернете являются полномочными только для доменных имен верхнего уровня (например *хот),* но не для поддоменов (например *lucernepublishlng.com).* Полномочные серверы для *хот,* полномочны только для имен типа *lucernepublishing.com,* но не для доменов третьего уровня, например *example.lucernepublishing.com.* Однако внутри пространства имен фирмы Lucerne Publishing сервер или полномочные серверы для *example.lucernepublishing.com* могут выполнять эту же функцию по отношению к домену *widgets.example.lucernepublishing.com.*

Зоны DNS

Зона DNS (DNS zone) — это единая часть пространства имен, обслуживаемая полномочным сервером. Сервер может обслуживать и несколько зон, а зона может содержать один или несколько доменов. Например, один сервер может быть полномочным для зон *microsoft.com* и *lucemepublishing.com,* каждая из которых содержит более двух доменов.

Смежные домены, например *хот, .lucernepublishing.com* и *example.lucernepublishing.com* можно превратить в отдельные зоны, применив делегирование, при котором ответственность за поддомен внутри пространства имен DNS присваивается отдельному объекту.

Файлы зон (zone files) содержат записи ресурсов зон, в которых сервер является полномочным. Во многих реализациях DNS-сервера данные зон хранятся в текстовых файлах; DNS-серверы на контроллерах доменов под управлением Windows 2000 или Windows Server 2003 могут также хранить зонную информацию в Active Directory.

Распознаватели DNS

Распознаватель DNS (DNS resolver) — это служба, использующая протокол DNS для запросов информации у DNS-серверов. Распознаватели DNS взаимодействуют либо с удаленными DNS-серверами, либо с ПО DNS-сервера на локальном компьютере. В Windows Server 2003 функцию распознавателя DNS выполняет служба DNS-клиента. Она же обеспечивает кэширование информации о соответствии DNS-имен и IP-адресов.

Записи ресурсов

Записи ресурсов (resource records) — это информация, хранимая в базе данных DNS и используемая для ответа на запросы DNS-клиентов. Каждый DNS-сервер содержит записи ресурсов, необходимые ему для ответа на запросы, относящиеся к его части пространства имен DNS. Записи ресурсов различаются по типам: например, адрес узла (A), каноническое имя (CNAME) или почтовый обменник (MX) (см. занятие 3).

Механизм работы DNS-запросов

Когда у клиента DNS возникает необходимость найти указанное приложением имя, он направляет на DNS-сервер запрос на разрешение имени. Каждое такое сообщение-запрос содержит следующую информацию.

- **Доменное имя DNS в виде FQDN.** DNS-клиент добавляет необходимые для образования FQDN суффиксы, если этого уже не сделала клиентская программа.
- **Тип запроса.** Запись ресурса либо тип операции запроса.
- **Определение класса доменного имени DNS.** Для службы DNS-клиент этот класс всегда определяется как класс Интернета (IN).

Например, FQDN-имя компьютера *host-a.example.microsoft.com* и тип запроса определяется как запись ресурса A, соответствующая этому имени. Запрос DNS можно представить, как вопрос клиента к серверу, содержащий два подвопроса: «Есть ли компьютер с именем *hostname.example.microsoft.com* и на нем запись ресурса A?» Получив ответ от сервера, клиент получает сведения о записи ресурса A и узнает IP-адрес соответствующего компьютера.

Методы разрешения в DNS

Существует несколько способов разрешения DNS-запросов. Как правило, клиент обращается к DNS-серверу, который затем разрешает запрос, используя собственную базу данных записей ресурсов. Однако иногда DNS-клиенту достаточно обратиться к своему кэшу, чтобы получить ответ на запрос без обращения к серверу. Другим способом разрешения запросов DNS является *рекурсия* (recursion), при которой DNS-сервер в процессе разрешения имени обращается от имени клиента к другим DNS-серверам. Получив ответ на запрос, DNS-сервер пересылает его клиенту. Наконец, есть еще один метод разрешения запросов DNS — итерация, в процессе которой клиент пытается разрешать имена, обращаясь к дополнительным DNS-серверам. При этом клиент направляет отдельные дополнительные запросы на основе ссылок, предоставленных DNS-серверами.

Этапы жизненного цикла запроса DNS

Вообще говоря, процесс запроса DNS делится на два этапа:

- запрос имени инициируется на клиентском компьютере и передается для разрешения в службу DNS-клиента;
- если запрос не удается разрешить локально, он перенаправляется на DNS-серверы.

Эти процессы описаны более подробное далее.

Этап 1: локальный распознаватель

На рис. 4-1 показан порядок обработки запроса DNS, когда клиент настроен на рекурсивные запросы. В такой ситуации, если информация о запрашиваемом имени отсутствует в кэше DNS-клиента, он направляет запрос на DNS-сервер, который далее становится ответственным за получение ответа на запрос от имени клиента.

На рисунке запросы и ответы обозначены соответственно 3 и О. Запросы более высокого порядка (вторые, третьи...) выполняются, только если предыдущий запрос оказался безрезультатным. Например, 3-2 выполняется только после неудачи 3-1.

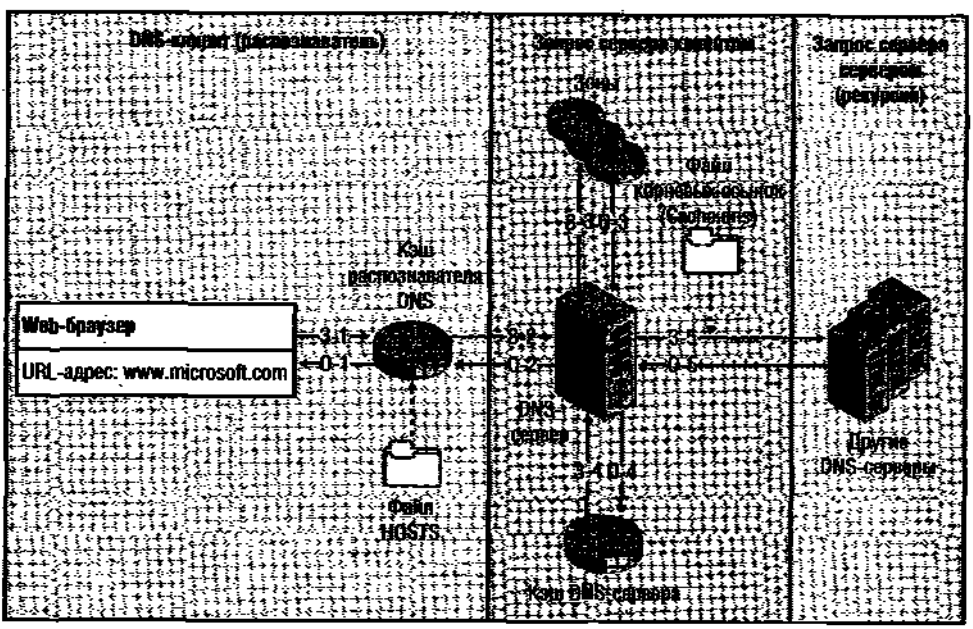


Рис. 4-1. Локальный распознаватель

Процесс запроса инициируется программой на локальном компьютере, когда та обращается к доменному имени в DNS. В примере на рис. 4-1 Web-браузер обращается к Домену *www.microsoft.com.* Запрос поступает в службу DNS-клиента (кэш распознавателя DNS), и выполняется попытка разрешить имя на основании информации из локального кэша. В случае успеха программа получает ответ, и процесс завершается.

В кэш локального распознавателя информация именования попадает из двух источников:

- если файл *Hosts* сконфигурирован для локального использования, все сопоставления имен узлов и адресов из этого файла автоматически загружаются в кэш при запуске службы DNS-клиента, также при обновлении файла *Hosts;*

а записи ресурсов, полученные в ответ на предыдущие DNS-запросы, копируются в кэш и хранятся в нем некоторое время.

Если запрос не удается разрешить с помощью кэша, процесс разрешения продолжается и клиент пересылает запрос на DNS-сервер.

Этап 2: запрос DNS-сервера

DNS-клиент использует список серверов для поиска в порядке предпочтения. Этот список содержит все предпочтительные и альтернативные DNS-серверы, сконфигурированные для каждого из активных сетевых подключений в системе. Сначала клиент запрашивает DNS-сервер, определенный как предпочтительный в окне подключения Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties]. Если основной DNS-сервер недоступен, используются дополнительные. На рис. 4-2 приведен пример списка основного и дополнительных DNS-серверов, сконфигурированных в Windows Server 2003.

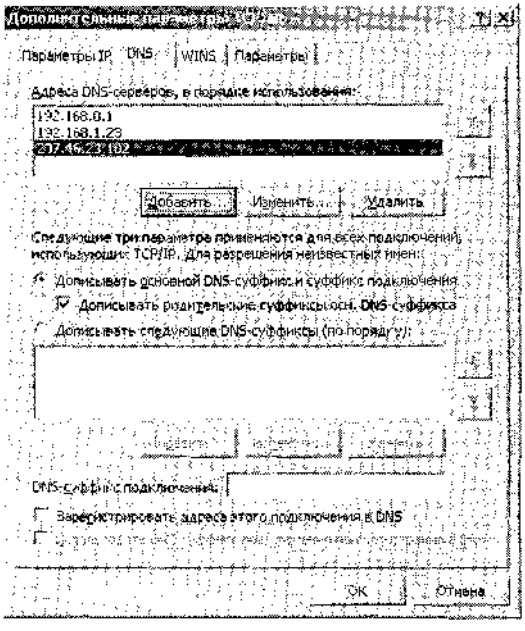


Рис. 4-2. Основной и дополнительные DNS-серверы

Получив запрос, DNS-сервер первым делом проверяет наличие нужной информации в локальной зоне сервера. При положительном результате сервер возвращает полномочный ответ, то есть на основании информации локальной зоны.

Не найдя нужную информацию в локальной зоне, сервер проверяет локальный кэш запросов и при положительном результате дает ответ на основе этой информации, и процедура обработки запроса завершается.

Рекурсия

Если информации о запрашиваемом имени нет на основном сервере — ни в кэше, ни в зонной базе данных — процесс запроса продолжается и зависит QT варианта настройки DNS-сервера. По умолчанию разрешение имен выполняется по методу рекурсии, когда DNS-сервер от имени клиента запрашивает другие DNS-серверы. В такой ситуации DNS-сервер практически превращается в DNS-клиент.

Если на DNS-сервере запрещена рекурсия, клиент выполняет итерационные запросы, используя корневые ссылки, возвращенные DNS-сервером. *Итерация* — это процесс повторных запросов DNS-клиентом различных DNS-серверов.

Подготовка к экзамену На экзамене достаточно знать, что *рекурсия* подразумевает обращение DNS-сервера к другим серверам, когда он не в состоянии ответить на запрос. Отдельных вопросов об итерации нет.

Корневые ссылки

Корректная реализация рекурсии предусматривает, что DNS-сервер должен сначала определить точку начала поиска в пространстве имен DNS. Эта информация предоставляется в форме *корневых ссылок* (root hints) — списка записей ресурсов, используемых службой DNS для обнаружения полномочных серверов в корне доменного дерева пространства имен DNS.

По умолчанию в среде Windows Server 2003 DNS-сервёры используют предварительно определенный файл корневых ссылок *Cache, dns,* который хранится в папке *WINDOWS\System32\Dns.* Его содержимое загружается в память сервера при запуске службы. На рис. 4-3 показан пример файла корневых ссылок по умолчанию.

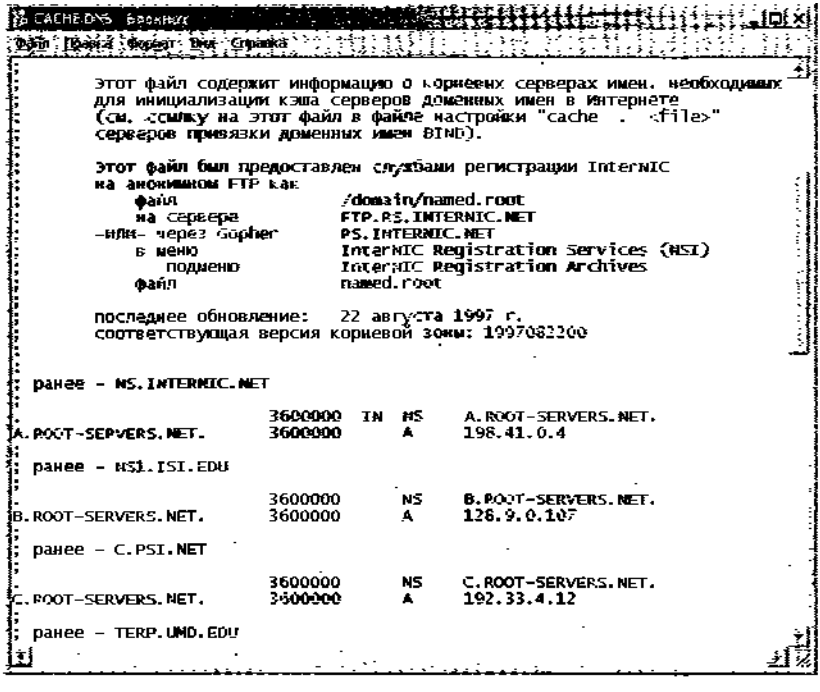


Рис. 4–3. Файл корневых ссылок

В Windows Server 2003 файл корневых ссылок уже содержит адреса корневых серверов в пространстве имен DNS Интернета. Таким образом, при использовании службы DNS-сервер в среде Windows Server 2003 для разрешения DNS-имен Интернета файл корневых ссылок не требует ручной настройки. Однако при использовании службы DNS в частной сети его можно редактировать или заполнить записями, указывающими на

частные внутренние корневые DNS-серверы. Следует заметить, что на корневом DNS-сервере наличие корневых ссылок не допускается, поэтому на таком сервере Windows Server 2003 автоматически удаляет файл *Cashe.dns.*

Пример запроса

Здесь иллюстрируется (рис. 4-4) стандартный механизм обработки DNS-запросов. Клиент запрашивает свой предпочтительный DNS-сервер, который в свою очередь рекурсивно запрашивает вышестоящие DNS-серверы. Предполагается, что на DNS-клиенте и всех DNS-серверах кэш пуст. Клиент пытается разрешить имя *example.lucemepublishing.com* в IP-адрес.

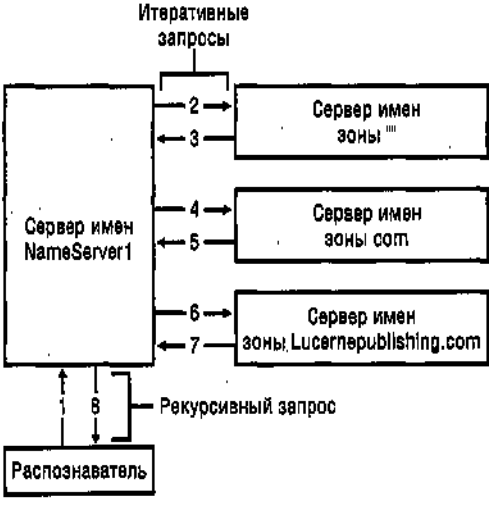


Рис. 4-4. Процесс рекурсии

После поступления запроса от DNS-клиента происходит следующее.

1. Клиент обращается к NameServerl с запросом на разрешение имени *example, lucernepublishing.com.*
2. Сервер NameServerl проверяет свой кэш и базу данных зоны и, не найдя ответа, обращается к полномочному (то есть корневому) серверу Интернета с запросом на разрешение *example.lucernepublishing.com.*
3. Корневому серверу Интернета ответ неизвестен, поэтому он возвращает ссылку на полномочный сервер домена *xom.*
4. Сервер NameServerl обращается к серверу домена *xom* с запросом на разрешение *example.lucernepublishing.com.*
5. Полномочному серверу *xom* точный ответ также не известен, поэтому он отвечает ссылкой на полномочный сервер домена *lucernepublishing.com.*
6. Сервер NameServerl направляет аналогичный запрос на полномочный сервер домена *lucernepublishing.com.*
7. Полномочный сервер домена *lucernepublishing.com* возвращает требуемый IP-адрес.
8. Сервер NameServerl отвечает на запрос, сообщая клиенту IP-адрес, соответствующий имени *example.lucernepublishing.com.*

Типы ответов на запросы

Наиболее популярные варианты ответов на запросы:

- полномочный ответ;
- положительный ответ;
- ответ-ссылка;
- отрицательный ответ.

Полномочный (authoritative) ответ — это положительный ответ клиенту в виде DNS-сообщения с установленным в 1 битом полномочности.

Этот бит показывает, что ответ получен от сервера, полномочного за разрешение запрошенного имени.

Положительный (positive) ответ содержит запрошенную запись ресурса, соответствующую запрошенному имени и типу записи, определенному в исходном запросе.

Ответ-ссылка (referral) — содержит дополнительные записи ресурсов, не соответствующие имени или типу в запросе. Ответ этого типа клиент получает, если DNS-сервер не поддерживает рекурсию. Такой ответ позволяет клиенту продолжить поиск, используя итерацию, то есть опрос других DNS-серверов. Например, если запрашивается узел *www* и для этого имени в зоне не удается найти запись ресурса A, но есть только запись ресурса CNAME, DNS-сервер может указать в ответе клиенту информацию о CNAME. Если клиент поддерживает итерацию, он может самостоятельно использовать ссылки для полного разрешения нужного имени.

Отрицательный (negative) ответ от сервера указывает на один из двух возможных результатов рекурсивных попыток сервера получить полный и полномочный ответ на запрос:

- полномочный сервер сообщает, что запрашиваемое имя не существует в указанном пространстве имен DNS;
- полномочный сервер отвечает, что запрашиваемое имя существует, но нет соответствующих ему записей, указанного в запросе типа.

Получив ответ на запрос, распознаватель передает результаты (положительные или отрицательные) программе, инициировавшей запрос, и копирует их в кэш.

Механизм работы кэша

DNS-клиент и DNS-сервер поддерживают собственные кэши. Кэширование повышает эффективность работы DNS и сокращает сетевой трафик, связанный с DNS-запросами.

Кэш DNS-клиента

Кэш DNS-клиента еще называют кэшем распознавателя. При запуске службы DNS-клиент все соответствия имен узлов и IP-адресам из статического файла *Hosts* загружаются в кэш распознавателя. Файл *Hosts* хранится в папке *WINDOWS\System32\Drivers\Etc*.

Совет При добавлении новых записей в файл *Hosts* они немедленно загружаются в кэш распознавателя DNS.

Кроме записей из файла *Hosts* в кэше распознавателя DNS хранятся записи, получаемые клиентом в качестве ответа от DNS-сервера. Кэш распознавателя DNS очищается при остановке службы DNS-клиента.

Кэш DNS-сервера

Выполняя рекурсивные запросы от имени клиентов, DNS-серверы какое-то время хранит записи ресурсов в своем кэше. Эти кэшированные записи содержат информацию, получаемую в ответ на запросы клиентов. DNS-клиентов, сервер может использовать эту информацию для ответа на запросы других клиентов.

Кэш DNS-сервера очищается при остановке службы DNS-сервер. Кроме того, можно очистить кэш DNS-сервера вручную с помощью консоли *DNS:* в дереве консоли Щелкните правой кнопкой значок сервера и выберите Очистить кэш (Clear Cache). При наличии *Средств поддержки Windows* (Windows Support Tools), кэш очищается командой iscmd /clearcache.

Время жизни (TTL) определяется для всех записей ресурсов, сохраненных в кэше — как распознавателя DNS, так и DNS-сервера. Это время, в течение которого запись ресурса в кэше может использоваться для ответов на запросы. По умолчанию TTL составляет 3600 се---д (1 час), но этот параметр можно изменить как на уровне зоны, так и отдельной записи.

Примечание В DNS используется многоуровневый механизм кэширования, который значительно ускоряет разрешение имен. У такого подхода есть и недостаток: при разрешении запросов с использованием кэшированной информации клиенты не сразу замечают последние изменения в DNS. В общедоступном Интернете на обновление кэшей уходит до четырех часов — лишь после этого пользователи получают доступ к новой информации, причем это не зависит от значения TTL.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите материал занятия. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

Вы администратор сети с основным DNS-сервером, полномочным для зоны *lucernepublishing.com.* Вы также установили два сервера кэширования, которые пересылают все запросы основному серверу. Большая часть запросов, поступающих на серверы кэширования, касается имен внутри домена *lucernepublishing.com.* Какой параметр основного сервера следует изменить, чтобы сократить трафик запросов DNS между серверами кэширования и основным сервером?

Какой домен является корневым для пространства имен с FQDN *first.domainl.local?*

a. Никакой: у этого пространства имен нет корневого домена.
b. *domainl.*
c. *local.*
d. "" (пустая строка).

Что делает распознаватель в первую очередь при разрешении DNS-имени?

a. Проверяет локальный кэш.
b. Считывает файл *Hosts.*
c. Выполняет широковещание в локальной подсети.
d. Направляет запрос на локальный DNS-сервер.

Компьютеры сети включены после перерыва в электроснабжении. DNS-клиент обращается с рекурсивным запросом на локальный DNS-сервер, пытаясь разрешить интернет-имя, для которого данный сервер не является полномочным. Что происходит в первую очередь?

a. DNS-клиент разрешает имя на основании информации из собственного кэша.
b. DNS-сервер разрешает имя на основании информации из собственного кэша.
c. DNS-сервер пересылает рекурсивный запрос вышестоящему DNS-серверу.
d. DNS-сервер обращается к корневым серверам, указанным в файле *Cache.dns.*

Резюме

* Пространство имен DNS представляет собой иерархию с уникальным корневым доменом и неограниченным числом поддоменов. Полное доменное имя (FQDN) — это имя узла DNS в пространстве имен указывающее на положение узла в иерархии по отношению к корню доменного дерева DNS. Пример FQDN: *hostl.subdomain.microsoft.com.*
* Зона DNS — это непрерывная часть пространства имен, обслуживаемая полномочным сервером. Сервер может выполнять роль полномочным в одной или нескольких зонах, а зона может содержать один или несколько смежных доменов. Сервер DNS является полномочным для зоны, если он обслуживает ее в качестве основного или дополнительного DNS-сервера. Зона DNS хранит записи ресурсов, необходимые для ответов на запросы в пределах своей части пространства имен DNS.
* Служба DNS-клиента (или распознаватель) прежде всего пытается разрешить имена компьютеров на основе информации локального кэша, который помимо прочего содержит файл *Hosts.* Не найдя имя в кэше, распознаватель обращается к DNS-серверу. Если DNS-сервер также не может разрешить имя на основе зонной информации или данных локального кэша, по умолчанию он рекурсивно обращается к другим DNS-серверам от имени клиента.
* Рекурсия — процесс запроса DNS-сервером других серверов от имени DNS-клиента. Для правильного выполнения рекурсии DNS-сервер должен знать, где начинать поиск в пространстве имен DNS — эту информацию он берет из хранящегося на сервере файла корневых ссылок *Cache.dns.*
* Время жизни (TTL) определяется для всех кэшируемых записей ресурсов. До истечения времени жизни запись ресурса из кэша используется для ответов на запросы.

Занятие 3. Развертывание DNS-серверов

В частных сетях DNS-серверы обслуживают запросы клиентами имен компьютеров в частном пространстве имен. Однако соответствующим образом настроенные и подключенные к Интернету DNS-серверы позволяют клиентам разрешать имена Интернета, не запрашивая напрямую внешние DNS-серверы.

Изучив материал этого занятия, вы сможете:

- *S* установить и настроить DNS-сервер;
- *S* создать зоны DNS и записи ресурсов;
- *S* описать различия между разными видами серверов: основными, дополнительными, кэширования и серверами зон-заглушек;
- *S* создать сервер кэширования;
- *S* описать некоторые из наиболее популярных типов записей ресурсов;
- *S* просматривать и очищать кэш DNS-сервера.

Продолжительность занятия — около 60 минут.

Установка службы DNS-сервера

По умолчанию на всех компьютерах с Windows Server 2003/XP устанавливается и запускается служба DNS-клиента. А служба DNS-сервер не устанавливается по умолчанию ни в одной из ОС Windows. Чтобы ее установить в Windows Server 2003, нужно сначала добавить роль DNS-сервера утилитой *Управление данным сервером* (Manage Your Server).

После добавления этой роли в группе программ, **Администрирование (Administrative Tools)** появляется значок консоли *DNS* — главного средства настройки и наблюдения DNS-серверов, зон, доменов и записей ресурсов.

Примечание Вместо добавления роли DNS-сервера можно установить службу DNS-сервера с помощью мастера *Установка и удаление программ* (Add or Remove Programs) в *Панели управления*. Выберите **Установка компонентов Windows (Add/Remove Windows Components)** и с помощью *Мастера компонентов Windows* (Windows Component Wizard) установите подкомпонент *DNS* компонента *Сетевые службы* (Networking Services).

Установка DNS-сервера выполняется так.

1. Вставьте в дисковод установочный компакт-диск Windows Server 2003.
2. Убедитесь, что компьютеру назначен статический адрес.
3. Щелкните **Пуск (Start)** и затем **Управление данным сервером (Manage Your Serv**
4. В открывшемся окне щелкните **Добавить или удалить роль (Add or Remove a Ro**
5. На странице **Предварительные шаги (Preliminary Steps)** щелкните **Далее** (Next).
6. На странице **Роль сервера (Server Role)** выберите в списке ролей **DNS-сервер (DNS Server)** и щелкните **Далее** (Next).
7. На странице **Сводка выбранных параметров (Summary of Selections)** щелкните **Дал** По завершении установки компонента *DNS-сервер* начнет работу *Мастер настройки DNS-сервера* (Configure a DNS Server Wizard).
8. Настройте установленный DNS-сервер, следуя указаниям *Мастера настройки DNS-сервера* и принимая все значения по умолчанию.

Конфигурирование DNS-сервера

Настройка параметров DNS-сервера и создание новых зон значительно упрощается, если воспользоваться *Мастером настройки DNS-сервера*. Он автоматически запускается при добавлении роли DNS-сервера. Если мастер уже закончил работу, проверить и изменить параметры DNS-сервера можно в консоли *DNS* [ее значок есть в меню **Пуск (Start)/ Администрирование (Administrative Tools)].** DNS-сервер можно также настроить в окне свойств сервера в консоли *DNS,* вовсе не обращаясь к *Мастеру настройки DNS-сереера*.

Чтобы открыть окно *Мастера настройки DNS-сервера* после установки DNS-сервера, в консоли *DNS* щелкните нужный сервер правой кнопкой и выверите **Настроить DNS-сервер (Configure a DNS Server)** (рис. 4-5).

Создание зон

Есть два вида зон: прямого и обратного просмотра. В первых выполняется сопоставление FQDN-имен IP-адресам, а во вторых, наоборот, IP-адреса сопоставляются полным доменным именам. Таким образом, зоны прямого просмотра обслуживают запросы по разрешению FQDN-имен в IP-адреса, а зоны обратного просмотра разрешают IP-адреса в FQDN-имена.

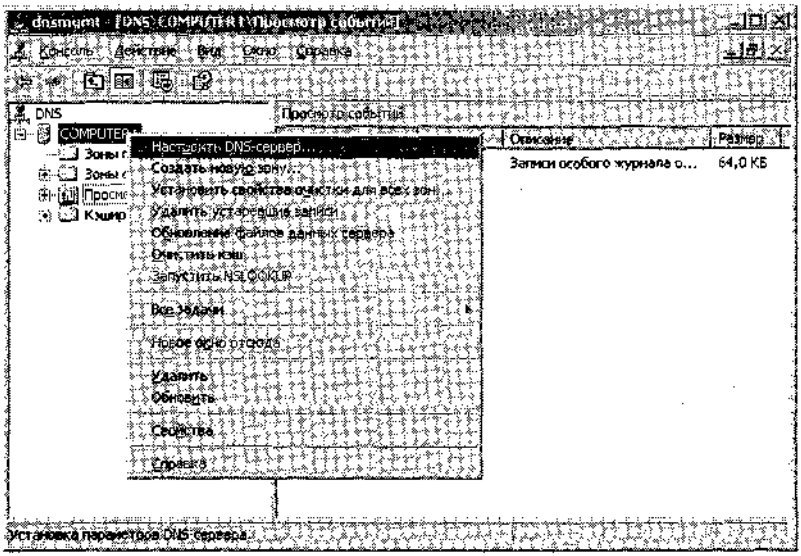


Рис. 4-5. Запуск *Мастера настройки DNS-сереера*

Примечание Можно создать корневой сервер, назначив зоне имя из одной точки «.». В этом случае сервер нельзя настроить на пересылку запросов другим серверам имен.

Зоны прямого и обратного просмотра создаются средствами *Мастера настройки DNS-сереера* или консоли *DNS*. В последнем случае нужно щелкнуть правой кнопкой папку **Зоны прямого просмотра (Forward Lookup Zones)** или **Зоны обратного про (Reverse Lookup Zones)** и в контекстном меню выбрать **Создать новую зону (New Zo** (рис. 4-6). Откроется окно *Мастер создания новой зоны* (New Zone Wizard).

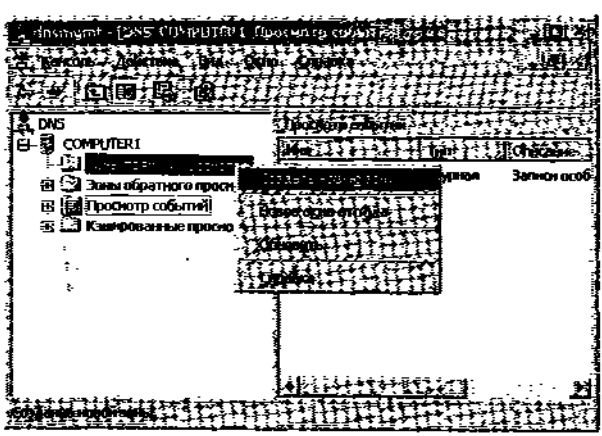


Рис. 4-6. Создание новой зоны

Типы зон

Мастер создания новой зоны позволяет настроить роль сервера в каждой обслуживаемой им зоне.

- **Основная** зона хранит базовые данные для всех доменов в зоне. Резервная копия базы данных зоны может создаваться в дополнительной зоне.
- **Дополнительная зона** — полномочная резервная зона для основной зоны или других дополнительных зон.
- Зона-заглушка (размещается на сервере) — копия зоны, содержащая только записи ресурсов полномочных DNS-серверов *главной зоны* (master zone).

Типы серверов

Тип DNS-сервера определяется типом зоны, которая на нем размещается (на сервере кэширования зоны вообще может не быть, но если она есть, то тип также определяется по типу зоны).

Основные серверы

Основной сервер создается при добавлении основной зоны при помощи *Мастера создания новой зоны* (New Zone Wizard), *Мастера настройки DNS-сервера* (Configure a DNS Server Wizard) или утилит командной строки.

Основной сервер является центральным местом обновления зоны. Вновь созданным зонам всегда назначается этот тип. В Windows Server 2003 основную зону развертывают одним из двух способов: как стандартную основную зону или как основную зону, интегрированную с Active Directory.

Стандартная основная зона может размещаться только на одном сервере. Данная модель уязвима, так как сервер становится *точкой критического отказа* (single point of failure) — если основной сервер зоны недоступен, внести изменения в зону нельзя. Однако запросы имен зоны продолжают обслуживать оставшиеся доступными дополнительные серверы зоны.

В интегрированной с Active Directory зоне хранение и репликация данных выполняется централизованно, вместе с Active Directory. Такая зона значительно устойчивее к отказам и по умолчанию превращает все контроллеры домена в домене с работающими DNS-серверами в основные серверы. Основные зоны, интегрированные с Active Directory, разрешается создавать только на DNS-серверах, одновременно являющихся контроллерами домена Active Directory. Развертывание зон, интегрированных с Active Directory, подробно обсуждается в главе 5.

Дополнительные серверы

Технические требования к проектированию DNS рекомендуют, чтобы каждую зону обслуживали по меньшей мере два DNS-сервера. Для стандартных основных зон дополнительные серверы позволяют разместить зону на других серверах сети.

Дополнительные серверы позволяют сократить трафик DNS-запросов там, где зонная информация запрашивается особо часто. Кроме того, если основной сервер недоступен, разрешение имен в зоне берет на себя дополнительный сервер.

Дополнительные серверы получают информацию о зоне от *главных серверов* (master servers). Главным может быть основной или другой дополнительный сервер. Серверы, главные по отношению к дополнительному серверу, определяются при создании дополнительной зоны сервера одним из трех способов: при помощи *Мастера создания новой зоны, Мастера настройки DNS-сервера* или средствами командной строки.

Совет Дополнительные серверы рекомендуется размещать как можно ближе к клиентам, активно запрашивающим имена данной зоны. Также имеет смысл разместить дополнительные серверы за маршрутизатором, в других подсетях либо обеспечить их доступность по подключениям глобальной сети (WAN). Так обеспечивают эффективное использование дополнительного сервера в качестве резервного в случаях, когда узким местом становятся промежуточные сетевые соединения между DNS-серверами и клиентами, нуждающимися в зонной информации.

Серверы зон-заглушек

Такие DNS-серверы обслуживают *зоны-заглушки* (stub zones) — сокращенные копии зон, содержащие только список полномочных серверов имен основной зоны. DNS-сервер, обслуживающий зону-заглушку, разрешает запросы узлов основной зоны, запрашивая указанные в списке серверы имен. Зоны-заглушки чаще всего применяются для поддержания в родительской зоне свежего списка серверов имен дочерней зоны.

Серверы кэширования

На серверах кэширования зоны не размещаются, и они не могут быть полномочными в конкретном домене. Такие серверы хранят информацию, кэшируемую при запросах на разрешение имен.

Применяя данный вид сервера, следует иметь в виду, что сразу после запуска он не хранит никакой кэшированной информации. Данные накапливаются позже — в процессе обслуживания запросов клиентов. Однако при наличии медленного WAN-канала между сайтами такой сервер может оказаться как нельзя кстати, поскольку после заполнения кэша трафик через WAN-канал значительно падает. DNS-запросы разрешаются быстрее, а значит увеличивается быстродействие сетевых приложений. Кроме того, серверы кэширования не поддерживают перенос зон, который также создает значительную нагрузку на WAN-канал. Наконец, серверы кэширования весьма полезны на сайте, где DNS используется локально, а администрирование доменов или зон нежелательно.

Подготовка- к экзамену Когда надо минимизировать трафик разрешения имен через WAN-подключения, не увеличивая при этом трафик переноса зон, рекомендуется установить сервер кэширования.

По умолчанию служба DNS на стороне сервера работает в режиме сервера кэширования. Такие серверы практически не нуждаются в настройке, а устанавливаются они так.

1. Добавьте роль DNS-сервера.
2. Не настраивайте DNS-сервер (как это обычно делается) на размещения каких-либо зон.
3. Убедитесь, что корневые ссылки сервера сконфигурированы и обновлены.

Создание записей ресурсов

Новые зоны содержат только две записи ресурсов: начальную запись зоны (SOA), соответствующую данной зоне, и запись сервера имен (NS), относящуюся к DNS-серверу этой зоны. После создания зоны ее надо заполнить дополнительными записями ресур-

сов. Одни записи добавляются автоматически, а другие (такие как записи MX и CNAME) нужно определить вручную.

Чтобы вручную добавить в зону запись ресурса, щелкните значок зоны в консоли DNS правой кнопкой и выберите запись ресурса, которую планируете создать (рис. 4-7).

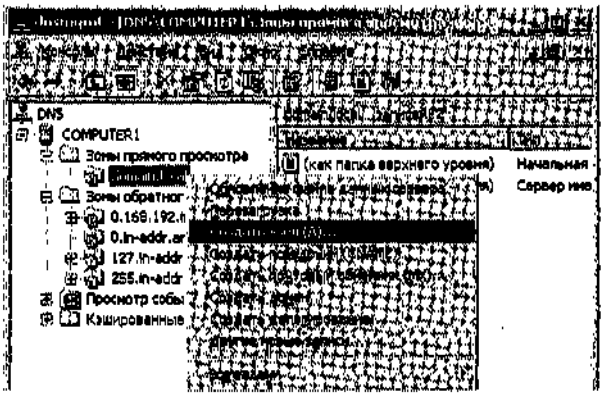


Рис. 4-7. Создание записей ресурсов

Запись ресурса в зоне создается так.

1. В дереве консоли **DNS** щелкните нужную зону правой кнопкой и выберите **Другие новые записи (Other New Records).** Откроется окно **Тип записи ресурса (Resource Record Type).**
2. В списке **Выбор типа записи ресурса (Select a Resource Record Type)** выберите тип записи создаваемого ресурса и щелкните кнопку **Создать запись (Create Record).**
3. В окне **Новая запись ресурса (New Resource Record)** введите информацию о записи ресурса и щелкните OK.
4. Щелкните **Готово (Done),** чтобы вернуться в консоль *DNS.*

Формат записи ресурса

Формат записи ресурсов определяется контекстом, в котором он используется. Например, при просмотре и создании DNS-ответов записи ресурсов представлены в пакетах в двоичном виде. В консоли *DNS* записи ресурсов представлены графически, так что их легко просматривать и изменять. Однако в самом источнике — файле базы данных зоны — записи ресурсов представлены в виде текстовых записей. В действительности, при создании записей ресурсов в консоли *DNS* автоматически добавляются текстовые записи в соответствующий файл базы данных зоны.

В этих файлах зоны записи ресурсов имеют следующий синтаксис (табл. 4-3):

<*Владелец*> TTL <*Класс*> <Тип> <Данные о ресурсе>.

Большинство записей ресурсов представляют собой однострочные текстовые записи. Если запись длиннее одной строки, информация заключается в круглые скобки. Во многих реализациях DNS только начальная запись зоны (SOA) может содержать больше одной строки. Для облегчения чтения в файлы зон часто добавляются пустые строки и понятные человеку комментарии, DNS-сервер такие вставки игнорирует. Комментарии начинаются точкой с запятой (;), а заканчиваются возвратом каретки.

Табл. 4-3. Стандартные поля записей ресурсов

Имя	Описание
Владелец	Имя узла или домена DNS, которому принадлежит данная запись ресурса
Время жизни (TTL)	32-битное целое число, определяющее время (в секундах), в течение которого DNS-сервер или клиент хранит в кэше данную запись. По истечении этого срока запись удаляется из кэша. Это поле необязательно, и, если оно не определено, используется минимальное TTL, определенное в начальной записи зоны (SOA)
Класс	Определяет используемое семейство протоколов. Для DNS-серверов в Windows записям ресурсов всегда назначается класс Интернета, или, сокращенно, IN. Это поле необязательно и автоматически не создается
Тип	Тип записи ресурса, например A или SRV
Данные о ресурсе	Данные записи ресурса. Поле переменной длины, содержащее информацию, определенную типом записи ресурса. Например, в записи ресурса A это 32-битный IP-адрес, соответствующий узлу, определенному в поле владельца

Типы записей

Ниже перечислены наиболее популярные типы записей из числа создаваемых вручную:

- адреса узла (A);
- каноническое имя (CNAME);
- почтовый обменник (MX);
- указатель (PTR);
- локатор службы (SRV).

Запись ресурса узла сети A — это самый распространенный тип записей в базе данных зоны. Эти записи хранят информацию о соответствии доменных имен компьютеров (или узлов сети) и их IP-адресов и добавляются в зону несколькими способами:

- вручную — запись ресурса A для статического компьютера-клиента TCP/IP создается средствами консоли *DNS* или утилиты командной строки Dnscmd;
- на компьютерах под управлением Windows 2000/XP/Server 2003 для динамической регистрации и обновления их собственных записей ресурсов A в DNS при изменениях IP-адресов используется служба DHCP-клиента;
- клиенты под управлением более ранних версий Windows, поддерживающие DHCP, могут регистрировать и обновлять записи ресурсов A с помощью прокси. (Однако на данный момент эту возможность предоставляет только служба *DHCP* из состава Windows Server 2003.)

Созданная в консоли *DNS* строка записи ресурса A, сопоставляющая имени узла сети *server1.lucernepublishing.com* IP-адрес *172.16.48.1,* в файле зоны *lucernepublishing.com.dns* выглядит так:

```
server1  A  172.16.48.1.
```

Подготовка к экзамену Если команда ping показывает наличие связи с компьютером по его IP-адресу, но не по имени, это означает, что в DNS отсутствует запись ресурса A. Можно попробовать решить эту проблему командой Ipconfig /registerdns — но только в том случае, если это компьютер под управлением Windows 2000/XP/Server 2003.

Запись ресурса с каноническим именем (CNAME) позволяет ссылаться на узел сети более чем по одному имени. Например, широко известные имена серверов *(ftp, www)* обычно регистрируются как записи ресурса с каноническим именем (CNAME). Они сопоставляют имя узла сети, определенного для данной службы (например *ftp.lucernepublishing.com),* обычной записи ресурса-компьютера A, на котором размещается данная служба (например *server-boston. lucernepublishing. com).*

Записи ресурсов CNAME также рекомендуются, когда:

- узел сети, определенный в записи ресурса A в той же зоне, нужно переименовать;
- родовому имени стандартного сервера (например *www)* нужно сопоставить группу отдельных компьютеров (у каждого из которых собственная запись ресурса A), предоставляющих одинаковый сервис (например, группу резервных Web-серверов).

Созданная с помощью консоли *DNS* запись ресурса CNAME, сопоставляющая псевдоним *ftp.lucernepublishing.com* имени узла сети *ftpl.lucernepublishing.com,* представляется в файле зоны *lucernepublishing. com. dns* такой записью:

ftp CNAME ftp1.lucernepublishin.com.

Записи ресурса почтового обменника (MX) используются почтовыми приложениями для поиска почтового сервера внутри зоны. Такие записи сопоставляют доменное имя (например *lucernepublishing.com),* указываемое в адресе электронной почты (например *joe@lucernepublishing.com)*, записи ресурса-компьютера A, на котором размещается почтовый сервер домена. Этот тип записи позволяет DNS-серверу обрабатывать адреса электронной почты, в которых конкретно не указан почтовый сервер.

Часто в целях обеспечения отказоустойчивости и возможности использования другого почтового сервера создается несколько записей MX — на тот случай, если основной сервер станет недоступным. Серверы упорядочены по приоритетам, причем чем меньше значение переменной приоритета, тем предпочтительнее запись. Созданные в консоли *DNS* записи ресурсов MX представляются в файле зоны *lucernepublishing.com.dns* текстовыми строками вида:

@ MX 1 mailserver1.lucernepublishing.com.
@ MX 10 mailserver2.lucernepubiishing.com,
@ MX 20 mailserver3.lucernepublishing.com.

Примечание Здесь символ @ обозначает имя локального домена, содержащееся в электронном адресе.

Записи ресурса указателя (PTR) используются только в зонах обратного просмотра для поддержки обратного разрешения IP-адресов в имена узлов сети или FQDN. Обратные просмотры выполняются в зонах, корень которых расположен в домене *in-addr.arpa.* Записи PTR добавляются в зоны так же — автоматически и вручную, как и записи ресурсов A.

Созданная в консоли *DNS* запись ресурса указателя, сопоставляющая IP-адрес *172.16.48.1* имени узла сети *serverl.lucernepublishing.com,* представляется в файле зоны строкой:

1 PTR server1.lucernepublishing.com.

Примечание Здесь *1* соответствует имени, присвоенному узлу сети в домене *172.16.48. и addr.orpa.* Этот домен, который также является именем обслуживаемой зоны, соотве' ствует подсети *172.16.48.0.*

Запись ресурса локатора службы (SRV) определяет местоположение конкретных служ в домене. Поддерживающие S R V клиентские приложения могут использовать DNS дл извлечения записей SRV, определяющих нужные серверы приложений.

Active Directory в Windows Server 2003 — пример поддерживающего SRV приложение Служба Netlogon обнаруживает контроллеры путем поиска службы LDAP в записях SRV

Совет В с е записи S R V, необходимые для работы контроллера домена A c t i v e D i r e c t o r y хранятся в файле *Netlogon.dns* в папке *Windows\System32\Config.* Если таких записей і зоне DNS нет, их можно загрузить автоматически, исполнив из командной строкг N e t d i a l /fix (при условии, что установлены *Средства поддержки Windows (Windowi Support Tools)* с установочного компакт-диска Windows Server 2003].

Выполняя поиск контроллера домена *lucernepublishing.com,* DNS-клиент направляет SRV-запрос:

_ldap._tcp.lucernepublishing.com.

а DNS-сервер возвращает клиенту все Записи, удовлетворяющими этим условиям.

Хотя большая часть записей ресурсов S R V создается автоматически, иногда их создают в консоли *DNS* для обеспечения отказоустойчивости или в процессе устранения неполадок сетевых служб. В следующем примере показаны текстовые строки двух записей SRV, созданных вручную в консоли *DNS:*

```
ldap.tcpSRV    0   0   389    dc1.lucernepublishing.com
       SRV     10  0   389    dc2.lucernepublishing.com
```

Здесь LDAP-серверу (контроллеру домена) с высшим приоритетом 0 назначается порт 389 на узле сети *dcl.lucernepublishing.com.* Второй контроллер домена с более низким приоритетом 10 получает порт 389 узла *dc2.lucernepublishing.com.* В обеих записях в поле коэффициента приоритета стоит 0, что означает отсутствие балансировки нагрузки между серверами равного приоритета.

Подготовка к экзамену На экзамене, как и в реальной жизни, наличие на компьютерах Windows 2000 Server или Windows Server 2003 позволяет развернуть Active Directory с минимальными усилиями, установив первые домены DNS в сети одновременно с доменами Active Directory. В этом нет ничего удивительного, так как только в среде Windows многие записи S R V, необходимые для нормальной работы A c t i v e D i r e c t o r y, создаются автоматически. Если надо развернуть DNS на UNIX-сервере и интегрировать его в инфраструктуру Active Directory, сконфигурируйте UNIX-сервер как дополнительный DNS-сервер.

Просмотр и очистка кэша DNS-сервера

Содержимое кэша DNS-сервера доступно для просмотра только в консоли *DNS.* Для этого в меню **Вид (View)** выберите **Р а с ш и р е н н ы й (Advanced)** (рис. 4-8).

После установки флажка **Расширенный,** в дереве консоли *DNS* появляется новая папка **Кэшированные просмотры (Cached Lookups),** представляющая в иерархическом формате кэш DNS-сервера (рис. 4-9).

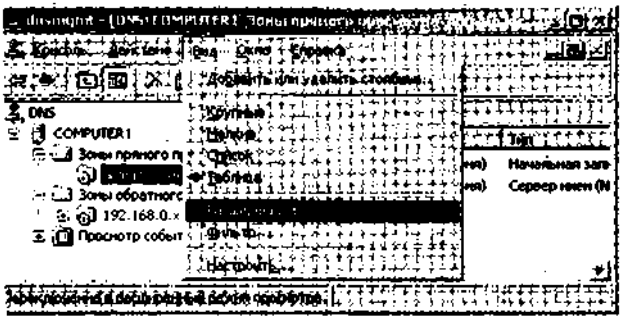


Рис. 4-8. **Включение расширенного вида консоли *DNS***

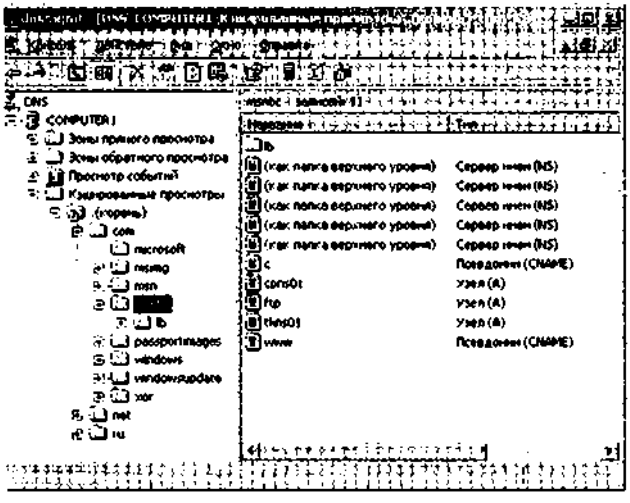


Рис. 4-9. Кэш DNS-сервера

Чтобы очистить кэш DNS-сервера, в консоли *DNS* щелкните значок DNS-сервера равой кнопкой и выберите **Очистить кэш (Clear Cache)** (рис. 4-10). Есть другие способы: перезапустить службу DNS-сервер или выполнить команду Dnscmd/clearcache.

Лабораторная работа. **Установка DNS-сервера**

Вы установите и сконфигурируете DNS-сервер на компьютере Computerl.

Упражнение 1. Установка компонента Windows DNS

Для выполнения этого упражнения нужно вставить в дисковод компьютера Computerl установочный компакт-диск Windows Server 2003.

. Войдите в систему Computerl как *Administrator* (Администратор).

, В *Панели управления* дважды щелкните **Установка и удаление программ (Add or Remove Programs).**

В открывшемся окне **Установка и удаление программ (Add or Remove Programs)** щелкните **Установка компонентов Windows (Add/Remove Windows Components)** и на странице **Компоненты Windows (Windows Components)** *Мастера компонентов Windows* (Windows Components Wizard) выберите **Сетевые службы (Networking Services)** (не устанавливайте флажок компонента, а просто выделите его).

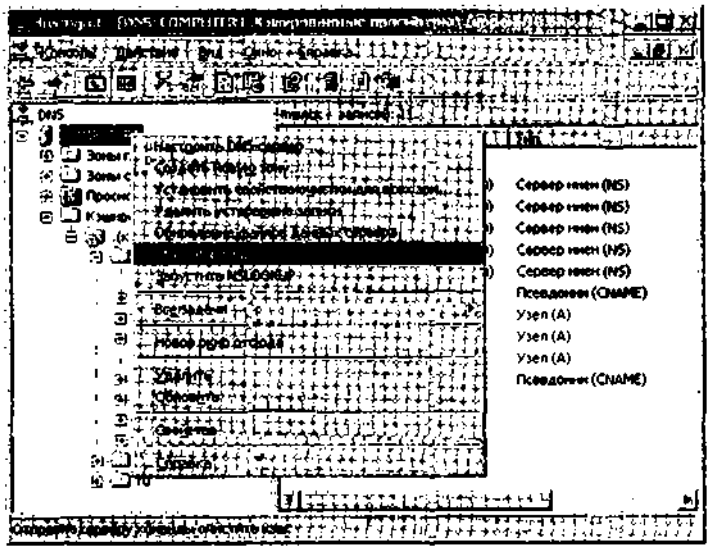


Рис. 4-10. Очистка кэша DNS-сервера

4. Щелкните кнопку **Состав (Details)** и в списке подкомпонентов компонента **Сетевые службы (Networking Services)** установите флажок DNS. Щелкните OK. В окне *Мастера компонентов Windows* поле флажка **Сетевые службы** должно быть выделенным серым.
5. Щелкните **Далее (Next). В** процессе установки нового компонента откроется страница **Настройка компонентов (Configuring Components).** По окончании установки откроется страница **Завершение мастера компонентов Windows (Completing the Windows Components Wizard).**
6. Щелкните **Готово (Finish)** и закройте окно **Установка и удаление программ.**

Упражнение 2. Создание подключения по телефонной линии

Вы создадите подключения к Интернету по телефонной линии. Если на Computerl уже есть интернет-подключение по выделенной линии, то это упражнение можно пропустить, но перед этим следует переименовать подключение в *MylSP*.

1. Войдите в систему на Computerl как *Администратор* (Administrator) и откройте окно **Сетевые подключения (Network Connections).**
2. **В** меню **Файл (File)** выберите **Новое подключение (New Connection),** чтобы запустить *Мастер новых подключений* (New Connection Wizard). Щелкните **Далее (Next).**
3. Щелкните **Далее** на странице **Тип сетевого подключения (Network Connection Ty** оставив вариант по умолчанию — **Подключить к Интернету (Connect to the Internet).**
4. На странице **Подключение к Интернету (Internet Connection)** щелкните **Далее,** приняв вариант по умолчанию — **Через обычный модем (Connect using a dial-up modem).**
5. На странице **Имя подключения (Connection Name)** в поле **Имя поставщика ус Name)** введите MylSP и щелкните **Далее.**
6. На странице **Введите телефонный номер (Phone number to dial)** введите телефонный номер провайдера в текстовом поле **Номер телефона (Phone Number).** Щелкните **Далее.**

7. На странице **Доступность подключения (Connection Availability)** примите вариант по умолчанию — **для всех пользователей (Anyone's Use)** и щелкните **Далее.**
8. На странице **Детали учетной записи в Интернете (Internet Account Information)** введите информацию учетной записи, полученную у интернет-провайдера, в поля **Имя пользователя (User Name), Пароль (Password)** и **Подтверждение (Confirm Password).**
9. Щелкните **Далее.** Откроется страница **Завершение мастера новых подключений (Completing The New Connection Wizard).** Щелкните **Готово (Finish).**
10. На странице **Подключение к MylSP (Connect MylSP)** щелкните кнопку **Свойства (Properties),** чтобы открыть окно **MylSP Свойства (MylSP Properties).**
11. На вкладке **Параметры (Options)** сбросьте флажки **Запрашивать имя, пароль, сертификат и т.д. (Clear the prompt for name and password, certificate, etc)** и **Запрашивать номер телефона (Prompt for phone number)** и щелкните ОК.

    Появится окно **Установка связи с MylSP (Connecting MylSP)** и компьютер начнет дозваниваться до интернет-провайдера. После подключения вы увидите подтверждающее сообщение в области уведомления на панели задач. Компьютер подключен к Интернету.

Упражнение 3. Настройка нового DNS-сервера

С помощью *Мастера настройки DNS-сервера* (Configure a DNS Server Wizard) вы выполните базовую настройку DNS-сервера. По завершении работы мастера DNS-сервер будет обслуживать прямые и обратные запросов имен домена *domain 1. local* и обрабатывать рекурсивные запросы от клиентов внутренней сети. Для нормальной работы *Мастера настройки DNS-сервера* необходимо интернет-подключение.

1. В сеансе *Администратор* (Administrator) на Computer! установите интернет-подключение через *MylSP.*
2. В дереве консоли *DNS* щелкните значок COMPUTER1 правой кнопкой и выберите **Настроить DNS-сервер (Configure a DNS Server).** Откроется окно *Мастера настройки DNS-сервера* (Configure a DNS Server Wizard).
3. Щелкните **Далее** (Next). Откроется страница **Выбор действия по настройке (Select Configuration Action).**
4. Выберите **Создать зоны прямого и обратного просмотра (Create a forward and reverse lookup zones)** и щелкните **Далее.**
5. На странице **Зона прямого просмотра (Forward Lookup Zone)** щелкните **Далее,** приняв значение по умолчанию — **Да, создать зону прямого просмотра (рекомендуется)** (Yes...)
6. На странице **Тип зоны (Zone Type)** щелкните **Далее,** приняв значение по умолчанию — **Основная зона (Primary Zone).**
7. На странице **Имя зоны (Zone Name)** в поле **Имя зоны (Zone Name)** введите domain"!,1ocal и щелкните **Далее.**
8. На странице **Файл зоны (Zone File)** щелкните **Далее,** приняв значение по умолчанию — **Создать новый файл (Create a new file with this file name).**
9. На странице **Динамическое обновление (Dynamic Update)** щелкните **Далее,** приняв значение по умолчанию — **Запретить динамические обновления (Do not allow dynamic updates).**
10. На странице **Зона обратного просмотра (Reverse Loolup Zone)** щелкните **Далее,** приняв значение по умолчанию — Да... (Yes...).
11. На странице **Тип зоны (Zone Type)** щелкните **Далее,** приняв значение по умолчанию — **Основная зона (Primary Zone).**
12. На странице **Имя зоны обратного просмотра (Reverse Lookup Zone)** в поле **Код сети (ID) (Network ID)** введите 192.168.0. Имя зоны обратного просмотра автоматически

появится в поле **Имя зоны обратного просмотра (Reverse Lookup Zone Name).** Щелкните **Далее.**

13. На странице **Файл зоны (Zone File)** щелкните **Далее,** приняв значение по умолчанию — **Создать новый файл (Create a new file with this file name).**
14. На странице **Динамическое обновление (Dynamic Update)** щелкните **Далее,** приняв значение по умолчанию — **Запретить динамические обновления (Do not allow dynamic updates).**
15. На странице **Серверы пересылки (Forwarders)** щелкните **Далее,** приняв значение по умолчанию'— Нет... (No...).
16. На странице **Завершение мастера настройки DNS-сервера (Completing the Configurea DNS Server Wizard)** щелкните **Готово (Finish).**
17. В консоли *DNS* раскройте в левой панели дерево консоли, чтобы увидеть новую зону *domain I. local* в папке **Зоны прямого просмотра (Forward Lookup Zones).** Новая зона *192.168.0An-addr.arpa* также появилась в папке **Зоны обратного просмотра (Reverse Lookup Zones).**

Упражнение 4. Тестирование DNS-сервера

Windows Server 2003 позволяет проверить настройку DNS-сервера с помощью двух тестов, выполняемых на компьютере DNS-сервера. Они выполняются на вкладке **Наблюдение (Monitoring)** окна свойств сервера в консоли *DNS.*

1. В сеансе *Администратор* (Administrator) на Computerl установите интернет-подключение через *MylSP.*
2. В дереве консоли *DNS* щелкните COMPUTER1 правой кнопкой и выберите **Свойства (Properties).**
3. На вкладке **Наблюдение (Monitoring)** окна свойств сервера установите флажки **Простой запрос к этому DNS-серверу (A Simple query against this DNS server)** и **Рекурсивный запрос к другим DNS-серверам (A recursive query to other DNS servers).**
4. Щелкните **Тест (Test Now). В** области **Результаты теста (Test Results)** должна появиться информации об успехе проверок.
5. Щелкните OK, чтобы закрыть окно свойств Computerl.
6. Закройте сеанс на Computerl.

Подготовка к экзамену Нужно знать тесты DNS-сервера. Во-первых, запомните, что простой тест основывается на обратном просмотре адреса замыкания на себя *127.0.0.1.* Поэтому если этот тест не удается пройти, нужно убедиться, что запись с именем *1* находится в зоне обратного просмотра с именем *0.0.127.in-addr.arpa* [видима в консоли *DNS* только в режиме *Расширенный* (Advanced)]. Во-вторых, рекурсивный тест проверяет способность взаимодействия DNS-сервера с другими DNS-серверами и правильность настройки корневых ссылок.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите материал занятия. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы только что обновили запись ресурса узла сети. Какую еще запись ресурса, связанную с первой, нужно обновить?

2. На DNS-сервере не удается выполнить рекурсивный тест. Допустим, несмотря на это, сервер успешно взаимодействует с другими DNS-серверами. Назовите две возможные причины такого поведения.
3. Какая запись ресурса используется для разрешения доменных имен, указываемых в адресах электронной почты, в IP-адрес связанного с доменом почтового сервера?
   a. PTR.
   b. MX.
   c. A.
   d. CNAME.
4. На новом DNS-сервере создается зона "", а затем — поддомены этого корневого домена. Какая функция будет недоступна этому серверу?
   a. Сервер не сможет кэшировать имена.
   b. Сервер сможет работать только как сервер пересылки.
   c. Сервер не сможет разрешать имена Интернета.
   d. Сервер не сможет подключиться к Интернету.

Резюме

- DNS-серверы являются полномочными для зон, которые на них размещаются. Зоны прямого просмотра отвечают на запросы об IP-адресах, а зоны обратного просмотра — на запросы о полных доменных именах.
- DNS-сервер, на котором размещается основная зона, называется основным DNS-сервером. Основные DNS-серверы хранят исходную зонную информацию. В Windows Server 2003 можно использовать зоны двух типов: стандартные основные зоны или зоны, интегрированные с Active Directory. В последнем случае данные зоны хранятся в Active Directory.
- DNS-сервер, на котором размещается дополнительная зона, называется дополнительным DNS-сервером. Дополнительные DNS-серверы являются полномочными резервными серверами для основного сервера. Серверы, от которых дополнительные серверы получают зонную информацию, называются главными. Главным может быть как основной сервер зоны, так и другой дополнительный сервер.
- Серверы кэширования пересылают все запросы другим DNS-серверам и сами не поддерживают базу данных о зонах, однако они кэшируют ответы других DNS-серверов и таким образом способствуют ускорению разрешения имен в сетях, не содержащих зоны.
- Новые зоны содержат только две записи ресурсов: запись ресурса начальной записи зоны (SOA), содержащей информацию о самой зоне, и запись ресурса сервера имен (NS), соответствующая локальному DNS-серверу данной зоны. После создания зоны в нее должны добавляются дополнительные записи ресурсов. Наиболее распространены записи ресурсов следующих типов: адреса узла (A), канонического имени (CNAME), почтового обменника (MX), локатора службы (SRV) и указателя (PTR).

Занятие 4. **Настройка DNS-клиентов**

Настройка DNS-клиентов в общем случае состоит из настройки имен компьютеров, определения суффиксов DNS этих имен, DNS-серверов, используемых для разрешения имен, а также конфигурирования поведения DNS-клиентов при выполнении запросов. Также можно задать порядок обновления DNS-клиентами собственных записей в DNS.

Изучив материал этого занятия, вы сможете:

- *S* определять DNS-имена;
- *S* задавать основной DNS-суффикс компьютера;
- *S* задавать суффиксы DNS сетевых подключений;
- */* задавать список DNS-серверов для сетевых подключений;
- *S* задавать список поиска по суффиксам в сетевых подключениях;
- *S* настраивать динамическое обновление DNS-клиентов;
- *S* просматривать и очищать кэш DNS-клиента.

Продолжительность занятия — около 60 минут.

Настройка параметров клиента

Настройка компьютеров DNS-клиентов в сетях Windows Server 2003 предусматривает выполнение как минимум следующих задач.

- **Задание DNS-имени компьютера или узла на каждом компьютере.** Например, в полном доменном имени *clientl.example.microsoft.com* крайняя левая метка— это DNS-имя компьютера *client 1.*
- **Определение на компьютере основного суффикса DNS.** Добавляя этот суффикс после имени узла, получаем полное имя компьютера. В предыдущем примере основной суффикс DNS — *example.microsoft.com.*
- **Определение списка DNS-серверов, используемых клиентами для разрешения DNS-имен.** Этот список состоит из основного DNS-сервера, а также (при необходимости) дополнительных DNS-серверов, к которым клиент обращается в случае недоступности основного сервера.

Кроме того, в зависимости от потребностей настраиваемых DNS-клиентов выполняют дополнительные операции.

- **Задание списка поиска по DNS-суффиксам,** то есть порядок поиска при запросе коротких (неполных) доменных имен.
- **Задание для каждого конкретного адаптера на клиентском компьютере DNS-суффиксов подключений.** Например, узел *hostl.lucernepublishing.com,* подключенный к двум подсетям через разные сетевые адаптеры в одной подсети может иметь имя *hostl.subnetl.microsoft.com,* а в другой — *hostl.subnet2.microsoft.com.*

ш **Изменение порядка динамического обновления DNS.**

Далее перечисленные задачи обсуждаются более подробно.

Определение имен компьютеров

DNS-имя компьютера или узла — это фактически крайняя слева метка в полном доменном имени (FQDN). Например, в имени *wkstnl.example.microsoft.com* это *wkstnl.* Имя компьютера можно изменить на вкладке **Имя компьютера** (Computer Name) окна **Свойства системы (System Properties).**

Примечание Чтобы открыть окно **Свойства системы (System** Properties), щелкните значок **Мой компьютер (My Computer)** правой кнопкой и выберите **Свойства (Prope** либо дважды щелкните **Система** (System) в *Панели управления.*

Имя компьютера должно удовлетворять требованиям к DNS-символам, определенных в RFC 1123, то есть его длина не должна превышать 63 байта и может состоять лишь из следующих символов:

я прописные буквы от A до Z;

а строчные буквы от а до z;

- цифры от 0 до 9;
- дефисы (-);

Примечание На практике в DNS-именах регистр не учитывается.

Использование NetBIOS-имен

Если в сети поддерживаются пространства имен DNS и NetBIOS, можно присвоить компьютерам разные имена для каждого пространства имен, но так делать не рекомендуется. Имена компьютеров с Windows 2000/XP/Server 2003 должны удовлетворять требованиям, сформулированным выше, а также ограничениям, накладываемым NetBIOS. Иначе говоря, длина имени не может превышать 15 символов.

Определение основного суффикса DNS

Основной суффикс DNS задается и изменяется в окне **DNS-суффикс и NetBIOS-имя компьютера (DNS Suffix and NetBIOS Computer Name)** (рис. **4-11).**

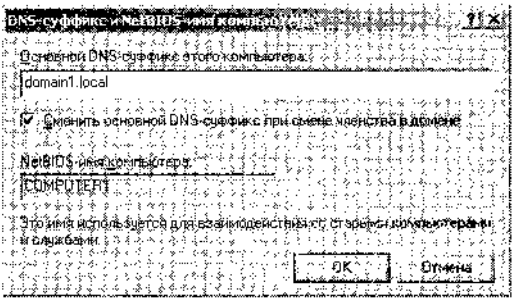


Рис. 4-11. Определение первичного суффикса DNS

Чтобы Открыть это окно, в окне Свойства системы (System **Properties)** перейдите на вкладку Имя **компьютера (Computer Name)** и щелкните кнопку **Изменить (Change).** В окне **Изменение имени компьютера (Computer Name** Change) щелкните кнопку **Дополнительно (More).**

По умолчанию основной суффикс DNS совпадает с именем домена Active Directory, которому принадлежит данный компьютер. Если компьютер не является членом домена, значение основного суффикса DNS по умолчанию не определяется.

Задание DNS-суффиксов подключений

Щелчком кнопки **Дополнительно (Advanced)** в окне **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties]** откройте окно **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** и на вкладке **DNS** (рис. 4-12) задайте DNS-суффикс данного подключения.

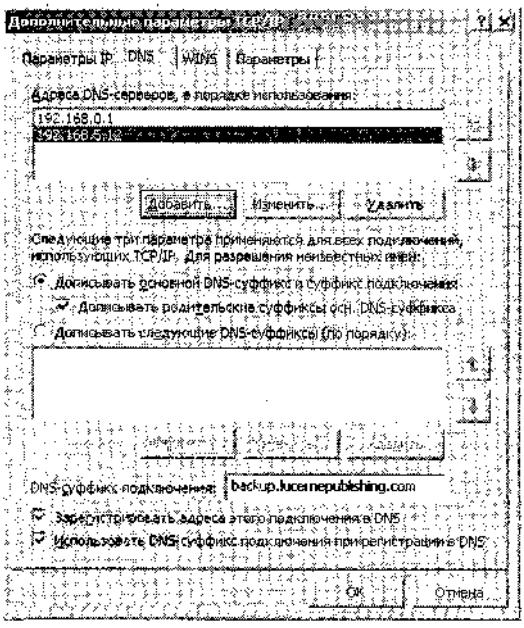


Рис. 4-12. Определение суффикса подключения

Объединение DNS-суффикса и DNS-имени компьютера или узла представляет собой полное доменное имя (FQDN) конкретного адаптера на компьютере. Например, многоадресный сервер *host-a* можно именовать как по основному, так и связанному с подключением доменному имени (рис. 4-13).

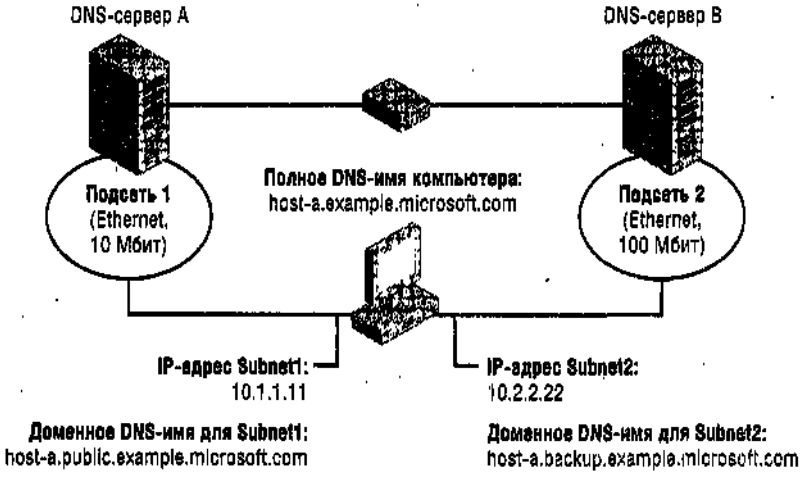


Рис. 4-13. Использование суффиксов подключения

В данном примере компьютер сервера *host-a* связан с двумя разными подсетями — *Subnetl* и *Subnet?,* — которые также связаны как резервные точки через два маршрутизатора, за счет чего образуются дополнительные маршруты между ними. В данной конфигурации *host-a* предоставляет доступ к локальной сети через подключения с разными именами:

и имя *host-a.public.example.microsoft.com* позволяет получить доступ через первое подключение — *Subnet 1* по низкоскоростной (10 Мбит) локальной сети Ethernet, и обеспечивает обычный доступ пользователей для удовлетворения стандартных потребностей в службах файлов и печати;

- имя *host-a.backup.example.microsoft.com* обеспечивает доступ через второе подключение — *Subnet2* по локальной сети Ethernet с более высокой скоростью (100 Мбит), и применяется для резервного доступа приложений сервера и администраторов, которым требуется выполнять особые задачи, например устранять неполадки сервера, выполнять резервное копирования или организовать зонные передачи между серверами.

К компьютеру также можно подключиться, не указывая конкретное подключение, достаточно обратиться по его полному имени *host-a.example.microsoft.com.*

Сконфигурированный таким образом DNS-клиент под управлением Windows 2000/XP/Server 2003 способен регистрировать отдельные записи ресурсов в базе данных DNS для трех своих имен и IP-адресов (табл. 4-4).

Табл. 4-4. Полные имена многоадресного узла сети

DNS-имя	IP-адреса	Описание
host-a.example.microsof.com	10.1.1.11, 10.2.2.22	Полное имя компьютера. Компьютер регистрирует в зоне *example.microsoft.com* записи ресурсов A и PTR, сопоставляющие этому имени всё сконфигурированные IP-адреса
host-a.public.example.microsoft.com	10.1.1.11	DNS-имя первого локального подключения; регистрируются записи ресурсов типа A и PTR, сопоставляющие этому имени IP-адрес 10.1.1.11 в зоне *public, example.microsoft. com*
host-a.backup.example.microsoft.com	10.2.2.22	DNS-имя второго локального подключения; регистрируются записи ресурсов типа A и PTR, сопоставляющие этому имени IP-адрес 10.2.2.22 в зоне *public.example.microsoft.com*

Определение списка DNS-серверов

Не найдя ответа на запрос в кэше, DNS-клиент пытается разрешить имя через основное подключение.— оно указывается первым в списке, выдаваемом командой Ipconfig, — запрашивая адрес у основного DNS-сервера этого подключения. Хотя для каждого сетевого адаптера обычно можно задавать свой список DNS-серверов, лучше все-таки настроить все адаптеры одинаково — это сделает разрешение DNS-имен более предсказуемым.

Каждое подключение, настроенное на компьютере DNS-клиента, может содержать не один, а целый список DNS-серверов. Это значительно облегчает разрешение имен. Основной и один дополнительный DNS-сервер для подключения определяется в окне **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties]** (рис. 4-14).

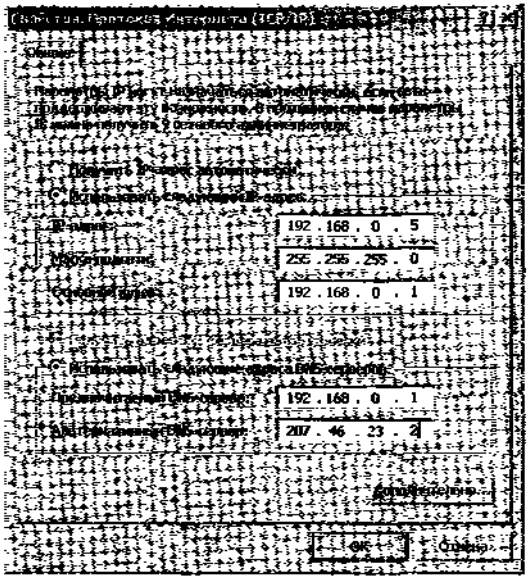


Рис. 4-14. Определение основного и дополнительного DNS-серверов

Однако можно задать список с любым количеством DNS-серверов — это делается в окне **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings). В** данном списке первый сервер в списке рассматривается как основной, или предпочтительный, а остальные считаются дополнительными и опрашиваются одновременно.

Разрешая имя, DNS-клиент опрашивает DNS-серверы в следующем порядке.

1. DNS-клиент направляет запрос первому серверу в списке DNS-серверов предпочтительного адаптера и ждет ответа в течение секунды.
2. Не получив ответа, DNS-клиент обращается к первым DNS-серверам в списках всех используемых адаптеров и ждет ответа 2 секунды.
3. Если за 2 секунды ответ не поступает ни от одного сервера, распознаватель направляет запросы всем DNS-серверам на всех используемых адаптерах и ждет ответа еще 2 секунды.
4. Если по истечении этого времени не ответит ни один сервер, распознаватель посылает запросы всем DNS-серверам на всех используемых адаптерах и ждет еще 4 секунды.
5. Если ответа все равно нет, распознаватель посылает запросы всем DNS-серверам на всех используемых адаптерах и ждет еще 8 секунд.

Получив ответ на любом из указанных этапов, служба DNS-клиента прекращает запросы, копирует ответ в кэш и передает ответ клиенту. Если DNS-клиент не получает ответа в течение 8 секунд с начала последнего запроса, распознаватель сообщает о превышении времени ожидания, то есть о невозможности разрешить имя.

Определение списка поиска суффиксов DNS

Служба DNS-клиента дополняет любое вводимое в запросе имя суффиксами DNS, если выполняется любое из условий:

- указано неполное имя, состоящее из одной метки;
- имя состоит из нескольких меток, но является неполным, и DNS-клиент распознает его как таковое.

Поиск с использованием DNS-суффиксов по умолчанию

Служба DNS-клиента сначала добавляет к неполному имени основной доменный суффикс локального компьютера. Если при этом разрешить имя не удается, DNS-клиент добавляет суффикс подключения, присвоенный сетевому адаптеру. Если и после этого не удается получить ответ, служба DNS-клиента добавляет родительский суффикс основного суффикса DNS.

Например, полное имя многоадресного компьютера — *computerl.domainl.microsoft.com,* а сетевым адаптерам на Computed присвоены суффиксы подключения *subnet!.domain Lmicrosoft.com* и *subnet2.domainl.microsoft.com* соответственно. Если на этом компьютере ввести compute r2 в поле адреса в Internet Explorer и нажать Enter, локальная служба DNS-клиент сначала попытается разрешить это имя, запрашивая *computer2.domainl.microsoft, com.* Если такой запрос ничего не даст, DNS-клиент запросит имена *computer2.subnetl.domainl.microsoft.com* и *computer2.subnet2.domainl.microsoft.com.* Если и это н ' е поможет, служба DNS-клиента запросит имя *computer2.microsoft.com.*

Пользовательский список поиска суффиксов DNS

Такой список задают в окне **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** (рис. 4-15).

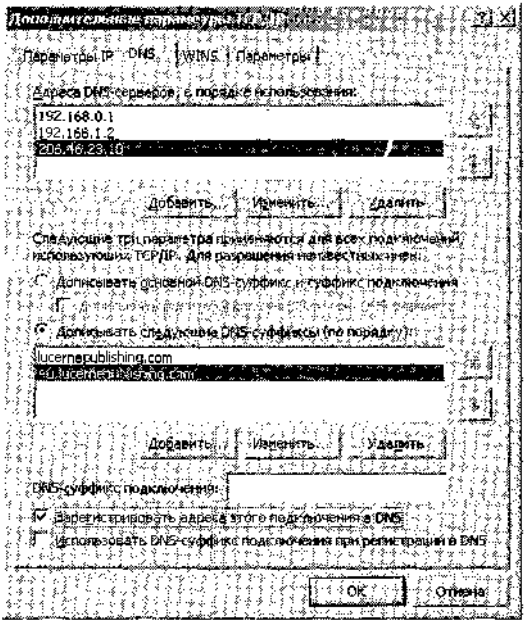


Рис. 4-15. Добавление суффиксов DNS в запросах

Вариант **Дописывать следующие DNS -суффиксы (по порядку) (Append these DNS suffixes)** позволяет задать список DNS-суффиксов, добавляемых к неполным именам. Если такой список задан, DNS-клиент добавляет эти DNS-суффиксы в порядке их следования и не подставляет никакие другие доменные имена. Например, если в списке суффиксов (рис. 4-15) запросить неполное, состоящее из одной метки имя *coffee,* DNS-клиент сначала выполнит запрос *coffee.lucernepublishing.com,* а затем — *coffee.eu.lucernepublishing.com.*

Настройка динамического обновлении

При соответствующей настройке DNS-серверы под управлением Windows 2000/Server 2003 принимают динамические обновления записей ресурсов A и PTR. Сами обновления должны выполняться либо клиентом DNS под управлением Windows 2000/XP/Server 2003, либо DHCP-сервером (от имени DNS-клиента) под управлением Windows 2000/Server 2003.

Подготовка к экзамену На экзамене нужно знать, что DNS-серверы под управлением UNIX, поддерживающие B I N D версии 8 - . 1 . 2 или более поздней принимают динамические обновления.

Динамические обновления возможны, только если доменный суффикс на клиенте совпадает с именем зоны, размещенной на основном DNS-сервере. Иначе говоря, чтобы запись компьютера с именем *client 1* динамически обновлялась в зоне *lucemepublishing.com,* полное доменное имя этого компьютера должно быть *clientl.hicernepublishing.com* и клиент должен определить в качестве 'Основного DNS-сервер, обслуживающий зону *hicernepublishing.com.*

Стандартный порядок обновления DNS-клиентов

По умолчанию DNS-клиенты со статическими IP-адресами и соответствующими доменными суффиксами пытаются регистрировать и обновлять записи ресурсов A и PTR, обращаясь к основному DNS-серверу. А клиенты, получающие адрес у DHCP-сервера, регистрируют и обновляют через основной DNS-серзер только записи ресурсов A. В последнем случае записи ресурсов PTR обновляются DHCP-сервером при выделении IP-адреса в аренду. Для клиентов Windows, которые не поддерживают динамическое обновление, например DNS-клиентов под управлением Windows Me или Windows NT 4, обновление записей ресурсов обоих типов A и PTR может от их имени выполнять соответствующим образом настроенный DHCP-оервср,

Чтобы настроить DNS-клиент на выполнение динамических обновлений в DNS. установите флажок Зарегистрировать адреса этого подключения в DNS (Register this connection's adresses in DNS) на вкладке DNS окна Дополнительные параметры TCP/IP (Advanced TCP/IP Settings) (рис. 4-15). (Этот флажок установлен по умолчанию.) DNS-клиент станет регистрировать и обновлять полное имя компьютера (основное доменное имя). Если определен DNS-суффикс для подключения, можно также настроить DNS-клиент на динамическую регистрацию и обновление полного имени FQDN, основанного на этом суффиксе: Использовать DNS-суффикс подключения при регистрации в DNS (Для этого нужно отметить флажок Use this connection's suffix in DNS registration). (По умолчанию этот флажок не установлен.)

Чтобы заставить DNS-клиент регистрировать записи ресурсов A и PTR, исполните команду ipconfig /registerdns.

Примечание Для клиентов общего доступа к подключению к Интернету (ICS) динамическое обновление DNS настраивается иначе. Получив IP-адрес в службе ICS DNS-клиенты под управлением Windows 2000/XP/Server 2003 обновляют свои записи в DNS, только когда установлен-флажок Использовать DNS-суффикс подключения при регистрации в DNS. При этом не нужно определять суффикс подключения — полное доменное имя образуется только на базе основного DNS-суффикса.

Настройка параметров TCP/IP DNS-клиентов

Ниже описаны процедуры настройки параметров TCP/IP на клиентах, необходимые для нормальной их работы в DNS.

1. Откройте папку **Сетевые подключения (Network Connections).**
2. Щелкните настраиваемое подключение правой кнопкой и выберите **Свойства (Properties).**
3. **В** окне свойств подключения на вкладке **Общие (General)** (для подключения по локальной сети) или на вкладке **Сеть (Networking)** (для других подключений) выберите компонент **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)]** и щелкните кнопку **Свойства (Properties).** Откроется окно **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties].** *
4. Если адреса DNS-серверов должен назначать DHCP-сервер, выберите вариант **Получить адрес DNS-сервера автоматически (Obtain DNS server address automatically).**
5. Если адреса DNS-серверов планируется настраивать вручную, выберите вариант **Использовать следующие адреса DNS-серверов (Use the following DNS server addresses)** и в полях **Предпочитаемый DNS-сервер (Preferred DNS Server)** и **Альтернативный DNS-сервер (Alternate DNS Server)** введите IP-адреса для основного и дополнительного DNS-серверов.
6. Чтобы настроить дополнительные параметры DNS, щелкните кнопку **Дополнительно (Advanced)** и на вкладке **DNS** выполните следующее.
   a. Чтобы задать IP-адрес дополнительного DNS-сервера, щелкните верхнюю кнопку **Добавить (Add)** и введите IP-адрес DNS-сервера.
   b. Чтобы изменить порядок разрешения неполных DNS-имен, выберите одну из возможностей:
      a чтобы клиент разрешал неполные имена, добавляя основной DNS-суффикс и суффиксы каждого подключения (если они определены) выберите **Дописывать основной DNS-суффикс и суффикс подключения (Append primary and connec specific DNS suffixes).** Если надо, чтобы выполнялся поиск по родительским суффиксам основного DNS-суффикса вплоть до доменов второго уровня, установите флажок **Дописывать родительские суффиксы осн. DNS-суффикса (Append parent suffixes of the primary DNS suffix);**
      a чтобы клиент разрешал неполные имена, добавляя суффиксы из заданного списка, выберите **Дописывать следующие DNS-суффиксы (по порядку) (Append these DNS suffixes),** а затем щелкните **Добавить (Add),** чтобы создать список суффиксов.
   c. Чтобы задать DNS-суффикс подключения, укажите его в поле **DNS-суффикс подключения (DNS suffix for this connection).**
   d. Динамическое обновление DNS выполняется так:
      a чтобы клиент регистрировал IP-адреса подключения в DNS под полным именем локального компьютера, установите флажок **Зарегистрировать адреса этого подключения в DNS (Register this connection's addresses in DNS).** Этот флажок установлен по умолчанию. При этом нужно, чтобы основной DNS-суффикс компьютера совпадал с доменом,- обслуживаемым основным (предпочитаемым) DNS-сервером;
      a чтобы клиент регистрировал IP-адреса подключения с полным доменным именем на базе DNS-суффикса подключения, установите флажок **Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in DNS registration).** По умолчанию этот флажок сброшен;

- чтобы полностью запретить динамические обновления любых DNS-имен, сбросьте флажок **Зарегистрировать адреса этого подключения в DNS (Register this connection's addresses in DNS)** для всех подключений в папке **Сетевые подключения (Network Connections).**

Просмотр и очистка кэша распознавателя DNS

Не следует путать кэш распознавателя DNS, или кэш DNS-клиента, с кэшем DNS-сервера. Именно первый проверяется DNS-клиентами до обращения к DNS-серверу. Новые записи добавляются в кэш распознавателя при получении DNS-клиентом ответов от DNS-сервера.

Содержимое клентского кэша просматривают командой ipconfig /displaydns. Она возвращает как записи, загруженные из локального файла *Hosts,* так и любые записи ресурсов, полученные в процессе разрешения имен.

Кэш распознавателя DNS очищается командой ipconfig/flushdns или перезапуском службы *DNS-клиент* в консоли *Службы* (Services) **[Пуск Start)/Администрирование (Administrative Tools)].**

Подготовка к экзамену Запомните следующие команды управления DNS:

1. Ipconfig /displaydns — отображение содержимого кэша DNS-клиента;
2. Ipconfig /flushdns — очистка кэша DNS-клиента;
3. Ipconfig /registerdns — обновление всех DHCP-аренд и регистрация DNS-имен в зонах DNS, поддерживающих динамическое обновление.

Имейте в виду, что команда Ipconfig /registerdns работает только на клиентах под управлением Windows 2000/XP/Server 2003.

Подготовка к экзамену Помните что иногда команда Ipconfig /flushdns, позволяет добиться результата от действий по устранению неполадок DNS. Допустим, UNIX-компьютер не реагирует на эхо-запрос ping с Windows-компьютера. Вы вручную создаете запись ресурса A для UNIX-компьютера, чтобы устранить неполадку, но UNIX-компьютер все равно не откликается на ping. Причина в том, что в кэше клиента сохранился предыдущий отрицательный ответ. Проблему решит очистка кэша DNS-клиента, то есть надо выполнить на Windows-компьютере команду Ipconfig /flushdns. Это заставит Windows-клиент выполнить полноценный запрос на разрешение имени UNIX-компьютера.

Лабораторная работа 1. **Настройка основного DNS-суффикса**

Вы зададите основной DNS-суффикс на Computerl и Computer2 и проследите, к чему это приведет, с помощью консоли *DNS.*

Упражнение 1. Определение DNS-суффиксов

В этом упражнении вы зададите основные DNS-суффиксы на компьютерах Computerl и Computer2.

1. Войдите в систему Computerl как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система** (System). Откроется окно **Свойства системы (System Properties).**

3. На вкладке **Имя компьютера (Computer Name)** щелкните кнопку **Изменить (Change).** Откроется окно **Изменение имени компьютера (Computer Name Change).**
4. Щелкните **Дополнительно (More).** В окне **DNS-суффикс и NetBIOS-имя компьютера (DNS suffix and NetBIOS computer name)** в поле **Основной DNS-суффикс этого компьютера (Primary DNS Suffix Of This Computer)** введите domain1.local. Щелкните OK.
5. В окне **Изменение имени компьютера** щелкните OK. Появится сообщение о необходимости перезагрузки компьютера, чтобы изменения вступили в силу. Щелкните OK.
6. В окне **Свойства системы (System Properties)** щелкните OK. Откроется окно **Изменение параметров системы (System Settings Change)** с предложением немедленной перезагрузки. Щелкните Да (Yes).
7. Пока компьютер Computed перезагружается, выполните ту же процедуру на Computer!, назначив основной DNS-суффикс *domain I, local.* Перезагрузите Computer!.

Упражнение 2. Проверка изменений в DNS

Вы проверите изменения, выполненные в упражнении 1.

1. Войдите в систему Computerl *как Администратор* (Administrator).
2. Исполните команду ping computerl.
3. Ответьте на вопрос: как изменился суффикс в листинге результатов работы команды ping?
4. Выйдите из системы Computerl.

Лабораторная работа 2. Настройка рекурсии на DNS-сервере

Вы настроите DNS-сервер на Computerl на выполнение рекурсивных запросов DNS-имен Интернета, поступающих с компьютера Computer2. Затем направите рекурсивный запрос с Computer2 и изучите результаты.

Поскольку компьютеру Computer! присвоен частный адрес, он может взаимодействовать с Интернетом только через службу преобразования адресов, например NAT или ICS. Поэтому прежде всего надо настроить ICS на Computerl.

Упражнение 1. Включение ICS

В этом упражнении вы включите ICS на Computerl, что обеспечит преобразование адресов всех компьютеров в локальном сегменте сети и позволит им взаимодействовать с интернет-узлами. ICS также предоставляет адреса DHCP-клиентам локального сегмента и заставляет их использовать ICS-компьютер как DNS-сервер. После включения ICS служба DNS-сервер на сервере ICS рекурсивно разрешает DNS-запросы, поступающие от локальных клиентов.

1. Войдите в систему Computerl *как Администратор* (Administrator).
2. Откройте папку **Сетевые подключения** (Network **Connections).**
3. Если подключение *MylSP'b* окне **Сетевые** подключения активно, щелкните его значок правой кнопкой и выберите **Отключить (Disconnect).**
4. После отключения щелкните правой кнопкой **MylSP** и выберите Свойства **(Properties).**
5. В окне **MylSP — свойства (MylSP Properties)** на вкладке Дополнительно (Advanced) в области **Общий доступ к подключению к Интернету (Internet Connection Sharing)** установите флажок **Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера (To connect through this computer's Internet connection).** Щелкните OK.

6. Прочитайте текст в окне **Сетевые подключения (Network Connections)** и щелкните Да (Yes). В этот момент компьютеру будет назначен IP-адрес *192.168.0.1.* Связь может временно нарушиться, пока система будет вносить изменения.
7. Выйдите из системы Computer2 и перезагрузите его.

Упражнение 2. Выполнение рекурсивных запросов

В этом упражнении вы воспользуетесь утилитой *Сетевой монитор* (Network Monitor) для записи DNS-запроса от Computer2. После выполнения рекурсивного запроса компьютером Computerl вы исследуете результаты записи и проверите, загружены ли новые записи в кэш DNS-сервера.

1. На Computerl установите интернет-подключение через *MylSP:*
2. Войдите в систему Computer2 как *Администратор* (Administrator) и откройте окно командной строки.
3. Исполните команду ipconfig /all. Служба ICS автоматически определит Computerl в качестве DNS-сервера компьютера Computer2. Иначе говоря, Computer2 направляет все DNS-запросы на Computerl.
4. Выполните команду ipconfig /flushdns, которая очистит кэш распознавателя и заставит Computer2 для разрешения DNS-имен обращаться к DNS-серверу.
5. На Computerl откройте *Сетевой монитор* (Network Monitor) и начните запись.
6. Вернитесь к Computer2 и запустите Internet Explorer. В окне с информацией об активизации усиленных средств безопасности отметьте флажок, чтобы это сообщение больше не появлялось, и щелкните OK.
7. В поле адреса Internet Explorer введите htpp : / / w w w . windowsupdate. c o m и нажмите Enter. Подключение должно пройти успешно.
8. Перейдите к Computerl и в окне **Сетевой монитор** щелкните кнопку **Закончить запись и отобразить данные (Stop and view capture).**
9. В окне **Запись данных: 1 (Сводка) [Capture: 1 (Summary)]** найдите и дважды щелкните первый DNS-кадр записи. Обратите внимание, что полное доменное имя, запрошенное в первой строке, — *www.windowsupdate.com.*
10. В центральной панели раскройте узел **DNS Flags.** Вы увидите ряд сообщений с флагами, Следует обращать внимание на сообщения с флагами 1 — именно они верны.
11. Ответьте, какие DNS-флаги установлены в 1? в 0? Флаг **Recursive Query Desired** означает, что при ответе на запрос DNS-сервер при необходимости осуществляет рекурсию.
12. Закройте *Сетевой монитор.* Не сохраняйте результаты записи или какие-либо записи в базе данных.
13. Откройте консоль *DNS.* (Если она уже открыта, закройте ее и вновь откройте.) В дереве консоли выберите значок **Computerl.**
14. В меню **Вид** (V i e w) выберите **Расширенный (Advanced).** В дереве консоли появится новая папка с именем **Котированные просмотры (Cached Lookups).**
15. Раскройте узлы **Каптированные просмотры** и **.(корень) [.(root)].** В папке **.(корень)** найдите запись с каноническим именем CNAME *www.windowsupdate.com.* Computerl выполнил рекурсию, чтобы ответить на рекурсивный запрос от Computer2. Служба DNS-сервера разместила в кэше записи, поступившие в ответ на этот запрос.
16. Выйдите из системы обоих компьютеров.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы заметили, что на компьютере *client 1* не удается получить эхо-ответ ping от компьютера *client2.lucernepublishing.com,* но если в этой команде указать IP-адрес, запрос выполняется успешно. Оказалось, что нет записи ресурса A для *client2.lucemepublishing.com,* и вы создали ее вручную. Что еще нужно сделать, чтобы успешно получить ответ на ping компьютера *client2.lucemepublishing.coml*
2. Как настроить изолированный сервер *Bingl* на динамическую регистрацию записи ресурса A в зоне *humongousinsurance.com,* не присваивая при этом компьютеру основной DNS-суффикс? (Предполагается, что в зоне *humongousinsurance.com* разрешены динамические обновления.)

Резюме

- Основной DNS-суффикс — это суффикс, при добавлении которого к имени узла образуется полное доменное имя.
- Полное имя, полученное за счет добавления к имени компьютера или узла DNS-суффикса подключения, назначается конкретному адаптеру компьютера. Этот суффикс задается на вкладке **DNS** окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settngs).**
- Разрешая неполные имена, служба DNS-клиента сначала добавляет основной DNS-суффикс к неполному имени и пытается разрешить полученное имя. При отрицательном результате DNS-клиент последовательно добавляет к неполному имени суффиксы подключений и повторно выполняет запросы. Если и это не помогает, служба DNS-клиента добавляет к имени родительский суффикс основного DNS-суффикса и выполняет еще один, последний запрос.
- По умолчанию DNS-клиенты под управлением Windows 2000/XP/Server 2003 динамически регистрируют и обновляют свои записи ресурсов в DNS. Клиенты со статическими IP-адресами обновляют записи ресурсов типов A и PTR, а получающие IP-адреса от DHCP-сервера обновляют только записи ресурсов A, а обновлением записей ресурсов PTR занимается DHCP-сервер. Чтобы DNS-клиент принудительно произвел регистрацию, выполняют команду Ipconfig /registerdns или перезагружают компьютер.
- Для просмотра кэша DNS-клиента служит команда ipconfig /displaydns, а для очистки кэша—ipconfig /flushdns.

Пример из практики

Вас пригласили в качестве консультанта в компанию Northwind Traders, штаб-квартира которой расположена в г, Берлингтоне, штат Вермонт. Произошло слияние Northwind Traders с фирмой Adventure Works, расположенной в г. Карибу, штат Мэн. В штаб-квартирах каждой из компаний есть офисная сеть с интегрированная с Active Directory зоной. Два офиса соединены выделенной линией с пропускной способностью 128 кбит/с (рис. 4-16).

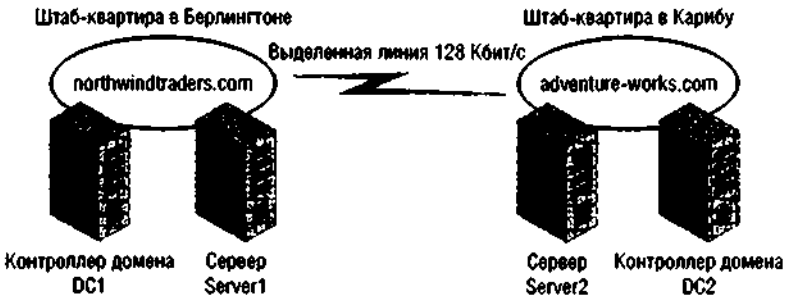


Рис. 4-16. Объединенные сети Northwind и AdventureWorks

1. **В** отношении каких серверов можно предположить, что они выполняют функцию DNS-серверов? Почему?
2. Пользователи обеих штаб-квартир жалуются, что не обеспечивается разрешение DNS-имен компьютеров другой штаб-квартиры. Какой DNS-сервер можно развернуть в каждом из офисов, чтобы исправить положение?
3. В Northwind Traders планируют открыть офис-сателлит в Берлингтоне, но не размещать в нем никаких зон. Предполагается, что пользователи этого офиса будут активно использовать Интернет для маркетинга и исследований. Что сделать, чтобы обеспечить максимальную производительность разрешения DNS-имен в этом офисе?

Практикум по устранению неполадок

На этом практикуме вы устраните неполадки разрешения имен на Computerl и Computer2.

1. Войдите в систему Computerl как *Администратор* (Administrator).
2. Из командной строки исполните nbtstat -R.
3. Исполните команду ping compute r2. Вы должны успешно получить эхо-ответ.
4. Обратитесь к описанию процедуры отключения разрешения имен NetBIOS в занятии 1 и на Computerl отключите NetBIOS на подключении по локальной сети.
5. Из командной строки исполните nbtstat -R.
6. Выполните команду ping computer2. На этот раз эхо-ответ получить не удастся.
7. Выполните команду ping computer2. domain 1. local. И эта попытка будет безуспешной.
8. Допустим, на Computerl работает DNS-сервер. Ответьте, почему не удается получить эхо-ответ на ping узла *computer2.domainl.local!*
9. Откройте новое окно командной строки Ц, выполните команду

   ```
   dnscmd . /Config ..AllZones /AllowUpdate 1
   ```

   Она включит динамическое обновление во всех зонах, обслуживаемых локальным DNS-сервером.
10. Войдите в систему Computer2 как *Администратор* (Administrator).
11. На Computer2 на вкладке **DNS** окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** подключения локальной сети установите флажок **Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in Registration).** Два раза щелкните OK, а затем — **Закрыть (Close).**

12. На Computer2 откройте новое окно командной строки и исполните ipconfig /registerdns.
13. Вернитесь к Computer!, откройте новое окно командной строки и исполните ping computer2. Эхо-ответа нет, так как в кэше локальной службы DNS-клиента сохранился отрицательный ответ на предыдущий запрос. Нужно очистить кэш, прежде чем удастся получить положительный ответ от выполнения команды ping.
14. На Computerl выполните команду ipconfig /flushdns.
15. На Computerl выполните ping computer2. Теперь эхо-ответ возвращается успешно.
16. Вновь включите NetBIOS для подключения по локальной сети на Computerl.
17. Выйдите из системы обоих компьютеров.

Ц Резюме главы

- В сетях Windows Server 2003 существуют две системы имен: DNS и NetBIOS. При разрешении имен компьютеров служба DNS-клиента в Windows Server 2003 всегда пытается сначала разрешить имя в DNS, а затем уже в NetBIOS.
- Имена и протокол DNS необходимы для нормальной работы доменов Active Directory и для совместимости с Интернетом и интрасетями. Длина имени DNS-узла не должна превышать 63 байта.
- Пространство имен DNS является иерархическим; в нем один корень, который может иметь любое количество поддоменов. Полное доменное имя (FQDN) — это DNS-имя узла сети в пространстве имен, указывающее на положение узла в иерархии по отношению к корню дерева доменов DNS, например *hostl.subdomain.microsoft.com.*
- Зона DNS — это непрерывная часть пространства имен, управляемая полномочным сервером. Сервер полномочный для нескольких зон, а зона может состоять из одного или более смежных поддоменов. DNS-сервер является полномочным для зоны, если он поддерживает базу данных зоны. Полномочные DNS-серверы делятся на основные и дополнительные. В каждой зоне DNS хранятся записи ресурсов, позволяющие ответить на любые запросы, относящиеся части пространства имен DNS данной зоны.
- в В процессе разрешения имен служба DNS-клиента (или распознавателя) сначала обращается к локальному кэшу. Если найти нужное имя не удается, распознаватель запрашивает DNS-сервер. Если DNS-сервер не в состоянии разрешить имя на основе своих полномочных записей или информации кэша, он выполняет рекурсивные запросы от лица клиента.
- Рекурсия — процесс, в котором DNS-сервер запрашивает другие серверы от имени DNS-клиента. Чтобы правильно выполнить рекурсию, сервер должен знать, где начать поиск имен в пространстве имен bNS. Такую информацию он берет из файла корневых ссылок *Cache, dns,* который хранится на компьютере сервера.
- Сервер кэширования пересылает запросы другим DNS-серверам и не поддерживает базу зонных данных. Однако он кэширует ответы от других DNS-серверов и таким образом повышает быстродействие разрешения имен в сети, в которой нет зон.
- Новые зоны содержат только две записи ресурсов: начальную запись данной зоны (SOA) и запись сервера имен (NS), относящуюся к DNS-серверу, обслуживающему эту зону. Далее в зону добавляют дополнительные записи ресурсов. Наиболее распространены записи ресурсов следующих типов: адреса узла (A), каноническое имя (CNAME), почтовый обменник (MX), локатор службы (SRV) и указатель (PTR).

я По умолчанию DMS-клиенты под управлением Windows 2000/XP/Server 2003 динамически регистрируют и обновляют свои записи ресурсов в DNS. Клиенты со статическими IP-адресами обновляют записи ресурсов типов A и PTR, а получающие IP-адрес средствами DHCP обновляют только записи ресурсов A — обновление записей ресурсов PTR берет на себя DHCP-сервер. Для принудительной динамической регистрации-DNS-клиент служит команда ipconfig /registerdns (или перезагрузка компьютера).

- Просмотр кэша DNS-клиента выполняется командой ipconfig /displaydns, аочистка кэша — командой ipconfig /flushdns.

Л Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Нужно запомнить последовательность операций при разрешении имен службой DNS-клиента, а также понимать место кэша DNS-клиента, кэша DNS-сервера и рекурсии в этих операциях.
- Необходимо понимать функции записей ресурсов типов: A, PTR, CNAME, MX и SRV.
- Надо понимать разницу между основной и дополнительной зонами, а также зоной-заглушкой.
- Требуется знать, зачем нужен файл *Cache.dns.*

ш **Нужно** разбираться, когда и зачем используются команды: Nbtstat -c, Nbtstat -R, Ipconfig /displaydns,Ipconfig /flushdns и Ipconfig /registerdns.

в Необходимо знать преимущества серверов кэширования.

и Нужно понимать, какие DNS-клиенты поддерживают динамические обновления DNS, какие записи обновляют по умолчанию DHCP-клиенты и клиенты, не использующие DHCP. Наконец, надо знать параметры окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** и как они влияют на динамическое обновление.

Основные термины

NetBIOS — API-интерфейс, служащий в более ранних сетях Microsoft для связи и взаимодействия между компьютерами. Система именования и разрешение имен — лишь две из множества служб NetBIOS.

Полное доменное имя ~ Fully Qualified Domain Name, FQDN — DNS-имя, уникально идентифицирующее компьютер в сети. Пример: *clientl.microsoft.com.*

Рекурсий ~ recursion — процесс, в котором DNS-сервер направляет запрос на разрешение имени другим DNS-серверам от имени DNS-клиента.

Рекурсивный запрос ~ recursive query — запрос клиента, требующего от сервера выполнить рекурсию.'

Зона-заглушка ~ stub zone — копия зоны, содержащая только записи ресурсов, указывающие на полномочные DNS-серверы для главной зоны.

Вопросы и ответы

Занятие 1. Лабораторная работа

9. Обратите внимание на протоколы, присутствующие в зафиксированных кадрах. В окне **Сетевой монитор (Network Monitor)** NBT обозначает протокол NetBT, а DNS — протокол DNS. На основе протоколов и описания записанных данных определите, какой из методов разрешения имен использован для разрешения имени Computer2 — DNS или NetBIOS. Почему использован именно этот метод, а не другой?
Правильный ответ: использовано разрешение имен NetBIOS, поскольку, хотя Windows Server 2003 и должно поддерживаться разрешение DNS-имен, в данной сети еще не сконфигурирован DNS-сервер и служба DNS недоступна. В таких случаях Windows Server 2003 для разрешения имен компьютеров в IP-адреса применяет протокол NetBT и механизм NetBIOS.

Занятие 1. Закрепление материала

1. Вы администратор сети из 10 компьютеров с Windows Server 2003 и 200 компьютеров с Microsoft Windows XP Professional. В сети установлен DNS-сервер DNS1, обслуживающий зону *lucernepublishing.com.* Зона также настроена на возможность динамического обновления. DHCP-сервер отвечает за определение IP-конфигурации всех компьютеров под управлением Windows XP Professional. Один из этих компьютеров, *cl.lucemepublishing.com,* доступен только по IP-адресу, но не по имени. Как зарегистрировать этот компьютер в DNS (выберите из списка)?
   a. Выполнить команду Nbtstat -R.
   b. Выполнить команду Ipconfig /registerdns.
   c. Выключить и перезагрузить *cl.lucemepublishing.com.*
   й. Выполнить команду Nbtstat /registerdns.
   Правильные ответы: Ь, **с**
2. Что из нижеперечисленного является корректным NetBIOS-именем компьютера?
   a. *hostl.microsoft.com.*
   b. hostl_local.
   c. *hostlOjnicrosoft.*
   d. *hostl-microsoft.*
   Правильный ответ: b
3. Какую команду применяют для очистки локального кэша NetBIOS-имен?
   Правильный ответ: Nbtstat -R.

Занятие 2. Закрепление материала

1. Вы администратор сети с основным DNS-сервером, полномочным для зоны *lucernepublishing.com.* Вы также установили два сервера кэширования, которые пересылают все запросы основному серверу. Большая часть запросов, поступающих на серверы кэширования, касается имен внутри домена *lucernepublishing.com.* Какой параметр основного сервера следует изменить, чтобы сократить трафик запросов DNS между серверами кэширования и основным сервером?
   Правильный ответ: можно увеличить время жизни (TTL) записей ресурсов на зоны.

2. Какой домен является коренным для пространства имен с FQDN *first.domainl.local.?*
   a. Никакой: у этого пространства имен нет корневого домена.
   b. *domain 1.*
   c. *local.*
   d. "" (пустая строка).

   Правильный ответ: d. '
3. Что делает распознаватель в первую очередь при разрешении DNS-имени?
   a. Проверяет локальный кэш.
   b. Считывает файл *Hosts.*
   c. Выполняет широковещание в локальной подсети.
   d. Направляет запрос на локальный DNS-сервер.

   Правильный ответ: a.
4. Компьютеры сети включены после перерыва в электроснабжении. DNS-клиент обращается с рекурсивным запросом на локальный DNS-сервер, пытаясь разрешить Интернет-имя, для которого данный сервер не является полномочным. Что происходит в первую очередь?
   a. DNS-клиент разрешает имя на основании информации из собственного кэша.
   b. DNS-сервер разрешает имя на основании информации из собственного кэша.
   c. DNS-сервер пересылает рекурсивный запрос вышестоящему DNS-серверу.
   d. DNS-сервер обращается к корневым серверам, указанным в файле *Cache.dns.*

   Правильный ответ: *A.*

Занятие 3. Закрепление материала

1. Вы только что обновили запись ресурса узла сети. Какую еще запись ресурса, связанную с первой, нужно обновить?

   Правильный ответ: запись указателя PTR, относящуюся к этому же узлу.
2. На DNS-сервере не удается выполнить рекурсивный тест. Допустим, что несмотря на это сервер успешно взаимодействует с другими DNS-серверами. Назовите две возможные причины такого поведения.

   Правильный ответ: DNS-сервер настроен как корневой сервер либо файл корневых сл лок неправильно сконфигурирован.
3. Какая запись ресурса используется для разрешения доменных имен, указываемых в адресах электронной почты, в IP-адрес связанного с доменом почтового сервера?
   a. PTR.
   b. MX.
   c. A.
   d. CNAME.

   Правильный ответ: Ь.
4. На новом DNS-сервере создается зона "", а затем — подцомены этого корневого домена. Какая функция будет недоступна этому серверу?
   a. Сервер не сможет кэшировать имена.
   b. Сервер сможет работать только как сервер пересылки.
   c. Сервер не сможет разрешать имена из Интернета.
   d. Сервер не сможет подключиться к Интернету.

   Правильный ответ: c.

Занятое 4. Лабораторная работа 1. Упражнение 2

3. Ответьте на вопрос: как изменился суффикс в листинге результатов работы команды ping?

   Правильный ответ: до получения ICMP-отклика сообщение команды ping'выглядит так: Обмен пакетами с computerl.domain!.local [192.168.0.1] с 32 байт данных: (Pinging computerl. domainl.local [192.168.0.1] with 32 bytes of data:).

Занятие 4. Закреплению материала

1. Вы заметили, что на компьютере *client 1* не удается получить эхо-ответ ping от компьютера *client2.lucemepublishing.com,* но если в этой команде указать IP-адрес, запрос выполняется успешно. Оказалось, что нет записи ресурса A для *client2.lucemepublishing.com,* и вы создали ее вручную. Что еще нужно сделать, чтобы успешно получить ответ на ping компьютера *ctient2Jucernepublishing.com".*

   Правильный ответ: на *client 1* нужно выполнить команду Ipconfig /flushdns, чтобы очистить кэш и удалить из него отрицательный ответ. .

2. Как настроить изолированный сервер *Bing]* на динамическую регистрацию записи ресурса A в зоне *humongousimurance.com,* не присваивая при этом компьютеру основной DNS-суффикс? (Предполагается, что в зоне *humongousinsurance.com* разрешены динамические обновления.)

   Правильный ответ: в окне Дополнительные параметры TCP/IP (Advanced TCP/IP Settings) задайте DNS-суффикс подключения *hv.mongoiisinsurance.com,* я затем установите флажок, предписывающий использовать суффикс подключения при регистрации в DNS. Наконец, определите IP-адрес основного DNS-сервера зоны *humongousmsumnce.com,* как основной (предпочтительный) DNS-сервер для *Bingl.*

Пример из практики

1. В отношении каких серверов можно предположить, что они выполняют функцию DNS-серверов? Почему?

   Правильный ответ: DC1 и DC2. Зоны, интегрированные с Active Directory, должны размещаться на контроллерах домена.

2. Пользователи обеих штаб-квартир жалуются, что не обеспечивается разрешение DNS-имен компьютеров другой штаб-квартиры. Какой DNS-сервер можно развернуть в каждом из офисов, чтобы исправить положение?

   Правильный ответ: в каждой из штаб-квартир развернуть дополнительный сервер с полномочной информацией удаленной зоны, интегрированной с Active Directory?

3. В Northwind Traders планируют открыть офис-сателлит в Берлингтоне, но не размещать в нем никаких зон. Предполагается, что пользователи этого офиса будут активно использовать Интернет для маркетинга и исследований. Что сделать, чтобы обеспечить максимальную производительность разрешения DNS-имен в этом офисе?
   Правильный ответ: для увеличения эффективности разрешения DNS-имен рекомендуется развернуть DNS-сервер кэширования.

Практикум п о устранению неполадок

8. Допустим, на Computerl работает DNS-сервер. Ответьте, почему не удается получить эхо-ответ на ping узла *computer2.domain I. local?*

   Правильный ответ: в зоне *domainl.local* нет записи ресурса A, указывающей на Computer2.

Развертывание инфраструктуры DNS

Темы экзамена

- Настройка DNS-сервера.
- Настройка параметров DNS-зон.
- Настройка пересылки DNS.
- Управление параметрами DNS-зон.
- Управление параметрами DNS-сервера.

В этой главе

Система доменных имен (Domain Name System, DNS) — слишком важный элемент сетевой инфраструктуры, чтобы просто развернуть ее на одном сервере и забыть. В средних и крупных организациях DNS должна пронизывать всю сеть и постоянно обновляться. На. сетевых администраторах лежит ответственность за поддержку этой инфраструктуры — задача, которая требует понимания таких нюансов, как зонные передачи, делегирование, зоны-заглушки, циклическое обслуживание и расстановка по адресу. Материал этой главы исключительно важен, поэтому чаще других встречается в вопросах экзамена.

В этой главе описываются основные параметры конфигурации DNS-серверов и зон, большая часть которых доступна для просмотра и изменения в окнах свойств серверов и зон. Кроме того, здесь рассказывается, как и зачем реализуют делегирование и зоны-заглушки в сетях Windows Server 2003.

Прежде всего

Для изучения материалов этой главы вам потребуется:

- два физически объединенных в сеть компьютера с именами Computer 1 и Computer2 и установленной на них ОС Windows Server 2003. Компьютеру Computerl следует назначить статический адрес 192.168.0.1/24, а Computer^ — настроить на автоматическое получение адреса. На Computer2 надо определить альтернативную конфигурацию с адресом 192.168.0.2/24. На обоих компьютерах следует задать основной DNS-суффикс *domain 1.local;*
- *и* телефонная линия и учетная запись у интернет-провайдера для доступа по телефонной линии (если будет использоваться выделенное подключение, ему надо назначить имя MylSP, при этом, возможно, потребуется внести коррективы в упражнения);
- установить на компьютере Computerl подкомпонент *Средства сетевого монитора* (Network Monitor Tools) компонента *Средства управления и наблюдения* (Management and Monitoring Tools). Файл журнала с именем Name Resolution 1 следует сохранить в папке *Мои документы\Мои записи* (My Documents\My Captures) на Computerl. Эта запись данных, созданная до развертывания DNS в сети, позволит получить сведения о сетевом трафике после выполнения команды Ping compute r2 на Computerl;
- установить подкомпонент *DNS* компонента *Сетевые службы* (Networking Services). После установки на DNS-сервере создается основная зона прямого просмотра по имени *domain 1.local,* а также основная зона обратного просмотра, соответствующая пространству имен 192.168.0.0/24. Обе зоны настраиваются на прием безопасных и небезопасных обновлений. В зоне *domain 1.local* должны существовать записи ресурсов А, соответствующие компьютерам Computerl и Computer2;
- установить на Computerl набор *Средства поддержки Windows* (Windows Support Tools);
- создать удаленное подключение к Интернету с именем MylSP на Computerl и разрешить общий доступ к этому подключению (ICS). После включения ICS компьютер Computer2 должен получить обновленную конфигурацию IP. (Если вместо учетной записи доступа по телефонной линии используется выделенное подключение к Интернету, сконфигурируйте выделенное подключение в соответствии с описанными выше требованиями.);
- установить флажок **Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in DNS registration)** на вкладке **DNS** окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** подключения **Подключение по локальной сети (Local Area Connection)** на компьютере Computer2.

Занятие 1. Настройка параметров DNS-сервера

После установки DNS-сервер настраивают в соответствии потребностями компании. На этом занятии обсуждаются параметры, которые конфигурируются в окне свойств сервера в консоли *DNS.* Имейте в виду, что действие этих параметров распространяется не на одну зону, а на сервер в целом.

Изучив материал этого занятия, вы сможете:

- сконфигурировать DNS-сервер для прослушивания запросов, поступающих на конкретные сетевые адаптеры;
- сконфигурировать DNS-сервер для пересылки всех или части DNS-запросов на вышестоящий DNS-сервер;
- определить, когда необходимо изменять корневые ссылки.

Продолжительность занятия — около 45 минут.

Общие сведения о вкладках окна свойств DNS-сервера

Это окно позволяет настроить параметры, действие которых распространяется на DNS-сервер и все размещенные на нем зоны. Чтобы открыть окно свойств DNS-сервера, в дереве консоли *DNS* щелкните нужный DNS-сервер правой кнопкой и выберите **Свойства (Properties)** (рис. 5-1).

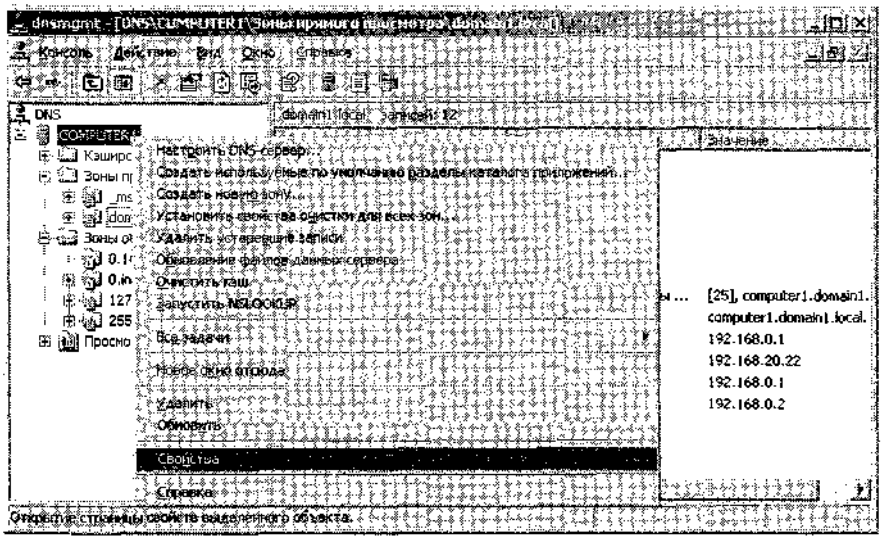


Рис. 5-1. Открытие окна свойств DNS-сервера

Окно свойств DNS-сервера содержит восемь вкладок, подробно описанных ниже.

Вкладка *Интерфейсы*

На вкладке **Интерфейсы (Interfaces)** указывается, на каком из своих IP-адресов DNS-сервер должен принимать DNS-запросы. Например, на многоадресном DNS-сервере с одним IP-адресом для локальной сети и другим — для Интернета, можно запретить обслуживать DNS-запросы, поступающие не из локальной сети. Для этого DNS-сервер настраивают на прослушивание только внутреннего IP-адреса компьютера (рис. 5-2).

По умолчанию параметры на данной вкладке разрешают DNS-серверу прослушивать все IP-адреса, назначенные локальному компьютеру.

Прежде всего

Для изучения материалов этой главы вам потребуется:

- два физически объединенных в сеть компьютера с именами Computerl и Computer2 и установленной на них ОС Windows Server 2003. Компьютеру Computerl следует назначить статический адрес 192.168.0.1/24, а Computer2 — настроить на автоматическое получение адреса. На Computer2 надо определить альтернативную конфигурацию с адресом 192.168.0.2/24. На обоих компьютерах следует задать основной DNS-суффикс *domain 1.local;*
- телефонная линия и учетная запись у интернет-провайдера для доступа по телефонной линии (если будет использоваться выделенное подключение, ему надо назначить имя MylSP, при этом, возможно, потребуется внести коррективы в упражнения);
- установить на компьютере Computerl подкомпонент *Средства сетевого монитора* (Network Monitor Tools) компонента *Средства управления и наблюдения* (Management and Monitoring Tools). Файл журнала с именем Name Resolution 1 следует сохранить в папке *Мои документы\Мои записи* (My Documents\My Captures) на Computerl. Эта запись данных, созданная до развертывания DNS в сети, позволит получить сведения о сетевом трафике после выполнения команды Ping computer2 на Computerl;
- установить подкомпонент *DNS* компонента *Сетевые службы* (Networking Services). После установки на DNS-сервере создается основная зона прямого просмотра по имени *domain I. local,* а также основная зона обратного просмотра, соответствующая пространству имен 192.168.0.0/24. Обе зоны настраиваются на прием безопасных и небезопасных обновлений. В зоне *domain 1.local должны* существовать записи ресурсов А, соответствующие компьютерам Computerl и Computer2;
- установить на Computerl набор *Средства поддержки Windows* (Windows Support Tools);
- создать удаленное подключение к Интернету с именем MylSP на Computerl и разрешить общий доступ к этому подключению (ICS). После включения ICS компьютер Computer2 должен получить обновленную конфигурацию IP. (Если вместо учетной записи доступа по телефонной линии используется выделенное подключение к Интернету, сконфигурируйте выделенное подключение в соответствии с описанными выше требованиями.);
- установить флажок **Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in DNS registration)** на вкладке **DNS** окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** подключения **Подключение по локальной сети (Local Area Connection)** на компьютере Computer2.

Занятие 1. Настройка параметров DNS-сервера

После установки DNS-сервер настраивают в соответствии потребностями компании. На этом занятии обсуждаются параметры, которые конфигурируются в окне свойств сервера в консоли *DNS.* Имейте в виду, что действие этих параметров распространяется не на одну зону, а на сервер в целом.

Изучив материал этого занятия, вы сможете:

- *S* сконфигурировать DNS-сервер для прослушивания запросов, поступающих на конкретные сетевые адаптеры;
- *S* сконфигурировать DNS-сервер для пересылки всех или части DNS-запросов на вышестоящий DNS-сервер;
- *S* определить, когда необходимо изменять корневые ссылки.

Продолжительность занятия — около 45 минут.

Общие сведения о вкладках окна свойств DNS-сервера

Это окно позволяет настроить параметры, действие которых распространяется на DNS-сервер и все размещенные на нем зоны. Чтобы открыть окно свойств DNS-сервера, в дереве консоли *DNS* щелкните нужный DNS-сервер правой кнопкой и выберите **Свойства (Properties)** (рис. 5-1).

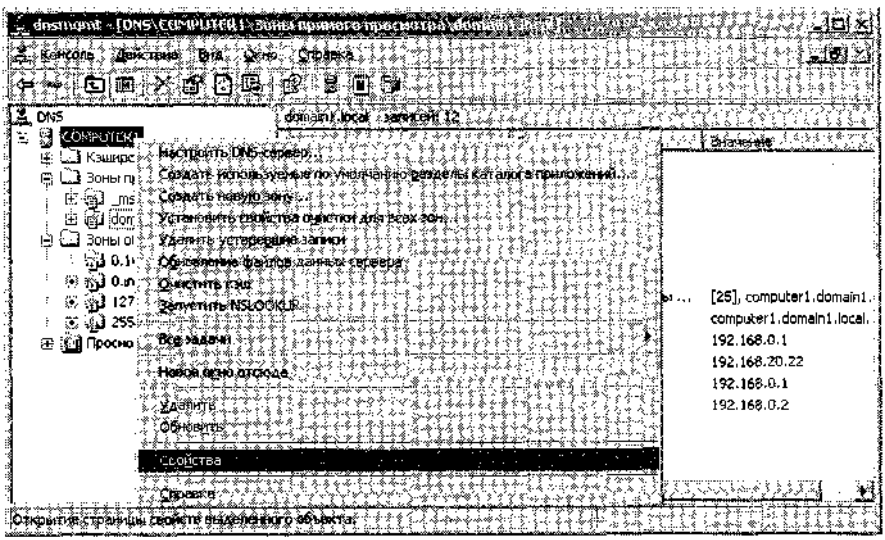


Рис. 5-1. Открытие окна свойств DNS-сервера

Окно свойств DNS-сервера содержит восемь вкладок, подробно описанных ниже.

Вкладка *Интерфейсы*

На вкладке **Интерфейсы (Interfaces)** указывается, на каком из своих IP-адресов DNS-сервер должен принимать DNS-запросы. Например, на многоадресном DNS-сервере с одним IP-адресом для локальной сети и другим — для Интернета, можно запретить обслуживать DNS-запросы, поступающие не из локальной сети. Для этого DNS-сервер настраивают на прослушивание только внутреннего IP-адреса компьютера (рис. 5-2).

По умолчанию параметры на данной вкладке разрешают DNS-серверу прослушивать все IP-адреса, назначенные локальному компьютеру.

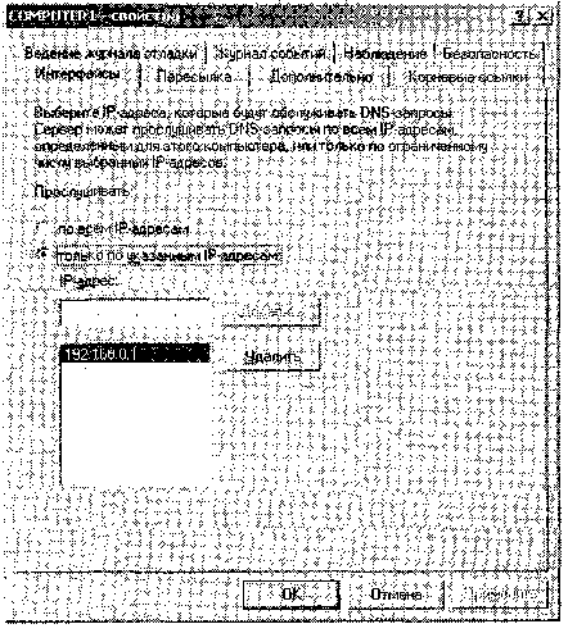


Рис. 5-2. Вкладка *Интерфейсы*

Вкладка *Пересылка*

Вкладка **Пересылка (Forwarders)** позволяет перенаправлять DNS-запросы, поступающие на локальный DNS-сервер, на вышестоящие DNS-серверы, называемые *серверами пересылки* (forwarders). Здесь также указывают IP-адреса пересылки, а также доменные имена, при наличии которых в поле адреса запрос подлежит пересылке. Например, на рис. 5-3 все запросы в адрес домена *lucernepublishing.com* должны пересылаться на DNS-сервер 207.46.132.23. После получения ответа на запрос, переправленный на адрес 207.46.132.23, локальный сервер пересылки перешлет его клиенту, от которого поступил исходный запрос. Такой процесс называется *условной пересылкой* (conditional forwarding).

В любом случае DNS-сервер прибегает к пересылке только в случае неспособности разрешить запрос с применением собственных полномочных данных (данных основной или дополнительной зон) или данных в кэше.

Совет Чтобы указать срок ожидания сервером пересылки ответа от другого такого же сервера, введите нужное значение в поле **Время ожидания пересылки (сек) (Number of seconds before forward queries time out).** Значение по умолчанию — 5.

Использование пересылки

Иногда требуется запретить DNS-серверам напрямую взаимодействовать с внешними серверами. Например, если организация подключена к Интернету по медленному WAN-каналу, повысить эффективность разрешения имен можно перенаправлением всех DNS-запросов через один сервер пересылки (рис. 5-4). Кэш сервера DNS-сервера пересылки будет наполняться информацией и избавлять от лишних запросов на разрешение одних и тех же имен.

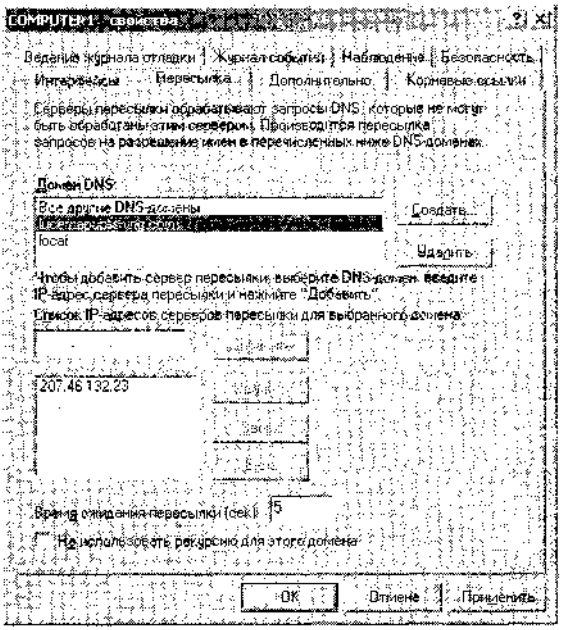


Рис. 5-3. Вкладка *Пересылка*

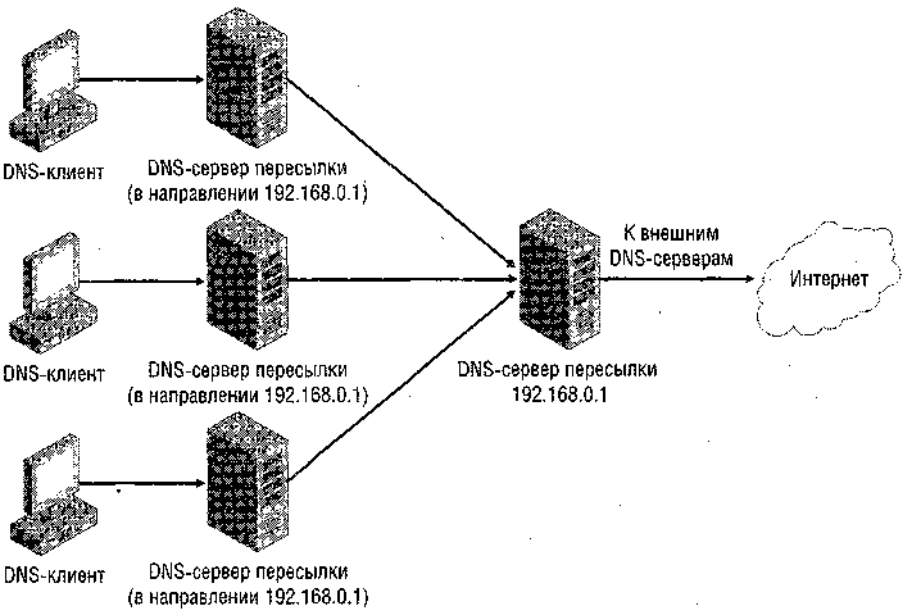


Рис. 5-4. Использование пересылки для консолидации кэширования

Другое стандартное применение пересылки — предоставить DNS-клиентам и серверам в защищенной брандмауэром сети возможность безопасно разрешать внешние имена. Если DNS-серверу или пользователям внутренней сети разрешить направлять ите-

ративные запросы внешним DNS-серверами, придется открыть на брандмауэре DNS-порты, что небезопасно. Однако, настроив внутренний DNS-сервер на пересылку внешних запросов единственному серверу пересылки, расположенному за брандмауэром, и открыв на брандмауэре только один порт, по которому обмениваются эти серверы, вы сможете организовать полноценное разрешение имен, не открывая сеть для доступа внешних серверов (рис. 5-5).

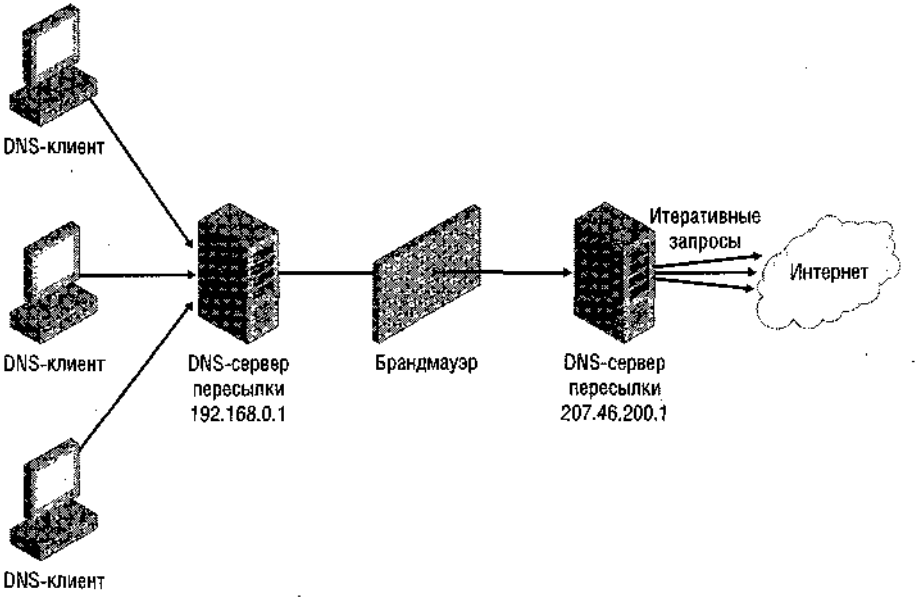


Рис. 5-5. Защищенный обмен итеративными запросами между серверами пересылки

Отключение рекурсии

Вкладка **Пересылка** позволяет запретить рекурсию при запросах определенного домена, пересылаемых на вышестоящий сервер. При включенной рекурсии (по умолчанию), если сервер пересылки не сумел разрешить полное доменное имя (FQDN), запрос передается на локальный DNS-сервер. Это позволяет повысить отказоустойчивость: если вышестоящий сервер пересылки недоступен, разрешение имен берет на себя локальный DNS-сервер.

Однако если в такой конфигурации по умолчанию сервер пересылки доступен, но не в состоянии разрешить запрос, последующая рекурсия и переход к локальному DNS-серверу обычно излишни и вызывают ненужную задержку при возвращении клиенту негативного ответа. Таким образом, отключение рекурсии при запросах, которые в соответствии с конфигурацией подлежат пересылке, сокращает время предоставления отрицательных ответов, но только в ущерб отказоустойчивости.

В ситуации, когда серверы пересылки сконфигурированы на пересылку, а рекурсия отключена, локальный DNS-сервер называется *ведомым* (slave), потому что при невозможности разрешить запрос самостоятельно он полностью полагается на сервер пересылки.

Вкладка *Дополнительно*

Вкладка **Дополнительно (Advanced),** показанная на рис. 5-6, позволяет включать, отключать и настраивать некоторые функции DNS-сервера, в том числе рекурсию, *циклическое обслуживание* (round robin), механизм устаревания и очистки и расстановку по адресу (см. занятие 3).

Примечание На вкладке **Пересылка** рекурсия отключается для определенных запросов доменов, а вкладка **Дополнительно** позволяет отключать рекурсию для всех запросов, поступающих на локальный DNS-сервер.

Примечание Отключение рекурсии на вкладке **Дополнительно** DNS-сервера делает невозможным доступ к серверам пересылки, поэтому вкладка **Пересылка** становится неактивной.

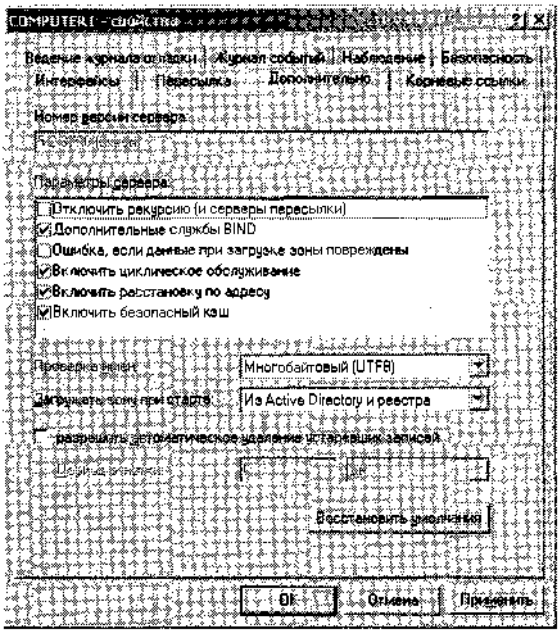


Рис. 5-6. Вкладка *Дополнительно*

Вкладка *Корневые ссылки*

Вкладка **Корневые ссылки (Root Hints),** показанная на рис. 5-7, содержит копию информации, хранящейся в файле *WINDOWS\System32\Dns\Cache.dns.* На DNS-серверах, обслуживающих запросы имен Интернета, эту информацию менять не надо. Однако если определить в частной сети корневой DNS-сервер (с именем «.»), придется полностью удалить файл *Cache.dns.* (На корневом DNS-сервере вкладка **Корневые ссылки** недоступна.)

Кроме того, на DNS-сервере в крупном частном пространстве имен можно использовать эту вкладку для удаления ссылок на корневые серверы Интернета и определения корневых серверов частной сети.

Примечание Раз в несколько лет список корневых серверов в Интернете слегка изменяется. В *Cache.dns* указано и так очень много доступных корневых серверов, поэтому нет особой необходимости после незначительных изменений немедленно обновлять файл корневых ссылок. Однако иногда это делать придется. Последнее известное нам обновление списка состоялось 5 ноября 2002 г. Самая свежая версия есть на сайте *ftp://rs.internic.net/domain/named.cache*.

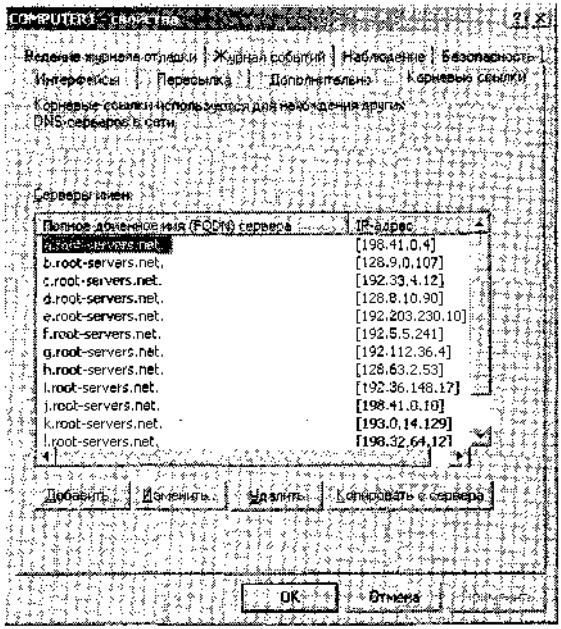


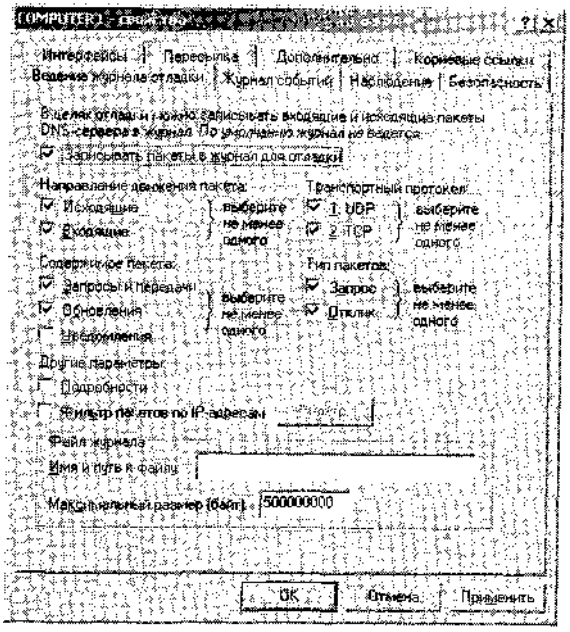
Рис. 5-7. Вкладка *Корневые ссылки*

Вкладка *Ведение журнала отладки*

Вкладка **Ведение журнала отладки (Debug Logging)** (рис. 5-8) позволяет определять порядок ведения журнала отладки DNS-сервера. Эта информация исключительно полезна для устранения неполадок сервера. Поскольку запись всех пакетов потребует слишком много ресурсов, на этой вкладке можно выбрать, какие пакеты регистрировать: пакеты определенного транспортного протокола, с определенным IP-адресом в поле источника, определенного направления или типа (см. занятие 1 главы 6).

Вкладка *Журнал событий*

Журнал событий DNS можно просматривать в узле **Просмотр событий (Event Viewer)** консоли *DNS*.



На вкладке **Журнал событий (Event Logging)** (рис. 5-9) определяют, какие события должны регистрироваться в журнале событий **DNS:** лишь ошибки или ошибки и предупреждения. Можно также полностью отключать регистрацию событий DNS. Для более сложной фильтрации событий **DNS** служит вкладка **Фильтр (Filtering)** окна **Свойства: События DNS (DNS Events Properties).** Чтобы его открыть, щелкните узел **Просмотр событий** в дереве консоли *DNS* правой кнопкой и выберите **Свойства (Properties).**

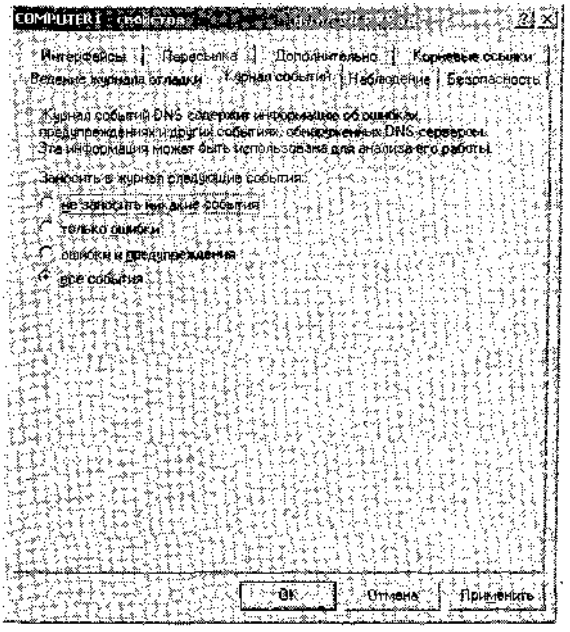


Рис. 5-9. Вкладка *Журнал событий*

Вкладка *Наблюдение*

Вкладка **Наблюдение (Monitoring)** служит для проверки работы DNS с помощью двух простых тестов. Первый — это запрос локального DNS-сервера. Для успешного выполнения этого теста серверу достаточно ответить на запросы прямого и обратного разрешения на основании собственной базы данных.

Второй тест — рекурсивный запрос корневого DNS-сервера. DNS-сервер должен «суметь» подключиться к корневым серверами, указанными на вкладке **Корневые ссылки (Root Hints).**

Вкладка **Наблюдение** (рис. 5-10) также позволяет задавать график автоматического выполнения этих тестов. Результаты тестов — запущенных вручную или автоматически — отображаются в области **Результаты теста (Test Results).**

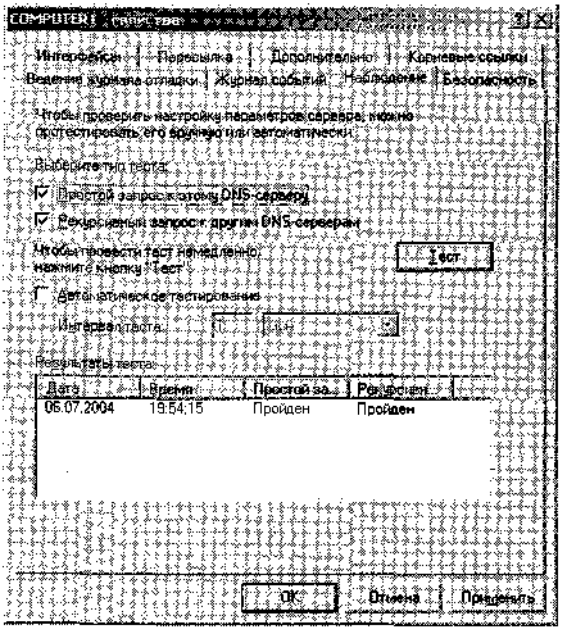


Рис. 5-10. Вкладка *Наблюдение*

Вкладка *Безопасность*

Вкладка **Безопасность (Security)** (рис. 5-11) отображается, только если DNS-сервер одновременно выполняет функции контроллера домена. Здесь определяют пользователей, которым предоставляется право просматривать, конфигурировать и изменять параметры самого DNS-сервера и его зон. Окно, открываемое щелчком кнопки **Дополнительно (Advanced),** позволяет более точно определить разрешения DNS-сервера.

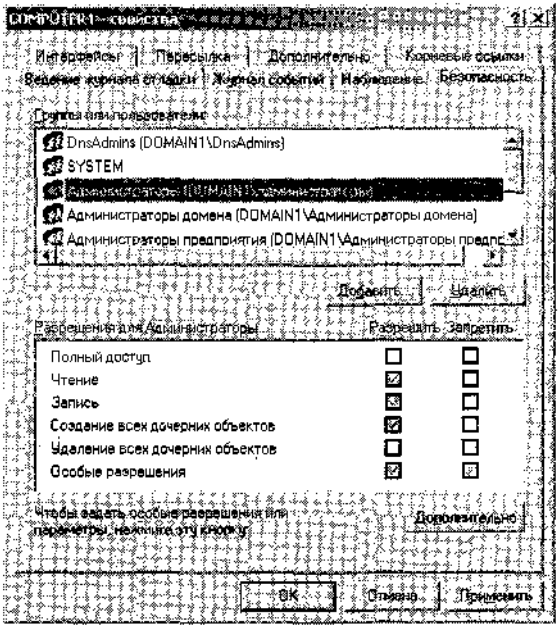


Рис. 5-11. Вкладка *Безопасность*

Лабораторная работа 1. **Сравнение трафика разрешения в NetBIOS и DNS**

На этой лабораторной работе вы запишете трафик разрешения имен и сравните запись с результатом аналогичной записи, выполненной на занятии 1 главы 4.

Упражнение 1. Запись трафика разрешения имен

Средствами *Сетевого монитора* (Network Monitor) вы запишете трафик разрешения имен при запросе с Computer2 и затем сравните результат с содержимым файла, уже записанного на Computerl.

1. Войдите в систему Computer2 как *Администратор* (Administrator).
2. Установите *Сетевой монитор* (Network Monitor) на Computer2, как описано в занятии 1 главы 3.
3. Откройте окно **Сетевой монитор (Network Monitor).**
4. Если отроется окно с предложением выбрать сеть, щелкните OK. В окне **Выбор сети (Select a Network)** настройте сетевой монитор на регистрацию трафика локальной сети.
5. Щелкните кнопку **Начать запись данных (Start Capture).**
6. Следующие операции заставят Computer2 связаться с Computerl с запросом на разрешение имен.

   Выполните команду `nbtstat -R` — она удалит из кэша информацию о соответствии NetBIOS-имен.

   Выполните команду `ipconfig /flushdns`, чтобы удалить из кэша информацию о соответствии DNS-имен.

Выполните команду ping compute r1. Вы должны получить эхо-ответ. Обратите внимание, что в листинге работы команды суффикс *domain 1. local* добавляется к *computerl.*

7. Вернитесь в окно **Сетевой монитор** и щелкните **Закончить запись и отобразить данные (Stop and View Capture).** Откроется окно **Запись данных (Capture)** с информацией о только что записанных кадрах.
8. Сохраните результаты записи трафика в папке *Мои документы\Мои записи* (My Documents\My Captures) в файле с именем Name Resolution 2.
9. Сравните трафик, записанный в файлах Name Resolution 1 и Name Resolution 2. Ответьте на следующие вопросы.

   Каково основное различие между записями?

   Чем объясняется различие в методах разрешения имен?
10. Закройте все открытые окна на Computerl и Computer2. Отклоните все предложения сохранить открытые файлы.
11. Выйдите из системы Computerl и Computer2.

Лабораторная работа 2. **Проверка записи ресурса-службы SRV в DNS, соответствующей Active Directory**

После первичной установки службы каталогов Active Directory надо убедиться, что установщик создал запись ресурса-службы (SRV) в DNS. Вы создадите домен Active Directory, повысив роль Computerl до контроллера домена, а затем средствами консоли *DNS* проверите наличие соответствующей записи ресурса SRV *domain 1.local,* нового домена Active Directory. Наконец, вы присоедините Computer2 к новому домену.

Упражнение 1. Установка Active Directory

В этом упражнении вы установите Active Directory и повысите роль Computerl до контроллера нового домена.

1. Войдите в систему Computerl *как Администратор* (Administrator).
2. Отключите Computerl от Интернета.
3. Щелкните **Пуск ^агт)\Администрирование (Administrative Too1в)\Управление данным сервером (Manage Your Server).**
4. **В** окне **Управление данным сервером (Manage Your Server)** щелкните **Добавить или удалить роль (Add or Remove a Role).**
5. На странице **Предварительные шаги (Preliminary Steps)** мастера щелкните **Далее (Next).**
6. На странице **Роль сервера (Server Role)** в списке выберите **Контроллер домена (Active Directory) [Domain Controller (Active Directory)]** и щелкните **Далее.**
7. Проверьте выбор на странице **Сводка выбранных параметров (Summary of Selections)** и щелкните **Далее.**
8. На странице приглашения **Мастера установки Active Directory (Active Directory Installation Wizard)** щелкните **Далее.**
9. Прочитайте текст на странице **Совместимость операционных систем (Operating System Compatibility)** и ответьте на вопрос.

   Какое ограничение налагается на клиентов под управлением Microsoft Windows 95 и Microsoft Windows NT 4 SP3 или более ранней версии?
10. Щелкните **Далее.** На странице **Тип контроллера домена (Domain Controller Type)** оставьте вариант по умолчанию — **Контроллер домена в новом домене (Domain Controller for a New Domain)** и щелкните **Далее.**

11. На странице **Создать новый домен (Create New Domain)** оставьте вариант по умолчанию — **Новый домен в новом лесу (Domain in a New Forest)** и щелкните **Далее.**
12. На странице **Новое имя домена (New Domain Name)** ведите полное DNS-имя нового домена — domainl. local и щелкните **Далее.**
13. На странице **NetBIOS-имя домена (NetBIOS Domain Name)** оставьте имя **DOMAIN1** без изменений и щелкните **Далее.**
14. На странице **Папки базы данных и журналов (Database and Log Folders)** оставьте параметры по умолчанию и щелкните **Далее.**
15. На странице **Общий доступ к системному тому (Shared System Volume)** оставьте параметры по умолчанию и щелкните **Далее.**
16. На странице **Диагностика регистрации DNS (DNS Registration Diagnostics)** ознакомьтесь с результатами диагностики и щелкните **Далее.**
17. На странице **Разрешения (Permissions)** выберите вариант по умолчанию **Разрешения, совместимые только с серверами Windows 2000 или Windows Server 2003 (Permissions Compatible only With Windows 2000 or Windows Server 2003 Operating Systems).**

    Подготовка к экзамену Если необходимо продолжить использовать сервер удаленного доступа (RAS) под управлением Windows NT 4 в сети Active Directory, следует выбрать вариант **Разрешения, совместимые с серверами пред-Windows 2000 (Permissions Compatible With Pre-Windows 2000 Operating Systems).** Иначе пользователи домена, подключающиеся через RAS, не смогут пройти аутентификацию. Поддержку RAS можно настроить и после завершения работы *Мастера установки Active Directory* — для этого группу *Все* (Everyone) надо включить в группу *Пред-Windows 2000 доступ* (Pre-Windows 2000 Compatible Access). (Это позволит членам группы *Все* получить доступ для чтения в рамках всех групп и пользователей домена.) На экзамене следует помнить что, эту операцию можно выполнить и в командной строке, выполнив

    ```
    net localgroup "pre-Windows 2000 compatible access" everyone /add
    ```

18. На странице **Пароль администратора для режима восстановления (Directory Services Restore Mode Administrator Password)** введите и подтвердите надежный пароль. Этот пароль необходим при входе под учетной записью *Администратор* (Administrator) в режиме восстановления службы каталога. Щелкните **Далее.**
19. Просмотрите страницу **Сводка (Summary)** и щелкните кнопку **Далее,** чтобы начать установку.
20. По завершении установки щелкните **Готово (Finish).** *Мастер установки Active Directory* предложит перезагрузить Windows, чтобы изменения вступили в силу. Перезагрузите компьютер.

Упражнение 2. Проверка записи ресурса SRV в DNS

Вы проверите наличие новой записи ресурса SRV в зоне *domainl.local.*

1. С компьютера Computerl войдите в домен *Domain 1* как *Администратор* (Administrator). Используйте пароль, назначенный учетной записи *Администратор* на Computerl.
2. Если появится последняя страница *Мастера настройки сервера* (Configure Your Server Wizard) с информацией, что сервер является теперь контроллером домена, щелкните **Готово (Finish).**

3. Откройте консоль *DNS.* Последовательно разверните узлы **COMPUTER!, Зоны прямого просмотра (Forward Lookup Zones)** и **Domain!.local.** В узле **Domain 1.local** указаны шесть поддоменов, созданных установщиком Active Directory.
4. В дереве консоли *DNS* найдите запись ресурса SRV **_ldap._tcp.dc._msdcs.domainl.local.** Для этого последовательно открывайте узлы, соответствующие меткам записи в порядке слева направо, начиная с узла Domain 1.local. Например, разверните узлы **msdcs.domainl.local. Dc** и **_tcp.** Вы должны увидеть в правой панели запись службы (SRV) **_ldap,** как показано на рис. 5-12.

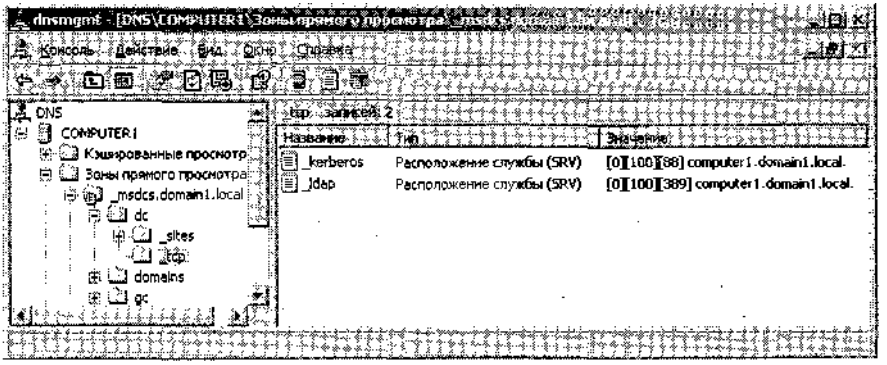


Рис. 5-12. Записи ресурсов SRV для контроллера домена

-эта запись служит для поиска контроллеров домена *domain 1.local,* и ее следует в первую очередь проверять после установки Active Directory.

5. В дереве консоли *DNS*найдите запись ресурса **SRV_ldap._tcp.gc._msdcs.domainl.local.** Эта запись нужна для поиска глобальных каталогов Active Directory в домене *domain 1.local.*
6. На этом проверка заканчивается — записи созданы успешно. Выйдите из системы Computerl.

Упражнение 3. Присоединение компьютера к новому домену

Вы присоедините Computer2 к новому домену.

1. Войдите в систему Computer2 *как Администратор* (Administrator).
2. Откройте окно утилиты *Система* (System) из *Панели управления.*
3. На вкладке **Имя компьютера (Computer Name)** щелкните кнопку **Изменить (Change).**
4. **В** окне **Изменение имени компьютера (Computer Name Changes)** в области **Является членом (Member of)** выберите **домена (domain).**
5. В текстовом поле **Домен (Domain)** введите domain 1. local и щелкните OK.
6. В окне **Изменение имени компьютера (Computer Name Changes)** введите имя пользователя и пароль учетной записи, у которой есть полномочия на присоединение Computer2 к домену Domainl. В поле пользователя введите администратор (administrator), а в поле пароля — пароль учетной записи *Администратор* (Administrator). Щелкните OK.
7. В информационном окне **Изменение имени компьютера (Computer Name Changes)** щелкните OK.
8. Перезагрузите компьютер Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Как пересылка позволяет укрепить безопасность обработки DNS-запросов?
2. Как в окне свойств DNS-сервера запретить многоадресному DNS-серверу реагировать на DNS-запросы, поступающие на конкретные сетевые адаптеры?
3. Вы администратор сети, состоящей из одного домена. Вы установили новый DNS-сервер с именем DNS1, отвечающий за обработку запросов на разрешение имен Интернета, поступающих от клиентов локального домена. Однако, несмотря на наличие подключения DNS1 к Интернету, он не проходит рекурсивный тест на вкладке **Наблюдение (Monitoring)** окна свойств сервера. Что из перечисленного может быть причиной сбоя?
   a. DNS1 установлен вне локальной сети, за брандмауэром.
   b. На DNS1 размещается зона «.».
   c. Корневые ссылки не обновлены и остались в конфигурации по умолчанию.
   d. DNS1 не сконфигурирован на пересылку всех запросов вышестоящему серверу.
4. Какие из перечисленных обстоятельств могут служить причиной изменения (но не удаления) значений корневых ссылок по умолчанию на вкладке **Корневые ссылки (Root Hints)** окна свойств DNS-сервера? (Выберите все подходящие варианты.)
   a. Изменился состав корневых серверов Интернета.
   b. Сервер не планируется использоваться в качестве корневого.
   c. На сервере отключена рекурсия.
   d. Сервер не используется для разрешения имен Интернета.

Резюме

- Вкладка **Интерфейсы (Interfaces)** окна свойств DNS-сервера служит для определения IP-адресов, на которых DNS-сервер должен прослушивать DNS-запросы.
- Вкладка **Пересылка (Forwarders)** окна свойств сервера DNS позволяет настроить пересылку DNS-запросов с локального DNS-сервера на вышестоящий DNS-сервер, или сервер пересылки. Здесь также можно отключать рекурсию при запросах определенных доменов.
- Настроив внутренний DNS-сервер на пересылку внешних запросов единственному серверу пересылки, расположенному за брандмауэром, и открыв на брандмауэре только один порт, по которому обмениваются эти серверы, можно организовать разрешение имен, не открывая сеть для доступа внешних серверов
- Вкладка **Корневые ссылки (Root Hints)** предоставляет удобный интерфейс для модификации содержимого файла *Cache.dm*. На DNS-серверах, используемых для разрешения имен Интернета, эти записи изменять не обязательно. Однако на DNS-серверах в крупном частном пространстве имен можно использовать эту вкладку для удаления ссылок на корневые серверы Интернета и определения корневых серверов частной сети. Наконец, если определить в частной сети корневой DNS-сервер (с именем «.»), придется полностью удалить файл *Cache.dns*.
- Вкладка **Наблюдение (Monitoring)** служит для проверки работы DNS с помощью двух простых тестов: запроса локального DNS-сервера и рекурсивного запроса корневого DNS-сервера.

Занятие 2. Настройка свойств зоны и передачи

Страницы свойств зон облегчают решение массы задач по управлению и администрированию инфраструктурой DNS, в том числе настройку и управление зонными передачами, включение динамических обновлений и изменение типов зон.

Изучив материал этого занятия, вы сможете:

- настраивать зону DNS для поддержки динамических обновлений;
- изменять тип зоны DNS;
- размещать данные зоны в базе данных Active Directory;
- добавлять в зону записи ресурсов серверов имен (NS);
- настраивать зонные передачи с дополнительных зон;
- описать события, инициирующие зонную передачу;
- описать процесс зонной передачи.

Продолжительность занятия — около 70 минут.

Свойства DNS-зоны

Основной инструмент настройки параметров зоны — окно свойств зоны в консоли *DNS*. В окне свойств стандартной зоны пять вкладок: **Общие (General), Начальная запись зоны (SOA) [Start Of Authority (SOA)], Серверы имен (Name Servers), WINS** и **Передачи зон (Zone Transfers). В** окне свойств зон, интегрированных в Active Directory, есть шестая вкладка **Безопасность (Security),** на которой определяют разрешения на доступ к зоне.

Чтобы открыть окно свойств зоны, в консоли *DNS* щелкните узел нужной зоны правой кнопкой и выберите **Свойства (Properties),** как показано на рис. 5-13.

Вкладка *Общие*

Вкладка **Общие (General)** (рис. 5-14) позволяет временно приостановить разрешение имен и определить четыре базовых параметра: тип зоны (в том числе интеграцию с Active Directory), имя файла зоны, динамическое обновление и устаревание.

Состояние зоны

Кнопка **Пауза (Pause)** служит для приостановки/запуска разрешения имен в зоне. Обратите внимание, что здесь нельзя остановить или запустить службу DNS-сервера.

Тип зоны

Щелчок кнопки **Изменить (Change)** открывает окно **Изменение типа зоны (Change Zone Type),** как показано на рис. 5-15.

Здесь можно изменить тип зоны: основная, дополнительная или зона-заглушка. *Основная зона* (primary zone) хранит самые свежие записи и параметры зоны. В стандартной, не интегрированный **с** Active Directory зоне разрешается только один основной DNS-сервер, хранящий единственную версию базы данных зоны с доступом для чтения

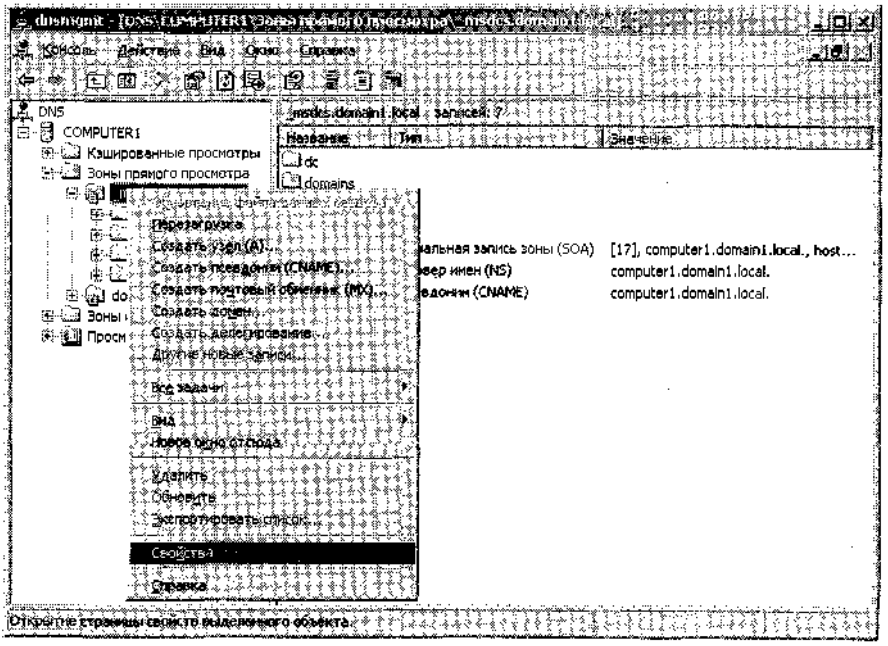


Рис. 5-13. Открытие окна свойств зоны

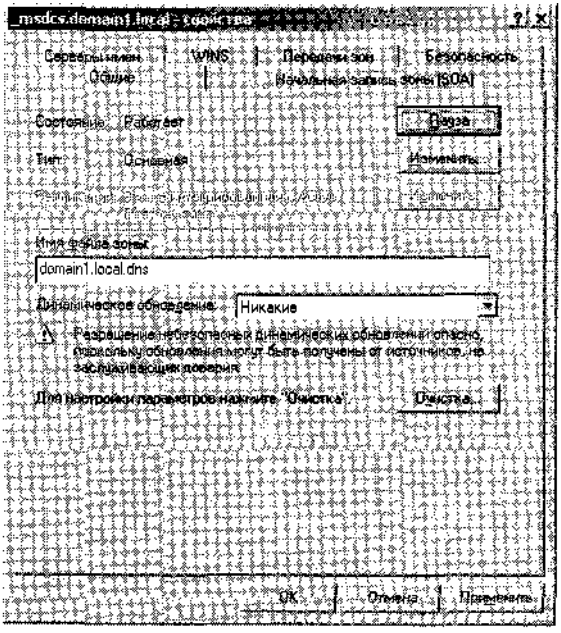


Рис. 5-14. Вкладка *Общие*

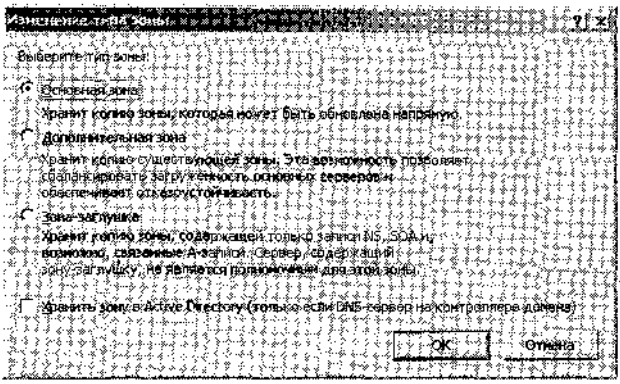


Рис. 5-15. Окно *Изменение типа зоны*

и записи. *Дополнительная зона* (secondary zone) — это копия «только для чтения» основной зоны; она предназначена для повышения эффективности и отказоустойчивости зоны. *Зона-заглушка* (stub zone) представляет собой копию базы данных зоны, содержащую только записи ресурсов, необходимые для поиска полномочных DNS-серверов данной зоны. (Подробнее о зонах-заглушках — в занятии 5.)

Интеграция со службой Active Directory

Флажок **Хранить зону** в **Active Directory (Store the Zone in Active Directory)** в окне **Изменение типа зоны (Change Zone Type)** позволяет разместить информацию основной зоны в базе данных Active Directory, а не в папке *WINDOWS\System32\Dns*. В этом случае данные зоны реплицируются вместе с базой данных Active Directory. В большинстве случаев это избавляет от необходимости настраивать зонные передачи на дополнительные серверы.

Подготовка к экзамену Перемещение стандартного основного сервера на дополнительный выполняется так: зона передается на дополнительный сервер, а затем роль дополнительного сервера повышается до основного. После этого можно удалить исходный основной сервер.

Есть масса преимуществ интеграции зоны DNS в Active Directory. Во-первых, Active Directory автоматически реплицирует зоны, что избавляет от необходимости настраивать отдельный механизм для передачи зоны. Повышается отказоустойчивость и производительность за счет наличия многих основных серверов с копией базы данных для чтения и записи, поддерживающих *репликацию с несколькими хозяевами* (multimaster replication). Во-вторых, Active Directory поддерживает обновление и репликацию отдельных свойств записей ресурсов. Устранение передачи большого числа полнообъемных записей ресурсов позволяет снизить нагрузку на сеть при передаче зон. Наконец, интеграция с Active Directory позволяет определить разрешения на доступ к хранимым записям и предотвратить неправомочное обновление.

Примечание Если есть возможность интегрировать зону в Active Directory, обязательно используйте ее. Это значительно облегчит администрирование, укрепит защиту и сократит до минимума трафик передачи зон. По этой причине принимать решение об установке стандартной основной или дополнительной зоны придется только при развертывании DNS-сервера на компьютере, который не является контроллером домена Active Directory.

Если информация зоны хранится в базе данных Active Directory, на вкладке Общие становится доступной соответствующая кнопка **Изменить (Change)** (рис. 5-16). Она позволяет настроить параметры репликации интегрированной с Active Directory зоны.

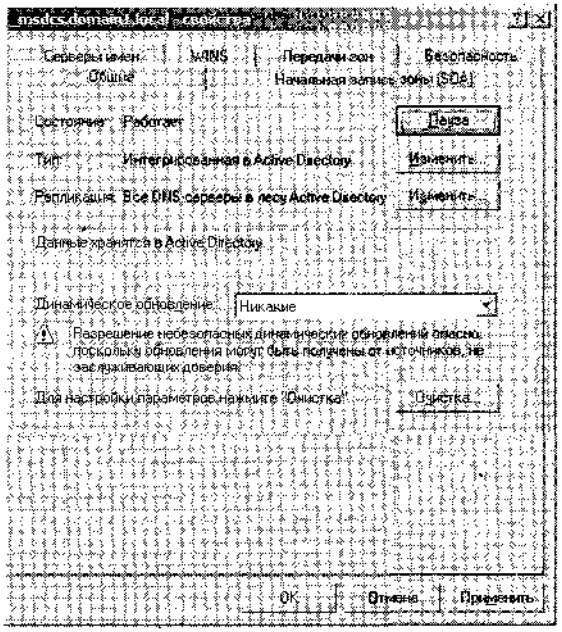


Рис. 5-16. Кнопка *Изменить*, служащая для настройки репликации зоны

По щелчку кнопки **Изменить** открывается окно **Изменение области видимости зоны репликации (Change Zone Replication Scope)** (рис. 5-17), где можно выбрать один из четырех параметров (табл. 5-1). Здесь определяют, на какие серверы леса Active Directory должны скопироваться данные зоны.

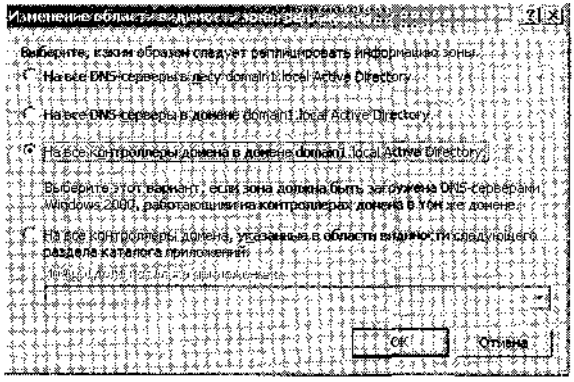


Рис. 5-17. Настройка границ репликации зоны

Табл. 5-1. Варианты репликации зоны

Вариант	Описание
На все DNS-серверы в лесу Active Directory (To all DNS Servers in the Active Directory forest)	Данные зоны реплицируются на все DNS-серверы, размещенные на контроллерах домена леса Active Directory. Обычно это вариант предусматривает самую обширную область репликации
На все DNS-серверы в домене Active Directory (To all DNS Servers in the Active Directory domain)	Данные зоны реплицируются на все DNS-серверы размещенные на контроллерах домена Active Directory
На все контроллеры домена в домене Active Directory (To all domain controllers in the Active Directory domain)	Данные зоны реплицируются на все контроллеры домена Active Directory. Этот вариант выбирают, когда надо, чтобы DNS-серверы под управлением Windows 2000 загружали зону Active Directory
На все контроллеры домена, указанные в области видимости следующего раздела каталога приложений (To all domain controllers specified in the scope of the following application directory partition)	Данные зоны реплицируются на все контроллеры домена, относящиеся к области видимости указанного раздела каталога приложений. Чтобы зона размещалась в указанном разделе каталога приложений, обслуживающий зону DNS-сервер должен принадлежать этому каталогу

Выбирая один из указанных вариантов, имейте в виду, что чем шире границы репликации, тем больший сетевой трафик она вызывает. Например, репликация интегрированной с Active Directory зоны на все DNS-серверы леса создаст намного больший трафик, чем копирование данных DNS-зоны на все DNS-серверы одного домена Active Directory этого же леса. С другой стороны, репликация данных зоны на все DNS-серверы леса значительно ускоряет разрешение имен и повышает отказоустойчивость

Разделы каталогов приложений и репликация в DNS

Раздел каталога приложений (application directory partition) — это раздел каталога, реплицируемый на указанное подмножество контроллеров домена под управлением Windows Server 2003.

Встроенные разделы каталогов приложений

Для каждого домена Active Directory в DNS существуют два встроенных раздела каталога приложений: *DomainDnsZones* и *ForestDnsZones.* Первый реплицируется на все DNS-серверы, являющиеся контроллерами домена Active Directory, а второй — на все DNS-серверы, выполняющие функции контроллеров доменов леса Active Directory. Каждому из этих разделов каталога соответствует поддомен DNS и полное доменное имя (FQDN). Например, в домене Active Directory *bern.lucernepublishing.com* с корневым доменом в лесе *lucernepublishing.com* соответствуют встроенные каталоги раздела приложений DNS с полными именами *DomainDnsZones.bern.lucernepublishing.com* и *ForestDnsZones. lucernepublishing. com*.

Выбор варианта **На все DNS-серверы в лесу Active Directory** в окне **Изменение области видимости зоны репликации (Change Zone Replication Scope)** по сути требует сохранять данные DNS-зоны в разделе *ForestDnsZones,* а выбор **На все DNS-серверы в домене Active Directory** — в разделе *DomainDnsZones.*

Примечание В случае повреждения или удаления этих разделов каталогов приложений их можно восстановить средствами консоли *DNS:* щелкните узел сервера правой кнопкой и выберите **Создать используемые по умолчанию разделы каталога приложений (Create Default Application Directory Partitions).**

Создание нестандартных разделов каталогов приложений

Вы вправе создать собственные нестандартные разделы каталогов приложений для использования с DNS и разместить реплики этого раздела на выбранных контроллерах домена в следующей последовательности.

Сначала создают раздел командой

Dnscmd <*имя сервера*> /createdirectorypartition <*полное доменное имя*>

а затем в раздел добавляют другие DNS-серверы командой

Dnscmd <*имя сервера*> /enlistdirectorypartition <*полное доменное имя*>

Например, раздел каталога приложений *SpecialDns* на компьютере Serverl в домене *Active Directory* *contoso.com* создают командой

Dnscmd serverl /createdirectorypartition SpecialDns.contoso.com

а затем в раздел добавляют компьютер Server2 командой

Dnscmd server2 /enlistdirectorypartition SpecialDns.contoso.com

Примечание Правом создания разделов каталогов приложений наделены члены группы *Администраторы предприятия* (Enterprise Admins).

Чтобы сохранить данные DNS в нестандартном разделе каталога приложений, в окне **Изменение области видимости зоны репликации** выберите вариант **На все контроллеры домена, указанные в области видимости следующего раздела каталога приложений** и выберите раздел каталога из раскрывающегося списка. Этот вариант доступен только при наличии нестандартных разделов каталогов приложений DNS.

Репликация с серверами под управлением Windows 2000

Контроллеры доменов под управлением Windows 2000 не поддерживают разделы каталогов приложений, поэтому, если требуется, чтобы данные зоны были доступными DNS-серверам под управлением Windows 2000, в окне **Изменение области видимости зоны репликации** надо выбрать вариант **На все контроллеры домена в домене Active Directory. В** этом случае данные реплицируются не просто на все DNS-серверы, одновременно являющимися контроллерами домена, а абсолютно на все контроллеры независимо от того, есть на них DNS-сервер или нет.

Подготовка к экзамену Будьте готовы отвечать на вопросы, касающиеся принципов построения и команд разделов каталогов приложений, а также вариантов в окне **Изменение области видимости зоны репликации (Change Zone Replication Scope).**

Имя файла зоны

По умолчанию стандартным зонам, не интегрированным в Active Directory, сопоставляется файл, имя которого создается путем добавления к имени зоны расширения *.dm*. Текстовое поле **Имя файла зоны (Zone file name)** на вкладке **Общие (General)** позволяет изменить заданное по умолчанию имя этого файла.

Динамические обновления

На вкладке **Общие** также можно настроить зону на прием динамических обновлений записей ресурсов. Существуют три варианта динамического обновления (рис. 5-18) интегрированных в Active Directory зон: **Никакие (None), Небезопасные и безопасные (Nonsecure and secure)** и **Только безопасные (Secure only).** В стандартных зонах доступны только два варианта: **Никакие (None)** и **Небезопасные и безопасные (Nonsecure and secure).**

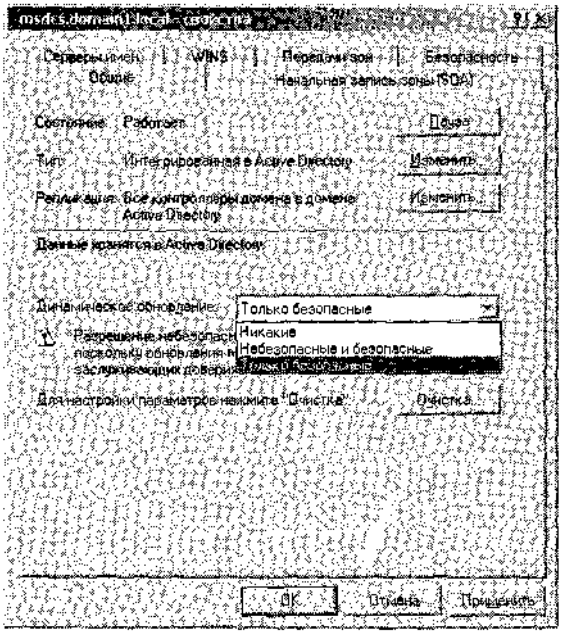


Рис. 5-18. Варианты динамического обновления

При выборе варианта Никакие выполнять регистрацию и обновление записей придется вручную. В остальных двух вариантах клиенты автоматически создают и/или обновляют собственные записи ресурсов. Эта функция избавляет от массы работы по ручному администрированию записей зон, особенно для DHCP- и мобильных клиентов. Рис. 5-19 иллюстрирует типичный процесс динамического обновления.

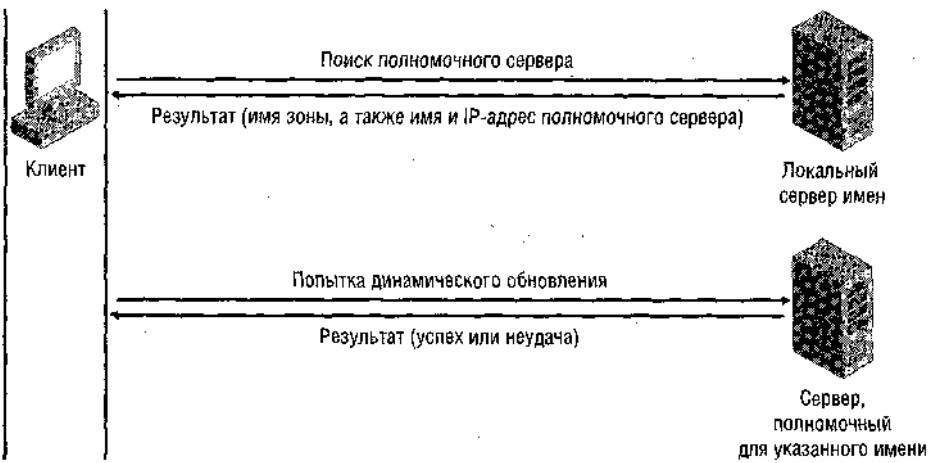


Рис. 5-19. Процесс динамического обновления

При любом событии-триггере динамического обновления на DNS-клиенте служба DHCP (а не DNS) на клиенте пытается выполнить динамическое обновление записи ресурса A на DNS-сервере. Процесс обновления организован так, что при изменении IP-конфигурации DHCP-сервером эта информация немедленно направляется DNS-серверу. Пытаясь выполнить обновление, служба DHCP-клиента обращается на все сетевые подключения, в том числе не поддерживающие DHCP. Успешность динамического обновления в первую очередь зависит от того, поддерживает ли зона такие обновления.

События-триггеры динамического обновления

Следующие события заставляют DHCP-клиент направлять на DNS-сервер запрос на динамическое обновление:

* назначение, отмена или изменение IP-адреса в свойствах протокола TCP/IP любого из установленных сетевых подключений локального компьютера;
- изменения или обновление параметров аренды IP-адреса на любом из установленных сетевых подключений локального компьютера— например, при перезапуске компьютера или выполнении команды Ipconfig /renew;
- выполнение команды Ipconfig /registerdns на DNS-клиенте для ручного обновления регистрации имени клиента в DNS;
- включение компьютера DNS-клиента;
- повышение роли рядового сервера в зоне до контроллера домена.

Безопасное динамическое обновление

Безопасные динамическое обновление возможны только в зонах, интегрированных в Active Directory. [В окне свойств стандартных зон отсутствует вариант **Только безопасные (Secure only).]** При таком обновлении используется безопасный протокол аутентификации Kerberos: он служит для создания безопасного контекста и проверки, что клиент, обновляющий запись ресурса, действительно является его владельцем.

Примечание Отправку динамических обновлений на DNS-сервер поддерживают только клиенты под управлением Windows 2000/XP/Server 2003, но не клиенты с Windows NT/95/98/Me. Однако DNS-клиент (например DHCP-сервер) может выполнять динамическое обновление от имени других клиентов при условии, что он настроен соответствующим образом.

Безопасное динамическое обновление и группа DnsUpdateProxy

При включенном безопасном динамическом обновлении изменять записи зоны разрешается только владельцам, то есть компьютерам, изначально зарегистрировавшим запись. Это ограничение может помешать, когда DHCP-сервер сконфигурирован для регистрации записей ресурсов-узлов (A) от имени клиентов, не поддерживающих динамическое обновление. В таких случаях владельцем записи становится не клиент, а DHCP-сервер. Если в дальнейшем ОС клиента обновляется до Windows 2000 или другой ОС, поддерживающей динамическое обновление, компьютер не будет признан владельцем и, следовательно, не сможет обновлять собственные записи. Аналогичная неполадка возможна при отказе DHCP-сервера, регистрировавшего записи от имени клиентов: резервный DHCP-сервер не сможет обновлять такие записи.

Для предотвращения подобных проблем в группу безопасности *DnsUpdateProxy* присоединяют DHCP-серверы, которые регистрируют записи от имени других компьюте-

ров. Члены этой группы не сохраняют информацию о владельце обновляемых записей ресурсов в DNS. Ясно, что это ослабляет защиту таких записей, пока их не зарегистрирует реальный владелец.

Подготовка к экзамену Почти наверняка на экзамене встретятся вопросы о *DnsUpdateProxy* — будьте готовы к ним.

Устаревание

Щелчок кнопки **Очистка (Aging)** на **Общие (General)** открывает окно **Свойства очистки зоны (Zone Aging/Scavenging Properties),** показанное на рис. 5-20. Здесь настраивается механизм обнаружения и очистки устаревших записей из базы данных зоны.

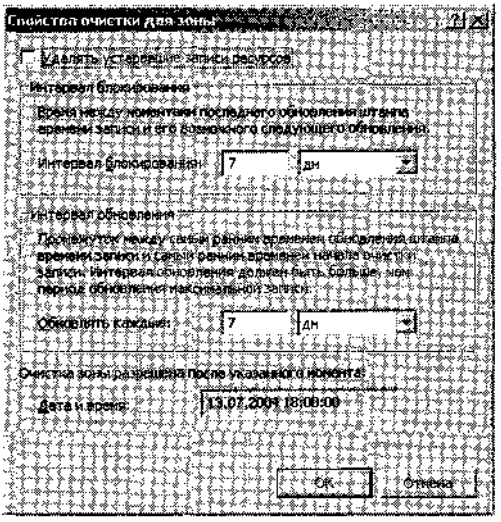


Рис. 5-20. Окно *Свойства очистки зоны*

Включение устаревания. Под *устареванием* (aging) в DNS подразумевается процесс присвоения временной метки динамически зарегистрированным записям ресурсов и затем отслеживания возраста записи. Устаревшие записи ресурсов подлежат удалению, или *очистке* (scavenging). Очистка поддерживается только при включенном устаревании. По умолчанию устаревание и очистка отключены.

При включении устаревания в конкретной зоне необходимо задействовать эту функцию на уровне как зоны, так и сервера. Чтобы включить устаревание на уровне зоны, в окне **Свойства очистки зоны (Zone Aging/Scavenging Properties)** установите флажок **Удалять устаревшие записи ресурсов (Scavenge Stale Resource Records).** Активизация устаревания на уровне серверов выполняется так: в консоли *DNS* щелкните значок сервера правой кнопкой и выберите **Установить свойства очистки для всех зон (Set Aging/ Scavenging For All Zones),** в окне **Свойства очистки зоны (Server Aging/ Scavenging Properties)** установите флажок **Удалять устаревшие записи ресурсов (Scavenge Stale Resource Records).**

После включения устаревания все динамически зарегистрированные записи в зоне получают метку времени, которая регулярно обновляется DHCP-сервером или клиентом при динамическом обновлении записи. Созданным вручную записям ресурсов назначается метка *0,* указывающая, что механизм устаревания на них не действует.

Примечание Если включен механизм устаревания и очистки, DNS-серверы под управлением ОС, предшествующих Windows 2000 не в состоянии считывать соответствующие зонные файлы.

Интервал блокирования (no-refresh interval) — период времени после создания метки времени, в течение которого зона или сервер отклоняет запросы на обновление этой метки. Эта функция устраняет излишние обновления, которые создают дополнительную нагрузку на сервер и инициируют ненужный трафик передачи зон! Интервал блокирования по умолчанию равен 7 дням.

Интервал обновления (refresh interval) — промежуток между самым ранним временем обновления метки времени и самым ранним временем начала очистки записи. Иначе говоря, очистка записи зоны начинается по истечении интервала блокирования и интервала обновления. Интервал обновления по умолчанию равен 7 дням. Таким образом, по умолчанию очистка записей ресурсов начинается через 14 дней.

Совет При изменении интервалов блокирования и обновления рекомендуется соблюдать правило: интервал обновления должен быть равным или большим, чем интервал блокирования.

Очистка в зоне выполняется автоматически или вручную. Автоматическая очистка включается на вкладке **Дополнительно (Advanced)** свойств DNS-сервера. Если она отключена, можно выполнить очистку вручную: щелкните значок сервера в дереве консоли *DNS* правой кнопкой и выберите **Удалить устаревшие записи (Scavenge Stale Resource Records).**

Вкладка *Начальная запись зоны (SOA)*

Вкладка **Начальная запись зоны (SOA) [Start of Authority (SOA)]** (рис. 5-21) позволяет настроить начальную запись ресурса для зоны. При загрузке зоны DNS-сервер использует запись ресурса SOA для получения базовой, полномочной информации о зоне. Эта запись также содержит сведения о том, как часто выполняется передача зоны между основным и дополнительным серверами.

Поле **Серийный номер (Serial Number)** вкладки **Начальная запись зоны (SOA)** содержит номер редакции файла зоны. Этот номер увеличивается на единицу при каждом изменении записи ресурса или увеличении этого числа вручную щелчком кнопки **Увеличить (Increment).**

Когда зоны настроены на выполнение зонных передач, главный сервер периодически опрашивается на предмет серийного номера зоны. Такой запрос называется *запросом SOA* (SOA query). Если результаты запроса SOA показывают, что серийные номера главной и локальной зоны равны, передача зон не выполняется. Однако если серийный номер зоны на главном сервере больше, дополнительный сервер инициирует передачу.

Поле **Основной сервер (Primary Server)** содержит полное имя компьютера основного DNS-сервера зоны. Оно должно заканчиваться точкой.

Ответственное лицо (Responsible Person) — когда это поле заполнено, оно содержит запись ресурса о человеке (RP), ответственном за управление зоной, то есть его ящик электронной почты в домене. Значение в этом поле должно заканчиваться точкой.

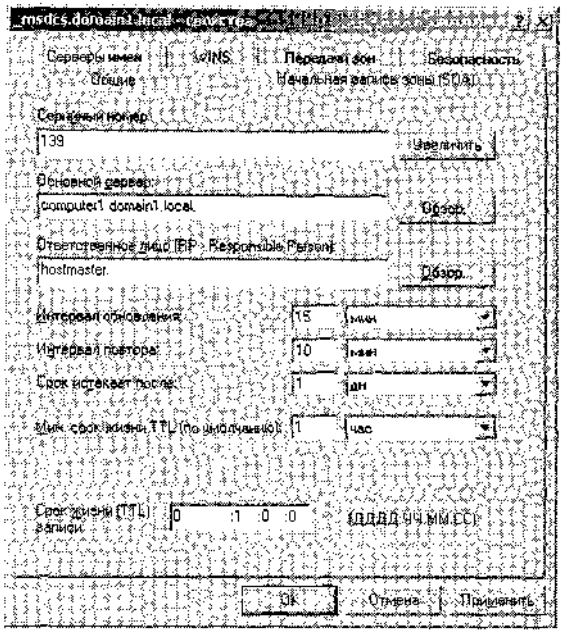


Рис. 5-21. Вкладка *Начальная запись зоны (SOA)*

Интервал обновления (Refresh Interval) — значение, определяющее период запроса на обновление зоны дополнительным DNS-сервером у главного сервера. По истечении интервала регенерации дополнительный DNS-сервер запрашивает у главного копию запись ресурса SOA, сравнивает серийный номер со своим и, если они различаются, запрашивает передачу зон у основного DNS-сервера. По умолчанию этот интервал составляет 15 минут.

Подготовка к экзамену Увеличение интервала обновления позволяет сократить трафик передачи зон.

Интервал повтора (Retry Interval) определяет время между неудачной передачей зоны и запросом на повторную попытку этой операции. Обычно он меньше интервала регенерации. Значение по умолчанию — 10 минут.

Срок истекает после (Expires After) — время, на протяжении которого дополнительный сервер продолжает отвечать на запросы от DNS-клиентов, не имея контакта с главным сервером. По истечении этого срока данные считаются ненадежными. Значение по умолчанию — 1 день.

Мин. ерок жизни TTL (по умолчанию) [Minimum (Default) TTL] время жизни всех записей ресурсов в зоне. Значение по умолчанию — 1 час.

Значение TTL не касается записей ресурсов в полномочных зонах, а определяет время существования записи ресурса в кэше неполномочных DNS-серверов.

Подготовка к экзамену Если помимо основного сервера в сети установлены серверы кэширования, то, увеличив минимальное TTL, можно снизить трафик разрешения имен между кэширующими и основным сервером.

Срок жизни (TTL) записи (TTL For This Record) — TTL текущей запись ресурса SOA. Это значение переопределяет значение по умолчанию в предыдущем поле.

Вот как выглядит запись ресурса SOA в текстовом файле зоны:

```
@IN SOA computed . domain"!. local,  hostmas ter. domain"!. local. (
    5099       ; serial number
    3600       ; refresh (1 hour)
    600        ; retry (10 mins)
    86400   ;   expire (1 day)
    60 )       ; minimum TTL (1 min)
```

Вкладка *Серверы имен*

Вкладка **Серверы имен (Name Server)** (рис. 5-22) служит для настройки записи ресурса NS. Подобные записи нельзя создать в другом месте консоли *DNS*.

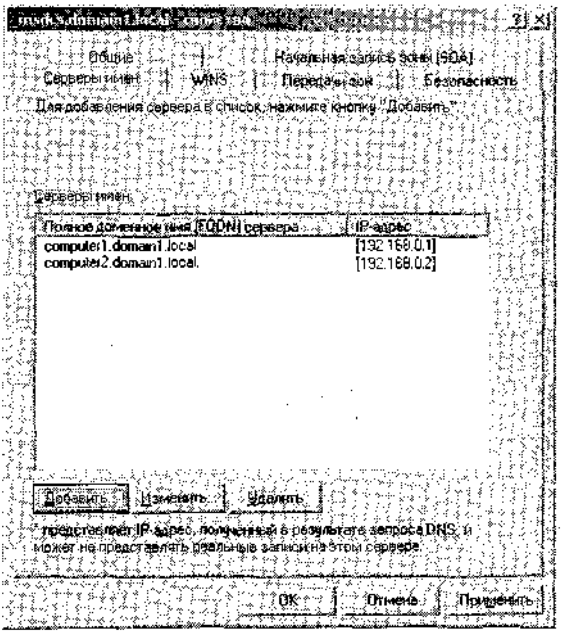


Рис. 5-22. Вкладка *Серверы имен*

Записи ресурса NS нужны для определения полномочных серверов имен в данной зоне. Запись ресурса NS первого основного сервера зоны создается автоматически.

Примечание . Каждая зона должна содержать в корне по крайней мере одну запись ресурса NS.

Вот пример записи NS в файле базы данных зоны *lucernepablishing.com:*

```
@  NS    dhs1.lucernepublishing.com.
```

Здесь символ «@» представляет зону, определенную записью SOA в том же файле. Таким образом, полная запись четко сопоставляет домен *lucernepublishing.com* DNS-серверу, размещенному на компьютере *dnsl.lucernepublishing.com*.

Подготовка к экзамену По умолчанию передачи в основных зонах разрешены только на серверы, указанные на вкладке **Серверы имен.** Это новое ограничение, появившееся в Windows Server 2003.

Вкладка *WINS*

Вкладка **WINS** (рис. 5-23) (или **WINS-R** в зоне обратного просмотра) служит для настройки поддержки разрешения имен WINS-серверами данной зоны в ситуациях, когда DNS-серверы не в состоянии ответить на запрос разрешения имени.

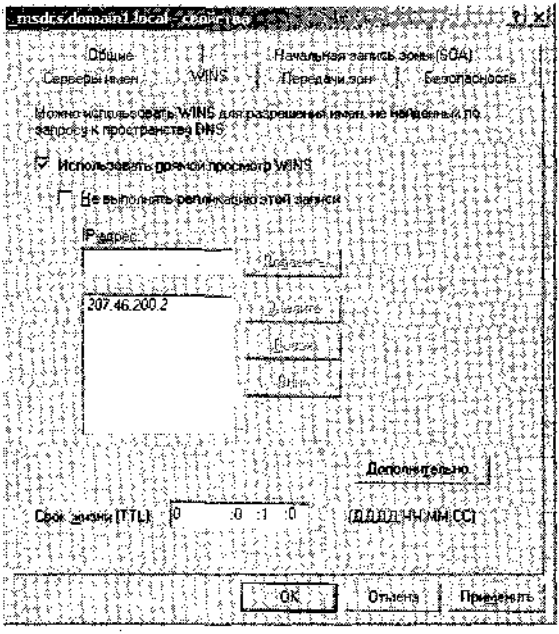


Рис. 5-23. Вкладка *WINS*

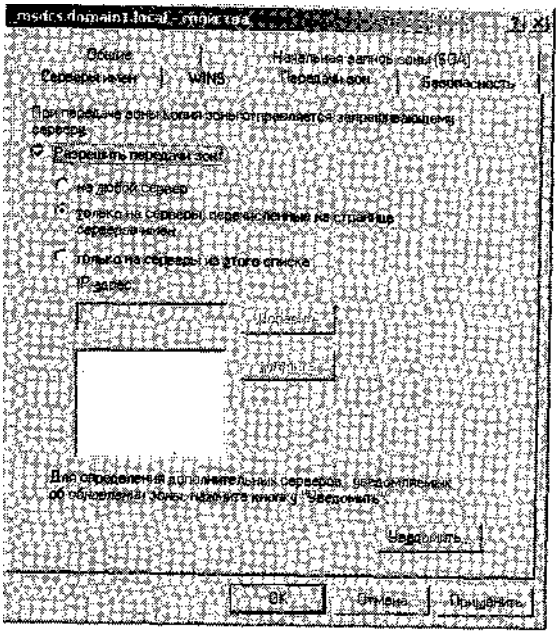
Подготовка к экзамену После настройки разрешения средствами WINS в зоне прямого просмотра определенная на вкладке **WINS** запись ресурса WINS, указывающая на WINS-сервер, добавляется в базу данных зоны. Аналогично, при настройке поиска WINS-R для зоны обратного просмотра в базу добавляется соответствующая запись ресурса WINS-R.

Вкладка *Передачи зон*

Вкладка **Передачи зон (Zone Transfers)** (рис. 5-24) позволяет ограничивать зонные передачи с локального главного сервера. По умолчанию в основных зонах передача на дополнительные серверы либо полностью запрещена, либо ограничена серверами имен, перечисленными на вкладке **Серверы имен (Name Server).** Первое ограничение применяется на DNS-серверах, созданных в окне **Управление данным сервером (Manage Your Server),** а второе — посредством *Мастера компонентов Windows* (Windows Components Wizard). В дополнение к указанным ограничениям вы вправе определить ограничения

передач зон, выбрав вариант **только на серверы из этого списка (only to the following servers)** и задав IP-адреса разрешенных дополнительных серверов.

В дополнительных зонах по умолчанию запрещены зонные передачи в другие дополнительные зоны, но эту функцию легко включить, установив флажок **Разрешить передачи зон (Allow zone transfers).**



'ис. 5-24. Вкладка *Передачи зон*

На заметку В Windows 2000 на вкладке **Передачи зон** окна свойств основных зон по умолчанию разрешались переносы на любой сервер, но это создавало брешь в защите. Подумайте сами: зачем разрешать любому пользователю, имеющему доступ к DNS-серверу, создавать дополнительный сервер и просматривать записи ресурсов вашей сети? Ограничение передач зон по умолчанию - намного разумнее, так как предотвращает неправомочное копирование данных зоны.

Уведомление. Вкладка **Передачи зон** также позволяет задавать вторичные серверы, уведомляемые об обновлении зоны. Для этого при установленном флажке **Разрешить передачи зон** надо щелкнуть кнопку **Уведомить (Notify).** При этом откроется одноименное окно (рис. 5-25), в котором определяют дополнительные серверы, автоматически уведомляемые об обновлении зоны на локальном главном сервере. По умолчанию при включении передач зон все серверы, перечисленные на вкладке **Серверы имен (Name Servers),** автоматически уведомляются об обновлении зон.

Уведомление и инициирование передачи зоны. В стандартных зонах передача зоны происходит при любом из трех событий:

- по окончании периода обновления регенерации записи ресурса SOA основной зоны;
- при загрузке дополнительного сервера. В этих двух случаях дополнительный сервер инициирует запрос SOA, чтобы узнать, не произошло ли обновление зоны, - только в этом случае выполняется передача;

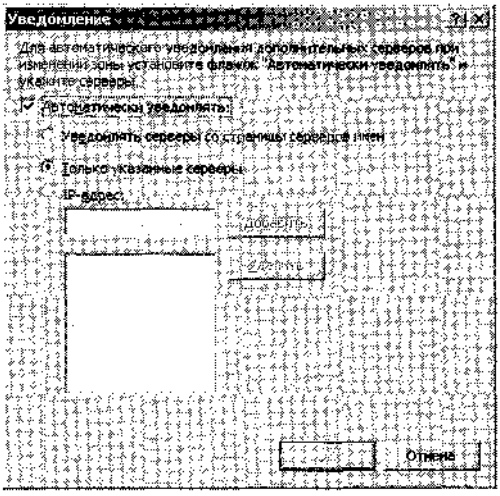


Рис. 5-25. Окно *Уведомление*

- при изменении конфигурации основного сервера, который сконфигурирован на уведомление указанных дополнительных DNS-серверов об обновлении зоны.

Дополнительный сервер выполняет добавочную **(IXFR)** или полную. (AXFR) передачу зоны на главный сервер (рис. 5-26). По умолчанию на компьютерах с Windows 2000 Server или Windows Server 2003 выполняются запросы **IXFR. В** этом случае по сети передаются только измененные данные. Windows NT Server не поддерживает добавочные переносы и выполняет только запросы **AXFR,** то есть на дополнительный сервер передается вся база данных зоны.

Основные DNS-серверы под управлением Windows Server 2003 поддерживают оба вида передачи.

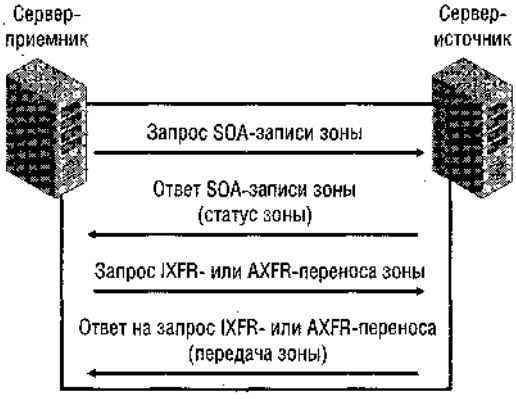


Рис. 5-26. Согласование при передаче зоны

Примечание В интегрированных с Active Directory зонах настраивать зонные передачи или уведомление на контроллерах домена или DNS-серверах не нужно, так как они выполняются автоматически в процессе репликации.

Лабораторная работа. **Развертывание дополнительного DNS-сервера**

На этой лабораторной работе вы создадите дополнительную зону и затем сконфигурируете зонные передачи между основной и дополнительной зонами.

Упражнение 1. Создание дополнительной зоны

Вы установите DNS-сервер на Computer2 и на новом DNS-сервере сконфигурируете дополнительную зону.

Внимание! Предполагается, что на Computerl уже установлен DNS-сервер с помощью *Мастера компонентов Windows* (Windows Components Wizard) (см. занятие 3 главы 4). В этом случае передачи из зоны *Domain!.local* включены по умолчанию, но ограничены полномочными серверами имен. Если DNS-сервер установлен на Computerl путем добавления роли DNS-сервера в окне **Управление данным сервером (Manage Your Server),** передачи во всех локальных зонах по умолчанию отключены. В этом случае до начала упражнения надо позаботиться о включении зонных передач в зоне *Domain!.local* и запретить передачу на серверы, перечисленные на вкладке **Серверы имен (Name Servers).**

1. Войдите в систему Computer2 как *Администратор* (Administrator).
2. На Computer2 установите *Средства поддержки Windows* (см. занятие 2 главы 3), в состав которых входит утилита командной строки Dnscmd.
3. На Computer2 установите подкомпонент-службу *DNS* (см. занятие 3 главы 4). В этом упражнении можно без каких-либо последствий отклонить любые сообщения о том, что у Computer2 есть динамически назначенный IP-адрес. Не меняйте адресную конфигурацию Computer2.
4. По завершении установки DNS откройте окно командной строки и выполните команду

   ```
   dnscmd computerl/recordadd domainl.local ns computer2.domain1.local.
   ```

   Она добавит запись NS в *domainl.local,* соответствующую Computer2, то есть превратит его в полномочный сервер зоны. По умолчанию при установке DNS-сервера с помощью *Мастера компонентов Windows* зонные передачи разрешены только на полномочные серверы.
5. На Computer2 в дереве консоли *DNS* щелкните правой кнопкой **Зоны прямого просмотра (Forward Lookup Zones)** и выберите **Создать новую зону (New Zone).**
6. **В** окне **Мастер создания новой зоны (New Zone Wizard)** щелкните Далее (Next).
7. На странице **Тип зоны (Zone Type)** выберите **Дополнительная зона (Secondary Zone)** и щелкните **Далее.**
8. На странице **Имя зоны (Zone Name)** в текстовом поле введите domainl. local и щелкните **Далее.**
9. На странице **Основные DNS-серверы (Master DNS Server)** в текстовом поле **IP-адрес (Address)** введите 192.168.0.1 и щелкните **Добавить (Add),** а затем — **Далее.**
10. На странице **Завершение мастера создания новой зоны (Completing The New Zone Wizard)** щелкните **Готово (Finish).**
11. **В** дереве консоли *DNS* разверните узел **Зоны прямого просмотра,** щелкните узел **Domainl.local** правой кнопкой и выберите **Передать зону с основного сервера (Transfer From Master).**

12. При сбое загрузки подождите минуту и повторите попытку. Повторяйте операцию, пока зона успешно не загрузится.
13. Когда в консоли *DNS*компьютера Computer2 появится копия зоны *domain 1.local^* изучите окно свойств зоны и элементы меню **Действие (Action).**
14. Щелкните узел **DNS** в консоли *DNS* правой кнопкой и выберите **Подключение к DNS-сервёру (Connect to DNS Server).**
15. **В** открывшемся окне **Подключение к DNS-серверу (Connect to DNS server)** выберите вариант **другой компьютер (the following computer)** и в соответствующем текстовом поле введите COMPUTER1.
16. Щелкните OK. В дереве консоли *DNS* над узлом **COMPUTER2** появится узел **COMPUTER1.** Изучите оба узла в консоли DNS на Computer2 и ответьте на следующие вопросы.

    Какие команды меню **Действие (Action)** доступны для зоны *domain I. local* в узле COMPUTER2 и какие недоступны для той же зоны в узле COMPUTER1?

    Можно ли создавать или конфигурировать записи ресурсов *domainl.local* через узел COMPUTER2 в консоли *DNS!*

Упражнение 2. Просмотр параметров настройки уведомления

Вы просмотрите конфигурации уведомления о передачах зон по умолчанию.

1. Войдя с Computer2 в домен *Domainl как Администратор* (Administrator), разверните узел **COMPUTER1** в консоли DAW и откройте окно свойств основной зоны *Domainl.local.*
2. На вкладке **Серверы имен (Name Servers)** указан Computer2 (его вы добавили в упражнении 1).
3. На вкладке **Передачи зон (Zone Transfers)** щелкните кнопку **Уведомить (Notify).** Откроется окно **Уведомление (Notify).** По умолчанию основная зона автоматически уведомляет серверы, указанные на вкладке **Серверы имен,** об изменении зон, то есть Computer2 автоматически получит уведомление. Получив уведомление от основного сервера и являясь дополнительным DNS-сервером, Computer2 инициализирует запрос IXFR добавочной передачи зоны. Щелкните кнопку **Отмена (Cancel).**
4. В окне свойств *Domainl.local* перейдите на вкладку **Начальная запись зоны (SOA) [Start Of Authority (SOA)]** и ответьте на следующие вопросы.

    Как долго DNS-сервер на Computer2 будет обслуживать запросы DNS-клиентов после потери связи с Computerl?

    Как часто в соответствии с конфигурацией Computer2 запрашивает на Computerl изменения зоны?

    Через какое время после обнаружения отсутствия связи с Computerl при запросе SOA компьютер Computer2 повторит попытку?

    Если другой основный DNS-сервер *dns.domain2.local* успешно получит с Computer2 ответ на запрос об IP-адресе Computerl, как долго соответствующая Computer2 запись ресурса A сохранится в кэше *dns.domain2.bcan*
5. Щелкните OK, чтобы закрыть окно свойств *Domainl.local.*
6. В консоли *DNS* щелкните значок **Computerl** правой кнопкой и выберите **Удалить (Delete).**
7. В открывшемся информационном окне подтвердите удаление щелчком Да (Yes). Computerl удаляется из консоли *DNS* на Computer2, но параметры сервера в консоли *DNS* на Computerl остаются неизменными.
8. Выйдите из системы Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Опишите порядок, в котором дополнительные серверы выясняют необходимость инициации передачи зоны.
2. В чем различие между запросами IXFR и AXFR?
3. В сети несколько DHCP-серверов, некоторые из которых сконфигурированы на регистрацию записей в DNS от имени клиентов под управлением ОС предшествующей Windows 2000. В DNS разрешены только безопасные обновления, однако обнаружилось, что некоторые записи в DNS не обновляются должным образом. Что предпринять?
4. Вы отвечаете за администрирование WAN-сети компании Proseware. Штаб-квартира компании расположена в Рочестере, а два филиала — в Буффало и Сиракузах. Сеть компании состоит из одного домена; в ней одна основная DNS-зона в штаб-квартире, обслуживаемая компьютером под управлением Windows Server 2003, и по дополнительной DNS-зоне в каждом филиале. Пользователи жалуются на отсутствие доступа к удаленным филиалам. Администраторы обнаружили, что пропускная способность канала между штаб-квартирой и филиалами перегружена зонными передачами, причем новые передачи инициируются до окончания предыдущих. Что из перечисленного позволит решить проблему наименьшими усилиями?
   a. Установить в сети Active Directory и повысить роль серверов, обслуживающих дополнительные DNS-зоны, до контроллеров домена.
   b. Увеличить пропускную способность подключений, установив волоконно-оптическое подключение между филиалами.
   c. Увеличить интервал обновления на основном DNS-сервере.
   d. Увеличить интервал обновления на дополнительных DNS-серверах.
5. Администратор установил TTL в основной DNS-зоне в 5 минут. Какие наиболее вероятные последствия этого шага?
   a. Записи ресурсов в кэше основного DNS-сервера будут удаляться по истечении 5 минут.
   b. При разрешении имен, для которых сервер является полномочным, DNS-клиентам придется запрашивать сервер чаще.
   c. Дополнительные серверы будут инициировать передачу зоны каждые 5 минут.
   d. Узлы будут чаще перерегистрировать свои записи в DNS.
6. Что не является преимуществом хранения DNS-зон в базе данных Active Directory?
   a. Менее частые передачи.
   b. Меньше усилий по администрированию.
   c. Меньшая нагрузка на сеть.
   d. Безопасное динамическое обновление.

Резюме

- При развертывании DNS-сервера на контроллере домена появляется возможность размещения базы данных зоны в Active Directory. Это позволяет сократить трафик передачи зон, укрепить защиту, облегчить администрирование и повысить

отказоустойчивость. Данные зоны можно реплицировать на все DNS-серверы леса Active Directory, на все DNS-серверы домена Active Directory, на все контроллеры домена Active Directory или на все серверы определенного раздел каталога приложений.

- Если DNS-зона поддерживает динамическое обновление, DNS-клиенты могут регистрировать и обновлять свои записи ресурсов на DNS-сервер. При поддержке безопасных динамических обновлений право обновления записи предоставляется только владельцу. Безопасное динамическое обновление поддерживается только в зонах, интегрированных с Active Directory. Клиенты под управлением Windows 2000/XP/Server 2003 поддерживают динамическое обновление.
- Группа *DnsUpdateProxy* обычно объединяет DHCP-серверы, динамически обновляющие данные DNS от имени клиентов. При регистрации записей ресурсов в DNS члены этой группы не оставляют информации о владельце. Это позволяет предупредить неполадки, возникающие из-за конфликта владельцев в зонах, поддерживающих только безопасное динамическое обновление.
- Вкладка **Начальная запись зоны (SOA) [Start Of Authority (SOA)]** служит для настройки начальной записи зоны и нескольких параметров, которые затрагивают передачи зон, в том числе интервал блокирования, интервал обновления, срок и минимальное время жизни (TTL).
- Вкладка **Передачи зон (Zone Transfers)** служит для управления передачей из локальной зоны. По умолчанию зонные передачи либо полностью запрещены, либо ограничены только серверами, указанными на вкладке **Серверы имен (Name Servers).** Такое ограничение определяется типом зоны и методом установки DNS-сервера.

Занятие 3. Настройка дополнительных свойств DNS-сервера

Дополнительные свойства DNS-сервера — это 9 параметров, определяемые на вкладке **Дополнительно (Advanced)** окна свойств DNS-сервера и касающиеся таких серверных функций, как рекурсия, циклическое обслуживание и расстановка по адресу.

Изучив материал этого занятия, вы сможете:

- *S* рассказать о функциях и предназначении всех параметров на вкладке **Дополнительно** окна свойств DNS-сервера;
- */* восстановить значения по умолчанию всех дополнительных параметров сервера.

Продолжительность занятия — около 50 минут.

Дополнительные параметры сервера

При запуске DNS-сервер под управлением Windows Server 2003 берет параметры из загрузочного информационного файла, реестра или базы данных Active Directory. Вкладка **Дополнительно** позволяет изменять место хранения конфигурации (рис. 5-27).

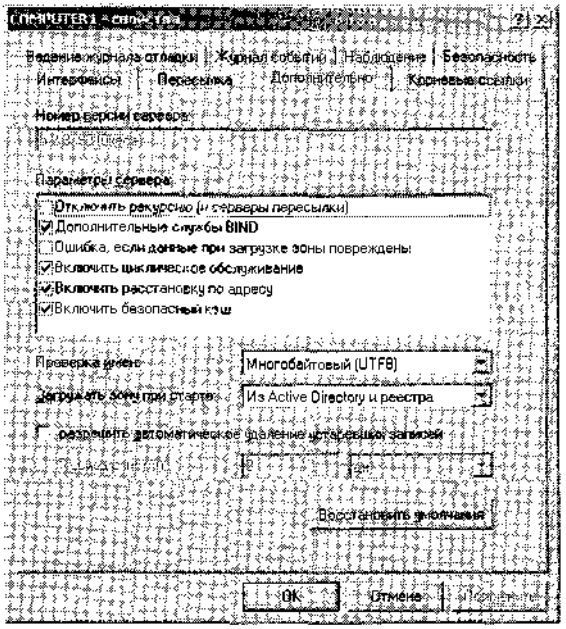


Рис. 5-27. Вкладка *Дополнительно* окна свойств DNS-сервера

Настройка сервера состоит из шести флажков, которые принимают состояние «включен» или «отключен», и трех параметров, касающихся выбора конфигурации (табл. 5-2).

Табл. 5-2. Установочные значения (по умолчанию) параметров DNS

Параметр	Значение
Отключить рекурсию (Disable Recursion)	Отключен
Дополнительные службы BIND (BIND Secondaries)	Включен
Ошибка, если данные при загрузке зоны повреждены (Fail on load if bad zone data)	Отключен
Включить циклическое обслуживание (Enable Round Robin)	Включен
Включить расстановку по адресу (Enable Netmask Ordering)	Включен
Включить безопасный кэш (Secure Cache Against Pollution)	Включен
Проверка имен (Name checking)	**Многобайтовый (TJTF8) [Multibyte (UTF8)]**
Загружать зону при старте (Load zone data on startup)	**Из Active Directory и реестра (From Active Directory and registry)**
Разрешить автоматическое удаление устаревших записей (Enable automatic scavenging of stale records)	Отключен. При включении требуется дополнительная настройка

В большинстве случаев эти значения не требуют изменения — их настраивают в особых ситуациях. Более подробно эти параметры обсуждаются в следующих разделах.

Подготовка к экзамену Знание этих параметров активно проверяется на экзамене. Особое внимание уделите изучению параметров **Отключить рекурсию, Включить циклическое обслуживание** и **Включить расстановку по адресу.**

Параметры по умолчанию восстанавливаются так.

1. В дереве консоли *DNS* щелкните нужный DNS-сервер правой кнопкой и выберите **Свойства (Properties).**
2. На вкладке **Дополнительно (Advanced)** щелкните кнопку **Восстановить умолчания (Reset to Default)** и затем OK.

Флажок *Отключить рекурсию*

Этот флажок по умолчанию сброшен, поэтому DNS-сервер выполняет рекурсию при разрешении клиентских запросов, только если особая конфигурация клиента не запрещает такое поведение. При рекурсии DNS-сервер запрашивает другие серверы от имени клиента и пытается полностью разрешить полное доменное имя (FQDN). Запросы выполняются итеративно, пока сервер не получит ответ от полномочного сервера. Затем сервер пересылает запрос клиенту.

При установленном флажке **Отключить рекурсию** DNS-сервер не разрешает запрос клиента, а возвращает ему *ссылки* (referrals), или записи ресурсов, которые позволяют DNS-клиенту выполнять итерационные запросы и разрешить полное доменное имя. Этот вариант подходит, к примеру, когда клиентам надо разрешать имена Интернета, а локальный DNS-сервер содержит записи ресурсов только частного пространства имен. Другая ситуация, в которой надо отключить рекурсию, — когда из-за конфигурации или местоположения в локальной сети DNS-сервер неспособен разрешать внешние DNS-имена.

Внимание! Отключение рекурсии на DNS-сервере на вкладке **Дополнительно** делает невозможным использование серверов пересылки, а вкладка **Пересылка (Forwarders)** становится неактивной.

Флажок *Дополнительные службы BIND*

Этот флажок по умолчанию установлен, поэтому DNS-серверы под управлением Windows Server 2003 не используют формат быстрой передачи зон на дополнительные DNS-серверы, совместимые с BIND. Это ограничение обеспечивает совместимость передачи зон с ранними версиями BIND.

Примечание BIND — это стандартная реализация DNS, написанная и перенесенная на большинство имеющихся версий ОС UNIX.

Формат быстрой передачи (Fast transfer format) — эффективный механизм передачи данных зоны, поддерживающий сжатие данных и передачу нескольких записей в одном TCP-сообщении. Быстрая передача зоны всегда используется на DNS-серверах под управлением Windows, поэтому флажок **Дополнительные службы BIND** никак не влияет на связь между Windows-серверами. Следует помнить, что только 4.9.4 и более поздние версии BIND поддерживают такие передачи.

Если DNS-сервер выполняет зонные передачи с DNS-серверами, использующими BIND версии 4.9.4 или более поздние, отключите этот флажок, чтобы использовались быстрые передачи.

Примечание На момент написания этих строк самая последняя версия BIND — 9.2.2.

- **Включение/отключение поддержки формата быстрой передачи зон**

1. **В** дереве консоли *DNS* щелкните нужный DNS-сервер правой кнопкой и выберите **Свойства (Properties).**
2. На вкладке **Дополнительно (Advanced)** в списке **Параметры сервера (Server Options)** установите флажок **Дополнительные службы BIND (BIND Secondaries)** и щелкните OK.

Флажок *Ошибка, если данные при загрузке зоны повреждены*

По умолчанию этот флажок сброшен, и DNS-сервер под управлением Windows Server 2003 загружает зону, даже если обнаруживает ошибки в файле базы данных зоны. Ошибки регистрируются в журнале, но загрузка продолжается. Далее DNS-сервер пытается как обычно обслуживать запросы имен загруженной зоны.

Однако, если установить флажок **Ошибка, если данные при загрузке зоны повреждены,** DNS-сервер не станет загружать файле базы данных зоны, в котором есть ошибки.

Флажок *Включить расстановку по адресу*

По умолчанию этот флажок установлен и вынуждает DNS-сервер под управлением Windows Server 2003 в ответ на запрос от клиента на разрешение простого имени компьютера, которому соответствует несколько записей ресурсов-узлов (A), в первую очередь возвращать IP-адрес из подсети клиента.

Примечание Многоадресные компьютеры обычно регистрируют несколько записей ресурсов A для одного имени узла. Когда клиент пытается разрешить имя многоадресного компьютера, обращаясь к DNS-серверу, тот возвращает список всех записей ресурсов, удовлетворяющих условиям запроса. Затем DNS-клиент пытается связаться с первым IP-адресом в списке и при сбое последовательно запрашивает все IP-адреса из списка. Флажки **Включить расстановку по адресу** и **Включить циклическое обслуживание** каждый по своему изменяют порядок записей ресурсов в возвращаемом списке.

Простой пример: приоритет локальной сети

Многоадресному компьютеру serverl.lucernepublishmg.com сопоставлены три записи ресурсов A, соответствующие трем его IP-адресам в зоне *lucernepublishing.com*. Записи располагаются в таком порядке в зоне (файле зоны файле или Active Directory):

```
serverl   IN A   192.168.1.27
serverl   IN A   10.0.0.14
serveП    IN A   172.16.20.4
```

Когда распознаватель DNS-клиента с IP-адресом 10.4.3.2 запрашивает у сервера IP-адрес узла serverl.lucernepublisliing.com, DNS-сервер замечает, что IP-адрес источника-клиента (10.0.0.0) соответствует идентификатору сети (класс A) адреса 10.0.0.14 в списке записей ресурсов и переупорядочивает адреса в возвращаемом списке:

```
server1   IN A   10.0.0.14
server1   IN A   192.168.1,27
server1   IN A   172.16.20.4
```

Если в списке нет соответствующих IP-адресу клиента записей ресурсов локальной сети, список остается без изменений.

Сложный пример: приоритет локальной подсети

В сети с IP-подсетями (маски подсети не по умолчанию) в списке ответа DNS-сервер размещает IP-адреса, соответствующие клиентским идентификаторам сети и подсети перед адресами, в которых совпадает только сетевой идентификатор.

Допустим, многоадресному компьютеру server1.lucernepublishing.com соответствуют четыре записи ресурса — по одной на каждый из его четырех IP-адресов в зоне *lucernepublishing.com*. Два из них относятся к отдельным сетям, а в остальных двух адресах сети совпадают, но из-за нестандартной маски сети 255.255.248.0 они располагаются в различных подсетях. В файле зоны или Active Directory эти записи ресурсов упорядочены так:

```
server1   IN A   192.168.1.27
server1   IN A   172.16.22.4
server1   IN A   10.0.0.14
server1   IN A   172.16.31.5
```

Если IP-адрес клиента — 172.16.22.8, оба IP-адреса в одной с клиентом сети 172.16.0.0 размещаются в начале списка ответа. Однако адрес 172.16.22.4 размещается до адреса 172.16.31.5, потому что соответствует IP-адресу клиента после наложения адреса подсети 172.16.20.0. Переупорядоченный список выглядит так:

```
server1   IN A   172.16.22.4
server1   IN A   172.16.31.5
server1   IN A   192.168.1.27
server1   IN A   10.0.0.14
```

Отключают расстановку по адресу так.

1. В дереве консоли *DNS* щелкните нужный DNS-сервер правой кнопкой и выберите **Свойства (Properties).**
2. На вкладке **Дополнительно (Advanced)** в списке **Параметры сервера (Server Options)** сбросьте флажок **Включить расстановку по адресу (Enable Netmask Ordering)** и щелкните **ОК.**

Подготовка к экзамену В билетах экзамена на звание MCSE расстановку по адресу часто называют параметром LocalNetPriority, который аналогичен соответствующему параметру утилиты командной строки Dnscmd.

Флажок *Включить циклическое обслуживание*

Этот флажок установлен по умолчанию, в этом случае при запросе адреса многоадресного узла DNS-сервер под управлением Windows Server 2003 выполняет ротацию элементов в списке, возвращаемом клиенту. Это один из простейших способов балансировки сетевой нагрузки между сетевыми адаптерами активно обслуживающих клиентские запросы многоадресных компьютеров. Эта функция также часто используется для

балансировки запросов среди нескольких серверов, предоставляющих идентичные сетевые сервисы, например, среди Web-серверов, обслуживающих один Web-сайт.

Примечание На многоадресных компьютерах упорядочение по адресу приоритетнее циклического обслуживание. Тем не менее, при включении обеих функций циклическое обслуживание используется как дополнительный метод сортировки записей.

Пример циклического обслуживания

У Web-сервера serverl.lucernepublishing.com есть три сетевых адаптера с тремя разными IP-адресами. Соответствующие записи ресурсов в зоне выглядят так:

```
served  IN A  10.0.0.1
served  IN A  1.0.0.0.2
serveП  IN A  10.0.0.3
```

Первый DNS-клиент Client!, запросивший имя Web-сервера, получит список в обычном (без изменений) порядке. Однако следующий клиент, Client2, получит случайно переупорядоченный список, например такой:

```
serverl  IN A  10.0.0.2
serverl  IN A  10.0.0.3
serverl  IN A  10.0.0.1
```

Отключение циклического обслуживания

Циклическое обслуживание отключается сбрасыванием флажка **Включить циклическое обслуживание (Enable round robin)** на вкладке **Дополнительно** окна свойств DNS-сервера. В этом случае при запросе многоадресного компьютера клиенты получают с DNS-сервера записи ресурсов в том порядке, в каком они определены в зоне.

Флажок *Включить безопасный кэш*

По умолчанию этот флажок установлен и запрещает DNS-серверу размещать в кэше небезопасные и «мусорные» ссылки. Сервер кэширует только записи с именами, соответствующими запрошенному домену. Все ссылки, полученные с других DNS-серверов, и ответы на запросы попросту игнорируются.

Если запрошено имя *example.microsoft.com* и в ответе-ссылке указано имя не из дерева доменов *microsoft.com* (например *msn.com),* ответ отбрасывается. Эта функция не позволяет неправомочным компьютерам выдавать себя за другие сетевые серверы.

Если этот флажок отключен, сервер кэширует все записи, полученные в ответ на DNS-запрос, в том числе и те, имена в которых не соответствуют имени запрошенного домена.

Поле со списком *Проверка имен*

По умолчанию в этом поле выбран вариант **Многобайтовый (UTF8) [Multibyte (UTF8)],** и DNS-служба проверяет все доменные имена на предмет соответствия формату UTF (Unicode Transformation Format). Unicode — это схема кодирования символов двумя байтами, совместимая с традиционным 1-байтовым US-ASCII-форматом, который поддерживает двоичное представление большинства языков.

На рис. 5-28 показаны четыре метода проверки имен, доступные для выбора в поле **Проверка имен** (табл. 5-3).

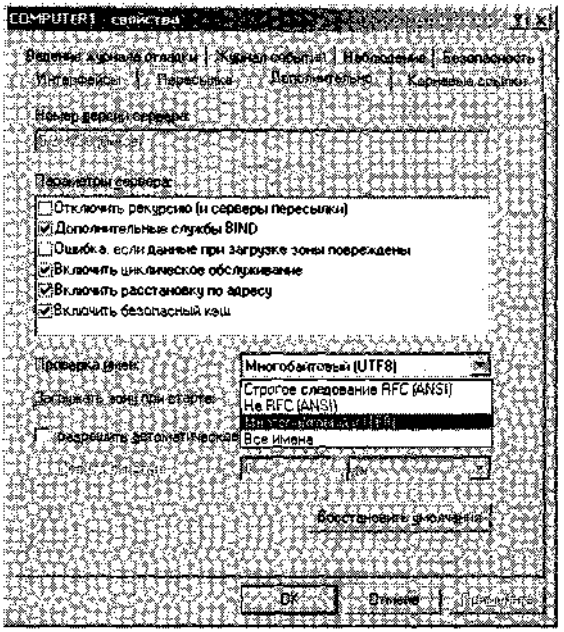


Рис. 5-28. Методы проверки имен

Табл. 5-3. Методы проверки имен

Метод	Описание
Строгое следование RFC (ANSI) [Strict RFC (ANSI)]	Строгая проверка имен в соответствии с ограничениями, определенными в RFC 1123, то есть разрешены только буквы верхнего и нижнего регистра (A-Z, a-z), цифры (0-9) и дефис (-). DNS-имя может начинаться с цифры
Не RFC (ANSI) [Non RFC (ANSI)]	Разрешены нестандартные имена, даже не отвечающие стандарту RFC 1123
Многобайтовый (UTF8) [Multibyte (UTF8)]	Разрешено распознавание символов, отличающихся от ASCII, в том числе Unicode-символов, которые обычно кодируются несколькими октетами. В этом варианте многобайтовые символы могут представляться в виде UTF-8, поддерживаемом Windows Server 2003. Длина имен в формате UTF-8 не. должна превышать ограничения, определенного в RFC 2181, то есть не более 63 октетов на метку и 255 в расчете на имя. Число символов нельзя узнать по длине, так как длина некоторых символов UTF-8 превышает один октет. В этом варианте поддерживаются доменные имена с использованием других алфавитов, не только латинского
Все имена [All Names]	Разрешаются имена в любом формате

Несмотря на гибкость, предоставляемую UTF-8, рекомендуется использовать вариант **Строгое следование RFC (ANSI)** при выполнении передач зоны на серверы не под управлением Windows и не поддерживающие UTF-8. Хотя DNS-серверы, не поддержи-

вающие UTF-8, могут оказаться способными принимать передачи зон с именами в формате UTF-8, они не поддерживают запись/загрузку таких имен в/из файла.

Остальные два варианта проверки имен — Не RFC (ANSI) и **Все** имена — рекомендуется применять, только когда этого требует определенное приложение.

Поле со списком *Загружать зону при старте*

По умолчанию в этом поле выбран вариант **Из Active Directory и реестра,** то есть DNS-серверы в Windows Server 2003 инициализируются с параметрами, указанными в базе данных Active Directory и реестре.

В поле со списком есть еще два варианта (рис. 5-29): **Из реестра (From Registry)** и **Из файла (From File).**

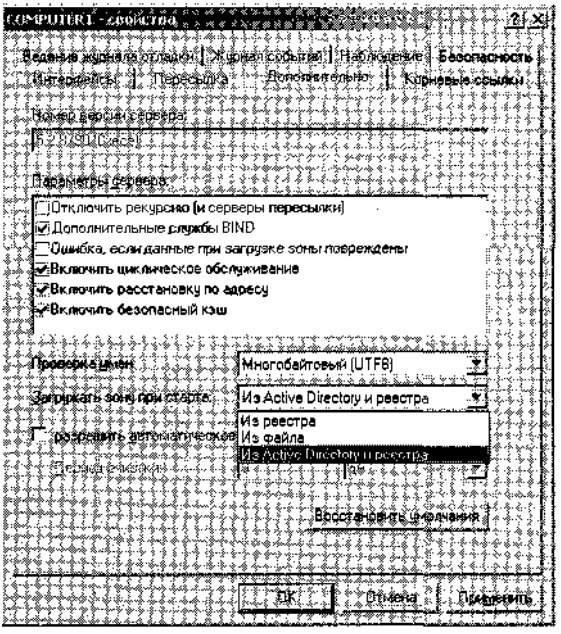


Рис. 5-29. Параметры инициализации сервера

При выборе первого варианта DNS-сервер считывает параметры из реестра Windows, а если выбрать второй, DNS-сервер загружает с параметры из загрузочного файла, похожего на те, что используются на BIND-серверах. Обычно такой файл называется Named.boot; он должен быть в старом (BIND 4), а не новом формате BIND 8. При использовании загрузочного файла на сервере применяются определенные в нем параметры, причем при конфликте с параметрами из реестра приоритет отдается параметрам из файла.

Флажок *Разрешить автоматическое удаление устаревших записей*

По умолчанию этот флажок сброшен, и DNS-серверы под управлением Windows Server 2003 автоматически не удаляют устаревшие записи ресурсов из зоны, в которой включен режим очистки.

Когда этот флажок установлен, очистка выполняется автоматически с периодичностью, определенной в свойствах зоны.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы сетевой администратор компании Lucerne Publis. Корпоративная сеть состоит из одного домена *lucemepublishing.com,* который подключен к Интернету через брандмауэр, расположенный на компьютере NS1. На NS1 также располагается DNS-сервер, причем.служба брандмауэра разрешает DNS-трафик между Интернетом и службой DNS на NS1, но не между Интернетом и внутренней сетью. На DNS-сервере включено циклическое обслуживание. Во внутренней сети расположены два компьютера NS2 и NS3 под управлением Windows Server 2003 — соответственно основной и дополнительный DNS-серверы. зоны *lucernepublishing.com*.

   Пользователи сети жалуются, что, указывая имена узлов, они подключаются к компьютерами локальной сети, но не могут подключиться таким способом к узлам Интернета, например *www.microsoft.com*.

   Какое из перечисленных ниже действий решает задачу, требуя минимальных усилий от администратора?

   a. Отключение рекурсии на NS2 и NS3.
   b. Включение расстановки по адресу на NS1.
   c. Конфигурирование NS2 и NS3 на использование NS1 в качестве сервера пересылки.
   d. Отключение циклического обслуживания на NS1.

2. Вы администратор крупной сети, состоящей из 10 доменов. Вы сконфигурировали стандартную основную зону в домене *mfg.lucernepublishing.com* на компьютере Serverl, на котором также расположен DNS-сервер, сконфигурировали UNIX-сервер Server2, на котором располагается дополнительная зона того же домена. UNIX-сервер поддерживает BIND 8.2.I.

   Обнаружилось, что зонные передачи между основным и Дополнительным серверами инициируют значительно больший трафик, чем ожидалось, и перегружают сетевые ресурсы.

   Что можно предпринять для снижения нагрузки на сеть, обусловленной передачами зон между основным и дополнительным серверами?

   a. Сбросить флажок **Дополнительные службы BIND (BIND Secondaries)** на Serverl.
   b. Сконфигурировать загрузочный файл на Serverl для инициализации совместимых с BIND параметров.
   c. Установить флажок **Дополнительные службы BIND (BIND Secondaries)** на Serverl.
   d. Сконфигурировать загрузочный файл на Server2 для поддержки быстрых зонных передач.

3. Какова роль циклического обслуживания? Какая функция приоритетнее: циклическое обслуживание или расстановка по адресу?

4. Вы ведущий администратор сети компании Proseware, имеющей четыре филиала. В каждом филиале собственная локальная сеть, подключенная к Интернету по линии T1. Используя технологию VPN, сети филиалов объединены в единую интрасеть; репликация обеспечивается Web-серверам, расположенными в каждом филиале. У этих четырех Web-серверов уникальные IP-адреса, но одно полное доменное имя (FQDN) *intranet.proseware.com* (рис. 5-30).

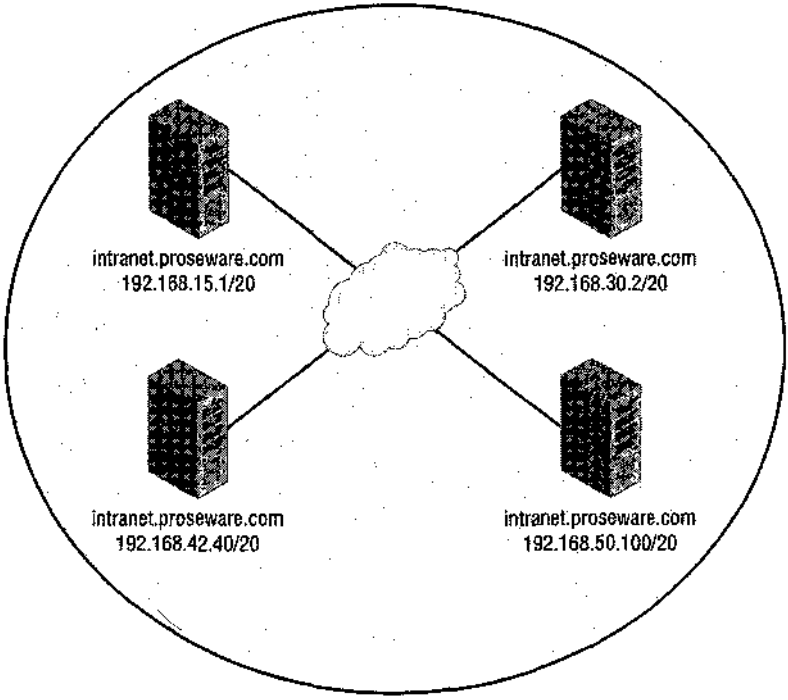


Рис. 5-30. Интрасетевые серверы компании Proseware

DNS-клиент сети Proseware с IP-адресом 192.168.33.5 направляет на DNS-сервер запрос на разрешение имени *intranet.proseware.com*. Предполагается, что на DNS-сервере включена функция **Включить расстановку по адресу (Enable Netmask Ordering).** Какой IP-адрес получит DNS-клиент? (Подсказка: выясните, у которого из четырех Web-серверов идентификатор подсети совпадает с идентификатором подсети клиента.)

Резюме

- Вкладка **Дополнительно (Advanced)** окна свойств DNS-сервера позволяет настраивать девять установочных параметров сервера.
- Флажок **Отключить рекурсию (Disable Recursion)** по умолчанию сброшен, поэтому DNS-сервер выполняет рекурсию при разрешении клиентских запросов только если такое поведение не запрещено особой конфигурацией клиента.
- Флажок **Дополнительные службы BIND (BIND Secondaries)** по умолчанию установлен, поэтому DNS-серверы под управлением Windows Server 2003 не используют формат быстрой передачи зон на дополнительные DNS-серверы, поддерживающие BIND. Это ограничение обеспечивает совместимость передачи зон с ранними версиями BIND.
- Флажок **Включить расстановку По адресу (Enable Netmask Ordering)** по умолчанию установлен и вынуждает DNS-сервер под управлением Windows Server 2003 в ответ на запрос от клиента на разрешение простого имени компьютера, которому соответствует несколько записей ресурсов-узлов (A), в первую очередь возвращать IP-адрес из подсети клиента.

- Флажок **Включить циклическое обслуживание (Enable round robin)** установлен по умолчанию и обеспечивает при запросе адреса многоадресного узла выполнение DNS-сервером под управлением Windows Server 2003 ротации элементов в списке записей ресурсов A, возвращаемом клиенту.

Занятие 4. **Создание делегирования зон**

Управление огромным пространством имен, например Интернетом, невозможно представить без делегирования администрирования доменов, которое подразумевает создание новой зоны при передаче ответственности за поддомен отдельному субъекту. Обычно в этой роли выступает автономная организация или филиал компании.

Делегирование зон создается в консоли *DNS* с помощью *Мастера делегирования* (New Delegation Wizard).

Изучив материал этого занятия, вы сможете:

- создать делегированную зону в рамках существующего пространства имен DNS;
- рассказать о преимуществах делегирования зон.

Продолжительность занятия — около 30 минут.

Делегирование зон

Делегировать зону означает предоставить полномочия на управление поддоменом пространства имен DNS, т. е. ответственность за записи ресурсов поддомена передается от владельца родительского домена владельцу поддомена. На рис. 5-31 управление доменом *microsoft.com* делегировано двум зонам: *microsoft.com* и *mydomain.microsoft.com*. Здесь администратор зоны *mydomain.microsoft.com* управляет записями ресурсов своего поддомена.

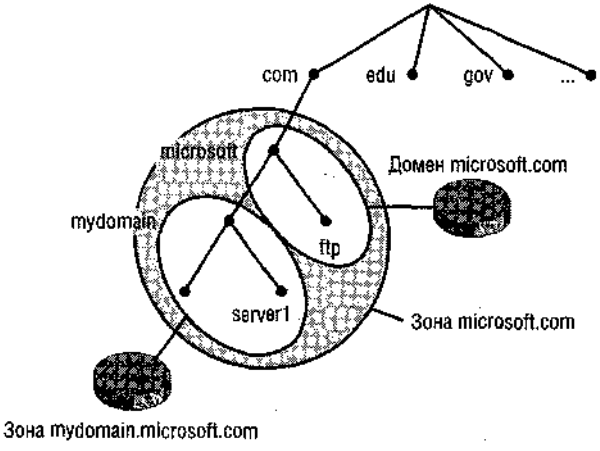


Рис. 5-31. Пример делегирования зон

Когда необходимо делегировать зоны

Делегировать зоны в рамках корпоративной сети рекомендуется, когда:

- нужно делегировать управление DNS-доменом филиалу или отдельному подразделению компании:
- необходимо распределить нагрузку по поддержке одной большой базы данных DNS среди многих серверов имен, чтобы повысить производительность разрешения имен и отказоустойчивость;
- требуется, чтобы структура имен узлов совпадала со структурой подразделений организации.

При определении структуры зон следует составить план, отражающий структуру организации.

Механизм делегирования

Для успешной реализации делегирования родительская зона должна содержать обе записи ресурсов — A и NS, указывающие на полномочный сервер вновь делегированного домена. Эти записи необходимы как для передачи полномочий новым серверам имен, так и предоставления ссылок клиентам, выполняющим итерационные запросы. В этом разделе описывается пример делегирования поддомена в новую зону.

Примечание При создании нового делегирования в консоли *DNS* указанные записи создаются автоматически.

На рис. 5-32 полномочному компьютеру DNS-сервера для вновь делегированного поддомена *example.microsoft.com* присвоено имя в соответствии с именем производного поддомена новой зоны *{nsl.us.example.microsoft.com)*. Чтобы информация об этом сервере была известной за пределами вновь делегированной зоны, в зоне *microsoft.com* надо создать две записи ресурсов *(Мастер делегирования* в консоли *DNS* создает эти записи автоматически):

- **запись NS, или *запись делегирования* (delegation record),** которая фактически и определяет делегирование и используется для извещения запрашивающих клиентов, что компьютер *nsl.us.example.microsoft.com* является полномочным для делегированного поддомена;
- **запись ресурса A, или *связывающая запись*** (glue record), служащая для разрешения имени сервера, указанного в записи NS, в IP-адрес. Связывающие записи необходимы, если сервер имен, полномочный для делегированной зоны, одновременно является членом делегированного домена. Процесс разрешения имени узла в этой NS-записи в адрес делегированного DNS-сервера иногда называют *отслеживанием связей* (glue chasing).

Примечание После создания делегирования в консоли *DNS* связывающая запись автоматически появляется в данных зоны, однако в консоли *DNS* эта запись не видна.

Допустим, внешнему DNS-серверу (действующему как клиент) нужно разрешить полное доменное имя *box.example.microsoft.com*. Когда сервер запрашивает сервер имен, полномочный для *microsoft.com* домена, он получает связывающую запись с информацией, что имя полномочного сервера имен для домена *example.microsoft.com* — nsl.us.example.microsoft.com, а его IP-адрес— 192.168.1.5. Далее клиент выполняет следующий итерационный запрос сервера имен *nsl.us.example.microsoft.com,* который и возвращает IP-адрес узла *box.example.microsoft.com*.

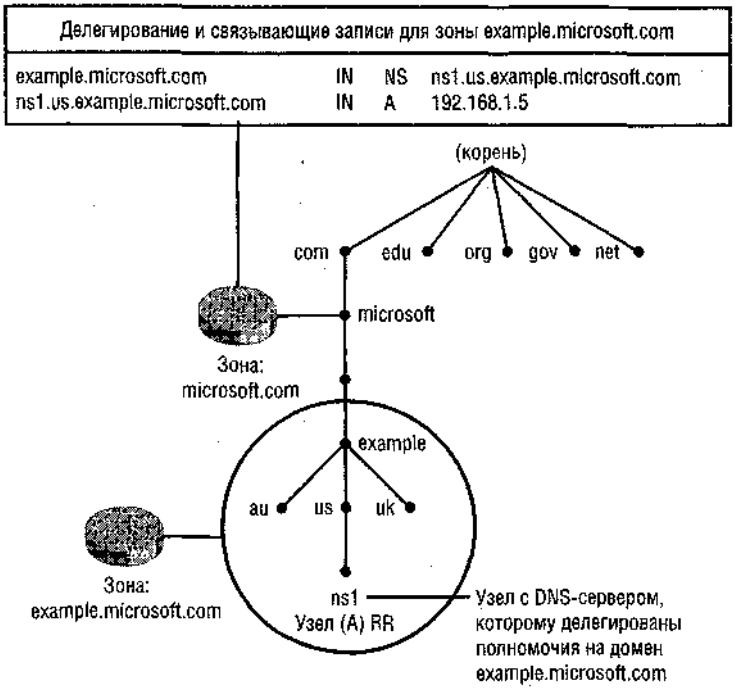


Рис. 5-32. Записи ресурсов при делегировании

Примечание Делегирование приоритетнее *пересылки* (forwarding). Если в предыдущем примере полномочный сервер в домене *microsoft.com* настроить на пересылку всех запросов, на которые он не в состоянии ответить самостоятельно, сервер все равйо будет разрешать имя *box.example.microsoft.com,* обращаясь к nsl.us.example.microsoft.com, а не к серверу пересылки, указанному на вкладке **Пересылка (Forwarders).**

Создание делегирования зоны

До делегирования создают домен, делегируемый серверу, на котором будет размещаться делегированная зона. Затем выполняют *Мастер делегирования* (New Delegation Wizard) на сервере, обслуживающим родительскую зону, щелкнув узел родительской зоны в консоли *DNS* правой кнопкой и выбрав **Создать делегирование (New Delegation).**

Мастер делегирования потребует задать имя делегируемого поддомена и имя по крайней мере одного сервера имен, который будет полномочным в новой зоне. По завершении мастера узел появляется в дереве консоли *DNS,* представляя вновь делегированный поддомен. Этот узел содержит запись делегирования (NS) о только что определенном полномочном сервере. Связывающая запись записывается в базу данных зоны, но не отображается в консоли *DNS.*

- **Создание делегирования зоны**

1. В дереве консоли *DNS* щелкните нужный домен правой кнопкой и выберите **Создать делегирование (New Delegation).** Откроется окно **Мастер делегирования (New Delegation Wizard).**
2. Следуя инструкциям *Мастера делегирования,* создайте новый делегированный домен.

Лабораторная работа. Создание делегирования зоны

Вы создадите новую зону на Computer2, которая станет делегированным поддоменом домена *domain!.local.* Затем создадите делегирование на Computerl, который свяжете с новой зоной на Computer2. В завершение вы проверите новую конфигурацию.

Упражнение 1. Создание зоны для делегирования

Вы создадите новую зону на Computer2.

1. Войдите в систему Computer2 как *Администратор* (Administrator).
2. В дереве консоли *DNS* щелкните узел **Зоны прямого просмотра (Forward Lookup Zones)** правой кнопкой и выберите **Создать новую зону (New Zone).** Откроется окно **Мастер создания новой зоны (New Zone Wizard).** Щелкните **Далее (Next).**
3. На странице **Тип зоны (Zone Type)** оставьте выбранный по умолчанию вариант — **Основная зона (Primary Zone)** и щелкните **Далее.**
4. В текстовом поле **Имя зоны (Name)** введите sub. domainl, local и щелкните **Далее.**
5. На странице **Файл зоны (Zone .File)** оставьте выбранный по умолчанию вариант — **Создать новый файл (Create a new file with this file name)** и щелкните Далее.
6. На странице **(Dynamic Update)** выберите **Разрешить любые обновления (Allow both nonsecure and secure dynamic updates)** и щелкните **Далее.**
7. На странице **Завершение мастера создания новой зоны (Completing the New Zone Wizard)** щелкните **Готово (Finish).**

Упражнение 2. Добавление записи ресурса-узла (A) в зону

Вы создадите записи в новой зоне, которые потребуются в дальнейшем для проверки делегирования зон.

1. С Computer2 войдите в домен *Domainl* как *Администратор* (Administrator).
2. В дереве консоли *DNS* щелкните узел **Sub.domainl.local** правой кнопкой и выберите **Создать узел (A) [New Host (A)].**
3. **В** окне **Новый узел (New Host)** в текстовом поле **Имя (Name)** введите compute r1.
4. В текстовом поле **IP-адрес (IP address)** введите 192. 168.0. 1 (текущий IP-адрес Computerl) и щелкните **Добавить узел (Add Host).** Появится информационное окно с сообщением об успешном создании записи узла.
5. Щелкните **OK.** Окно **Новый узел** останется открытым, а поля **Имя** и **IP-адрес** очистятся.
6. В поле **Имя** введите, computer2, а в поле **IP-адрес** введите текущий IP-адрес Computer2.
7. Щелкните **Добавить узел.** Появится информационное окно с сообщением об успешном создании записи узла.
8. Щелкните OK, а затем **Готово (Done).**
9. Выйдите из системы Computer2.

Упражнение 3. Создание делегирования

Вы создадите делегирование на Computerl, связанное с зоной *sub.domainl.local* на Computer2.

1. Войдите в систему Computerl под учетной записью *Администратор* (Administrator) домена *Domain 1.*

2. В дереве консоли *DNS* щелкните узел **Domain 1.local** правой кнопкой и выберите **Создать делегирование (New Delegation).**
3. **В** окне **Мастер делегирования (New Delegation Wizard)** щелкните **Далее** (Next).
4. В текстовом поле **Делегируемый домен (Delegated Domain)** введите sub и щелкните **Далее.**
5. На странице **Серверы имен (Name Servers)** щелкните **Добавить (Add).**
6. В окне **Новая запись ресурса (New Resource Record)** в текстовом поле **Полное доменное имя сервера (FQDN) (Server Fully Qualified Domain Name)** введите computer2. sub. Domainl. local. В текстовом поле **IP-адрес (IP Address)** введите текущий IP-адрес Computer2.
7. Щелкните **Добавить,** а затем OK.
8. На странице **Серверы имен** щелкните **Далее.**
9. На странице **Завершение мастера делегирования (Completing the New Delegation Wizard)** щелкните **Готово (Finished). В** дереве консоли *DNS* в зоне *domainl.local* появится подузел **Sub.**
10. Используя консоль *DNS,* ответьте на вопрос: сколько записей ресурсов-узлов (A), соответствующих домену *sub.domainl.local,* хранится на Computerl?

Упражнение 4. Проверка конфигурации

Вы проверите утилитой ping узлы вновь делегированного домена. Упражнение выполняется на Computerl, чтобы воспользоваться для разрешения имен его локальным DNS-сервером.

1. С Computerl войдите в домен *Domainl как. Администратор* (Administrator).
2. В окне командной строки выполните команду ping computerl. sub. domainl. local. В листинге работы утилиты указано, что узел computerl.sub.domainl.local отвечает с IP-адреса 192.168.0.1. Если эхо-ответ отсутствует, подождите 2 минуты и выполните команду ipconfig /flushdns.
3. Выполните команду ping computer2. sub. domainl. local. В листинге работы утилиты указано, что computer2.sub.domainl.local отвечает с IP-адреса 192.168.0.2. Если эхо-ответа нет, подождите 2 минуты и выполните команду ipconfig' /flushdns.
   Новые имена компьютеров разрешаются в IP-адреса даже при том, что локальный компьютер, Computerl, разрешает имена с применением локальной службы DNS-сервера, который не содержит никаких записей об узлах домена *sub.domainl.local.* Локальный DNS-сервер корректно пересылает запросы на разрешение имен узлов в поддомене *sub.domainl .local* на сервер имен, полномочный для этого домена, то есть на Computer2.
4. Выйдите из системы Computerl.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы проектируете пространство имен DNS для компании Proseware, владеющей зарегистрированным интернет-доменом *proseware.com*. Штаб-квартира Proseware расположена в Рочестере и два филиала — в Буффало и Сиракузах. В каждом отделении

своя ЛВС, управляемая местным сетевым администратором. Требуется установить по одному DNS-серверу в каждом отделении, причем домен *proseware.com* должен обслуживаться сервером штаб-квартиры. Кроме того, администраторы в Буффало и Сиракузах должны самостоятельно управлять DNS-именами и разрешением имен в своих сетях. Что из перечисленного ниже необходимо предпринять для решения поставленной задачи?

a. Создать стандартный основный сервер в Рочестере и разместить на нем зону *proseware.com*. Делегировать по подцомену каждому из филиалов. Сконфигурировать по дополнительному серверу в Буффало и Сиракузах, разместив на этих серверах делегированные поддомены.

b. Создать стандартный основный сервер в Рочестере и разместить на нем зону *proseware.com*. Сконфигурировать по дополнительному серверу в Буффало и Сиракузах для повышения производительности и отказоустойчивость зоны.

c. Создать DNS-сервер в Рочестере и разместить на нем стандартную основную зону *proseware.com*. Сконфигурировать DNS-серверы в Буффало и Сиракузах, разместив на каждом по стандартной основной зоне поддомена *proseware.com*. Создать делегирование с DNS-сервера в Рочестере каждому из этих поддоменов.

d. Создать DNS-сервер в Рочестере и разместить на нем стандартную основную зону *proseware.com*. Сконфигурировать DNS-серверы в Буффало и Сиракузах, разместив на каждом по стандартной основной зоне поддомена *proseware.com*. Создать по дополнительной зоне на каждом DNS-сервере, получающей передачи из основных зон, расположенных на двух других DNS-серверах.

2. Вы администратор корпоративной сети, состоящей из ЛВС штаб-квартиры и трех филиалов, расположенных в различных городах. Решено спроектировать новую инфраструктуру DNS и развернуть Active Directory. Нужно: во-первых, создать единый лес Active Directory во всех четырех отделениях, во-вторых, сократить до минимума время отклика для пользователей, подключающихся к ресурсами из любого места сети. Во всех отделениях есть контроллеры доменов с DNS-сервером. Что из перечисленного ниже лучше всего предпринять для решения поставленной задачи?

   a. Создать один домен Active Directory для всех четырех отделений и единую интегрированную в Active Directory DNS-зону, реплицируемую в пределах всего домена.

   b. Создать один домен Active Directory для всех четырех отделений и стандартную основную зону в штаб-квартире и по одной дополнительной зоне в филиалах.

   c. Создать домен Active Directory и домен DNS в штаб-квартире, делегировать по поддомену DNS каждому филиалу и создать интегрированную в Active Directory зону в каждом отделении, реплицируемую в рамках всего леса.

   d. Создать домен Active Directory и домен DNS в штаб-квартире, делегировать по поддомену DNS каждому филиалу и создать интегрированную в Active Directory зону в каждом отделении, реплицируемую в рамках всего домена.

3. Какие записи ресурсов создаются в родительской зоне при делегировании поддомена? В чем особые функции этих записей?

4. DNS-сервер NS1 обслуживает зону *lucemepublishing.com* и сконфигурирован на пересылку всех запросов имен, для которых не является полномочным. На NS1 поступает запрос на разрешение имени делегированного домена *sub.lucernepublishing.com*. Куда будет направлен запрос?

Резюме

- Делегировать зону — означает предоставить полномочия на управление поддоменом пространства имен DNS, то есть ответственность за записи ресурсов поддомена передается от владельца родительского домена владельцу поддомена.
- Делегировать зоны в рамках корпоративной сети рекомендуется в следующих ситуациях: когда нужно делегировать управление DNS-доменом филиалу или отдельному подразделению компании; когда необходимо распределить нагрузку по поддержке одной большой базы данных DNS среди многих серверов имен, чтобы повысить производительность разрешения имен и отказоустойчивость, и когда структура имен узлов должна совпадать со структурой подразделений организации.
- Для успешной реализации делегирования родительская зона должна содержать две записи ресурсов — A и NS, указывающие на полномочный сервер вновь делегированного домена. Эти записи необходимы как для передачи полномочий новым серверам имен, так и предоставления ссылок клиентам, выполняющим итерационные запросы. При определении делегирования в консоли DNS эти записи создаются автоматически.
- До делегирования создают домен, делегируемый серверу, на котором будет размещаться делегированная зона. Затем выполняют *Мастер делегирования* (New Delegation Wizard) на сервере, обслуживающем родительскую зону, щелкнув правой кнопкой узел родительской зоны в консоли *DNS* и выбрав в контекстном меню **Создать делегирование (New Delegation).**

Занятие 5. Развертывание зоны-заглушки

Зона-заглушка (stub zone) — это регулярно обновляемая сокращенная копия зоны, содержащая только записи NS главной зоны. Сервер, обслуживающий зону-заглушку, сам не разрешает запросы имен зоны, а перенаправляет их на серверы имен, указанные в записях ресурсов NS зоны-заглушки.

Изучив материал этого занятия, вы сможете:

- *S* создать зону-заглушку;
- *S* рассказать о преимуществах и ограничениях зон-заглушек.

Продолжительность занятия — около 30 минут.

Общие сведения о зонах-заглушках

При создании новой зоны с помощью *Мастера создания новой зоны* (New Zone Wizard) выбирают тип зоны: основная, дополнительная или зона-заглушка (рис. 5-33). Зона-заглушка поддерживает только те записи ресурсов NS, которые необходимы для обнаружения серверов имен главной зоны, определяемой по имени зоны-заглушки.

Основное предназначение зоны-заглушки — хранить и регулярно обновлять все записи ресурсов NS главной зоны. При определении зоны-заглушки нужно определить по крайней мере один, главный сервер имен, IP-адрес которого не изменяется. Информация о любых новых серверах имен, добавляемых в главную зону позже, автоматически обновляется в зоне-заглушке путем зонных передач. Записи ресурсов зоны-заглушки нельзя изменять — все изменения должны вноситься в исходную основную зону.

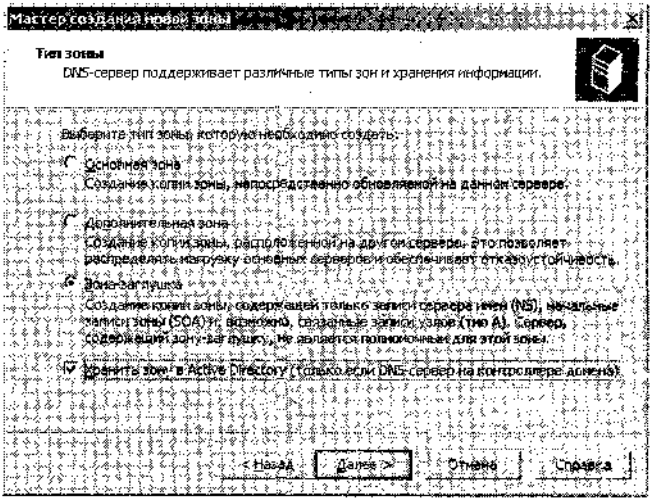


Рис. 5-33. Создание зоны-заглушки

•. Создание зоны-заглушки

1. 'В дереве консоли *DNS* щелкните DNS-сервер правой кнопкой и выберите Создать **новую** зону (New **Zone).** Откроется окно Мастер создания новой зоны (New **Zone Wizard).**
2. Следуя инструкциям мастера, создайте новую зону-заглушку.

Преимущества зон-заглушек

- Повышение производительности разрешения имен — зоны-заглушки позволяют DNS-серверу выполнять рекурсию на основании списка серверов имен, не обращаясь к корневому серверу.
- **Постоянное обновление информации** «чужой» зоны — регулярное обновление зоны-заглушки позволяет DNS-серверу поддерживать в актуальном состоянии список серверов имен другой зоны, например делегированной зоны на другом DNS-сервере.
- **Упрощение администрирования DNS** — размещение зон-заглушек в инфраструктуре DNS позволяет распространять информацию зоны, не прибегая к дополнительным зонам.

Внимание! Зоны-заглушки не выполняют той же функции, что и дополнительные зоны, и их нельзя использовать в качестве альтернативы при планировании отказоустойчивости, избыточности или балансировки нагрузки.

Когда применяются зоны-заглушки

Зоны-заглушки чаще всего используют для отслеживания полномочных серверов имен в делегированных зонах и обычно размещаются на родительских DNS-серверах делегированных зон.

DNS-сервер, делегировавший дочернюю зону другому DNS-серверу, обычно получает информацию о новых полномочных DNS-серверах в дочерней зоне, только когда соответствующие записи ресурсов добавляются в родительскую зону вручную. А зона-заглушка делегированной зоны позволяет DNS-серверу своевременно получать сведе-

ния об изменении состава полномочных серверов этой зоны. Эта функция подробно объясняется в следующем примере и иллюстрируется рис. 5-34.

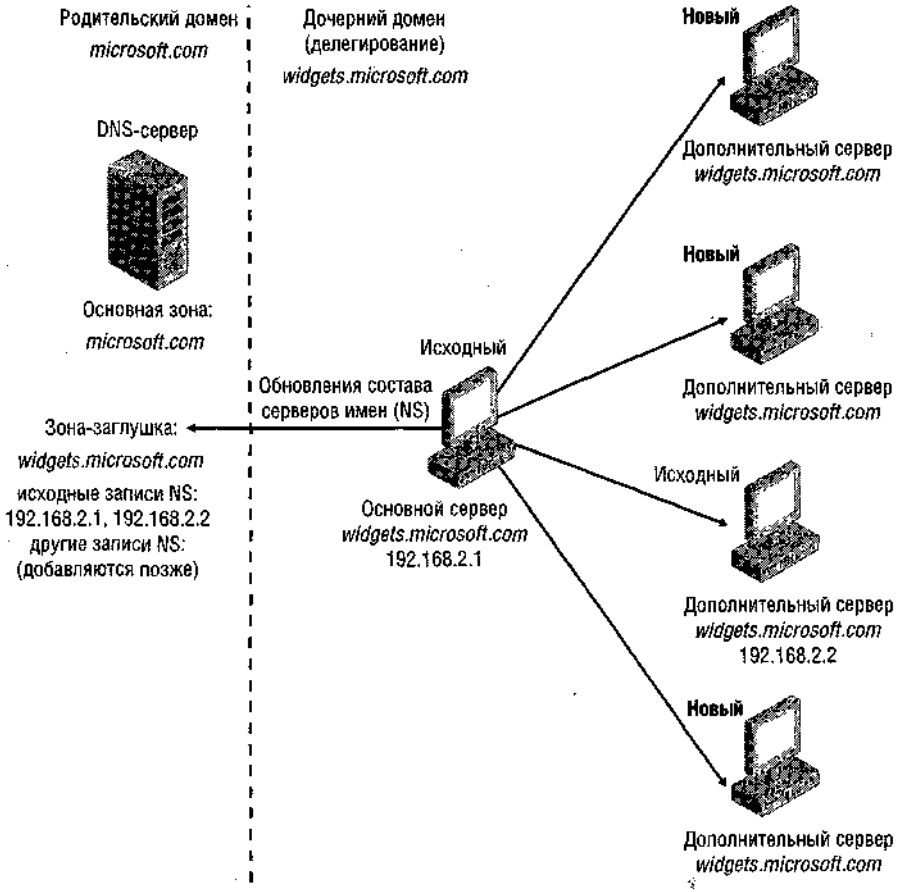


Рис. 5-34. Зоны-заглушки и делегирование

Подготовка к экзамену Почти наверняка на экзамене будут вопросы о зонах-заглушках. Очень важно помнить, в каких ситуациях их необходимо развертывать.

Пример зоны-заглушки

DNS-сервер, полномочный в родительской зоне *microsoft.com*, делегировал дочернюю зону *widgets.microsoft.com* отдельному DNS-серверу. На момент создания делегирования оно содержало только две записи ресурсов NS, соответствующие полномочным DNS-серверам зоны *widgets.microsoft.com*. Позднее администраторы этой зоны развернули в ней дополнительные полномочные DNS-серверы, но не уведомили об этом администраторов родительской зоны *microsoft.com*. В результате полномочный DNS-сервер родительской зоны ничего не «знает» о наличии новых полномочных DNS-серверов дочерней зоны *widgets.microsoft.com*, и продолжает запрашивать единственные известные ему два DNS-серверы.

Исправить ситуацию можно, сконфигурировав на полномочном DNS-сервере родительской зоны *microsoft.com* зону-заглушку дочерней зоны *widgets.microsoft.com*. Теперь при обновлении записей ресурсов зоны-заглушки на полномочном DNS-сервере зоны *microsoft.com* он запросит на главном сервере *widgets.microsoft.com* список полномочных DNS-серверов дочерней зоны. Кроме того, полномочный DNS-сервер родительской зоны узнает о новых серверах имен, полномочных в дочерней зоне *widgets.microsoft.com*, и сможет выполнять рекурсию на любые существующие полномочные DNS-серверы дочерней зоны.

Другие варианты использования зон-заглушек

Зоны-заглушки также применяются для упрощения процесса разрешения имен между доменами за счет исключения поиска в пространстве имен DNS общего родительского сервера. Зоны-заглушки подменяют дополнительные зоны, когда необходима DNS-связь между доменами, но избыточность данных основной зоны не нужна. Также важно, что зоны-заглушки облегчают разрешение имен и разгружают сетевые ресурсы, освобождая от объемных передач зон.

Рис. 5-35 иллюстрирует использование зон-заглушек для упрощения разрешения имен. Здесь запрос имени узла ns.mgmt.ldn.microsoft.com направляется на два сервера имен. Первый — полномочный в домене *mfg.wa.microsoft.com*. Ему приходится обращаться ко многим другим серверам имен, пока запрос попадет на сервер имен, полномочный для соответствующего домена *(mgmt.ldn.microsoft.com)*. Во втором случае на сервере имен есть зона-заглушка *mgmt.ldn.microsoft.com*, поэтому он «знает» адрес сервера, полномочного в *ns.mgmt.ldn.microsoft.com* и автоматически направляет рекурсивный запрос непосредственно на полномочный сервер.

Записи ресурсов зон-заглушек

Зона-заглушка содержит записи ресурсов SOA, NS и связывающие записи A полномочных DNS-серверов зоны. Запись SOA содержит идентификатор основного DNS-сервера исходной зоны (главного сервера) и другие параметры зоны, запись NS содержит список полномочных (основных и дополнительных) DNS-серверов зоны, а связывающая запись содержит IP-адреса полномочных DNS-серверов зоны.

Примечание Как в делегированных зонах, зоны-заглушки содержат связывающие записи данных зоны, но эти записи не отображаются в консоли *DNS*.

Разрешение с применением зоны-заглушки

Когда DNS-клиент обращается с рекурсивным запросом на DNS-сервер, хранящий зону-заглушку, тот разрешает запрос на основании записей ресурсов зоны-заглушки. Затем DNS-сервер запрашивает полномочные серверы, указанные в записи ресурса NS зоны-заглушки. Если DNS-серверу не удается обнаружить какой-либо из полномочных серверов имен, указанных в зоне заглушки, он предпринимает стандартную рекурсию.

DNS-сервер сохраняет записи ресурсов, полученные от полномочных серверов зоны-заглушки, в своем кэше, а не в самой зоне-заглушке, так как та хранит лишь записи SOA, NS и A, которые и возвращает в ответ на запросы. Запись ресурсов хранится в кэше на протяжении времени жизни (TTL), определенном в конкретной записи ресурсов. Срок записей SOA, NS и A, не записанных в кэш, истекает в соответствии с интервалом, определенном в записи ресурса SOA зоны-заглушки, которая создается при определении зоны-заглушки и обновляется в процессе передач из исходной основной зоны.

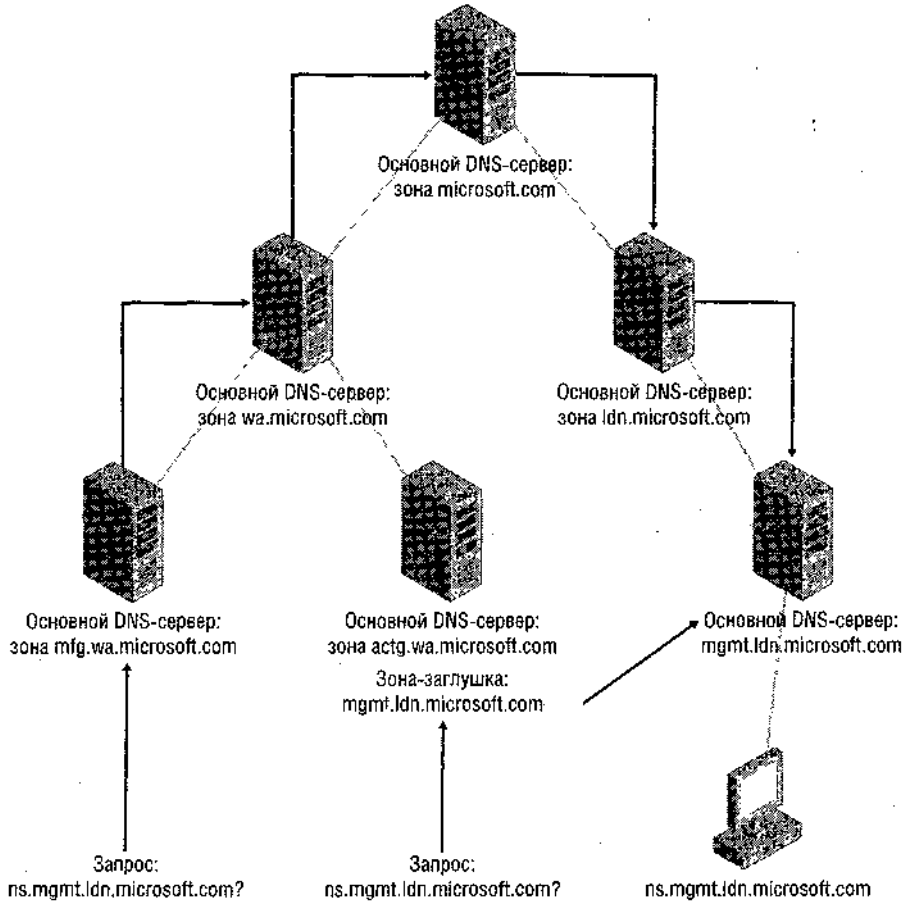


Рис. 5-35. Использование зон-заглушек для междоменного разрешения имен

Получив запрос с запретом рекурсии, DNS-сервер возвращает *ссылку* (referral), на серверы, указанные в зоне-заглушке.

Обновление зоны-заглушки

В процессе загрузки зоны-заглушки DNS-сервер запрашивает у главного сервера зоны записи: SOA, NS в корне зоны и A. В процессе обновления зоны-заглушки главный сервер запрашивает на DNS-сервере, обслуживающем зону-заглушку, те же записи ресурсов, которые нужны при загрузке зоны-заглушки. Периодичность выполнения зонной передачи (обновления) зоны-заглушки главным DNS-сервером задана в SOA. На случай сбоя в SOA также указан интервал повторения попытки обновления записей ресурсов. Если по истечении интервала повторения попытки обновления данные зоны обновить не удается, DNS-сервер прекращает использовать данные зоны-заглушки по истечении времени, определенного в поле *Действителен до* (Expires) записи SOA.

Консоль *DNS* позволяет выполнять следующие операции обновления зоны-заглушки:

- перезагрузка зоны-заглушки с локальной базы данных DNS-сервера, на котором она располагается;

- **передача с главного сервера** — обслуживающий зону-заглушку DNS-сервер определяет момент истечения срока серийного номера в записи SOA и выполняет передачу зоны с главного сервера зоны-заглушки;
- **перезагрузка с главного сервера** — в этом случае передача данных в зону-заглушку с главного сервера происходит независимо от серийного номера в записи SOA.

Подготовка к экзамену Очень важно понимать и помнить различия между этими тремя операциями, которые выполняются как в дополнительных зонах, так и зонах заглушках.

Лабораторная работа. **Развертывание зоны-заглушки**

Вы создадите зону-заглушку на Computer!., который запрашивает передачи зоны из делегированного поддомена *Sub. domain 1. local.*

Упражнение 1. Создание зоны-заглушки

Вы создадите зону-заглушку на Computer! с помощью *Мастера создания новой зоны* (New Zone Wizard).

Внимание! Здесь предполагается, что DNS-сервер установлен на Computer2 с помощью *Мастера компонентов Windows* (Windows Components Wizard) (см. занятие 3 главы 4). В этом случае передачи из зоны *Sub. domain I. local* разрешены по умолчанию, но ограничены полномочными серверами имен. Если же установить DNS-сервер на Computer2 путем добавления роли DNS-сервера в окне **Управление данным сервером (Manage Your Server),** зонные передачи во всех локальных зонах по умолчанию запрещены. В этом случае до начала упражнения надо позаботиться о разрешении передач .в зоне *Sub.domainl.local* и ограничении их серверами, указанными на вкладке **Серверы имен (Name Servers).**

1. С Computerl войдите в домен *Domainl* как *Администратор* (Administrator).
2. В командной строке выполните команду

   `dnscmd computer-2 /recordadd sub.domainl. local @ ns computerl .domainl. local`

   Она добавит Computerl на вкладку **Серверы имен (Name Servers)** окна свойств зоны *Sub.domainl.local* в консоли *DNS* на Computer2.
3. В консоли *DNS* щелкните узел **Зоны прямого просмотра (Forward Lookup Zones)** правой кнопкой и выберите **Создать новую зону (New Zone).**
4. **В** окне **Мастер создания новой зоны (New Zone Wizard)** щелкните **Далее** (Next).
5. На странице **Тип зоны (Zone Type)** выберите **Зона-заглушка (Stub Zone),** сбросьте флажок **Хранить зону в Active Directory (Store the zone in Active Directory)** и щелкните **Далее.**
6. На странице **Имя зоны (Zone Name)** в текстовом поле введите `sub.domainl.local` и щелкните **Далее.**
7. На странице **Файл зоны (Zone File)** оставьте выбранный по умолчанию вариант — **Создать новый файл (Create a new file with this file name)** и щелкните **Далее.**
8. На странице **Основные DNS-серверы (Master DNS Servers)** в текстовом поле **IP-номер (IP Address)** введите IP-адрес, назначенный компьютеру Computer2, и щелкните **Добавить (Add),** а затем **Далее.**

9. На странице **Завершение мастера создания новой зоны (Completing The New Zone Wizard)** щелкните **Готово (Finish).**

   В дереве консоли *DNS* в узле **Зоны прямого просмотра (Forward Lookup Zones)** появился узел локальной зоны *sub. domain 1. local.*
10. В дереве консоли *DNS* щелкните узел ***sub.domain 1.local*** правой кнопкой и выберите **Передать зону с основного сервера (Transfer from master).**

    Совет Если вы получите сообщение об ошибке, подождите 10 секунд и повторите п. 10 еще раз.

    После успешной загрузки зоны в узле отображаются только три записи ресурса: запись SOA самой зоны и записи ресурсов NS, указывающие на Computer2 и Computerl.
11. Выйдите из системы Computerl.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Для чего чаще всего применяют зоны-заглушки?
2. Что из перечисленного ниже *не является* преимуществом зоны-заглушки?
   a. Повышение эффективности разрешения имен.
   b. Поддержание данных о другой зоне в актуальном состоянии.
   c. Упрощение администрирования DNS.
   d. Повышение отказоустойчивости DNS-серверов.
3. Когда зону-заглушку предпочитают дополнительной зоне? Когда дополнительная зона предпочтительнее зоны-заглушки?

Резюме

- *Зона-заглушка* (stub zone) — это регулярно обновляемая сокращенная копия зоны, содержащая только записи NS главной зоны. Зоны-заглушки чаще всего используют для отслеживания полномочных серверов имен в делегированных зонах. Обычно зоны-заглушки размещаются на родительских DNS-серверах делегированных зон.
- Зоны-заглушки также применяются для упрощения процесса разрешения имен между доменами за счет исключения поиска в пространстве имен DNS общего родительского сервера.
- При определении зоны-заглушки нужно определить по крайней мере один, главный сервер имен, IP-адрес которого не изменяется. Информация о любых новых серверах имен, добавляемых в главную зону позже, автоматически обновляется в зоне-заглушке путем зонных передач.
- Зоны-заглушки не выполняют той же функции, что и дополнительные зоны, и их нельзя использовать в качестве альтернативы при планировании отказоустойчивости, избыточности или балансировки нагрузки.

Пример из практики

Вас пригласила в качестве консультанта компания Lucerne Publishing для оказания помощи в происходящем в компании переводе инфраструктуры DNS-серверов на Windows Server 2003.

Штаб-квартира Lucerne Publishing расположена в Люцерне, кроме того, есть еще два филиала в Берне и Женеве. В штаб-квартире развернут родительский домен *lucemepublishing.com*, а в бернском и женевском отделениях есть собственные поддомены и их контроллеры (рис. 5-36).

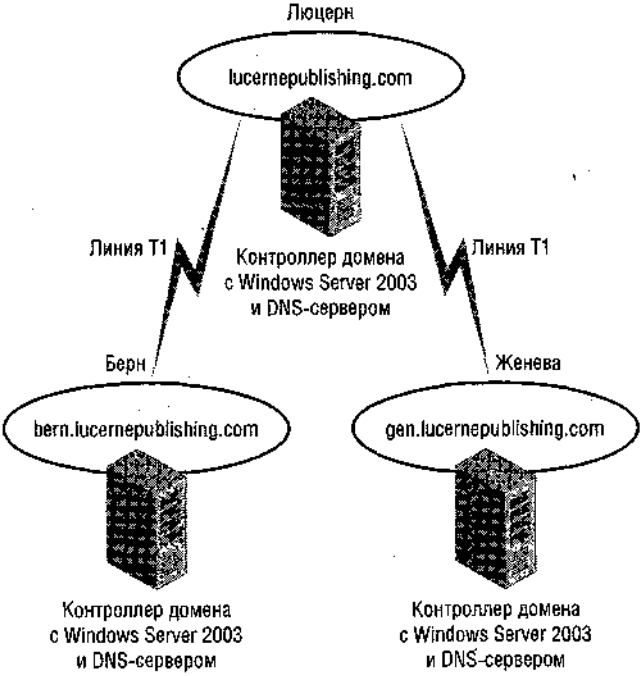


Рис. 5-36. Сеть компании Lucerne Publishing

Руководство требует решить следующие задачи:

a. Минимизировать трафик разрешения имен по WAN-каналам.
b. Минимизировать трафик репликации DNS по WAN-каналам.
c. Защитить трафик репликации DNS по WAN-каналам.
d. Оптимизировать трафик разрешения имен на клиентских компьютерах.

1. Какие задачи удастся решить за счет развертывания интегрированной с Active Directory зоны с заданными по умолчанию границами репликации на контроллерах домена всех трех отделений компании?
2. Если интегрированная в Active Directory зона развернута в домене *lucernepublishing.com*, какой вариант вы порекомендуете выбрать в окне **Изменение области видимости зоны репликации (Change Zone Replication Scope)** на рис. 5-37? Предполагается, что сокращение времени получения ответа на запрос о разрешении имен важнее, чем сокращение сетевого трафика.

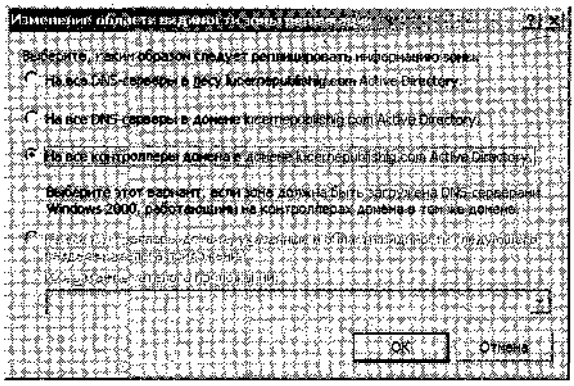


Рис. 5-37. Определение границ репликации в домене *lucernepublishing.com*

3. В бернском филиале работает 200 сотрудников. Руководство требует развернуть DNS так, чтобы сократить до минимума нагрузку на сетевых администраторов штаб-квартиры в Люцерне. Кроме того в штаб-квартире требуется обновлять на DNS-серверах информацию о всех новых полномочных серверах, развертываемых в бернском офисе. Что для этого надо предпринять?
4. ИТ-директор сообщает, что сетевые администраторы не смогли развернуть тестовый дополнительный DNS-сервер в одном из филиалов. Они задали правильный IP-адрес основного DNS-сервера под управлением Windows Server 2003 в штаб-квартире, тем не менее дополнительный сервер оказался не в состоянии получить данные основной зоны. При этом известно, что несколько лет тому назад удалось развернуть аналогичную тестовую сеть на базе Windows 2000. В чем наиболее вероятная причина неполадки?

Л Практикум по устранению неполадок

Вы исправите некорректно установленную Active Directory на Computerl путем автоматического воссоздания отсутствующих записей ресурсов SRV с помощью утилиты Netdiag. Затем вы сконфигурируете зону *domain 1.local для* поддержки только безопасных динамических обновлений. Это позволит предотвратить создание подставных сетевых компьютеров и перехват регистрации доменных компьютеров злоумышленниками.

1. С Computerl войдите в домен *Domain 1* как *Администратор* (Administrator).
2. В консоли *DNS* удалите следующие две записи ресурсов SRV: **_kerberos._tcp.dc._msdcs.domain 1.local** и **_ldap._tcp.dc._msdcs.domainl.local.**
3. Закройте консоль *DNS.* Позаботьтесь, чтобы Computerl был отключен от Интернета при выполнении следующей операции.
4. Выполните команду `netdiag /fix`.
5. Изучив результаты работы утилиты, вы увидите, что некоторые тесты пройти не удалось.
6. Откройте консоль *DNS* и откройте узел домена **_tcp.dc._msdcs.domainl.local.** В правой области отображаются две восстановленные записи, которые вы ранее удалили.
7. Закройте консоль *DNS.*
8. В командной строке выполните команду

```
dnscmd /zoneresettype domain"!.local/dsprimary.
```

Она превращает *domain I, local* в зону, интегрированную в Active Directory. Зоны этого типа поддерживают безопасные динамические обновления.

9. Выполните команду

```
dnscmd . / config domain"!. local /allowupdate 2
```

Она разрешит только безопасные обновления в *domainl.local.* Обновлять записи будет разрешено только компьютерам, их создавшим.

10. В консоли *DNS* откройте окно свойств зоны *Domainl.local.* На вкладке **Общие (General)** видно, что зона является интегрированной в Active Directory и в ней разрешены только безопасные динамические обновления.
11. Закройте консоль *DNS* и выйдите из системы Computer 1.

(J Резюме главы

- Вкладка **Пересылка (Forwarders)** окна свойств DNS-сервера позволяет перенаправлять DNS-запросы, поступающие на локальный DNS-сервер, на вышестоящие DNS-серверы, называемые *серверами пересылки* (forwarders). Здесь же можно запретить рекурсию для определенных запросов (из определенных доменов).
- Вкладка **Корневые ссылки (Root Hints)** окна свойств DNS-сервера предоставляет удобный интерфейс для модификации содержимого файла *Cache.dns.* На DNS-серверах, используемых для разрешения интернет-имен, эти записи изменять не обязательно. Однако на DNS-серверах в крупном частном пространстве имен эту вкладку можно использовать для удаления ссылок на корневые серверы Интернета и определения корневых серверов частной сети. Наконец, если определить в частной сети корневой DNS-сервер (с именем «.»), придется полностью удалить файл *Cache.dns.*
- При развертывании DNS-сервера на контроллере домена появляется возможность размещения базы данных зоны в Active Directory. Это позволяет сократить трафик передачи зон, укрепить защиту, облегчить администрирование и повысить отказоустойчивость. Данные зоны можно реплицировать на все DNS-серверы леса Active Directory, на все DNS-серверы домена Active Directory, на все контроллеры домена Active Directory или все серверы определенного раздела каталога приложений.
- Запись ресурса SOA содержит несколько параметров, касающихся передач,зон, в том числе интервал блокирования, интервал обновления, срок и минимальное время жизни (TTL).
- Если DNS-зона поддерживает небезопасное динамическое обновление, любые DNS-клиенты могут регистрировать и обновлять записи ресурсов на DNS-сервере. При поддержке безопасных динамических обновлений право обновления записи предоставляется только владельцу. Безопасное динамическое обновление поддерживается только в интегрированных в Active Directory зонах.
- Группа *Dns Update Proxy* обычно объединяет DHCP-серверы, динамически обновляющие данные DNS от имени клиентов. При регистрации записей ресурсов в DNS члены этой группы не оставляют информации о владельце, что позволяет предупредить неполадки, возникающие из-за конфликта владельцев в зонах, поддерживающих только безопасное динамическое обновление.
- Вкладка **Передачи зон (Zone Transfers)** позволяет ограничивать зонные передачи из локальной зоны. По умолчанию в основных зонах передача на дополнительные серверы либо полностью запрещена, либо ограничена серверами имен, перечислен-

ными на вкладке **Серверы имен (Name Server)** — все зависит от способа установки DNS-сервера.

- При включенной *расстановке по адресу* (netmask ordering) IP-адреса клиентской подсети ответа размещаются в верхних строках списка ответа.
- При включенном циклическом обслуживании riNS-сервер выполняет случайную ротацию элементов в возвращаемом клиенту списке записей ресурсов A. Это один из простейших способом балансировки сетевой нагрузки между сетевыми службами, активно обслуживающими клиентские запросы и предоставляющими одинаковые сервисы.
- Делегирование подразумевает создание новой зоны и передачу ответственности за поддомен в рамках пространства имен DNS отдельному субъекту.
- *Зона-заглушка* (stub zone) — это регулярно обновляемая сокращенная копия зоны, содержащая только записи SOA и записи ресурса NS главной зоны. Зоны-заглушки чаще всего используют для отслеживания полномочных серверов имен в делегированных зонах. Обычно зоны-заглушки размещаются на родительских DNS-серверах делегированных зон.

Ц Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Разберитесь с доступными вариантами репликации зоны, интегрированной в Active Directory.
- Запомните ситуации, в которых чаще всего используется пересылка.
- Запомните последствия включения/отключения циклического обслуживания, расстановки по адресу, дополнительных служб BIND и рекурсии.
- Разберитесь в различии между безопасными и небезопасными динамическими обновлениями.
- Запомните функцию группы *DnslIpdateProxy*.
- Изучите последствия увеличения/уменьшения интервала блокирования, интервала обновления, срока и минимального времени жизни (TTL) в записи ресурса SOA.
- Запомните ситуации, в которых применяются основные и дополнительные зоны, зоны-заглушки и зоны, интегрированные в Active Directory.
- Запомните ситуации, в которых применяют делегирование.

Основные термины

Раздел каталога приложений ~ application directory partition — раздел каталога, реплицируемый на указанное подмножество контроллеров домена под управлением Windows Server 2003 и содержащий информацию, используемую определенным приложением или службой, например DNS.

Итерация (итерационные запросы) ~ iteration (iterative queries) — процесс последовательного запроса различных DNS-серверов в процессе разрешения имени компьютера в IP-адрес.

Вопросы и ответы

Занятие 1. Лабораторная работа 1. Упражнение 1

9. Сравните трафик, записанный в файлах Name Resolution 1 и Name Resolution 2. Ответьте на следующие вопросы.

   Каково основное различие между записями?

   Правильный ответ: в Name Resolution 2 первые два кадра являются DNS-запросом имени computerl.domain!.local и ответом на этот запрос. В Name Resolution 1 для разрешения имени Computer2 в локальной сети использовался протокол NetBT. Это различие свидетельствует о том, что в качестве способа разрешения имен на смену NetBIOS пришла DNS.

   Чем объясняется различие в методах разрешения имен?

   Правильный ответ: в сетях Windows Server 2003 сначала применяется разрешение по протоколу DNS и лишь затем используется NetBIOS. Причина разрешения по протоколу NetBIOS в первом примере в том, что на тот момент не было завершено конфигурирование DNS в сети.

Занятие 1. Лабораторная работа 1. Упражнение 2

9. Какое ограничение налагается на клиентов под управлением Microsoft Windows 95 и Microsoft Windows NT 4 SP3 или более ранней версии?

   Правильный ответ: по умолчанию им не разрешается вход в домен через контроллер домена под управлением Windows Server 2003.

Занятие 1. Закрепление материала

1. Как пересылка позволяет укрепить безопасность обработки DNS-запросов?
   Правильный ответ: если DNS-серверу или пользователям внутренней сети разрешить направлять итерационные запросы внешним DNS-серверами, придется открыть на брандмауэре DNS-порты, что небезопасно. Однако, настроив внутренний DNS-сервер на пересылку внешних запросов единственному серверу пересылки, расположенному за брандмауэром, и открыв на брандмауэре только один порт, по которому обмениваются эти серверы, вы сможете организовать полноценное разрешение имен, не открывая сеть для доступа внешних серверов.
2. Как в окне свойств DNS-сервера запретить многоадресному DNS-серверу реагировать на DNS-запросы, поступающие на конкретные сетевые адаптеры?
   Правильный ответ: на вкладке Интерфейсы (Interfaces) сервер настраивается на прослушивание DNS-запросов только на одном IP-адресе.
3. Вы администратор сети, состоящей из одного домена. Вы установили новый DNS-сервер по имени DNS1, отвечающий за обработку запросов на разрешение имен Интернета, поступающих от клиентов локального домена. Однако, несмотря на наличие подключения DNS1 к Интернету, он не проходит рекурсивный тест на вкладке **Наблюдение (Monitoring)** окна свойств сервера. Что из перечисленного может быть причиной сбоя?
   a. DNS1 установлен вне локальной сети, за брандмауэром.
   b. На DNS1 размещается зона «.».

c. Корневые ссылки не обновлены и остались в конфигурации по умолчанию.

d. DNS1 не сконфигурирован на пересылку всех запросов вышестоящему серверу.

Правильный ответ: Ь.

4. Какие из перечисленных обстоятельств могут служить причиной изменения (но не удаления) значений корневых ссылок по умолчанию-на вкладке **Корневые ссылки (Root Hints)** окна свойств DNS-сервера? (Выберите все подходящие варианты.)

a. Изменился состав корневых серверов Интернета.

b. Сервер не планируется использоваться в качестве корневого.

c. На сервере отключена рекурсия.

d. Сервер не используется для разрешения имен Интернета.

Правильные ответы: a, d.

Занятие 2. Лабораторная работа. Упражнение 1

16. Какие команды меню **Действие (Action)** доступны для зоны *domain I. local* в узле COMPUTER2 и какие недоступны для той же зоны в узле COMPUTER!?

Правильный ответ: Передать зону с основного сервера (Transfer From Master) и Перезагрузить повторно зону с основного сервера (Reload From Master).

Можно ли создавать или конфигурировать записи ресурсов *domain I. local* через узел COMPUTER2 в консоли *DNS?*

Правильный ответ: нет, создавать или изменять записи ресурсов в *domainl.local* с узла COMPUTER2 нельзя.

Занятие 2. Лабораторная работа. Упражнение 2

5. **В** окне свойств *Domainl.local* перейдите на вкладку **Начальная запись зоны (SOA) [Start Of Authority (SOA)]** и ответьте на следующие вопросы.

Как долго DNS-сервер на Computer2 будет обслуживать запросы DNS-клиентов после потери связи с Computerl?

Правильный ответ: 1 день.

Как часто в соответствии с конфигурацией Computer2 запрашивает на Computerl изменения зоне?

Правильный ответ: каждые 15 минут.

Через какое время после обнаружения отсутствия связи с Computerl при запросе SOA компьютер Computer2 повторит попытку?

Правильный ответ: 10 минут.

Если другой основный DNS-сервер dns.domain2.local успешно получит с Computer2 ответ на запрос об IP-адресе Computerl, как долго соответствующая Computer2 запись ресурса А сохранится в кэше dns.domain2.1ocal?

Правильный ответ: 1 час.

Занятие 2. Закрепление материала

1. Опишите порядок, в котором дополнительные серверы выясняют необходимость инициации передачи зоны.

Правильный ответ: когда зоны настроены на выполнение зонных передач, главный сервер периодически опрашивается на предмет серийного номера зоны. Такой запрос называется запросом SOA (SOA query). Если результаты запроса SOA показывают, что се-

рийные номера главной и локальной зоны равны, передача зон не выполняется. Однако если серийный номер зоны на главном сервере больше, дополнительный сервер инициирует передачу.

2. В чем различие между запросами IXFR и AXFR?

   Правильный ответ: запросы IXFR инициируют добавочные зонные передачи, в которых передается только обновленная информация. С другой стороны, AXFR-запросы вызывают полную зонную передачу, в которых по сети пересылается все содержимое базы данных зоны.

3. **В** сети несколько DHCP-серверов, некоторые из которых сконфигурированы на регистрацию записей в DNS от имени клиентов ОС, предшествующей Windows 2000. В DNS разрешены только безопасные обновления, однако обнаружилось, что некоторые записи в DNS не обновляются должным образом. Что следует предпринять?

   Правильный ответ: добавьте DHCP-сервер во встроенную группу безопасности *DnsUpdateProxy*.

4. Вы отвечаете за администрирование WAN-сети компании Proseware. Штаб-квартира компании расположена в Рочестере, а два филиала — в Буффало и Сиракузах. Сеть компании состоит из одного домена; в ней одна основная DNS-зона в штаб-квартире, обслуживаемая компьютером под управлением Windows Server 2003, и по одной дополнительной DNS-зоне в каждом филиале. Пользователи жалуются на отсутствие доступа к удаленным филиалам.. Администраторы обнаружили, что пропускная способность канала между штаб-квартирой и филиалами перегружена зонными передачами, причем новые передачи инициируются до окончания предыдущих. Что из перечисленного позволит решить проблему наименьшими усилиями?

   a. Установить в сети Active Directory и повысить роль серверов, обслуживающих дополнительные DNS-зоны, до контроллеров домена.
   b. Увеличить пропускную способность подключений, установив волоконно-оптическое подключение между филиалами.
   c. Увеличить интервал обновления на основном DNS-сервере.
   d. Увеличить интервал обновления на дополнительных DNS-серверах.

   Правильный ответ: с.

5. Администратор установил TTL в основной DNS-зоне в 5 минут. Какие наиболее вероятные последствия этого шага?

   a. Записи ресурсов в кэше основного DNS-сервера будут удаляться по истечении 5 минут.
   b. При разрешении имен, для которых сервер является полномочным, DNS-клиентам придется запрашивать сервер чаще.
   c. Дополнительные серверы будут инициировать передачу зоны каждые 5 минут.
   d. Узлы будут чаще перерегистрировать свои записи в DNS.

   Правильный ответ: Ь.

6. Что не является преимуществом хранения DNS-зон в базе данных Active Directory?

   a. Менее частые передачи.
   b. Меньше усилий по администрированию.
   c. Меньшая нагрузка на сеть.
   d. Безопасное динамическое обновление.

   Правильный ответ: а.

Занятие 3. Закрепление материала

1. Вы сетевой администратор компании Lucerne Publis. Корпоративная сеть состоит из одного домена *lucemepublishing.com,* который подключен к Интернету через брандмауэр, расположенный на компьютере NS1. На NS1 также располагается DNS-сервер, причем служба брандмауэра разрешает DNS-трафик между Интернетом и службой DNS на NS1, но не между Интернет и внутренней сетью. На DNS-сервере включено циклическое обслуживание. Во внутренней сети расположены два компьютера NS2 и NS3 под управлением Windows Server 2003 — соответственно основной и дополнительный DNS-серверы зоны *iucemepublishing.com.*

   Пользователи сети жалуются, что, указывая имена узлов, они подключаются к компьютерами локальной сети, но не могу подключиться таким способом к узлам Интернета, например *www.microsoft.com.*

   Какое из перечисленных ниже действий решает задачу, требуя минимальных усилий от администратора?

   a. Отключение рекурсии на NS2 и NS3.
   b. Включение расстановки по адресу на NS1.
   c. Конфигурирование NS2 и NS3 на использование NS1 в качестве сервера пересылки.
   d. Отключение циклического обслуживания на NS1.

   Правильный ответ: c.

2. Вы администратор крупной сети, состоящей из 10 доменов. Вы сконфигурировали стандартную основную зону в домене *mfg.lucernepublishing.com* на компьютере Serverl, на котором также расположен DNS-сервер, а также конфигурировали UNIX-сервер Server2, на котором располагается дополнительная зона того же домена. UNIX-сервер поддерживает BIND 8.2.I.

   Обнаружилось, что зонные передачи между основным и дополнительным серверами инициируют значительно больший трафик, чем ожидалось, и перегружают сетевые ресурсы.

   Что можно предпринять для снижения нагрузки на сеть, обусловленной передачами зон между основным и дополнительным серверами?

   a. Сбросить флажок Дополнительные службы BIND (BIND Secondaries) на Serverl.
   b. Сконфигурировать загрузочный файл на Serverl для инициализации совместимых с BIND параметров.
   c. Установить флажок **Дополнительные службы BIND (BIND Secondaries)** на Serverl.
   d. Сконфигурировать загрузочный файл на Server2 для поддержки быстрых зонных передач.

   Правильный ответ: a.

3. Какова роль циклического обслуживания? Какая функция приоритетнее: циклическое обслуживание или расстановка по адресу?

   Правильный ответ: циклическое обслуживание обеспечивает ротацию записей ресурсов в списке ответа, возвращаемом сервером DNS-клиентам. Каждому следующему DNS-клиенту, запросившему имя многоадресного компьютера, возвращается список с другой записью ресурса вначале. Циклическое обслуживание менее приоритетно, чем расстановка по адресу. Когда установлен переключатель Включить расстановку по адресу (Enable Netmask Ordering), циклическое обслуживание используется как дополнительный механизм ротации возвращенных записей ресурсов многоадресного компьютера.

4. Вы ведущий администратор сети компании Proseware, имеющей четыре филиала. В каждом филиале собственная локальная сеть, подключенная к Интернету по линии T1. Используя технологию VPN, сети филиалов объединены в единую интрасеть; репликация обеспечивается Web-серверам, расположенными в каждом филиале. У этих четырех Web-серверов уникальные IP-адреса, но одно полное доменное имя (FQDN) *intranet.proseware.com* (рис. 5-30).

   DNS-клиент сети Proseware с IP-адресом 192.168.33.5 направляет на DNS-сервер запрос на разрешение имени *intranet.proseware.com*. Предполагается, что на DNS-сервере включена функция **Включить расстановку по адресу (Enable Netmask Ordering).** Какой IP-адрес получит DNS-клиент? (Подсказка: выясните, у которого из четырех Web-серверов идентификатор подсети совпадает с идентификатор подсети клиента.)
   Правильный ответ: 192.168.42.40.

Занятие 4. Лабораторная работа. Упражнение 3

10. Используя консоль *DNS,* ответьте на вопрос: сколько записей ресурсов-узлов (A), соответствующих домену *sub. domain 1. local* хранятся на Computerl?
    Правильный ответ: таких записей нет.

Занятие 4. Закрепление материала

1. Вы проектируете пространство имен DNS для компании Proseware, владеющей зарегистрированным Интернет-доменом *proseware.com*. Штаб-квартира Proseware расположена в Рочестере и два филиала — в Буффало и Сиракузах. В каждом отделении своя ЛВС, управляемая местным сетевым администратором. Требуется установить по одному DNS-серверу в каждом отделении, причем домен *proseware.com* должен обслуживаться сервером штаб-квартиры. Кроме того, администраторы в Буффало и Сиракузах должны самостоятельно управлять DNS-именами и разрешением имен в своих сетях. Что из перечисленного ниже необходимо предпринять для решения поставленной задачи?
   a. Создать стандартный основный сервер в Рочестере и разместить на нем зону *proseware.com*. Делегировать по поддомену каждому из филиалов. Сконфигурировать по дополнительному серверу в Буффало и Сиракузах, разместив на этих серверах делегированные поддомены.
   b. Создать стандартный основный сервер в Рочестере и разместить на нем зону *proseware.com*. Сконфигурировать по дополнительному серверу в Буффало и Сиракузах для повышения производительности и отказоустойчивость зоны.
   c. Создать DNS-сервер в Рочестере и разместить на нем стандартную основную зону *proseware.com*. Сконфигурировать DNS-серверы в Буффало и Сиракузах, разместив на каждом по стандартной основной зоне поддомена *proseware.com*. Создать делегирование с DNS-сервера в Рочестере каждому из этих поддоменов.
   d. Создать DNS-сервер в Рочестере и разместить на нем стандартную основную зону *proseware.com*. Сконфигурировать DNS-серверы в Буффало и Сиракузах, разместив на каждом по стандартной основной зоне поддомена *proseware.com*. Создать по дополнительной зоне на каждом DNS-сервере, получающей передачи из основных зон, расположенных на двух других DNS-серверах.

   Правильный ответ: c.

2. Вы администратор корпоративной сети, состоящей из ЛВС штаб-квартиры и трех филиалов, расположенных в различных городах. Решено спроектировать новую инфраструктуру DNS и развернуть Active Directory. Нужно: во-первых, создать единый лес Active Directory во всех четырех отделениях, и во-вторых, сократить до минимума время отклика для пользователей, подключающихся к ресурсами из любого места сети. Во всех отделениях есть контроллеры доменов с DNS-сервером. Что из перечисленного ниже лучше всего предпринять для решения поставленной задачи?

   a. Создать один домен Active Directory для всех четырех отделений и единую интегрированную в Active Directory DNS-зону, реплицируемую в пределах всего домена.
   b. Создать один домен Active Directory для всех четырех отделений и стандартную основную зону в штаб-квартире и по одной дополнительной зоне в филиалах.
   c. Создать домен Active Directory и домен DNS в штаб-квартире, делегировать по поддомену DNS каждому филиалу и создать интегрированную в Active Directory зону в каждом отделении, реплицируемую в рамках всего леса.
   d. Создать домен Active Directory и домен DNS в штаб-квартире, делегировать по поддомену DNS каждому филиалу и создать интегрированную в Active Directory зону в каждом отделении, реплицируемую в рамках всего домен.

   Правильный ответ: a.

3. Какие записи ресурсов создаются в родительской зоне при делегировании поддомена? В чем особые функции этих записей?

   Правильный ответ: записи ресурсов NS и A создаются в делегированном поддомене родительской зоны. Запись ресурса NS перенаправляет запросы на DNS-сервер, полномочный в делегированной зоне. Запись ресурса, которая называется связывающей (glue record), обеспечивает сопоставление имени компьютера, указанного в записи ресурса NS, и IP-адреса.

4. DNS-сервер NS1 обслуживает зону *lucemepublishing.com* и конфигурирован на пересылку всех запросов имен, для которых не является полномочным. На NS1 поступает запрос на разрешение имени делегированного домена *sub.lucemepublishing.com*. Куда будет направлен запрос?

   Правильный ответ: запрос будет направлен на сервер, полномочный в зоне sub.lucemepublishing.com зоны, а не на указанный сервер пересылки.

Занятие 5. Закрепление материала

1. Для чего чаще всего применяют зоны-заглушки?

Правильный ответ: зоны-заглушки чаще всего применяются в родительской зоне для хранения обновляемого списка записей ресурсов NS, соответствующих делегированным поддоменам.

2. Что из перечисленного ниже *не является* преимуществом зоны-заглушки?

   a. Повышение эффективности разрешения имен.
   b. Поддержание данных о другой зоне в актуальном состоянии.
   c. Упрощение администрирования DNS.
   d. Повышение отказоустойчивости DNS-серверов.

   Правильный ответ: d.

3. Когда зону-заглушку предпочитают дополнительной зоне? Когда дополнительная зона предпочтительнее зоны-заглушки?

   Правильный ответ: зона-заглушка оказывается очень кстати в случае делегирования поддомена и необходимости обеспечить актуальность записей ресурсов NS. Кроме того, зоны-заглушки служат для повышения эффективность разрешения имен, предоставляя ссылки на полномочные DNS-серверы других доменов. В любой из этих ситуаций зона-заглушка предпочтительнее дополнительного сервера, когда надо избежать расхода ресурсов, связанного с хранением полноценной базы данных дополнительной зоны, и нагрузки на сетевые ресурсы, связанные с передачами зоны. Дополнительная зона предпочтительнее зоны-заглушки, когда избыточность данных основной зоны и сокращение времени отклика важнее снижения нагрузки на сеть.

Пример из практики

1. Какие задачи удастся решить за счет развертывания интегрированной с Active Directory зоны с заданными по умолчанию границами репликации на контроллерах домена всех трех отделений компании?

   Правильный ответ: указанное решение позволяет решить все четыре задачи.

2. Если интегрированная в Active Directory зона развернута в домене *lucemepublishing.com*, какой вариант вы порекомендуете выбрать в окне **Изменение области видимости зоны репликации (Change Zone Replication Scope)** на рис. 5-37? Предполагается, что сокращение времени получения ответа на запрос о разрешении имен важнее, чем сокращение сетевого трафика.

   Правильный ответ: На все DNS-серверы в лесу Active Directory (To all DNS Servers in the Active Directory forest)

3. В бернском филиале работает 200 сотрудников. Руководство требует развернуть DNS так, чтобы сократить до минимума нагрузку на сетевых администраторов штаб-квартиры в Люцерне. Кроме того в штаб-квартире требуется обновлять на DNS-серверах информацию о всех новых полномочных серверах, развертываемых в бернском офисе. Что для этого надо предпринять?

   Правильный ответ: создайте делегированный домен bern.lucernepublishing.com и разверните зону-заглушку в штаб-квартире, содержащую записи NS основного сервера bern.lucernepublishing.com.

4. ИТ-директор сообщает, что сетевые администраторы не смогли развернуть тестовый дополнительный DNS-сервер в одном из филиалов. Они задали правильный IP-адрес основного DNS-сервера под управлением Windows Server 2003 в штаб-квартире, тем не менее дополнительный сервер оказался не в состоянии получить данные основной зоны. При этом известно, что несколько лет тому назад удалось развернуть аналогичную тестовую сеть на базе Windows 2000. В чем наиболее вероятная причина неполадки?

   Правильный ответ: по умолчанию в основных зонах Windows Server 2003 передача на дополнительные серверы либо полностью запрещена, либо ограничена серверами имен, перечисленными на вкладке Серверы имен (Name Server) — все зависит от способа установки DNS-сервера. После установки флажка Разрешить передачи зон (Allow zone transfers) и определения дополнительного сервера на вкладке Серверы имен (Name Server) в окне свойств зоны, создается необходимый ресурс NS и активизируются передачи зон.

ГЛАВА 6

Мониторинг и устранение неполадок DNS

Темы экзамена

- Наблюдение за работой DNS.

В этой главе

DNS — одна из важнейших служб сетей Microsoft Windows Server 2003, сбой которой приводит к неработоспособности Active Directory и большинства служб Интернета. Поэтому необходимо постоянно следить за работоспособностью DNS и при необходимости выполнять ее диагностику и восстановление.

Здесь описываются необходимые для мониторинга и устранения неполадок DNS инструменты и процедуры: утилита Nslookup, *журнал событий DNS* (DNS Events log), Replication Monitor и *журнал DNS* (DNS log).

Прежде всего

Для изучения материалов этой главы вам потребуется:

- два объединенных в сеть компьютера (Computerl и Computer2) под управлением Windows Server 2003. Компьютеру Computerl надо назначить статический адрес 192.168.0.1/24 и адрес основного DNS-сервера— 192.168.0.1. Computer2 нужно настроить на автоматическое получение собственного адреса и адреса DNS-сервера, а также определить альтернативную конфигурацию с адресом 192.168.0.2/24;
- учетная запись у интернет-провайдера (ISP) для подключения по телефонной линии (можно использовать и выделенную линию, но тогда придется переименовать ее в MylSP и внести коррективы в упражнения);
- установить DNS на Computerl. На этом DNS-сервере будет располагаться основная зона прямого просмотра *domain 1.local,* которую надо настроить на поддержку динамических обновлений. В зоне *domain 1.local*нужно создать записи ресурсов-узлов для Computerl и Computer2;

- назначить Computerl контроллером нового домена Active Directory и леса *domain I. local,* а Computer2 — рядовым членом этого домена. После установки Active Directory необходимо превратить DNS-зону *domain 1-local* в интегрированную с Active Directory и настроить ее на прием только безопасных динамических обновлений;
- подключение к Интернету по телефонной линии с именем MylSP на Computerl и поддержкой общего доступа к Интернету (ICS). Computer2 надо сконфигурировать для получения IP-конфигурации у ICS (если вместо телефонной используется выделенная линия, это требование также необходимо удовлетворить);
- на обоих компьютерах установить *Средства поддержки Windows* (Windows Support Tools);
- на вкладке **DNS** диалогового окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** для **Подключения по локальной сети (Local Area Connection)** на Computer2 установить флажок **Использовать DNS-суффикс подключения при регистрации в DNS (Use this connection's DNS suffix in DNS registration)** (это необходимо для динамических обновлений через ICS).

Занятие 1. Средства устранения неполадок DNS

Для устранения неполадок DNS чаще всего используют: утилиту Nslookup, *журнал событий DNS* (DNS Events log) и *журнал DNS* (DNS log). Nslookup позволяет напрямую направлять запросы DNS-серверам, а также просматривать содержимое зон. *Журнал событий DNS* — это файл, доступный для просмотра в консоли *Просмотр событий* (Event Viewer), в котором регистрируются ошибки и прочие события, связанные с работой службы DNS. *Журнал DNS,* или *отладочный журнал DNS* (DNS debug log) — это собственный журнал DNS-сервера, параметры которого задаются на вкладке **Ведение журнала отладки (Debug Logging)** окна свойств DNS-сервера. Можно настроить журнал так, чтобы регистрировать все входящие и исходящие сообщения DNS-сервера.

Изучив материал этого занятия, вы сможете:

- использовать утилиту Nslookup для выполнения запросов, просмотра и определения параметров и просмотра данных зоны;
- изучать зарегистрированные в журнале событий DNS ошибки и события службы DNS;
- настроить DNS-сервер на запись всех пакетов в файл Dns.log;
- найти и открыть файл Dns.log.

Продолжительность занятия — около 45 минут.

DNS-запросы с помощью Nslookup

Nslookup — утилита командной строки, присутствующая в большинстве ОС (и в Windows Server 2003) и позволяющая направлять тестовые запросы на DNS-серверы и получать подробные ответы в окне командной строки. Эта информация используется для диагностики и устранения неполадок сопоставления имен, проверки корректности добавления или обновления записей ресурсов в зоне и пр.

Nslookup можно выполнять как единовременную команду (неинтерактивный режим) или как программу, принимающую последовательность команд и запросов (интерактивный режим).

Простые запросы

В неинтерактивном режиме Nslookup позволяет определить 1P-адрес(а) узла по его имени. Например, следующая команда возвратит IP-адреса, соответствующие *полному доменному имени* (Fully Qualified Domain Name, FQDN) *www.microsoft.com:*

```
C:\>nslookup  www.microsoft.com
```

Результат выполнения команды может выглядеть так:

```
Server:   localhost
Address:  127.0.0.1

Non-authoritative  answer:
Name:     www.microsoft.akadns.net
Addresses:  207.46.230.220,  207.46.197.  102,  207.46.197.100,  207.46.230.218
Aliases:  www.microsoft.com
```

Разрешая запрос, Nslookup направляет указанное имя DNS-серверу, указанному в основном подключении локального клиентского компьютера. DNS-сервер возвращает ответ, используя собственный кэш или прибегнув к рекурсии.

Если надо проверить работоспособность DNS-сервера, отличного от указанного в основном подключения, нужно указать его в строке вызова Nslookup. Например, эта команда запрашивает разрешение имени *www.microsoft.com* на DNS-сервере с адресом 207.46.123.2:

```
nslookup  www.microsoft.com  207.46.1  38.20
```

Nslookup также позволяет разрешать IP-адреса в имена узлов. Вот листинг команды, возвращающей полное доменное имя, соответствующее адресу 207.46.249.222:

```
C:\>nslookup  207.46.249.222
Server:   localhost
Address:  127.0.0.1

Name:     www.microsoft.com
Address:  207.46.249.222
```

Примечание Обратный поиск выполняется на основании указателей (PTR), определенных в доменах обратного поиска. Такие есть не на всех узлах Интернета.

«Интерактивный режим

Если надо разрешить имена нескольких узлов или IP-адресов или в процессе устранения неполадки последовательно выполнить несколько операций, Nslookup используют в интерактивном режиме. Для этого просто выполните команду nslookup.

В интерактивном режиме Nsllokup принимает команды на выполнение различных операций, например отображения определенных сообщений в процессе передачи DNS-информации, эмуляции зонной передачи или поиска записи (или всех записей) определенного типа на указанном сервере. Чтобы узнать поддерживаемые команды, выполните команду Help или ? (рис. 6-1).

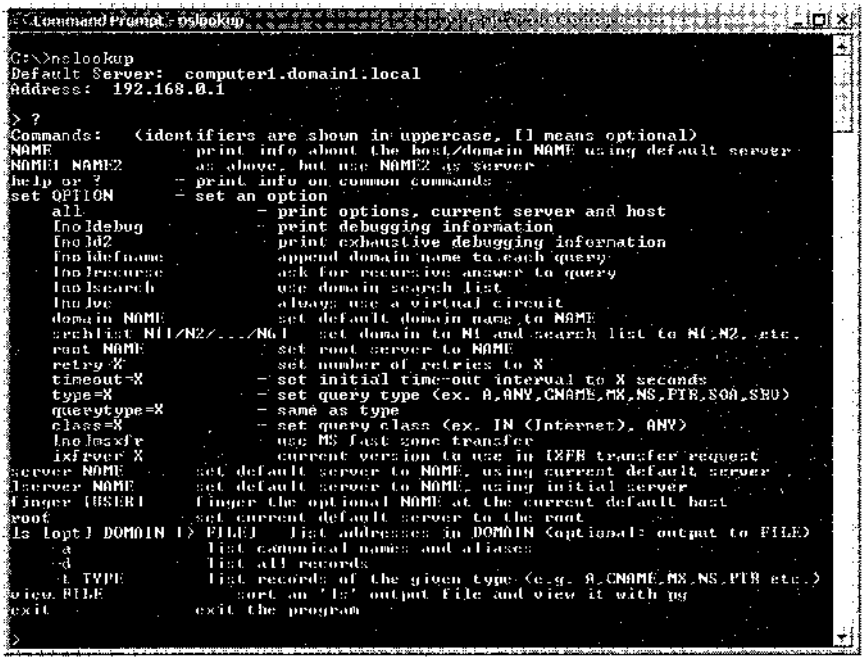


Рис. 6-1. Команды, поддерживаемые Nslookup

Параметры Nslookup

В интерактивном режиме есть команда set, позволяющая конфигурировать параметры программы Nslookup и изменять порядок обработки запросов, например переводить Nslookup в режим debug или nodebug (отладочный и обычный). По умолчанию действует режим nodebug. В отладочном режиме на экран выводятся полученные от DNS-сервера сообщения-ответы.

Внимание! Команды Nslookup чувствительны к регистру символов, использовать можно только строчные.

Чтобы увидеть значение всех параметров, выполните команду set all (рис. 6-2). В табл. 6-1 описаны наиболее часто используемые параметры Nslookup.

Табл. 6-1. Параметры, определяемый командой set

Параметр	Описание
set all	Вывод значений всех параметров
set [no]debug	Включение отладочного режима, в котором тображается больше информации об отправленном на сервер пакете и полученном ответе
set [no]d2	Включение отладочного режима Verbose Debug с детальной информацией о всех пакетах запросов и ответов, которыми обмениваются распознаватель и сервер

Табл. 6-1. *(окончание)*

Параметр	Описание
set domain=<имя *домена*>	Информирование распознавателя, какое доменное имя добавлять к запросам неполных имен, включая все имена, не содержащие завершающей точки
set timeout=<Значение *таймаута*>	Таймаут в секундах. Используется в медленных подключениях, где надо увеличить время ожидания ответа
set type=<тип *записи*> или set querytype=<тип *записи*> или set q=<*тип записи*>	Тип искомых записей ресурсов (например A, PTR или SRV). Чтобы заставить распознаватель искать все типы записей, выполните set type=all

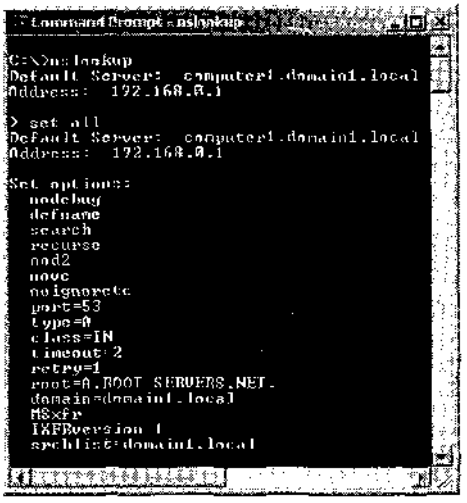


Рис. 6-2. Просмотр параметров Nslookup

Далее подробнее описывается, как выполнять наиболее распространенные задачи в интерактивном режиме программы Nslookup.

Поиск различных типов данных

По умолчанию Nslookup возвращает только записи ресурсов типа «адрес узла» (A). Чтобы запросить другие типы данных пространства имен домена используйте команды set type или set querytype (set q). Например, чтобы запросить вместо адресов узла записи ресурса «почтовый обменник» (MX), введите set q=mx, как показано далее:

```
C:\>nslookup
Default Server:  localhost
Address:  127.0.0.1

> set q=mx
> microsoft.com
Server:  .localhost
```

```
Address:  127.0.0.1
Non-authoritative  answer:
microsoft.com  MX preference = 10,  mai 1 exchanger = mailc.microsoft.com
microsoft.com  MX preference = 10,  mai 1 exchanger = maila.microsoft.com
microsoft.com  MX preference = 10,  mai 1 exchanger = mailb.microsoft.com

microsoft.com   nameserver = dns1.cp.ms ft.net
microsoft.com   nameserver = dns1.tk.ms ft.net
microsoft.com   nameserver = dns3.uk.ms ft.net
microsoft.com   nameserver = dns1.dc.ms ft.net
microsoft.com   nameserver = dns1.sj.ms ft.net
mailc.microsoft.com      internet addres s = 131.107.3.121
mailc.microsoft.com'     internet addres s = 131.107.3.126
maila.microsoft.com      internet addres s = 131.107.3.124
maila.microsoft.com      internet addres s = 131.107.3.125
mailb.microsoft.com      internet addres s = 131.107.3.122
mailb.microsoft.com      internet addres s = 131.107.3.123
dns1.cp.msft.net         internet addres s = 207.46.138.20
dns1.tk.msft.net         internet addres s = 207.46.245.230
dns3.uk.msft.net         internet addres s = 213.199.144.151
dns1.dc.msft.net         internet addres s = 64.4.25.30
dns1.sj.msft.net         internet addres s = 65.54.248.222>
```

Совет Чтобы запросить записи всех типов выполните команду set q=any.

Ответ на первый запрос об удаленном имени всегда является полномочным, а последующие — не обязательно. Это связано с тем, что первый раз локальный DNS-сервер связывается с DNS-сервером домена, полномочным для запрашиваемого имени. Локальный DNS-сервер кэширует эту информацию, и все последующие ответы формируются на основании содержимого кэша.

Прямой запрос другого сервера

Для пересылки запроса другому серверу имен напрямую служат команды server или 1se rve r. Для получения адреса сервера, на который следует переключиться, первая использует текущий сервер по умолчанию, а вторая — локальный.

После выполнения любой из этих команд все последующие запросы в текущем сеансе Nslookup выполняются на указанном сервере вплоть до нового переключения. Переключаются на новый сервер так:

```
C:\> nslookup
   Default Server:  name-serverl. lucernep  ublishing.com
   Address:   10.0.0.1

>server  nameserver2

   Default Server:  nameserver2.lucernep  ublishing.com
   Address:   10.0.0.2
>
```

Просмотр данных зоны с помощью Nslookup

Nslookup позволяет имитировать зонную передачу (команда Is), что позволяет увидеть все узлы удаленного домена. Синтаксис команды таков:

```
. ls [- a | d | t type] domain [> filename]
```

Команда 1s без дополнительных параметров возвращает список всех адресов и данные сервера имен. Параметр - а возвращает псевдоним и канонические имена, - d — все данные, а -t — фильтрует по типу. Вот листинг команды Is без дополнительных параметров:

```
>ls contoso.com
[nameserver1.contoso.com]
nameserver1.contoso.com.        NS server = ns1.contoso.com
nameserver2.contoso.com           NS    server = ns2.contoso.com
nameserverl      '                A     10,0.0.1
nameserver2                       A     10.0.0.2
>
```

Зонные передачи могут блокироваться на уровне DNS-сервера, и эта операция возможна лишь с авторизованных адресов или сетей. В случае безопасной зонной передачи возвращается сообщение об ошибке:

```
*** Can't list domain <example>.: Query refused
```

Подготовка к экзамену Помните, что команда Is эмулирует зонную передачу, а в Windows Server 2003 она по умолчанию защищена (безопасна). Перед запросом DNS-сервера убедитесь, что компьютеру, на котором работает Nslookup, разрешено выполнять зонную передачу.

Просмотр журнала событий DNS

Журнал событий DNS просматривают в узле **Просмотр событий (Event Viewer)** консоли *DNS* (рис. 6-3). Этот же журнал доступен в консоли *Просмотр событий* (Event Viewer) в узле **DNS-сервер (DNS Server).**

Рис. 6-3. Просмотр журнала событий DNS

В журнале событий DNS регистрируются ошибки DNS-сервера, и при неполадках сюда нужно заглянуть в первую очередь.

Настройка журнала событий DNS

По умолчанию в журнале событий DNS регистрируются все события, однако вы вправе ввести ограничения на типы регистрируемых событий на вкладке **Ведение журнала отладки (Event Logging)** окна свойств DNS-сервера, либо в окне свойств самого журнала в консоли *Просмотр событий*. Диалоговое окно **Свойства: DNS-сервер (DNS Events Properties)** предоставляет больше возможностей для управления и фильтрации сообщений.

Чтобы открыть окно **Свойства: DNS-сервер,** щелкните правой кнопкой узел **Просмотр событий** в консоли *DNS* и выберите **Свойства (Properties).** Окно содержит две вкладки: **Общие (General)** и **Фильтр (Filter).** Первая показана на рис. 6-4 и служит для определения имени файла журнала, его местоположения, максимального размера и даты истечения срока действия зарегистрированных событий.

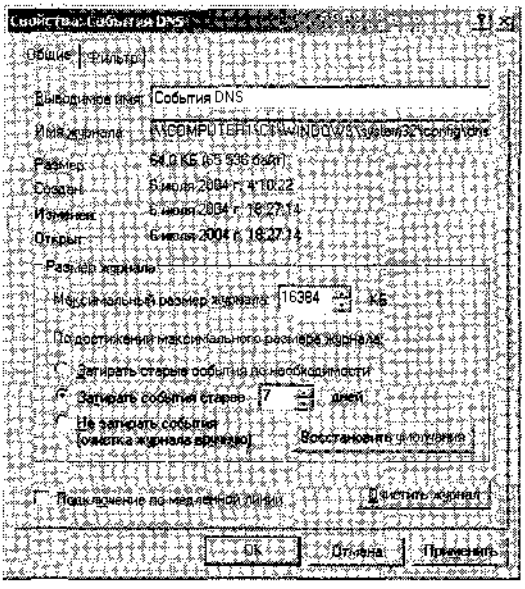


Рис. 6-4. Вкладка *Общие* окна *Свойства: DNS-сервер*

Вкладка **Фильтр** показана на рис. 6-5 и служит для настройки фильтрации событий по типу, источнику, идентификатору, дате и другим параметрам.

Отладочный журнал DNS

Помимо журнала событий DNS, служба DNS-сервера ведет-отдельный отладочный журнал — *WINDOWS\System32\pns\Dns.log*. Чтобы просмотреть этот файл, DNS-сервер нужно остановить. Кроме того, для просмотра понадобится WordPad или Microsoft Word, поскольку файл хранится в формате RTF.

По умолчанию в отладочном журнале DNS регистрируются только ошибки. Но его можно использовать и для регистрации всех входящих и исходящих DNS-пакетов локального сервера. По умолчанию на вкладке **Ведение журнала отладки (Event Logging)** окна свойств DNS-сервера сброшен флажок **Записывать пакеты в журнал для отладки (Log packets for debugging),** и все остальные элементы управления недоступны. После

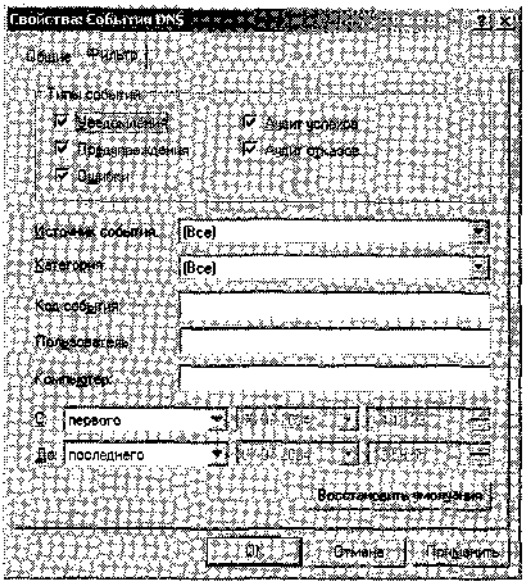


Рис. 6-5. Фильтрация зарегистрированных событий DNS

установки этого флажка (рис. 6-6) появляется возможность указать, какие DNS-пакеты будут регистрироваться в отладочном журнале.

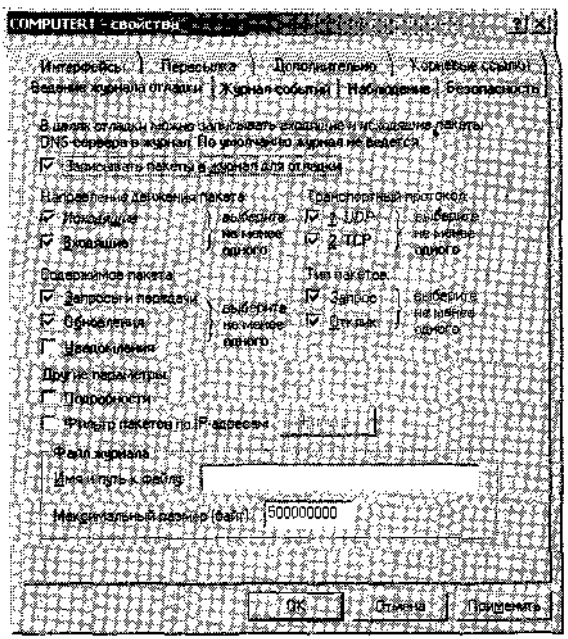


Рис. 6-6. Включение регистрации отладочной информации

На вкладке **Ведение журнала отладки** можно указать следующие типы регистрируемых событий:

- запросы;
- уведомления от других серверов;

- динамические обновления;
- содержимое раздела question сообщения DNS-запроса;
- содержимое раздела answer сообщения DNS-запроса;
- количество отправленных сервером запросов;
- количество полученных сервером запросов;
- количество DNS-запросов, поступивших на UDP-порт;
- количество DNS-запросов, поступивших на TCP-порт;
- количество отправленных сервером полных пакетов;
- **и** количество пакетов, записываемых сервером в зону.

Внимание! Не включайте регистрацию отладочной информации при обычной работе сервера, поскольку она отнимает массу процессорного времени и требует дополнительного места на жестком диске. Она нужна только при устранении неполадок DNS.

Лабораторная работа. **Использование инструментов устранения неполадок DNS**

Вы воспользуетесь программой Nslookup для выполнения базовых операций по устранению неполадок DNS. Также вы настроите журнал DNS на регистрацию пакетов и оцените результат.

Упражнение 1. Использование разовых команд Nslookup

В этом упражнении вы с помощью Nslookup выполните прямой и обратный запросы.

1. Войдите в систему Computerl *как. Администратор* (Administrator) и подключитесь к Интернету (если это еще не сделано).
2. Из командной строки исполните следующую команду:

   netsh interface ip set dns «local area connection» static 192.168.0.1.

   которая отправляет запрос локальному DNS-серверу до опроса удаленного DNS-сервера.
3. Выполните команду nslookup www.msn.com.

   Если вы получите сообщение о превышении времени ожидания, повторите команду. На экране вы должны увидеть примерно такой текст:

   ```
   Server:  computerl.domainl.local
   Address:  192.168.0.1

   Name:  www.msn.com
   Addresses:  207.68.171.254,  207.68.172,
   253,  207.68.172.254,  207.68.173.253
            207.68.173.254,  207.68.171.25  3
   ```

   Эти IP-адреса соответствуют полному DNS-имени *www.msn.com*.
4. Выполните команду nslookup 207.68.173.253.

Если вы получите сообщение о превышении времени ожидания, повторите команду. На экране вы должны увидеть примерно такой текст:

```
Server:   computer"!, domain"!, local
Address:  192.168.0.1

Name:     feeds2.msn.com
Address:  207.68.173.253
```

Упражнение 2. Nslookup в интерактивном режиме

В этом упражнении вы выполните Nslookup в интерактивном режиме и сравните данные, полученные в режимах Nodebug, D2 и Debug. Затем вы выполните запросы в зоне по умолчанию.

1. Если вы еще не вошли в систему на Computerl под учетной записью *Администратор* (Administrator), сделайте это.
2. Из командной строки" исполните следующую команду:

   ```
   dnscmd / zoneresetsecondaries domai.n1. local / nonsecure.
   ```

   Эта команда разрешает зонную передачу на любой сервер, что позволит просматривать все содержимое зоны *domain 1.local* средсвами Nslookup.
3. Выполните команду nslookup. На экране должен появиться текст, подобный приведенному далее. О том, что вы работаете в интерактивном режиме, говорит признак командной строки Nslookup — символ «правая угловая скобка» (>).

   ```
   Default Server:   computerl.domainl.local •
   Address:  192.168.0.1
   >
   ```

4. В командной строке Nslookup введите set all и нажмите Enter. Появится список всех текущих параметров Nslookup:

   ```
   Default Server:   computerl.domainl.local
   Address:  192.168.0,1

   Set options: •
      nodebug
      defname
      search
      recu.rse
    nod2
      novo
    noignoretc
      port=53
      type=A
    • class=IN
      timeout=2
      retry=1
      root=A.ROOT-SERVERS.NET.
      domain=domain1.local
      MSxfr
   ```

```
IXFRversion=1
srchlist=domain1.local
>
```

Обратите внимание, что первый параметр -nodebug. В этом случае Nslookup выводит краткую информацию.

5. В командной строке Nslookup выполните www. msnbc. com. Если вы получили сообщение о превышении времени ожидания, повторите команду. На экране должна появиться информация об имени, соответствующем псевдониму *yvww.msnbc.com*, а также IP-адрес(а), соответствующий FQDN-имени, и сам псевдоним *www.msnbc.cotn*.
6. В командной строке Nslookup выполните set d2. Nslookup перейдет в режим подробной отладки (Verbose Debug).
7. В командной строке Nslookup выполните set a11. Изучите результат и укажите два отличия между текущим списком параметров и списком параметров, выведенных в п. 4 (после выполнения команды set a11).
8. В командной строке Nslookup исполните www .msnbc. com. (не забудьте поставить точку после имени). Вы получите детализированный ответ, состоящий из разделов SendRequestO, Got Answer и Non-Authoritative Answer.
9. Просмотрите все эти разделы и ответьте на следующие вопросы.

   Что содержится в первых двух разделах?

   Почему эти разделы появились в результате запроса?

   Почему раздел answer считается *неполномочным* (non-authoritative)?
10. В командной строке выполните set nod2. Появится сообщение об отключении режима d2 возвращении в режим debug.
11. В командной строке выполните www.msnbc.com. (не забудьте поставить точку после имени).
12. Сравните листинг с результатом аналогичного запроса в п. 7. В чем различие между режимами d2 и debug?
13. В командной строке выполните set nodebug. Nslookup выйдет из отладочного режима.
14. Выполните Is domainl, local. На экран выводятся все записи ресурсов-узлов (A) и серверов имен (NS), определенных в домене *domainl.local*. Полное содержимое записей ресурсов не показано, так как Nslookup вышел из режима отладки.
15. Выполните set q=s rv. Эта команда ограничивает вывод только записями ресурсов-служб (SRV)..
16. Выполните Is -t domainl. local. Результат содержит все записи ресурсов типа SRV, определенные в домене *domainl.local*.

Совет Если надо просто просмотреть список всех записей ресурсов типа SRV в домене и не выполнять других запросов, можете объединить пп. 15 и 16, выполнив Nslookup ls -t srv domainl.local.

17. Выполните _ldap._tcp. На экране появится результат, похожий на приведенный ниже — полное содержимое записи ресурса SRV с именем _ldap._tcp:

```
Server:     computerl.domainl.local
Address:    192.168.0.1
```

```
_ldap._tcp.domain"!.local          SRV service location:
          priority       =  0
          weight         =  100
          port              =  389
          svr   hostname =  computerl.domainl. local
computer"!.domain"!.local internet address  =  192.168.0.1
computerl.domainl.local internet address  =  207.46.252.233
>
```

18. Выполните exit. Программа Nslookup завершит свою работу.
19. Выполните команду dnscmd /zoneresetsecondaries domainl, local /securens. Она восстановит параметры зонной передачи — снова станет доступной только серверам, указанным в записях NS базы данных зоны.
20. Закройте окно командной строки.

Упражнение 3. Отладка с применением журнала DNS

Вы включите регистрацию отладочных событий в журнале службы DNS-сервера и выполните запросы, чтобы в журнале появились записи о событиях. Затем вы остановите службу DNS-сервера и изучите сообщения, зарегистрированные в файле Dns.log.

1. Войдите в Domainl с компьютера Computerl под учетной записью *Администратор* (Administrator).
2. В дереве консоли *DNS* щелкните узел **COMPUTER!** правой кнопкой и выберите **Свойства (Properties).**
3. В окне свойств COMPUTER1 на вкладке **Ведение журнала отладки (Debug Logging)** установите флажок **Записывать пакеты в журнал для отладки (Log Packets For Debugging).** Остальные параметры станут доступны для изменения. Посмотрите, какие DNS-пакеты регистрируются в журнал по умолчанию, и щелкните OK.
4. Убедитесь, что Computerl подключен к Интернету и в командной строке выполните nslookup www. technet. com.* [не забудьте точку после полного имени (FQDN)].
5. Если вы получили сообщение о превышении времени ожидания, повторите п. 4.
6. Откройте консоль *Службы* (Services), щелкнув **Пуск ^ar1)\Администрирование (Administrative Too18)\Службы (Services).**
7. **В** правой панели консоли *Службы* найдите службу **DNS-сервер (DNS Server)** и остановите ее, в контекстном меню выбрав **Стоп (Stop).**
8. В *Проводнике Windows* перейдите в папку WINDOWS\System32\Dns. Щелкните файл Dns.log правой кнопкой и выберите **Открыть с помощью (Open With).**
9. В окне **Открыть с помощью (Open With)** в списке программ выберите **Текстовый редактор WordPad (WordPad)** и щелкните OK.
10. В открытом в WordPad файле *Dns.log* найдите последовательность сообщений запросов и ответов, сгенерированных при разрешении имени *www.technet.com*. Она выглядит примерно так:

```
13:49:42 848  PACKET  UDP Rev 192.168.0.1     0003  Q  [0001 0  N0ERR0R]
(3)www(7)technet(3°)com(0)

13:49:42 848  PACKET  UDP Snd 192.168.0 .1     36f6  Q  [0000     N0ERR0R]
(3)www(7)technet(3)com(0)
```

```
13:49:42 848 PACKET UDP Rev 207.68.11 2.30 36f6 R Q [0080
NOERROR] (3 )www(7)technet(3)com(0)

13:49:42 848 PACKET UDP Snd 207.68.14 4.151 36f6 Q [0000
NOERROR] (3) www(7)technet(3)com(0)

13:49:43 848 PACKET UDP Rev 207.68.14 4.151 36f6 R Q [0084 A
NOERROR] (3) www(7)technet(3)com(0)
```

11. Ответьте на следующий вопрос.

    Почему первое относящееся к www.technet.com сообщение в журнале помечено как относящееся к протоколу UDP, а также почему оно считается входящим (Rev, то есть Receive)?
12. Закройте файл *Dns.log.*
13. Запустите службу DNS-сервера в консоли *Службы.*
14. Сбросьте флажок **Записывать пакеты в журнал для отладки** на вкладке **Ведение журнала отладки** окна свойств COMPUTER1.
15. Закройте окно свойств COMPUTER1 щелчком OK и выйдите из системы Computet!.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Какую команду необходимо выполнить в командной строке для осуществления обратного разрешения IP-адреса 207.46.230.218?
2. Какая команда в командной строке утилиты Nslookup позволит просмотреть все содержимое зоны *contoso.com'?*
   a. ls -d contoso.com.
   b. ls -t contoso.com.
   c. ls -a contoso.com.
   d. ls -any contoso.com.
3. Какая команда в командной строке утилиты Nslookup вернет список всех записей ресурсов SRV в домене? .
   a. set q=srv.
   b. set q=srv *<имя домена>.*
   c. ls -t srv *<имя домена>.*
   d. ls -d srv *<имя домена>.*
4. Назовите два способа включения регистрации только ошибок и предупреждений в журнале событий DNS?
5. Вы включили регистрацию пакетов в журнале в окне свойств DNS-сервера. Что необходимо сделать, чтобы увидеть корректно отформатированное содержимое журнала?

Резюме

- Программа Nslookup позволяет отправлять тестовые запросы DNS-серверу и получать развернутые ответы в командной строке.

- В журнале событий DNS регистрируются ошибки службы DNS-сервера ОС Windows Server 2003. При неполадках DNS в первую очередь необходимо просмотреть журнал событий DNS в консоли *Просмотр событий* (Event Viewer).
- Служба DNS-сервера ведет собственный журнал событий, служащий для отладки: *WINDOWS\System32\Dns\Dns.log*.
- Чтобы включить регистрацию DNS-пакетов в файле Dns.log, установите флажок Записывать пакеты в журнал для отладки (Log Packets For Debugging) на вкладке Ведение журнала отладки (Debug Logging) окна свойств DNS-сервера.

Занятие 2 Средства мониторинга DNS

Для контроля работы DNS обычно применяют Replication Monitor и *Системный монитор* (System Monitor). Первый поддерживает мониторинг репликации DNS в интегрированных с Active Directory зонах, второй позволяет следить за любым из 62 связанных с DNS показателей.

Изучив материал этого занятия, вы сможете:

- использовать Replication Monitor для мониторинга репликации или данных зоны в DNS;
- использовать счетчики *Системного монитора* для контроля производительности DNS.

Продолжительность занятия — около 30 минут.

Replication Monitor

Replication Monitor (replmon.exe) — графическая утилита из состава *Средств поддержки Windows* (Windows Support Tools), позволяющая контролировать и устранять неполадки репликации Active Directory. Она незаменима для контроля передачи данных DNS в зонах, интегрированных с Active Directory.

Replication Monitor позволяет:

- принудительно выполнять репликацию данных DNS в самых разных областях репликации;
- определять сбой партнеров по репликации;
- отображать топологию репликации;
- опрашивать партнеров по репликации и генерировать отдельные списки удач и сбоев репликации;
- отображать изменения, которые пока не реплицированы с определенного партнера;
- отслеживать состояние репликации контроллеров домена различных лесов.

После установки пакета *Средства поддержки Windows* Replication Monitor запускается командой replmon (рис. 6-7).

Replication Monitor позволяет отслеживать репликацию Active Directory через определенные контроллеры домена сети. Однако по умолчанию в дереве консоли нет ни одного контроллера домена. Чтобы добавить контроллер домена, в дереве консоли *Replication Monitor* щелкните значок **Monitored Services** правой кнопкой и выберите **Add Monitored Server.** После добавления всех серверов, которые предполагается контролировать, конфигурацию консоли можно сохранить в INI-файле, а затем при необходимости открывать его из Replication Monitor.

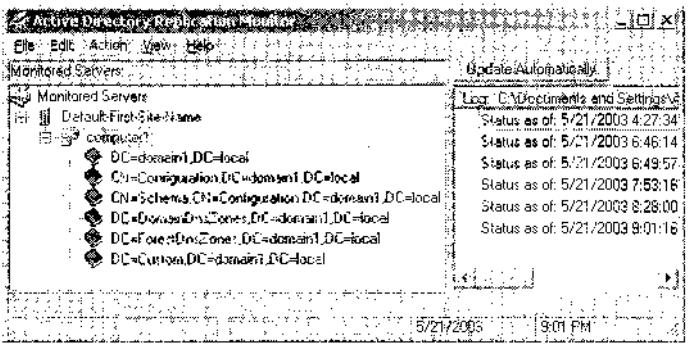


Рис. 6-7. Консоль *Replication Monitor*

Разделы каталога и интегрированные с Active Directory зоны

Установленные на сервере разделы Active Director}, можно увидеть, раскрыв соответствующий узел. Контроллеры домена, которые одновременно являются DNS-серверами и хранят одну интегрированную с Active Directory зону по умолчанию имеют реплику из пяти таких разделов.

Далее приводится описание пяти разделов домена Active Directory и зоны DNS с именем *contoso.com*.

- DC=contoso,DC=com — содержит объекты (такие как пользователи и компьютеры), относящиеся к локальному домену. Каждый контроллер домена хранит полную реплику раздела локального домена. Кроме тетю, здесь хранятся данные для совместимости с DNS-серверами Microsoft Windows 2000. Для хранения данных зоны DNS в разделе домена задайте в качестве области репликации зоны На все контроллеры домена в домене Active Directory (To all domain controllers in the Active Directory domain) (значение по умолчанию),
- **CN=Configuration,DC=contoso,DC=com** — здесь хранится топология репликации и прочая информация о конфигурации, которую необходимо реплицировать в рамках леса. Каждый контроллер леса хранит реплику раздела конфигурации. Но этот раздел не.включает данные зоны DNS.
- CN=Schema,DC=coiitoso,DC=com — здесь хранятся объекты классов *classSchema* и *attributeSchema,* определяющие типы объектов, которые разрешено хранить в лесу Active Directory. Каждый контроллер леса хранит реплику раздела схемы, в этом разделе также нет данных зоны DNS.
- DC=DomainDnsZones,DC=contoso,DC=com — встроенный раздел каталога приложений с именем *DomainDnsZon.es,* рештицируемый на все контроллеры домена Windows Server 2003, которые одновременно являются DNS-серверами в данном домене Active Directory. Чтобы данные зоны DNS хранились в разделе *DomainDnsZones,* задайте в консоли *DNSB* качестве области репликации зоны **На все DNS-серверы в домене Active Directory (To all DNS Servers in the Active Directory domain).**
- **DC=ForestDnsZones,DC=contoso,DC=com** — встроенный раздел каталога приложений с именем *ForestDnsZones,* решшцируемый на все контроллеры домена Windows Server 2003, которые одновременно являются DNS-серверами в лесу Active Directory. Для хранения данных зоны DNS в разделе *ForestDnsZones* задайте в консоли *DNS* в качестве области репликации зоны **На все DNS-серверы в лесу Active Directory (To all DNS Servers in the Active Directory forest).**

Вы также вправе создать собственные разделы каталогов приложений и привлекать определенные контроллеры домена для хранения реплики этих разделов. На рис. 6-7 показан такой раздел каталога приложений с именем Custom. Чтобы хранить данные зоны DNS в собственном разделе каталога приложений, выберите в консоли *DNS* в качестве области репликации вариант **На все контроллеры домена, указанные в области видимости следующего раздела каталога приложений (To all domain controllers specified in the scope of the following application directory partition)** и выберите в поле со списком нужный раздел.

Узнать раздел Active Directory, который используется для хранения данных определенной зоны DNS, можно либо в окне свойств зоны в консоли DNS, либо исполнив команду Dnscmd /zoneinfo.

Параметры команды Dnscmd, относящиеся к репликации DNS

Экзамен не предусматривает тщательной проверки знания утилиты Dnscmd, но она может сильно облегчить вам жизнь. Например, вместо «путешествия» сквозь многочисленные диалоговые окна, можно воспользоваться Dnscmd — как для определения, так и для смены области репликации зоны. Чтобы узнать область репликации зоны для домена *domain 1. local,* выполните следующую команду:

```
dnscmd /zoneinfo .domainl.local
```

и найдите в листиге строку directory partition. Область репликации зоны изменяют параметром /zonechangedirectorypartition, за которым следует любой из следующих: /domain (для всех DNS-серверов домена), /forest (для всех DNS-серверов леса) и /legacy (для всех контроллеров домена в домене). Например, чтобы задать в качестве области репликации зоны *domainl.local* все DNS-серверы домена, выполните такую команду:

```
dnscmd /zonechangedirectorypartition domainl.local /domain.
```

При наличии соответствующих прав можно даже выполнять эти команды удаленно. В этом случае после dnscmd просто указывается имя сервера.

Принудительная репликация интегрированной с Active Directory зоны

Если известно, в каком разделе каталога хранится информация зоны DNS, можно принудительно запустить ее репликацию с помощью Replication Monitor и избавиться от неполадок разрешения имен, вызванных устаревшими данными зоны.

Чтобы запустить репликацию интегрированной с Active Directory зоны, в консоли *Replication Monitor* щелкните соответствующий раздел правой кнопкой и выберите **Synchronize this partition with all servers.** Откроется окно, показанное на рис. 6-8.

С помощью этого диалогового окна можно реплицировать данные только на соседние (neighboring) серверы, на все серверы локального сайта или на все серверы всех сайтов

Обнаружение ошибок репликации

Ошибки DNS в интегрированных с Active Directory зонах могут возникать из-за неудавшейся репликации зоны. Replication Monitor позволяет их обнаружить: в меню **Action** выберите **Domain,** а затем **Search Domain Controllers for Replication Errors** (рис. **6-9).**

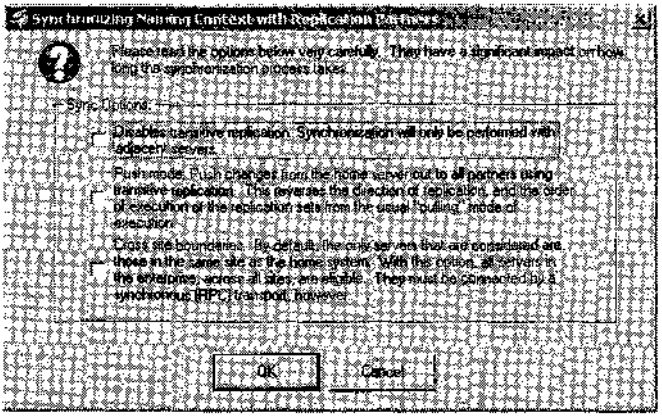


Рис. 6-8. Принудительный запуск репликации

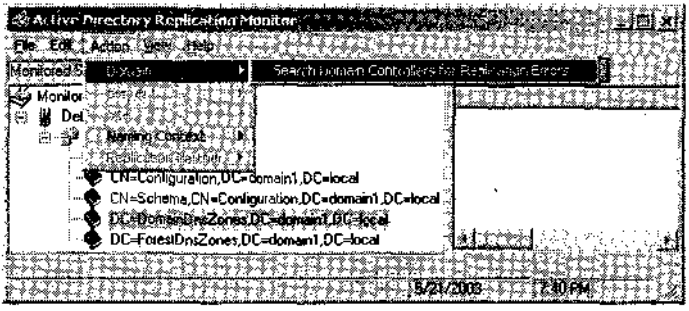


Рис. 6-9. Поиск ошибок репликации

Есть и другой способ: настроить Replication Monitor на отправку писем по электронной почте администратору при достижении определенного числа сбоев репликации. Для этого в меню View выберите **Options.** В диалоговом окне **Active Directory Replication Monitor Options** выберите **Notify When Replication Fails After Ibis Number of Attempts** и укажите количество сбоев, при котором должен оповещаться администратора. Установите флажок **Send mail to** и укажите в соответствующем поле адрес.

Подготовка к экзамену Replication Monitor предоставляет лишь базовые функции контроля и устранения неполадок репликации в Active Directory. Для более подробного анализа и устранения неполадок репликации в Active Directory служит Repadmin, другая утилита командной строки из состава *Средств поддержки Windows.*

Мониторинг производительности DNS с помощью *Системного монитора*

Системный монитор (System Monitor) • — утилита, расположенная в дереве консоли *Производительность* (Performance) и служащая для наблюдения за любым из сотен системных параметров в реальном времени. Каждый такой параметр [например % **загруженности процессора (% Processor Time)** или **Средняя длина очереди диска (Avg. Disk Queue Length)]** называется *счетчиком* (counter). Счетчики, относящиеся к одним сетевым подсистемам группируются в объекты производительности.

Системный монитор отображает графики, показывающие изменение значения счетчика в реальном времени (рис. 6-10).

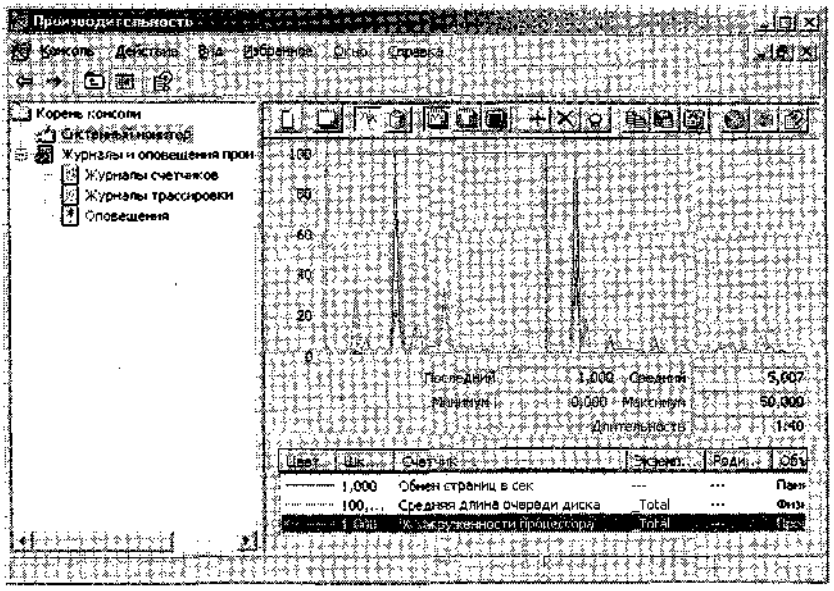


Рис. 6-10. Графики в окне *Системный монитор*

Чтобы открыть окно **Системный монитор (System Monitor),** откройте консоль *Производительность* (Performance), выбрав **Пуск (81arO\Администрирование (Administrative Tools) \Производительность (Performance)** (или выполните команду perfmon). В дереве консоли *Производительность* выберите узел **Системный монитор (System Monitor).**

Примечание Подробнее об использовании *Системного монитора* и счетчиков производительности — в главе 12.

Счетчики производительности DNS-сервера

В общем зачете объекты производительности DNS в *Системном мониторе* содержат 62 счетчика, которые применяются для измерения и наблюдения за различными параметрами сервера, в том числе:

- счетчики общей статистики производительности DNS-сервера, например суммарного количества обработанных запросов и ответов;
- счетчики TCP и UDP, определяющие количество DNS-запросов и ответов, пришедших/отправленных по этим протоколам;
- счетчики использования памяти, измеряющие использование и выделение памяти на DNS-сервере под управлением Windows Server 2003;
- счетчики рекурсивного поиска, оценивающие количество запросов/ответов DNS-сервера в рамках рекурсии в процессе поиска и разрешения имен DNS от имени клиента;
- счетчики поиска в WINS, оценивающие количество запросов/ответов WINS-сервера при использовании функции интеграции WINS с DNS-серверов;

- счетчики зонных передач, включая специальные счетчики для измерения: всех зонных передач (AXFR), добавочных зонных передач (DCFR) и активности уведомлений при обновлении зон DNS.

На заметку Большинство счетчиков производительности *Системного монитора* используются достаточно редко. При этом достаточно распространена шутка, что это важнейший инструмент администратора. А все потому, что, будучи запущенным и помещенным на видное место экрана, он своими графиками реального времени создает прекрасную иллюзию напряженной работы, которая так нравится начальству.

В табл. 6-2 описаны наиболее популярные счетчики производительности объекта DNS. Они дают представление о том, как часто DNS-сервер получает запросы и выдает ошибки.

Табл. 6-2. Счетчики производительности объекта DNS

Счетчик	Описание
Кэш-память (Caching Memory)	Общий объем количества системной памяти, используемой DNS-сервером для кэширования. Этот счетчик позволяет понять, действительно ли кэш помогает оптимизировать использование доступной памяти
Получено динамических обновлений (Dynamic Update Received)	Общее количество запросов на динамическое обновление, полученных DNS-сервером. Позволяет узнать, пытаются ли DNS-клиенты обновить свои DNS-адреса после включения динамического обновления
Отклонено динамических обновлений (Dynamic Update Rejected)	Общее количество отклоненных DNS-сервером запросов на динамическое обновление. Сравнивайте значение этого счетчика со счетчиком **Получено динамических обновлений,** чтобы определить количество систем, испытывающих проблемы с обновлением DNS-адреса
Записано в базу данных динамических обновлений (Dynamic Update Written To Database)	Общее количество динамических обновлений, записанных в БД DNS-сервера. Сравнение значения этого счетчика со счетчиком **Получено динамических обновлений** позволяет определить количество систем, успешно обновивших записи в DNS
Ошибок безопасных обновлений (Secure Update Failure)	Общее количество неудачных безопасных обновлений на DNS-сервере. Позволяет выявить клиенты, испытывающие проблемы с безопасными динамическими обновлениями. Сравнение показаний со счетчиком **Получено безопасных обновлений** позволяет оценить количество таких клиентов
Получено безопасных обновлений (Secure Update Received)	Общее количество полученных DNS-сервером запросов на безопасное обновление. Сравнение этого значения со счетчиком **Ошибок безопасных обновлений** позволяет оценить количество систем, успешно выполнивших безопасное обновление в DNS

Табл. 6-2. *(окончание)*

Счетчик	Описание
Общее число полученных запросов (Total Query Received)	Общее количество полученных DNS-сервером запросов. Дает общую картину использования DNS-сервера
Общее число полученных запросов/сек (Total Query Received/Sec)	Среднее количество запросов, поступающих на DNS-сервер в секунду. Дает общую картину использования DNS-сервера в сетях с высокой нагрузкой
Отправлено всего ответов (Total Response Sent)	Общее количество отправленных DNS-сервером ответов. Дает общую картину использования сервера
Отправлено всего ответов/сек (Total Response Sent/Sec)	Среднее количество ответов DNS-сервера в секунду. Дает общую картину использования DNS-сервера в сетях с высокой нагрузкой
Неудачных передач зоны (Zone Transfer Failure)	Общее количество сбоев зонных передач основного DNS-сервера. Помогает устранять неполадки разрешения имен
Получено запросов передач зоны (Zone Transfer Request Received)	Общее количество полученных основным DNS-сервером запросов зонной передачи. В сравнении со счетчиками **Неудачных передач зоны** и **Успешных передач зоны** дает общую картину передач зон
Успешных передач зоны (Zone Transfer Success)	Общее количество удачных зонных передач основного DNS-сервера. Помогает устранять неполадки разрешения имен.

Внимание! Не предоставляйте доступ к информации о производительности никому, кроме членов локальных групп *Пользователи журналов производительности* (Performance Log Users) и *Пользователи системного монитора* (Performance Monitor Users). Эти группы появились в Windows Server 2003.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Пользователи в штаб-квартире компании сообщают о невозможности установить надежное подключение к ресурсами своего филиала. Оба офиса находятся в одном домене Active Directory, *contoso.com*, в котором присутствуют DNS-серверы под управлением Windows Server 2003 и Wndows 2000. DNS-домен contoso.com настроен как зона, интегрированная в Active Directory. Как выполнить репликацию, чтобы наиболее свежие данные DNS были немедленно обновлены в сайтах, доступных по WAN-каналам?
2. Значения каких счетчиков производительности позволяют определить процентную долю неудачных запросов среди всех запросов на защищенное динамическое обновление?
3. Данные зоны adatum.com хранятся в разделе каталога приложений *DomainDnsZones*. Как добиться того, чтобы эта информация реплицировалась в рамках всего леса?

Резюме

- Replication Monitor — графическая утилита, позволяющая обнаруживать и устранять неполадки репликации в Active Directory. Без нее не обойтись при устранении неполадок передач DNS-зон, интегрированных с Active Directory.
- В дереве консоли Replication Monitor показанные установленные на серверах разделы Active Directory. Контроллеры домена, выполняющие функции DNS-серверов, на которых располагается одна интегрированная с Active Directory зона, по умолчанию содержат реплику пяти таких разделов.
- Найти раздел Active Directory, в котором хранятся данные DNS-зоны, можно, либо посмотрев в консоли *DNS* свойства зоны DNS, либо при помощи команды Dnscmd /zoneinfo. Если известно, в каком разделе каталога хранится информация зоны DNS, можно принудительно запустить репликацию этой зоны посредством Replication Monitor. Иногда это помогает устранить неполадки разрешения имен, вызванные устаревшими данными зоны.
- Неполадки DNS в интегрированных с Active Directory зонах могут возникать из-за ошибок репликации зоны. Replication Monitor помогает обнаруживать такие ошибки.
- *Системный монитор* (System Monitor) — утилита, расположенная в дереве консоли *Производительность* (Performance) и позволяющая наблюдать за любым из сотен системных параметров в реальном времени. Объект производительности DNS в *Системном мониторе* включает 62 счетчика.

Пример из практики

Вы системный администратор Trey Research, компании, разрабатывающей электрогенераторы, использующие энергию ветра и других возобновляемых источников. Штаб-квартира компании располагается в г. Монтерее, штат Калифорния, а единственный филиал — в г. Сиракузах, штат Нью-Йорк. Вернувшись из недельного отпуска вы обнаруживаете ряд технических неполадок.

1. Среди пришедших за неделю писем есть срочное сообщение от администратора филиала в Сиракузах, в котором он информирует, что его пользователи испытывают сложности разрешением имен компьютеров в офисе в Монтерее при обращении через виртуальную частную сеть (YPN). Администратор включил в письмо информацию из журнала событий DNS-сервера *ns5.treyresearch.net* в Сиракузах.

   Запрос на зонную передачу дополнительной зоны treyresearch.net отклонен главным DNS-сервером с адресом 192.168.0.15. Проверьте, разрешены ли зонные передачи на главном сервере 192.168.0.15. Для этого откройте консоль *DNS,* выберите сервер 192.168.0.15, а затем посмотрите параметры на вкладке **Передачи зон** окна свойств дополнительной зоны treyresearch.net. На их основании внесите изменения в конфигурацию на этой вкладке (и, возможно, на вкладке **Серверы имен),** чтобы разрешить зонные передачи на этот сервер.

   DNS-сервер в офисе в Монтерее установлен с помощью *Мастера компонентов Windows* (Windows Components Wizard).

   Что необходимо предпринять, чтобы клиенты сиракузского филиала получили возможность разрешать имена? Предполагается, что необходимо сохранить (или восстановить) параметры безопасности защиты по умолчанию для передач зон.

a. Сконфигурировать *ns5.treyresearch.net* на получение уведомлений об обновлениях зоны.

b. Добавить запись ресурса-узла A в зону *treyresearch.net*, указывающую на компьютер *ns5.treyresearch.net*.

c. Сконфигурировать зону *treyresearch.net*, разрешив зонные передачи на любой сервер.

d. Добавить запись ресурса NS в зону *treyresearch.net*, указывающую на компьютер *ns5.treyresearch.net*.

2. Спустя некоторое время после устранения очередной неполадки вы решили создать запись делегирования *syr.treyresearch.net* для офиса в Сиракузах, но позднее обнаружили, что пользователи офиса в Монтерее не в состоянии разрешать имена компьютеров филиала. Пытаясь устранить неполадку, вы воспользовались утилитой Nslookup на DNS-сервере *nsl.treyresearch.net* в офисе в Монтерее и получили следующий результат:

```
C:\>nslookup
Default Server:  ns1.treyresearch.net
Address:  192.168.0.15

ls treyresearch. net
 [ns1.treyresearch.net]
treyresearch.net.          A      1 92.168.0.15
treyresearch.net.          NS     server=ns1.treyresearch.net
treyresearch.net.          NS     server=ns5.treyresearch.net
gc._msdcs                  A      1 92.168.0.15
ns1                        A      192,  168.0.15
ns5                        A '    192.  168.1.2
DomainDnsZones             A      1 92.168.0.15
ForestDnsZones             A      1 92.168.0.15
syr                        NS     server = ns1.treyresearch.net
>
```

Подготовка к экзамену В набор *Средств поддержки Windows* (Windows Support Tools) входит утилита командной строки DNSLint, служащая в основном для устранения неполадок делегирования. Ее также можно использовать для проверки записей DNS репликации Active Directory и поиска записей различных типов на нескольких DNS-серверах.

Какая ошибка стала причиной неполадок разрешения имен?

3. Домен *syr.treyresearch.net* сконфигурирован как интегрированная с Active Directory зона в сиракузском филиале. В качестве области репликации зоны был выбран вариант **На все DNS-серверы в лесу Active Directory (All** DNS Servers in the Active Directory **forest).** Какой раздел в Replication Monitor используется для принудительной репликации данных зоны домена *syr.treyresearch.net?*

a. DC=treyresearch,DC=net.

b. DC=ForestDnsZones,DC=treyresearch,DC=net.

c. DC=ForestDnsZones,DC=syr,DC=treyresearch,DC=net.

d. ОС=ООотатОп82опе8,ОС=8уг,ОС=1reyre8e'агсп,ОС=пе1.

Практикум по устранению неполадок

На этом практикуме вы устраните неполадки разрешения имен.

1. Войдите в систему Computerl как *Администратор* (Administrator). Убедитесь, что консоль *DNS* не открыта.
2. Подключите Computerl с Интернету через подключение MylSP.
3. Войдите в домен с Computer2 *как Администратор* (Administrator).
4. Подключите Computer2 к Интернету и проверьте подключение: зайдите на какой-нибудь внешний Web-сайт, например *http://www.msn.com*. .
5. Вставьте в дисковод Computer2 прилагаемый компакт-диск.
6. Найдите и дважды щелкните командный файл *\70-291\labs\Chapter06\ch6a.bat*.
7. Еще раз проверьте подключение к Интернету, зайдя на другой Web-сайт, например *http://www.windowsupdate.com*. Доступ будет невозможен.
8. На Computer2 выполните команду dnscmd computerl /clearcache, которая очистит кэш DNS-сервера на Computerl.

   Подготовка к экзамену Запомните эту команду — она наверняка пригодится.

9. Из командной строки исполните nslookup www. msn. com. Разрешить имя не удастся.
10. С помощью утилиты Nslookup в режиме d2 отследите сообщения запроса и ответа внешнего доменного имени *www.msn.com*. (не забудьте поставить в конце точку). Подробно этот процесс описан в задании 2 занятия 1.
11. После получения ответа от Nslookup сравните значения Rcode в разделах SendRequest и Got Answer и ответьте на вопросы.

    Кто «виновник» ошибки — DNS-клиент или DNS-сервер? Почему?
12. Завершите работу Nslookup командой exit.
13. В другом окне командной строки на Computer2 выполните команду dnscmd computerl /info. На экран выводится информация о конфигурации DNS-сервера на Computerl.
14. Найдите колонку Configuration Flags. Здесь отключенные параметры отмечены нулем (0), включенные — единицей.

    Какие из включенных параметров DNS-сервера на Computerl могут помешать пользователям Computer2 разрешать имена Интернета?
15. Найдите на прилагаемом компакт-диске файл \70-291\Labs\Chapter06\Ch6b.bat и запустите его.

    Файл восстановит корректную конфигурацию DNS. (Он ничего не «испортит» в DNS и оставит корректные параметры без изменений.)
16. С помощью Internet Explorer убедитесь, что доступ к интернет-ресурсам по DNS-именам снова открыт.
17. Выйдите из систем Computerl и Computer2.

Резюме главы

- Nslookup — утилита командной строки, позволяющая опрашивать и устранять неполадки DNS-серверов.
- В журнале событий DNS регистрируются ошибки, возникающие в службе DNS-сервера ОС Windows Server 2003.

- Служба DNS-сервера ведет собственный отладочный журнал, записывая информацию в файл Dns.log в каталоге *\WINDOWS\System32\Dns*.
- Replication Monitor — утилита с графическим интерфейсом, служащая для наблюдения за репликацией Active Directory и устранения неполадок. Она позволяет выполнять принудительную репликацию интегрированных с Active Directory зон и обнаруживать в домене ошибки репликации.
- *Системный монитор* (System Monitor) позволяет отслеживать статистику работы компонентов Windows, в том числе DNS, в реальном времени. Объект производительности DNS в *Системном мониторе* содержит 62 счетчика.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Запомните основные команды и параметры утилиты Nslookup.
- Научитесь уверенно ориентироваться в сообщениях журнала событий DNS.
- Научитесь принудительно запускать репликацию и обнаруживать ошибки в интегрированных с Active Directory зонах.
- Запомните поименно разделы, в которых могут храниться данные интегрированных с Active Directory зон.

Основные термины

Реплика ~ replica — копия раздела Active Directory, хранящаяся на контроллере домена.

Схема ~ schema — набор определений всего множества объектов, которые разрешено хранить в каталоге. Схема определяет обязательные и дополнительные атрибуты каждого экземпляра класса, а также разрешенные родительские объекты.

classSchema — объект, определяющий классы в схеме. Служит шаблоном для построения объектов каталога данного класса. Примеры: User и Server.

attributeSchema — объект, определяющий атрибуты схемы. Определяет допустимое содержимое и синтаксис атрибута в каталоге. Примеры: User-Principal-Name и Telex-Number.

Рекурсивный запрос ~ recursive query — запрос, требующий от DNS-сервера выполнить рекурсию.

? Вопросы и ответы

Занятие 1. Лабораторная работа. Упражнение 2

7. В командной строке Nslookup выполните set all. Изучите результат и укажите два отличия между текущим списком параметров и списком параметров, выведенных в п. 4 (после выполнения команды set all)?
Правильный ответ: вместо Debug используется Nodebug, а вместо d2 — nod2.

9. Просмотрите все эти разделы и ответьте на следующие вопросы.
   Что содержится в первых двух разделах?
   Правильный ответ: первые два раздела соответствуют сообщениям запроса и ответа, которыми обменялись распознаватель и сервер.
   Почему эти разделы появились в результате запроса?
   Правильный ответ: потому что включен параметр dZ.
   Почему раздел answer считается *неполномочным* (non-authoritative)?
   Правильный ответ: потому что ответ на предыдущий такой же запрос был сохранен в кэше неполномочного сервера, и ответы он предоставляет именно оттуда, не обращаясь к полномочному серверу.
12. Сравните листинг с результатом аналогичного запроса в п. 7. В чем различие между режимами d2 и debug?
   Правильный ответ: в режиме d2, или Verbose Debug, отображаются сообщения как запроса, так и ответа, а в режиме Debug выводятся только ответы.

Занятие 1. Лабораторная работа. Упражнение 3

11. Ответьте на следующий вопросы (впишите ответ в специально отведенное место).
   Почему первое относящееся к www.technet.com сообщение в журнале помечено как относящееся к протоколу UDP, а также почему оно считается входящим (Rev, то есть Receive)?
   Правильный ответ: команда Nslookup www. technet. com — по сути DNS-запрос. DNS-запросы отправляются по транспортному протоколу UDP, а журнал настроен на регистрацию как DNS-запросов, так и всего DNS-трафика по UDP. Первый пакет помечен как Receive (прием) потому, что DNS-запрос создан на DNS-распознавателе, а не на протоколирующем трафик сервере. DNS-сервер получил запрос на разрешение имени *www.technet.com* с DNS-распознавателя.

Занятие 1. Закрепление материала

1. Какую команду необходимо выполнить в командной строке для осуществления обратного разрешения IP-адреса 207.46.230.218?
   Правильный ответ: nslookup 207.46.230.218.
2. Какая команда в командной строке утилиты Nslookup позволит просмотреть все содержимое зоны *contoso.com*!
   a. Is -d contoso.com.
   b. Is -t contoso.com.
   c. Is -a contoso.com.
   d. Is -any contoso.com.
   Правильный ответ: a.
3. Какая команда в командной строке утилиты Nslookup вернет список всех записей ресурсов SRV в домене?
   a. -set q=srv.
   b. set q=srv <domain name>.
   c Is -t srv <domain name>.
   d. Is -d srv <domain name>.
   Правильный ответ: c.

4. Назовите два способа включения регистрации только ошибок и предупреждений в журнале событий DNS?

   Правильный ответ: в консоли DNS откройте окно свойств DNS-сервера и на вкладке Журнал событий (Event Logging) выберите Ошибки и предупреждения (Errors and warnings). Второй способ: откройте в консоли DNS диалоговое окно Свойства: События DNS (DNS Events Properties) и на вкладке Фильтр (Filter) сбросьте флажки Аудит успехов (Success Audit) и Аудит отказов (Failure Audit).

5. Вы включили регистрацию пакетов в журнале в окне свойств DNS-сервера. Что необходимо сделать, чтобы увидеть корректно отформатированное содержимое журнала?
   Правильный ответ: остановить службу DNS-сервера и открыть файл WINDOWS\System32\Dns\Dns.log в текстовом редакторе, поддерживающего формат RTF, например в WordPad.

Занятие 2. Закрепление материала

1. Пользователи в штаб-квартире компании сообщают о невозможности установить надежное подключение к ресурсами своего филиала. Оба офиса находятся в одном домене Active Directory, *contoso.com,* в котором присутствуют DNS-серверы под управлением Windows Server 2003 и Windows 2000. DNS-домен contoso.com настроен как зона, интегрированная в Active Directory. Как выполнить репликацию, чтобы наиболее свежие данные DNS были немедленно обновлены в сайтах, доступных по WAN-каналам?
   Правильный ответ: выполните принудительную репликацию раздела домена с помощью Replication Monitor. Выберите вариант синхронизации через границы сайтов.

2. Значения каких счетчиков производительности позволяют определить процентную долю неудачных запросов среди всех запросов на защищенное динамическое обновление?

   Правильный ответ: Получено безопасных обновлений (Secure Update Received) и Ошибок безопасных обновлений (Secure Update Failure).

3. Данные зоны adatum.com хранятся в разделе каталога приложений *DomainDnsZones.* Как добиться, чтобы эта информация реплицировалась в рамках всего леса?
   Правильный ответ: измените границы репликации зоны на На все DNS-серверы в лесу Adatum.com Active Directory (To all DNS Servers in the Adatum.com Active Directory forest) Затем средствами Replication Monitor запустите репликацию каталога приложений *ForestDnsZones.*

Пример из практики

1. Что необходимо предпринять, чтобы клиенты сиракузского филиала получили возможность разрешать имена? Предполагается, что необходимо сохранить (или восстановить) параметры безопасности защиты по умолчанию для передач зон.
   a. Сконфигурировать *ns5.treyresearch.net* на получение уведомлений об обновлениях зоны.
   b. Добавить запись ресурса-узла A в зону *treyresearch.net,* указывающую на компьютер *ns5.treyresearch.net.*
   c. Сконфигурировать зону *treyresearch.net,* разрешив зонные передачи на любой сервер.
   d. Добавить запись ресурса NS в зону *treyresearch.net,* указывающую на компьютер *ns5.treyresearch.net.*

   Правильный ответ: d.

2. Спустя некоторое время после устранения очередной неполадки вы решили создать запись делегирования *syr.treyresearch.net* для офиса в Сиракузах, но позднее обнаружили, что пользователи офиса в Монтерее не в состоянии разрешать имена компьютеров филиала. Пытаясь устранить неполадку, вы воспользовались утилитой Nslookup на DNS-сервере *nsl.treyresearch.net* в офисе в Монтерее и получили следующий результат:

```
C:\>nslookup
Default Server:  ns1.treyresearch.net
Address:  192.168.0.15

ls treyresearch.net
 [ns1.treyresearch.net]
treyresearch.net.          A      1 92.168.0.15
treyresearch.net.          NS     server = ns1.treyresearch.net
treyresearch.net.          NS     server = ns5.treyresearch.net
gc.jusdcs    ·             A      1 92.168.0.15
ns1                        A      192.  168.0.15
ns5                        A      192.  168.1.2
DomainDnsZones             A      1 92.168.0.15
ForestDnsZones             A      1 92.168.0.15
syr                       · NS    server = ns1.treyresearch.net
>
```

Какая ошибка стала причиной неполадок разрешения имен?

Правильный ответ: домен *syr.treyresearch.net* был некорректно делегирован серверу *nsl.treyresearch.net*, который являетря DNS-сервером офиса в Монтерее. Указанный сервер должен располагаться в Сиракузах.

3. Домен *syr.treyresearch.net* сконфигурирован как интегрированная с Active Directory зона в сиракузском филиале. В качестве области репликации зоны был выбран вариант **На все DNS-серверы в лесу Active Directory (All DNS Servers in the Active Directory forest).** Какой раздел в Replication Monitor используется для принудительной репликации данных зоны домена *syr.treyresearch.nef*>.

   a. DC=treyresearch,DC=net.

   b. DC=ForestDnsZones,DC=treyresearch,DC=net.

   c. DC=ForestDnsZones,DC=syr,DC=treyresearch,DC=net.

   d. DC=DomainDnsZones,DC=syr,DC=treyresearch,DC=net.

   Правильный ответ: b.

Практикум по устранению неполадок

1. Кто «виновник» ошибки — DNS-клиент или DNS-сервер? Почему?

   Правильный ответ: DNS-сервер. Значение Rcode в разделе Got Answer — SERVFAIL (то есть отказ сервера).

2. Найдите колонку Configuration Flags. Здесь отключенные параметры отмечены нулем (0), включенные — единицей.

   Какие из включенных параметров DNS-сервера на Computerl могут помешать пользователям Computer2 разрешать имена Интернета?

   Правильный ответ: NoRecursion.

ГЛАВА 7

Конфигурирование DHCP-серверов и клиентов

Темы экзамена

- Управление протоколом DHCP:
  - управление DHCP-клиентами и арендой адресов.
  - управление базами данных DHCP;
  - управление диапазонами DHCP-адресов;
  - управление резервированием и клиентами с фиксированными IP-адресами.

В этой главе

Протокол DHCP (Dynamic Host Configuration Protocol) совместно с *системой доменных имен* (Domain Name System, DNS) играет ключевую роль в сетевой инфраструктуре Microsoft Windows Server 2003. Во всех сетях, за исключением, пожалуй, самых маленьких, DHCP обеспечивает настройку параметров IP-протокола, необходимых для взаимодействия с другими компьютерами сети. Как минимум определяются IP-адрес и маска подсети, но обычно дополнительно назначаются суффикс основного контроллера домена, основной шлюз, основной и дополнительные DNS- и WINS-серверы, а также некоторые другие свойства. В отсутствие надежных и автоматических средств предоставления клиентам конфигурационных параметров администраторы не справляются с быстро растущей ручной работой по настройке IP-протокола.

DHCP — стандартное средство протокола IP, призванное упростить администрирование IP-конфигураций. DHCP автоматически назначает IP-адреса и настраивает другие важные параметры сетевых клиентов.

Прежде всего

Для выполнения упражнений этой главы вам потребуется:

- два объединенных в сеть компьютера (Computer! и Computer2) под управлением Windows Server 2003. Computerl надо присвоить статический адрес 192.168.0.1/24 и статический адрес 192.168.0.1 — основному DNS-серверу. Computer2 надо настроить на автоматическое получение адреса, а также назначить ему альтернативную конфигурацию с адресом 192.168.0.2/24. На обоих компьютерах назначается суффикс основного контроллера DNS — domainl.local;
- установить на Computerl службу DNS и разместить основную зону прямого просмотра *domainl.local,* настроенную на прием динамических обновлений, а также внести в нее записи узлов для обоих компьютеров;
- назначить Computerl контроллером домена в новом домене и лесе Active Directory с именем *domainl.local.* Computer2 надо назначить членом этого домена. После установки службы Active Directory зону domainl.local необходимо интегрировать в Active Directory и настроить на прием только безопасных динамических обновлений;
- на Computerl определить подключение к Интернету по телефонной линии с именем MylSP и сделать общим через *службу общего доступа к Интернету* (Internet Connection Sharing, ICS). Computer2 должен получать свои IP-параметры от ICS. (Можно выбрать другой тип подключения к Интернету, но придется внести соответствующие коррективы в упражнения.);
- установить на Computerl и Computer2 *средства поддержки Windows* (Windows Support Tools);
- установить на Computer2 флажок **Использовать суффикс DNS подключения при регистрации в DNS (Use This Connection's DNS Suffix In DNS Registration)** на вкладке DNS диалогового окна **Дополнительные параметры TCP/IP (Advanced TCP/IP Settings)** локального сетевого подключения.

Занятие 1. **Настройка DHCP-сервера**

DHCP позволяет автоматически задавать IP-адреса, маски подсети и прочие параметры клиентских компьютеров локальной сети. Если в сети доступен DHCP-сервер, компьютеры, сконфигурированные получать IP-адреса автоматически, запрашивают и получают от него свои IP-параметры во время загрузки. Когда DHCP-сервер недоступен, клиенты автоматически получают альтернативную конфигурацию или адрес APIPA.

Настройка базового DHCP-сервера включает установку, авторизацию, настройку областей, исключений, резервирования и дополнительных параметров, активизацию областей и, наконец, проверку конфигурации.

Изучив материал этого занятия, вы сможете:

- *S* установить DHCP-сервер;
- *S* авторизовать DHCP-сервер;
- *S* создать и сконфигурировать диапазон адресов DHCP, включая границы адресов, исключения, резервирования и прочие параметры;
- *S* описать и реализовать правило 80/20 для серверов и диапазонов адресов DHCP;
- *S* активировать диапазон адресов;
- *S* настроить клиент для получения IP-адреса от DHCP-сервера;
- *S* применить команду ipconfig /renew для обновления аренды адреса на клиенте.

Продолжительность занятия — около 70 минут.

Преимущества протокола DHCP

При наличии в сети DHCP-сервера поддерживающие протокол DHCP клиенты автоматически получают IP-адреса и связанные с ними параметры при каждом запуске и подключении к сети. DHCP-сервер предоставляет конфигурацию обратившимся клиентам в форме аренды адреса.

Одно из основных преимуществ протокола DHCP заключается в том, что DHCP-серверы значительно сокращают время настройки компьютеров в сети. DHCP упрощает администрирование не только за счет предоставления клиентам IP-адресов, но и (при необходимости) адреса основного шлюза, адресов DNS- и WINS-серверов, а также других необходимых клиентам серверов. У DHCP есть еще одно преимущество: автоматическое назначение IP-адресов позволяет избежать ошибок конфигурирования, неизбежных при ручном определении параметров IP на каждом сетевом узле. В частности, DHCP предотвращает конфликты адресов, возникающие из-за ошибочного присвоения одинаковых IP-адресов двум сетевым узлам.

Установка службы DHCP-сервера

Перед установкой DHCP-сервера надо установить роль DHCP-сервера при помощи *Мастера компонентов Windows* (Windows Component Wizard) или в окне **Управление данным сервером (Manage Your Server).**

Чтобы установить роль DHCP-сервера из окна управления сервером, в меню **Пуск (Start)** выберите **Управление данным сервером (Manage Your Server),** щелкните **Добавить или удалить роль (Add or Remove a Role).** Далее в окне мастера выберите роль **DHCP-сервер (DHCP Server)** и два раза щелкните **Далее** (Next).

Чтобы запустить *Мастер компонентов Windows,* откройте *Панель управления* (Control Panel) и дважды щелкните значок **Add or Remove Programs (Добавление или удаление программ). В** открывшемся окне **Установка и удаление программ (Add or Remove Programs)** выберите **Установка компонентов Windows (Add/Remove Windows Components).** DHCP, как и DNS, является подкомпонентом компонента **Сетевые службы (Networking Services).**

Примечание Для установки и настройки компонентов Windows (в их числе DHCP), необходимо войти в систему под административной учетной записью, например члена локальной доменной группы безопасности *Администраторы DHCP* (DHCP Administrators) или глобальной группы *Администраторы домена* (Domain Admins).

Совет Компьютеру, на котором устанавливается сервер DHCP, назначьте статический IP-адрес.

По завершении работы мастера установки откройте консоль *DHCP* и убедитесь, что DHCP-сервер успешно установлен на компьютере. Чтобы открыть панель управления DHCP, щелкните **Пуск (Start)**/Администрирование (Administrative Toois)/DHCP.

Консоль *DHCP* (рис. 7-1) представляет собой интерфейс настройки и управления практически всех параметров DHCP-сервера, в том числе областей, исключений, резервирования и др.

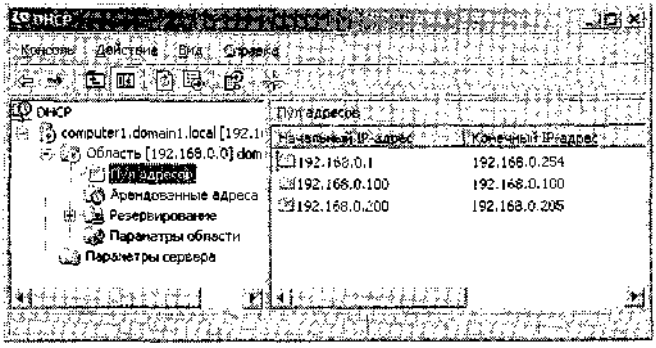


Рис. 7-1. Консоль *DHCP*

Авторизация сервера

DHCP-серверы, подлежащие интеграции с Active Directory, должны обязательно проходить авторизацию. В Active Directory могут состоять только контроллеры и члены домена, поэтому только такие серверы авторизуются в службе каталогов. Если в сети есть домены Active Directory, первый устанавливаемый DHCP-сервер должен быть авторизованным.

Авторизация в сетях Active Directory автономных или входящих в рабочую группу DHCP-серверов под управлением Windows 2000 Server или Windows Server 2003 невозможна, но они могут сосуществовать с такими сетями (хотя такая конфигурация не рекомендуется) при условии, что не развертываются в подсетях с авторизованными DHCP-серверам.

Автономные DHCP-серверы, работающие совместно с авторизованными серверами называются *ложными* (rogue servers). Обнаружив в своей подсети авторизованный сервер, ложный DHCP-сервер под управлением Windows Server 2003 или Windows 2000 Server автоматически отключает свою службу DHCP и прекращает предоставление клиентам IP-адресов.

Авторизовать DHCP-сервер, установленный на контроллере домена, просто: достаточно щелкнуть значок сервера в консоли *DHCP* правой кнопкой и выбрать **Авторизовать (Authorize).** Точно так же выполняется процедура авторизации на членах домена.

Внимание! DHCP-сервер можно устанавливать на контроллере домена, но это не рекомендуется по причинам, обсуждаемым в разделе «Вопросы безопасности».

Примечание Право предоставления или отмены авторизации DHCP-сервера предоставлено членам глобальной группы *Администраторы предприятия* (Enterprise Admins).

Авторизация DHCP-сервера в Active Directory выполняется так.

1. В дереве консоли *DHCP* выберите узел **DHCP.**
2. В меню **Действие (Action)** выберите **Список авторизованных серверов (Manage Authorized Servers).**
3. В окне **Управление авторизованными серверами (Manage Authorized Servers)** щелкните кнопку **Авторизовать (Authorize).**
4. В текстовом поле ведите имя или IP-адрес авторизуемого DHCP-сервера и щелкните OK.
5. В окне **Подтверждение авторизации (Confirm Authorization)** снова щелкните OK. В окне **Управление авторизованными серверами** щелкните кнопку **Закрыть (Close),** чтобы вернуться в консоль **DHCP.**

Настройка областей

Область DHCP (DHCP scope) представляет собой совокупность IP-адресов (например адреса из диапазона 192.168.0.11—192.168.0.254) логической подсети, которые DHCP-сервер присваивает клиентам. Помимо IP-адресов в областях определяют любые другие IP-параметры сетевых клиентов.

Подготовка к экзамену DHCP-серверу следует назначать адрес в соответствии с областью адресов, которой он управляет. Например, если область задана как 192.168.1.0/24, интерфейсу сервера в этом сегменте надо назначить статический адрес из этого диапазона.

Передаваемый DHCP-клиенту IP-адрес из определенной области называется *арендой* (lease). При передаче клиенту аренда становится активной. Адрес клиенту передается не навсегда, и клиент должен периодически обновлять аренду. По умолчанию продолжительность аренды составляет 8 дней.

Аренда обновляется в нескольких случаях. Прежде всего клиент автоматически обновляет аренду по истечении половины ее срока, а также при перезапуске. Обычно при перезагрузке DHCP-клиента он получает в аренду свой «старый» IP-адрес. Наконец, на DHCP-клиенте аренда обновляется командой Ipconfig /renew.

Область DHCP задается при помощи *Мастера создания области* (New Scope Wizard), который запускается так: щелкните значок DHCP-сервера в консоли *DHCP* правой кнопкой и выберите **Действие (Астлоп)\Создать область (New Scope).**

Ниже перечислены страницы *Мастера создания области,* на которых настраиваются свойства областей.

- **Имя области (Scope Name)** — определение имени области.
- **Диапазон адресов (IP Address Range)** — здесь указываются начальный и конечный IP-адреса, определяющие границы области, а также назначается маска подсети.
- **Добавление исключений (Add Exclusions)** — определение IP-адресов, исключаемых из заданного диапазона.
- **Срок действия аренды адреса (Lease Duration)** — настраивается продолжительность аренды, сведения о ней передаются DHCP-клиентам при предоставлении аренды.

- **Настройка параметров DHCP (Configure DHCP Option)** — на этой странице предлагается два варианта: продолжить настраивать дополнительные параметры DHCP-области в мастере либо сделать это позже в консоли *DHCP*.

  Внимание! Если вы решите продолжить настройку конфигурации позже, мастер не предоставит возможности активировать область — это придется сделать вручную. Только после этого сервер начнет предоставлять в аренду адреса из этой области.

- **Маршрутизатор (основной шлюз) [Router (Default Gateway)]** (дополнительная страница) — определение основного шлюза (и дополнительных шлюзов), назначаемого DHCP-клиенту.
- **Имя домена и DNS-серверы (Domain Name And DNS Servers)** (дополнительная страница) — имя домена и адреса DNS-серверов, которые назначаются клиентскому компьютеру.
- **WINS-серверы (WINS Servers)** — адреса WINS-серверов в предоставляемой клиенту конфигурации. Клиентам WINS-серверы нужны для разрешения NetBIOS-имен в IP-адреса.
- **Активировать область (Activate Scope)** (дополнительная страница) — здесь предоставляется возможность активировать диапазон сразу по завершении мастера.

  Описанные свойства можно изменить позже при помощи консоли *DHCP*.

Диапазон IP-адресов

Определяемый диапазон IP-адресов должен состоять из последовательных адресов, составляющих подсеть, в которой планируется развернуть службу DHCP. Вместе с тем из диапазона надо исключить адреса всех компьютеров сети, которым назначены статические адреса. Можно ограничить диапазон области так, чтобы статические адреса в него не входили. Есть .и другой способ: сконфигурировать область, охватывающую целую подсеть, а затем определить *диапазоны исключений* (exclusion ranges), содержащие исключаемые статические адреса.

Самый популярный метод одновременной поддержки в диапазоне статических и динамических адресов — зарезервировать первые 10 адресов подсети для серверов со статическими адресами, а DHCP-область начать с 11-го адреса. Например, в подсети 192.168.1.0 зарезервировать адреса 192.168.1.1-192.168.1.10 для серверов с неизменными адресами (DHCP-сервер, DNS-сервер, WINS-сервер и др.), а диапазон 192.168.1.11—192.168.1.254 назначить DHCP-области подсети (впрочем, с таким же успехом можно зарезервировать первые 20 адресов).

Если серверам сети уже назначены статические адреса из диапазона подсети, например 192.168.1.110 или 192.168.1.46, рекомендуется использовать диапазоны исключений, чтобы эти адреса не назначались другим компьютерам. Иначе придется сильно ограничить количество адресов для аренды, так как в подсети разрешается только один диапазон IP-адресов области.

Диапазоны исключения

Диапазон исключения (exclusion range) — это совокупность одного или нескольких IP-адресов из диапазона области, которые не должны предоставляться в аренду DHCP-клиентам. На рис. 7-2 показаны два диапазона исключения новой области, один из которых содержит только один IP-адрес. Если эти адреса включить в диапазон исключений, сервер никогда не предоставит их DHCP-клиентам в аренду.

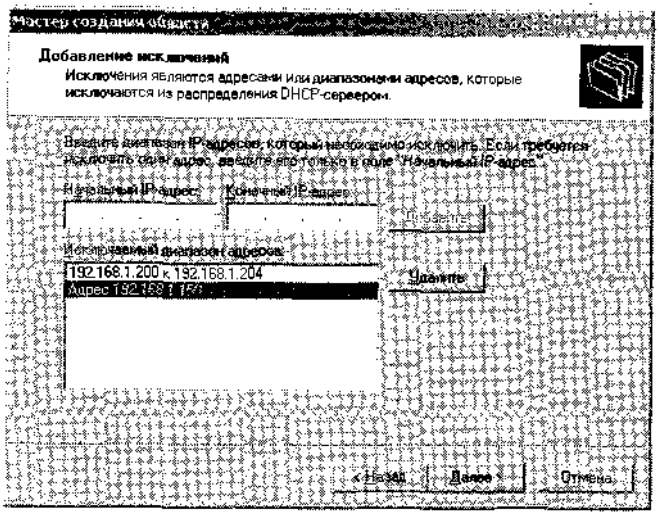


Рис. 7-2. Конфигурирование диапазона исключения

Диапазоны исключения можно использовать и на краях диапазонов. Например, определить область 192.168.1.1—192.168.1.254 с диапазоном исключения 192.168.1.1—192.168.1.10 (серверы подсети с настроенными вручную статическими IP-адресами).

Совет Windows Server 2003 требует назначать компьютерам со службой DHCP статические IP-адреса. Надо следить, чтобы эти IP-адреса не входили в диапазон области либо исключались из него.

После определения DHCP-области и указания диапазонов исключения, оставшиеся адреса составляют совокупность доступных адресов данной области, или *пул адресов* (address pool), которые сервер динамически назначает DHCP-клиентам.

Использование правила 80/20 для серверов и областей

Чтобы обеспечить отказоустойчивость службы DHCP в рамках конкретной подсети можно настроить два DHCP-сервера на обслуживание адресов одной подсети. В этом случае, если один сервер недоступен, предоставление новых адресов или обновление существующих адресов полностью берет на себя другой.

Для балансировки нагрузки между DHCP-серверами в подобной ситуации применяют проверенное на практике правило разделения адресов области между двумя серверами в соотношении 80/20. Например, если сервер Serverl настроить на обслуживание большей части (примерно 80%) адресов, арендой остальных адресов (20%) будет заниматься Server2.

Допустим, в обычной подсети с адресом 198.168.1.0, первые 10 адресов резервируются для статических адресов, а для определенной в подсети DHCP-области назначен диапазон 192.168.1.11-192.168.1.254. Для реализации правила 80/20 на Serverl и Server2 в области определяется один диапазон адресов, а исключения настраиваются по-разному. На Serverl диапазоном исключений являются 20% адресов конца диапазона, т. е. 192.168.1.205—192.168.1.254; таким образом, Serverl будет предоставлять в аренду адреса первые 80% адресов диапазона. На Server2 в диапазон исключений попадают начальные 80% адресов, т. е. 192.168.1.11—192.168.1.204. Server2 выделяет в аренду адреса из последних 20% диапазона области (рис. 7-3).

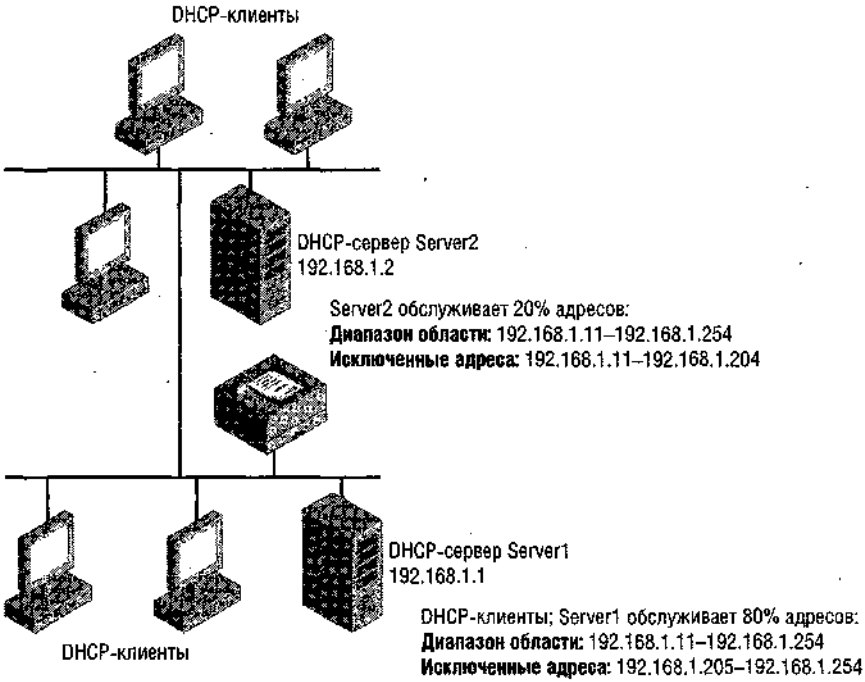


Рис. 7-3. Правило 80/20 в DHCP-подсетях

Создание резервирования

Резервирование (reservation) используется для создания постоянной аренды адреса, выделенного DHCP-сервером. Таким образом обеспечивается назначение неизменного адреса определенным устройствам в подсети. Например, в DHCP-области с диапазоном 192.168.1.11-192.168.1.254 можно зарезервировать IP-адрес 192.168.1.100 за сетевым адаптером с аппаратным адресом 00-bO-dO-01-18-86. При каждой перезагрузке компьютера с этим адаптером сервер распознает аппаратный MAC-адрес адаптера и предоставляет ему в аренду один и тот же IP-адрес — 192.168.1.100.

Чтобы создать резервирование в консоли *DHCP,* откройте нужную область, щелкните узел **Резервирование (Reservations)** правой кнопкой и выберите **Создать резервирование (New Reservations).** Откроется диалоговое окно **Создать резервирование (New Reservation)** (рис. 7-4). Настройте резервирование, указав нужные значения в полях **Имя клиента (Reservation name), IP-адрес (IP address)** и **MAC-адрес (MAC address).**

Резервирование не взаимозаменяемо со статической настройкой адреса. Некоторым компьютерам, в том числе DNS- или DHCP-серверу, нужно назначать IP-адреса вручную, а не автоматически средствами DHCP.

Однако резервирование вполне годится, если нужно присвоить конкретный адрес обыкновенному компьютеру. Этот метод позволяет закрепить адрес, сохранив другие преимущества DHCP: централизованное управление, предотвращение конфликтов адресов и назначение параметров области. Например, может оказаться, что определить конкретную IP-конфигурацию на сервере печати проще через централизованное резервирование, а не настройкой вручную на сервере. Наконец, нужно помнить, что резервирование возможно только для DHCP-клиентов. Иначе говоря, DHCP-сервер поддерживает резервирование арендованного адреса только за клиентами, настроенными на автоматическое получение IP-адреса.

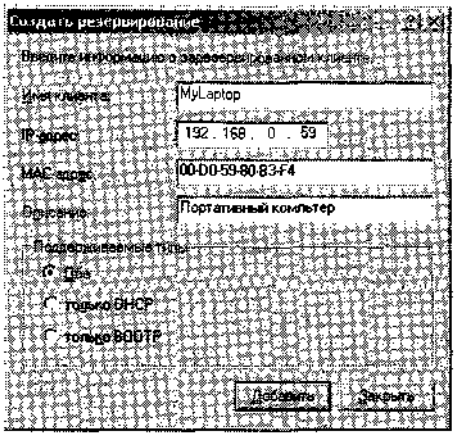


Рис. 7-4. Окно *Создать резервирование*

Подготовка к экзамену Будьте готовы к вопросам с ситуациями, в которых конкретный адрес одновременно резервируется и исключается. В таких случаях резервирование не работает.

Присвоение параметров DHCP

DHCP позволяет одновременно с выделением адреса в аренду предоставлять клиентам дополнительные конфигурационные данные, например адреса определенных серверов. В частности, клиентский компьютер, на котором в свойствах протокола TCP/IP задано автоматическое получение адреса DNS-сервера, берет этот адрес (или набор таких адресов) у DHCP-сервера.

Конфигурационные параметры настраиваются на уровне резервирования, области или сервера. Параметры уровня резервирования обладают наивысшим приоритетом, а параметры области предпочтительнее параметров сервера.

Чтобы настроить параметры для резервирования, выберите значок нужного резервирования в дереве консоли *DHCP,* а затем в меню **Действие (Action)** или в контекстном меню выберите команду **Настроить параметры (Configure Options).** Чтобы настроить параметры для области [по завершении *Мастера создания области* (New Scope Wizard)], выберите в дереве консоли *DHCP* папку **Параметры области (Scope Options),** а затем в меню **Действие** или в контекстном меню выберите команду **Настроить параметры** (рис. 7-5). Аналогично настраиваются параметры на сервере. Диалоговое окно, которое открывается при каждой из этих процедур, практически одинаково во всех трех случаях.

Доступно более 60 стандартных параметров DHCP, а наиболее часто используемые перечислены ниже.

- **003 Маршрутизатор (003 Router)** — список IP-адресов предпочтительных маршрутизаторов в одной с DHCP-клиентами подсети. Клиент отправляет этим маршрутизаторам IP-пакеты, адресованные удаленным узлам сети.
- **006 DNS-серверы (006 DNS Servers)** — IP-адреса DNS-серверов, к которым могут обращаться DHCP-клиенты с запросами на разрешение доменных имен узлов.
- **015 DNS-имя домена (015 DNS Domain Name)** — доменное имя, которое используется DHCP-клиентами в процессе разрешения неполных DNS.-имен. Этот параметр также позволяет клиентам осуществлять динамическое обновление в DNS.

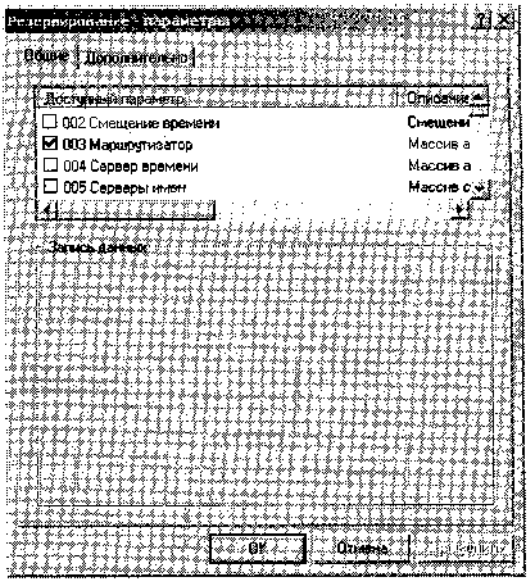


Рис. 7-5. Настройка параметров DHCP

- **044 WINS/NBNS-серверы (044 WINS/NBNS Servers)** — IP-адреса основного и дополнительного WINS-серверов.

в 046 Тип узла WINS/NBT (046 WINS/NBT Node Type) — предпочтительный метод разрешения NetBIOS-имен на DHCP-клиентах, например, узел Ь-типа (0x1) только для широковещательного метода либо узел h-типа (0x8) для смешанного использования методов «точка — точка» и широковещания.

- **051 Аренда (051 Lease)** — параметр, определяющий особый срок аренды; применяется только для удаленных клиентов. При определении этого параметра используются сведения об объявленном клиентом классе пользователя. (Подробнее о классах пользователей — в занятии 2.)

Активирование области

После определения и настройки область надо *активировать* (activate) — только после этого DHCP-сервер сможет приступить выделять из этой области адреса в аренду. Однако нельзя активировать новую область, пока в ней не определены параметры DHCP.

- **Активирование области**

1. **В** дереве консоли *DHCP* выберите нужную область.
2. В меню **Действие (Action)** выберите **Активировать (Activate).**

Примечание После активирования выбранной области вместо команды **Активировать** в меню **Действие** появляется команда **Деактивировать (Deactivate). В** производственной среде не стоит деактивировать область, если только не предполагается полностью прекратить ее использование.

Подготовка к экзамену Будьте готовы к вопросам с ситуациями, в которых DHCP не работает потому, что область не активирована либо сервер не авторизован.

Настройка клиента

Чтобы настроить клиент на получение IP-адреса от DHCP-сервера, откройте диалоговое окно **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties]** для соответствующего сетевого подключения. При выборе варианта **Получить IP-адрес автоматически (Obtain an IP address automatically)** клиент получает от DHCP-сервера IP-адрес, маску подсети и все параметры DHCP, кроме параметров DNS. Чтобы настроить клиент на получение параметров DNS с DHCP-сервера, нужно выбрать в том же окне вариант **Получить адрес DNS-сервера автоматически (Obtain DNS Server address automatically).** Если клиент до этого имел статический адрес, новая конфигурация вступает в силу сразу после закрытия открытых диалоговых окон.

Перенастройка клиентов с APIPA-адресами или альтернативной конфигурацией

Если клиент уже настроен на автоматическое получение IP-адреса и адреса DNS-сервера и в сети *не используется* служба ICS, то для получения новых IP-параметров от DHCP-сервера нужно обновить IP-конфигурацию командой ipconfig /renew или просто перезагрузить клиентский компьютер.

Перенастройка после iCS-подключения

ICS-подключение — это совместно используемое удаленное подключение на сервере, которое обеспечивает клиентам сети доступ в Интернет и автоматически присваивает клиентским компьютерам адреса из диапазона 192.168.0.x. Поскольку ICS конкурирует со службой DHCP-сервера, нужно сначала удалить любые совместно используемые ICS-подключения удаленного доступа на сервере и лишь затем устанавливать DHCP-компонент Windows или добавлять роль DHCP-сервера.

Перенастройка ICS-клиентов

ICS-клиенты уже настроены на автоматическое получение IP-адреса, поэтому теоретически они не требуют дополнительной перенастройки после перехода в DHCP-среду помимо простой перезагрузки. Однако на практике оказывается, что ICS-клиенты упрямо держатся за свои ICS-адреса даже после развертывания DHCP. Чтобы предотвратить подобные неприятности, можно после удаления ICS-подключения присвоить клиентскому компьютеру статический адрес (эта процедура разорвет ICS-подключение), а затем перезагрузить клиентский компьютер. После перезагрузки переход клиентов «на рельсы» DHCP проходит гладко — сразу после настройки на автоматическое получение адреса.

После установки и настройки DHCP-сервера новую автоматическую конфигурацию к бывшему ICS-клиенту применяют, как и к любому другому клиенту, имевшему ранее статический адрес: в диалоговом окне **Свойства: Протокол Интернета (TCP/IP) [Internet**

Protocol (TCP/IP) Properties] установите переключатель **Получить IP-адрес автоматически (Obtain An IP Address Automatically)** и при необходимости — **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically).**

Проверка конфигурации

После настройки и авторизации DHCP-сервера и активирования области нужно проверить работу службы на всех клиентских компьютерах. Перезагрузите компьютеры, DHCP-клиенты, (или воспользуйтесь командой Ipconfig /renew), а затем в командной строке выполните команду Ipconfig /all. Параметр /all заставляет утилиту Ipconf ig отобразить все параметры арендуемых адресов, включая и параметры DHCP.

Совет Если надо разрешить пользователям чтение информации о DHCP без права управления или изменения, можно включить их в локальную доменную группу безопасности *Пользователи DHCP* (DHCP Users).

Лабораторная работа. **Установка и настройка DHCP-сервера**

Вы установите и настроите новый DHCP-сервер. Поскольку в конфигурациях из двух компьютеров часто применяется служба ICS, в которой есть своя версия DHCP, вам вначале придется удалить общее подключение удаленного доступа и перезагрузить оба компьютера, и лишь затем продолжить установку DHCP-сервера. Это позволит предотвратить конфликт между двумя службами.

Внимание! Здесь предполагается, что служба ICS развернута для подключений по телефонной линии. Если же у вас другой тип подключения к Интернету, надо будет внести соответствующие изменения в процесс развертывания DHCP-сервера.

Упражнение 1. Удаление ICS-подключений

В ICS есть собственная служба адресации, несовместимая с адресацией DHCP-сервера. В этом упражнении вы удалите ICS-подключение, чтобы подготовить установку DHCP-сервера.

1. С Computerl войдите в *Domainl как Администратор* (Administrator).
2. Откройте папку **Сетевые подключения (Network Connections)** и отключите подключение **MylSP,** если оно активно.
3. Правой кнопкой щелкните значок **MylSP** и в контекстном меню выберите команду **Удалить (Delete). В** окне **Подтверждение удаления подключения (Confirm Connection Delete)** щелкните Да (Yes).
4. Перезапустите Computerl.
5. Перейдите к Computer2 и войдите в *Domainl* как *Администратор.*
6. Откройте окно командной строки и выполните команду

   ```
   netsh interface ip set address local static 192.168.0.2 255.255.255.0
   ```

   Она присвоит *Подключению по локальной сети* (Local Area Connection) статический адрес 192.168.0.2/24.

7. Затем выполните следующую команду:

   ```
   netsh interface ip set dns local static 192.168.0.1
   ```

   которая назначит адрес основного DNS-сервера в подключении по локальной сети — 192.168.0.1. Статический адрес и основной DNS-сервер нужны временно, до конфигурирования нового DHGP-сервера. Этот делается только для беспроблемного перехода от ICS к DHCP.
8. После выполнения команды перезагрузите Computer2.

Упражнение 2. Добавление роли DHCP-сервера

Вы добавите роль DHCP-сервера на Computerl. В ходе упражнения вы настроите и активируете новую область, а затем авторизуете новый DHCP-сервер. Перед началом упражнения вставьте в дисковод Computerl установочный компакт-диск Windows Server 2003.

1. С Computerl войдите в *Domainl как Администратор* (Administrator).
2. В командной строке выполните следующую команду:

   ```
   netsh interface ip set address local static 192.168.0.1 255.255.255.0
   ```

   Она присваивает указанный статический адрес подключению по локальной сети. Даже если Computerl изначально имел статический адрес, служба ICS переопределяет этот параметр, заменяя его динамическим адресом 192.168.0.1. А DHCP-серверу, как и другим критически важным серверам сети, обычно присваивают статические адреса.
3. В меню **Пуск (Start)** выберите **Администрирование (Administrative Too18)\Управление данным сервером (Manage Your Server),** чтобы открыть одноименное окно.
4. Щелкните **Добавить или удалить роль (Add or Remove a Role).** Откроется окно **Мастер настройки сервера (Configure Your Server Wizard).**
5. На странице **Предварительные шаги (Preliminary Steps)** щелкните **Далее** (Next).
6. На странице **Роль сервера (Server Role)** в списке **Роль сервера (Server Role)** выберите **DHCP-сервер (DHCP Server)** и щелкните **Далее.**
7. На странице **Сводка выбранных параметров (Summary Of Selections)** щелкните **Далее.** Откроется страница **Применение выбранных параметров (Configuring Components)** и начнется процесс установки DHCP-сервера.
8. По завершении установки DHCP-сервера откроется окно **Мастер создания области (New Scope Wizard).** На первой странице мастера щелкните **Далее.**
9. На странице **Имя области (Scope Name)** в поле **Имя (Name)** введите Test Scope.
10. Оставьте пустым текстовое поле **Описание (Description)** и щелкните **Далее.** Появится страница **Диапазон адресов (IP Address Range).**
11. На странице **Диапазон адресов (IP Address Range)** в поле **Начальный IP-адрес (Start IP Address)** введите 192.168.0.11, и в поле **Конечный IP-адрес (End IP Address)** — 192.168.0. 254. Убедитесь, что в поле маски подсети указано значение 255.255.255.0 и щелкните **Далее.**
12. На странице **Добавление исключений (Add Exclusions)** в поле **Начальный IP-адрес (Start IP Address)** введите 192. 168.0.100 и щелкните кнопку **Добавить (Add).** Адрес переместится в зону **Исключаемый диапазон адресов (Excluded Address Range).**

13. В текстовом поле **Начальный IP-адрес (Start IP Address)** введите 192.168. 0. 200, в текстовом поле **Конечный IP-адрес (End IP Address)** задайте 192.168.0. 205 и щелкните **Добавить. В** зоне **Исключаемый диапазон адресов (Excluded Address Range)** добавляется новый диапазон IP-адресов. Щелкните **Далее.**
14. На странице **Срок действия аренды адреса (Lease Duration)** ознакомьтесь с текстом и щелкните **Далее** (Next), принимая значение по умолчанию, равное 8 дням.
15. На странице **Настройка параметров DHCP (Configure DHCP Options)** щелкните Далее, принимая значение по умолчанию — **Да** (Yes).
16. На странице **Маршрутизатор (Основной шлюз) [Router(Default Gateway)]** в текстовом поле **IP-адрес (IP Address)** введите 192.168. 0.1 и щелкните **Добавить (Add).** Адрес переместится в нижнее окно. Щелкните **Далее.**
17. На странице **Имя домена и DNS-серверы (Domain Name And DNS Severs)** в поле **Родительский домен (Parent Domain)** введите domainl.local. В поле **IP-адрес (IP Address)** укажите 192.168.0.1 и щелкните **Добавить (Add).** Щелкните **Далее.**
18. На странице **WINS-серверы (WINS Servers)** щелкните **Далее.**
19. На странице **Активировать область (Activate Scope)** щелкните **Далее,** приняв вариант по умолчанию.
20. На странице **Завершение мастера создания области (Completing The New Scope Wizard)** щелкните **Готово (Finish). Мастер настройки сервера** сообщает, что на сервере настроена служба DHCP-сервером.
21. В окне **Мастер настройки сервера (Configure Your Server Wizard)** щелкните **Готово (Finish).**
22. Откройте консоль *DHCP,* в меню **Пуск (Start)** выбрав **Администрирование (Administrative Tools)\DHCP.**
23. **В** дереве консоли *DHCP* раскройте узел **Computerl.domainl.local.** Здесь расположены две вложенные папки: **Область (Scope)** и **Параметры сервера (Server Options).** Узел сервера отмечен направленной вниз красной стрелкой, информирующей, что DHCP-сервер пока не авторизован.
24. Щелкните значок сервера правой кнопкой и выберите **Авторизовать (Authorize).**
25. Нажмите F5, чтобы обновить содержимое консоли. Вместо красной стрелки появилась направленная вверх зеленая стрелка — сервер авторизован, (При необходимости повторите п. 24, пока не появится зеленая стрелка.)
26. Закройте консоль *DHCP.*

Упражнение 3. Настройка DHCP-клиента

Вы настроите Computer2 на автоматическое получение адреса. Это позволит компьютеру получить в аренду адрес у только что настроенного DHCP-сервера.

1. На Computerl, находясь в сеансе *Администратор* (Administrator) в домене *Domain 1,* откройте консоль *DNS.*
2. Удалите любые записи ресурсов типов A и PTR для Computer2 в зонах подсетей *domain I. local к* 192.168.0.x. Это обеспечит корректное создание и обновление записей новой области DHCP в DNS.
3. Закройте консоль *DNS.*
4. Перейдите к Computer2 и войдите в *Domainl* как *Администратор* (Administrator).

5. Откройте окно **Local Area Connection - свойства (Local Area Connection Properties),** а затем — окно **Свойства: Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP) Properties].**
6. На вкладке **Общие (General)** установите переключатели: **Получить IP-адрес автоматически (Obtain an IP Address Automatically)** и **Получить адрес DNS-сервера автоматически (Obtain DNS Server Address Automatically).** Щелкните OK.
7. В диалоговом окне **Local Area Connection — свойства (Local Area Connection Properties)** щелкните **Закрыть (Close).** При закрытии окна новая конфигурация вступает в действие.
8. В командной строке выполните команду ipconfig /registerdns.-

Упражнение 4. Проверка конфигурации

Вы проверите настройку клиента и сервера.

1. С Computer2 войдите в *Domain 1* как *Администратор* (Administrator).
2. В окне командной строки выполните команду Ipconf ig /a11. Утилита вернет сведения о новой IP-конфигурации, полученной от DHCP-сервера, в том числе IP-адрес 192.168.0.11. Параметры **Основной шлюз (Default Gateway), DHCP-сервер (DHCP Server)** и **DNS-сервер (DNS Server)** все установлены равными 192.168.0.1.
3. Перейдите к Computet!.
4. Войдите в систему Computerl как *Администратор.*
5. В дереве консоли *DHCP* раскройте узел **Область (Scope)** и выберите папку **Арендованные адреса (Address Leases).**
6. Щелкните папку **Арендованные адреса (Address Leases)** правой кнопкой и выберите **Обновить (Refresh).** Сколько активных арендованных адресов теперь отображается в правой панели консоли *DHCP1* Какому компьютеру присвоен адрес?
7. Закройте консоль *DHCP.*
8. Откройте консоль *DNS* и убедитесь, что для Computer2 создана новая запись ресурса A.
9. Выйдите из системы на обоих компьютерах.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы настроили область с диапазоном адресов 192.168.0.11-192.168.0.254. Однако DNS-серверу в той же подсети уже присвоен статический адрес 192.168.0.200. Как проще всего обеспечить совместимость адреса DNS-сервера и службы DHCP в данной подсети?
2. Какой из перечисленных серверов должен стать первым DHCP-сервером в сети? (Выберите все подходящие варианты.)
   a. Контроллер домена Windows Server 2003 в сети с Active Directory.
   b. Сервер рабочей группы Windows Server 2003 в сети, где нет доменов.
   c. Сервер рабочей группы Windows Server 2003 в сети с Active Directory.
   d. Рядовой сервер Windows 2000 Server в сети с Active Directory.

3. DHCP-область настроена с параметром *003 Маршрутизатор* (003 Router), который определяет адрес основного шлюза на клиентах. Однако после выполнения команды Ipconfig /all на клиенте Clientl обнаруживается, что клиент получает IP-адрес из назначенной области, но ему не назначается адрес основного шлюза. Какая самый вероятная причина неполадки?
   a. Clientl отключился от сети.
   b. IP-адрес для Clientl предоставлен в рамках резервирования.
   c. На уровне сервера не определены параметры области.
   d. Область не активирована.
4. Назовите две группы безопасности, кроме *Администраторы* (Administrators), которым предоставлено право управления DHCP-серверами.
5. В процессе работы *Мастера создания области* (New Scope Wizard) вы отказались от настройки каких-либо параметров DHCP. Впоследствии обнаруживается, что DHCP-сервер не присваивает адреса в заданной области. Какова наиболее вероятная причина неполадки?

Резюме

и При наличии работоспособного DHCP-сервера компьютеры, настроенные на автоматическое получение IP-адреса, при загрузке запрашивают и получают IP-параметры от DHCP-сервера.

в В сетях с Active Directory DHCP-серверы должны обязательно проходить авторизацию.

- Область DHCP — это непрерывный диапазон IP-адресов, определенных в единой логической подсети, которые DHCP-сервер предоставляет клиентам. После определения и настройки области ее надо активировать — только после этого DHCP-сервер сможет обслуживать клиентов.
- Диапазон исключений — это набор из одного или нескольких IP-адресов в пределах диапазона заданной области, которые не предоставляются в аренду клиентам. Для постоянного выделения адреса в аренду применяется резервирование.
- Вместе с арендуемым адресом DHCP-сервер предоставляет клиентам другие параметры, в том числе адреса основного шлюза или DNS-сервера.

Занятие 2. **Управление DHCP в сетях Windows**

В среде предприятия управление службой DHCP требует выполнения множества задач — от изменения состояния DHCP-сервера до восстановления сервера и применения утилит командной строки для настройки DHCP-сервера по WAN-подключениям. Кроме того, в корпоративных сетях часто существуют самые разнообразные ограничения топологии и другие практические ограничения, требующие доработки службы DHCP в соответствии с ситуацией. Умелые администраторы должны уметь приспосабливать службу DHCP, обеспечивая работу DHCP через маршрутизаторы или настраивая ее для поддержки нескольких логических подсетей в едином физическом сетевом сегменте.

Изучив материал этого занятия, вы сможете:

- *S* запустить, остановить, перезапустить, приостановить и возобновить работу службы DHCP-сервера средствами консоли *DHCP,* командной строки и консоли *Службы* (Services);
- *S* отключать службу DHCP-сервера;
- *S* использовать контекст утилиты Net shell (Netsh) для администрирования службы DHCP-сервера;
- *S* определять суперобласти, делая службу DHCP доступной в нескольких логических подсетях одной физической сети;
- *S* изменить адресацию в сети с DHCP-сервером;
- *S* архивировать и восстанавливать базу данных DHCP-сервера;
- *S* вручную уплотнять базу данных DHCP-сервера;
- *S* использовать классы параметров для настройки определенных параметров в подмножествах DHCP-клиентов.

Продолжительность занятия — около 70 минут.

Изменение состояния DHCP-сервера

Для запуска и остановки службы DHCP-сервера существуют самые разные средства: консоль *DHCP,* утилиты командной строки и консоль *Службы.*

Консоль *DHCP*

При выборе значка сервера в консоли *DHCP* в подменю **Все задачи (All Tasks)** меню **Действие (Action)** отображаются команды управления сервером: **Запустить (Start), Остановить (Stop), Приостановить (Pause), Продолжить (Resume)** и **Перезапустить (Restart).** Это же подменю есть в контекстном меню, которое открывается щелчком правой кнопкой значка DHCP-сервера.

- **Запуск/остановка DHCP-сервера**

1. В дереве консоли *DHCP* выберите нужный DHCP-сервер.
2. В меню **Действие (Action)** перейдите к **Все задачи** (All Tasks) и выберите:
   - а для запуска службы — **Запустить (Start);**
   - для остановки службы — **Остановить (Stop);**
   - D для временного прерывания работы службы — **Приостановить (Pause);**
   - для возобновления работы после приостановки — **Продолжить (Pause);**
   - для остановки и последующего автоматического перезапуска — **Перезапустить (Restart).**

Использование утилиты командной строки

Запустить, остановить, приостановить и продолжить работу службы DNS-сервера также можно, выполняя соответствующие команды командной строки:

- запуск—Net Start Dhcpserver;
- остановка — Net Stop Dhcpserver;
- приостановка — Net Pause Dhcpserver;
- возобновление — Net Continue Dhcpserver.

Консоль *Службы*

Консоль *Службы* (Services) — средство администрирования с графическим интерфейсом, которое открывается в меню **Пуск (Start)** при выборе **Администрирование (Administrative Toos) \ Службы (Services).** Для управления службой DHCP-сервера нужно дважды щелкнуть узел DHCP-сервера в списке служб в правой панели. Откроется диалоговое окно **DHCP Server (Локальный компьютер) — свойства (DHCP Server Properties)** (рис. 7-6).

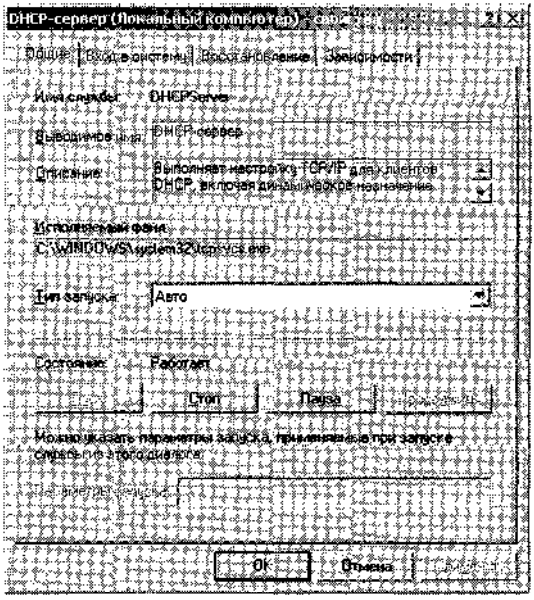


Рис. 7-6. Диалоговое окно *DHCP Server (Локальный компьютер) — свойства*

Консоль *Службы* дает дополнительные возможности помимо тех, что предоставляют консоль *DHCP* и утилиты командной строки. В поле со списком **Тип запуска (Startup Type)** доступен вариант **Отключено (Disabled),** при выборе которого служба вовсе не запускается. Это полезно, к примеру, когда нужно переместить базу данных DHCP на другой компьютер и надо быть уверенным, что старый сервер не запустится даже после перемещения.

Примечание Если в момент выбора параметра **Отключено (Disabled)** служба работает, то она отключится только после остановки и перезагрузки компьютера.

Управление DHCP средствами командной строки

В Windows Server 2003 есть командная среда Netshell (Netsh), позволяющая управлять работой и свойствами сервера. Для DHCP команды Netsh могут полностью заменить возможности управления, предоставляемые графическими консолями. Эта утилита полезна в следующих ситуациях.

- При управлении DHCP-сервером в глобальных сетях команды Netsh позволяют выполнять административные задачи через низкоскоростные сетевые подключения.

- При управлении большим количеством DHCP-серверов команды можно выполнять в пакетном режиме, чтобы автоматизировать повторяющиеся задачи по администрированию всех DHCP-серверов.

Чтобы войти в среду команды Netsh нужно просто выполнить эту команду в командной строке. На экране появится приглашение среды Netsh>. Для входа в контекст администрирования DHCP надо выполнить команду DHCP.

```
C:\>netsh
netsh>dhcp
netsh dhcp>
```

Примечание Не обязательно выполнять команды Netsh пошагово, например для просмотра итоговой конфигурации DHCP-сервера достаточно открыть командную строку и ввести одной строкой команду netsh dhcp server show all. Поэтапное перемещение по уровням позволяет на каждом уровне использовать команды Help, List или ?, которые дают список команд, доступных на текущем уровне.

Хотя контекст Netsh dhcp позволяет добавлять, удалять и выполнять мониторинг DHCP-серверов в сети, гораздо больше возможностей по управлению DHCP доступно в контексте Netsh dhcp server и Netsh dhcp server scope. Чтобы получить доступ в контекст Netsh dhcp server, нужно просто в контексте Netsh dhcp выполнить команду Server. Для доступа в контекст Netsh dhcp server scope введите в приглашении Netsh dhcp server> команду Scope *<1P-адрес области>*. Этот процесс проиллюстрирован ниже.

```
netsh>dhcp
netsh dhcp>server
netsh dhcp server>scope 192.168.0.0

Changed the current scope context to 192.168.0.0 scope,
netsh dhcp server scope>
```

В любом контексте доступны команды Help, List и ?, отображающие полный список доступных в данном контексте команд, а также информацию о порядке использования конкретной команды. Например, чтобы узнать о возможностях команды Set, в любом контексте Netsh выполните команду Set help.

Дополнительные сведения о Netsh есть также в справочной системе Windows Server 2003.

Примечание Чтобы управлять DHCP-сервером утилитой Netsh в командной строке, нужны полномочия члена локальной группы *Администраторы* (Administrators) или локальной группы *Администраторы DHCP* (DHCP Administrators) на компьютере сервера.

- **Интерактивное применение команд управления DHCP в командной строке**

1. Откройте окно командной строки.
2. Выполните netsh.
3. В приглашении Netsh> введите dhcp.

4. В приглашении Netsh dhcp> введите server <*имя_сервера*> или server <*IP-адрес сервера*>. Для управления локальным сервером просто выполните server.
5. Выйдя в нужный контекст, примените соответствующую команду среды Netshell для DHCP. Введите /? или help, чтобы отобразить меню подкоманды DHCP, либо введите list, чтобы отобразить список всех доступных подкоманд для управления DHCP.

Примечание Практические примеры использования утилиты Netsh есть в разделе «Практикум по устранению неполадок» этой и других глав.

Подключение клиентов к удаленным DHCP-серверам

Широковещательные DHCP-рассылки в сети позволяют клиентским компьютерам обнаруживать DHCP-серверы в локальной сети и получать IP-адреса от локального сервера. Однако по умолчанию маршрутизаторы не пропускают широковещательные пакеты в другие подсети. Поэтому если ничего не предпринять, придется в каждой физической подсети развертывать собственный DHCP-сервер, чтобы предоставить клиентам доступ к службе DHCP.

Но есть другие варианты: маршрутизаторы, поддерживающие спецификацию RFC 1542, которые настраиваются на пересылку широковещательных DHCP-сообщений, или *Агенты ретрансляции DHCP* (DHCP Relay Agents), которые обеспечивают перехват широковещательных DHCP-сообщений и доставку по сети на IP-адрес DHCP-сервера.

Перед пересылкой DHCP-сообщения на DHCP-сервер как маршрутизаторы с поддержкой RFC 1542, так и DHCP-агенты ретрансляции, вписывают собственный адрес в специальное поле (Giaddr) DHCP-сообщения. Эта информация указывает DHCP-серверу на идентификатор подсети, из которой исходит DHCP-запрос, и, соответственно, из какой области надо предоставлять адреса.

DHCP-агенты ретрансляции и маршрутизаторы, поддерживающие RFC 1542, подробно описаны в занятии 4 главы 9. О поле IP-адреса шлюза (Giaddr) — в занятии 3 главы 8.

Суперобласти

Суперобласть (superscope) — это группа областей, объединенная в единый объект администрирования, которая используется для поддержки *мультисетей,* то есть нескольких логических подсетей в едином логическом сегменте сети. Необходимость в мультисетях, как правило, возникает при росте числа узлов в физическом сегменте сети, превышающем емкость изначального адресного пространства. Создавая логически отделенную вторую область (например 207.46.150.0), чтобы добавить ее к начальной области (207.46.9.0), и, объединяя эти две области в единую суперобласть, можно удвоить адресное пространство физического сегмента сети. (В мультисетях для соединения логических подсетей также необходима маршрутизация.) Таким образом DHCP-сервер может предоставлять клиентам единой физической сети адреса нескольких областей.

Примечание Суперобласть содержит лишь список дочерних областей или областей-потомков, которые активируются совместно; в ней не настраиваются никакие другие параметры области.

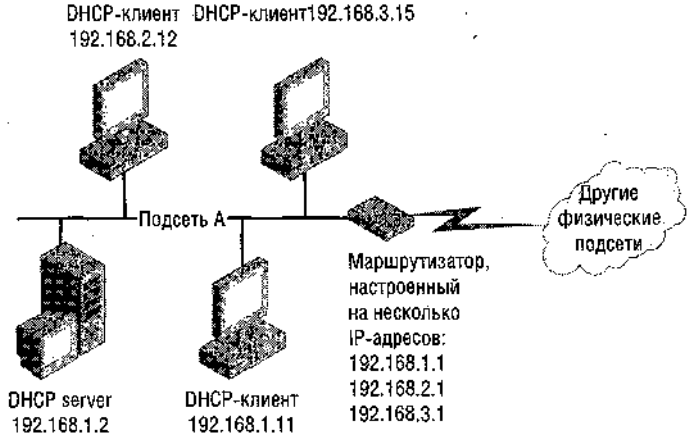
До суперобласти нужно создать обычную область. Лишь после этого создают суперобласть: щелкните значок DHCP-сервера в дереве консоли *DHCP* правой кнопкой и выберите **Создать суперобласть (New Superscope).** Начинает работу **Мастер создания суперобласти (New Superscope Wizard),** в котором нужно выбрать добавляемые область/области. Новые области также можно добавить в суперобласть позже.

Конфигурации суперобласти в мультисетях

В этом разделе рассказывается, как простую сеть, состоящую из одного физического сегмента сети и одного DHCP-сервера, можно с применением суперобластей преобразовать для поддержки мультисетевых конфигураций.

Суперобласть с локальными мультисетями

Рис. 7-7 иллюстрирует создание мультисетей в едином физическом сегменте сети (подсеть А) с одним DHCP-сервером.



Суперобласть с входящими в нее областями:
Область Scope 1:192.168.1.1 -192.168.1.254
Область Scope 2:192.168.2.1 -192.168.2.254
Область Scope 3:192.168.3.1 -192.168.3.254

Маска подсети у всех областей: 255.255.255.0

Рис. 7-7. Создание мультисетевой конфигурации в одном сегменте сети

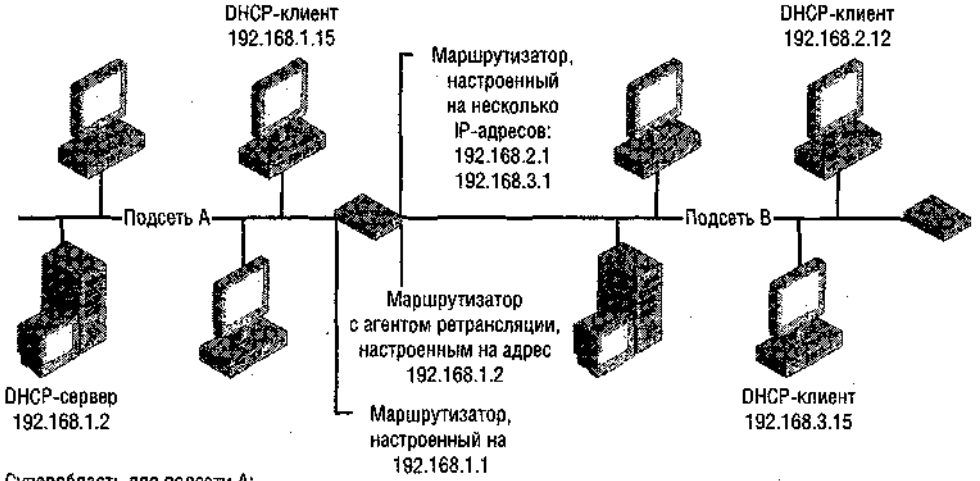
В этом варианте можно настроить суперобласть, содержащую все адреса исходной области (Scope 1) и дополнительных областей для поддерживаемых логических мультисетей (Scope2 и Scope3).

Примечание При использовании двух логических подсетей в одном физическом сегменте нужен маршрутизатор, который будет переправлять трафик между подсетями.

Суперобласть с удаленными мультисетями

На рис. 7-8 показана конфигурация, используемая для поддержки мультисетей в физической сети, отделенной от DHCP-сервера. В этом варианте суперобласть, определяемая на DHCP-сервере, включает две мультисети в удаленном сегменте, отделенном маршрутизатором. Поскольку обычно трафик DHCP ограничен локальной подсе-

тью, то для поддержки клиентов в удаленном сегменте используется DHCP-агент ретрансляции.



Суперобласть для подсети A:
Область Scope 1: 192.168.1.1 - 192.168.1.254
Маска подсети: 255.255.255.0

В суперобласть добавлены дочерние области подсети B:
Область Scope 2: 192.168.2.1 - 192.168.2.254
Область Scope 3: 192.168.3.1 - 192.168.3.254
Маска подсети: 255.255.255.0

Рис. 7-8. Маршрутизация в мультисетях

Суперобласть с поддержкой двух локальных DHCP-серверов

В отсутствие суперобластей наличие двух DHCP-серверов, предоставляющих в аренду адреса в одном сегменте, будет вызывать конфликты адресов (рис. 7-9).

В такой сети DHCP-сервер A управляет областью адресов, отличной от управляемой DHCP-сервером B, и ни один из них не имеет информации об адресах, управляемых другим. Проблемы возникают, когда клиент, которого до этого обслуживал сервер A, освобождает свое имя при выключении, а затем опять подключается к сети.

После перезагрузки клиент A пытается обновить аренду адреса. Однако, если сервер B ответит на запрос клиента A раньше сервера A, сервер откажется возобновлять аренду неизвестного ему адреса и отправит сообщение-отказ NACK. В результате клиент A потеряет старый адрес и будет вынужден искать новый. В процессе получения нового адреса клиент A может получить адрес, который поместит его в неправильную логическую подсеть.

На рис. 7-10 показано, как, используя суперобласти на обоих DHCP-серверах, можно избежать подобных проблем и управлять обеими областями предсказуемым и эффективным образом. В данном варианте оба сервера продолжают оставаться в одной физической подсети. Суперобласть, определяемая как на сервере A, так и на сервере B включает в качестве членов обе области, определенные в физической подсети. Чтобы предотвратить выдачу серверами адресов из чужой области, на каждом сервере полностью исключаются все адреса области, относящейся к другому серверу.

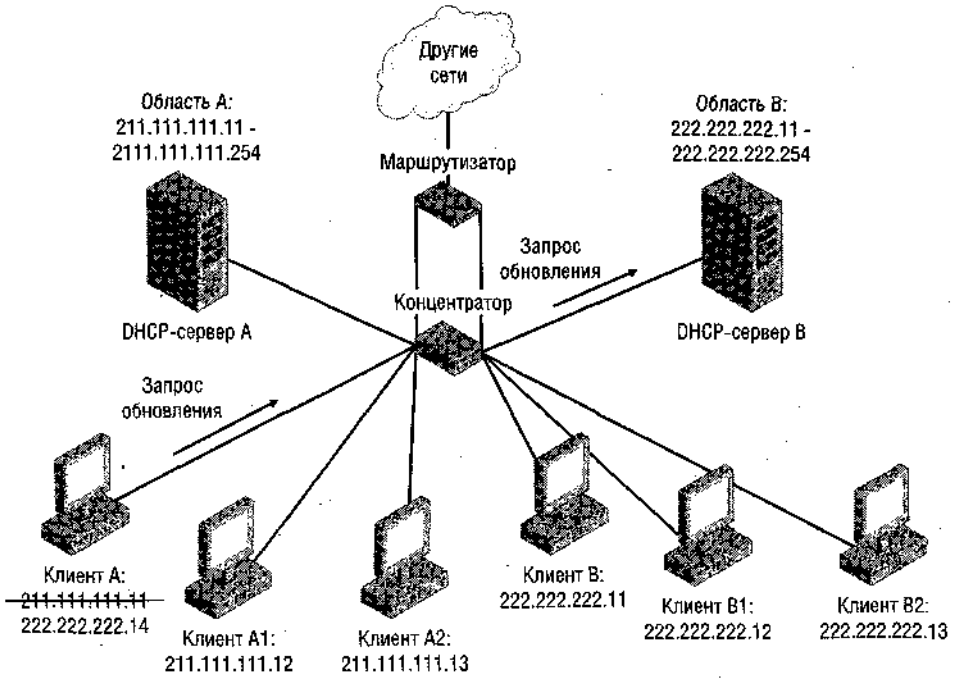


Рис. 7-9. Конфликты в подсети с двумя серверами

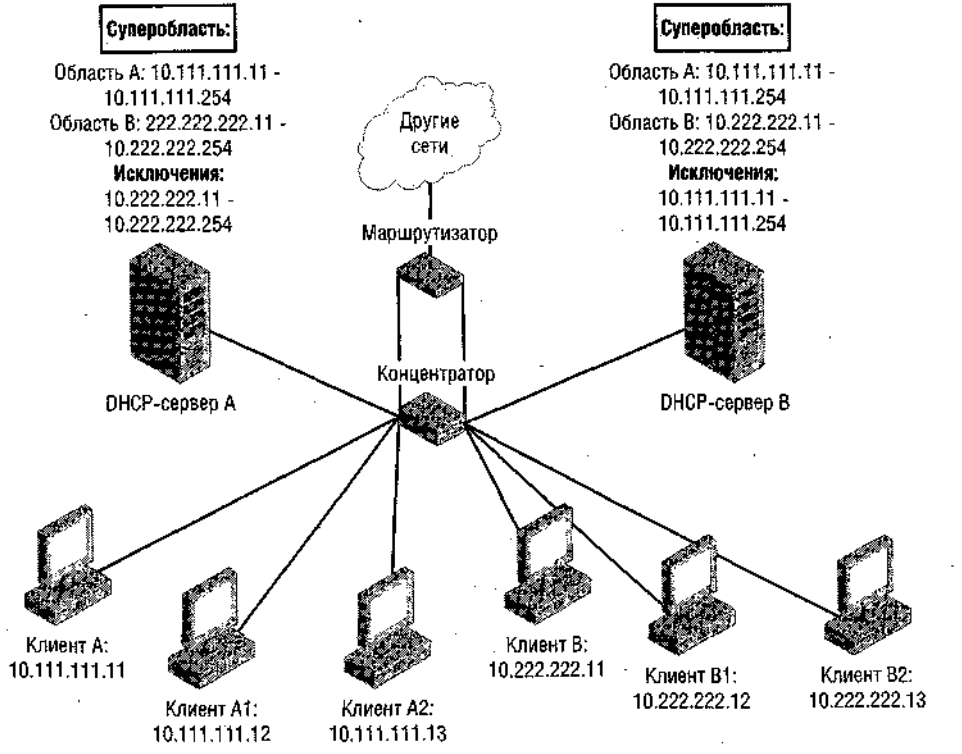


Рис. 7-10. Два сервера, использующие суперобласть

Здесь сервер В настроен на исключение области, управляемой сервером А, и наоборот. Эта конфигурация решает проблему отправки сообщений с отказом продлить аренду в ответ на запросы DHCP-клиентов, пытающихся обновить адреса, принадлежащие теперь исключенному диапазону. Поскольку каждый сервер теперь знает об области, управляемой другим сервером, он просто игнорирует запросы от клиентов, которые относятся к области другого сервера.

Изменение адресации в подсети

В процессе администрирования DHCP иногда требуется внести изменения или полностью поменять адресацию в подсети.

, Если надо просто изменить диапазон текущей области, вносят соответствующие коррективы в диапазон адресов или исключений для определенной в подсети DHCP-области.

Внимание! Изменяйте свойства области с осторожностью, чтобы не исключить активные адреса и не включить в перенастраиваемую область адреса из подсети, которые вручную назначены клиентским компьютерам.

Для перехода к совершенно новой области нужно сначала создать на DHCP-сервере новую область, а затем уже переходить к ней. Сначала создается и активируется новая область, а затем деактивируется старая. Не удаляйте деактивированную область, пока клиенты не перешли в новую. Для перехода клиентов нужно либо подождать, пока они автоматически не обновят свои адреса (по истечении половины установленного срока аренды), либо вручную обновить клиенты, последовательно выполнив команды Ipconfig /release и Ipconflg /renew на всех клиентских компьютерах. Когда все клиенты автоматически или принудительно перейдут на аренду адресов из новой области, можно спокойно удалять старую.

Подготовка к экзамену Можно активизировать обнаружение конфликтов на вкладке **Другие (Advanced)** окна свойств DHCP-сервера. Здесь задают число попыток обращения по адресу командой ping, предпринимаемых DHCP-сервером до присвоения этого адреса клиенту. Если есть ответ эхо-запрос, адрес не присваивается. Эта функция полезна, когда нужно развернуть новый DHCP-сервер взамен отказавшего.. В этом случае можно не обновлять базу данных DHCP-сервера и рассчитывать на то, что обнаружение конфликтов позволит не назначать другим клиентам уже задействованные адреса.

Архивирование базы данных DHCP-сервера

Архивирование, или резервное копирование, базы данных DHCP-сервера предотвратит потерю данных при ее повреждении или утрате.

DHCP-сервер поддерживает два метода архивирования: синхронный (автоматический), выполняемый ежечасно и асинхронный (вручную), который выполняется по команде **Архивировать (Backup)** в консоли *DHCP*. Для восстановления вручную пригодны только выполненные вручную архивы баз данных. Автоматические архивные копии используются для восстановления, лишь когда служба DHCP обнаруживает повреждение базы данных.

При архивировании сохраняется вся база данных DHCP, в том числе:

- все области, включая суперобласти и области мультисетей;
- резервирования;

- сведения об арендуемых адресах;
- все параметры, включая параметры сервера, области, резервирования и классов.

Однако некоторые данные DHCP не сохраняются ни при каком способе архивирования. Например, реквизиты динамического обновления в DNS. (Эти данные настраиваются на вкладке **Другие (Advanced)** окна свойств DHCP-сервера.)

Архивирование вручную

Чтобы создать архив базы данных DHCP вручную, щелкните значок DHCP-сервера в консоли *DHCP* правой кнопкой и выберите **Архивировать (Backup).** Для восстановления базы DHCP щелкните **Восстановить (Restore).**

Размещение архива

По умолчанию вручную сохраненная копия базы DHCP находится в папке *\Windows\System32\Dhcp\Backup*. Архив можно разместить в другой папке, указав ее при сохранении вручную или изменив стандартную папку в окне свойств DHCP-сервера.

Планируя стратегию архивирования, имейте в виду:

- при архивировании вручную не нужно останавливать службу DHCP, если только не нужно переносить базу данных на новый сервер;
- архивировать следует в локальную папку.

Перенос DHCP-сервера

При переносе DHCP-сервера с одного сервера на другой надо переместить базу данных DHCP на новый сервер. Для этого достаточно заархивировать ее, а затем восстановить в новом месте.

- **Архивирование базы данных DHCP на сервере-источнике**

1. **В** дереве консоли *DHCP* выберите нужный DHCP-сервер.
2. В меню **Действие (Action)** выберите **Архивировать (Backup).**
3. В окне **Обзор папок (Browse for Folder)** выберите папку для сохранения архивной копии базы данных DHCP и щелкните OK. Папка должна располагаться на локальном диске.
4. Остановите DHCP-сервер. Это предотвратит выделение новых адресов клиентам после сохранения базы данных.
5. В консоли *Службы* (Services) отключите службу DHCP-сервера. Для этого в диалоговом окне **DHCP Server (Локальный компьютер) — свойства (DHCP Server Properties)** в раскрывающемся списке **Тип запуска (Startup Type)** выберите **Отключено (Disabled)** и щелкните OK. Это предотвратит запуск DHCP-сервера после перемещения базы данных.
6. Скопируйте папку с архивом на новый DHCP-сервер.

- **Восстановление базы данных DHCP на новом сервере**

1. Установите роль DHCP-сервера!
2. В дереве консоли *DHCP* выберите нужный DHCP-сервер.
3. В меню **Действие (Action)** выберите **Восстановить (Restore).**
4. В окне **Обзор папок (Browse For Folder)** выберите папку с архивом и щелкните OK. В ответ на предложение остановить и перезапустить службу щелкните **Да** (Yes).

Архив, из которого восстанавливается база данных, должен создаваться вручную командой **Архивировать (Backup)** меню **Действие (Action)** консоли *DHCP*. Автоматически созданные службой DHCP копии непригодны для восстановления вручную.

Сжатие базы DHCP-сервера вручную

Для автономного сжатия и исправления баз данных Jet, в том числе баз данных служб DHCP или WINS, в Windows Server 2003 есть утилита Jetpack.exe.

Служба DHCP-сервера автоматически динамическое сжимает базу данных DHCP при работающем DHCP-сервере — это избавляет администраторов от необходимости часто пользоваться утилитой Jetpack.exe. Однако автономное сжатие более эффективное средство дефрагментации базы данных DHCP, чем динамическое сжатие.

Нужно запланировать периодическое применение Jetpack.exe для сжатия базы Jet, когда ее размер превышает 30 Мб. Кроме того, автономное сжатие рекомендуется при сообщениях об ошибках повреждения базы данных DHCP.

- **Сжатие/исправление базы данных DHCP выполняется так.**

1. На компьютере DHCP-сервера откройте окно командной строки.
2. Утилитой Jetpack.exe выполните сжатие в оффлайновом режиме. Правильный синтаксис команды выглядит так:

   jetpack <*имя базы данных*> <*имя временной базы данных*>

   Вот пример использования команды для сжатия базы DHCP.

```
cd WINDOWS\system32\dhcp
 net stop dhcpserver
 jetpack dhcp.mdb tmp.mdb
 net start dhcpserver
```

Использование классов параметров

Класс параметров (options class) это один из способов управлять на сервере параметрами, предоставляемыми клиентам внутри области. При наличии на сервере класса параметров клиенты соответствующего класса получают при настройке параметры, определенные для класса. Существует два типа классов параметров:

- классы *поставщиков* (vendors) применяются для назначения особых параметров клиентам, для которых определен конкретный тип поставщика;
- классы пользователей применяются для назначения параметров клиентам, имеющим потребность в одинаковых параметрах настройки DHCP.

Чтобы увидеть используемые классы параметров, выберите в контекстном меню узла сервера **Определить классы пользователей (Define User Classes), Определить классы вендоров (Define Vendor Classes)** или **Установить предопределенные параметры (Set Predefined Options).** По умолчанию параметры, настраиваемые для резервирований, области или сервера это параметры, принадлежащие классу поставщиков **Стандартные параметры DHCP (DHCP Standard Options)** и классу пользователей **Класс пользователей по умолчанию (Default User Class).**

Подготовка к экзамену DHCP-сервер в Windows Server 2003 содержит предопределенный класс пользователей **Класс маршрутизации и удал, доступа по умолчанию (Default Routing And Remote Access class).** Параметры этого класса применяются только к клиентам, которые запрашивают IP-конфигурацию, подключаясь через службу *Маршрутизация и удаленный доступ* (Routing And Remote Access). Один из таких параметров (он, скорее всего, встретится на экзамене) — *051 Аренда* (051 Lease). Настройка этого параметра позволяет установить для клиентов, работающих через удаленный доступ, более короткие сроки аренды, чем для остальных клиентов.

Реализация классов пользователей

Классы пользователей позволяют настроить особую конфигурацию DHCP на любом заранее определенном подмножестве DHCP-клиентов. Перед реализацией класс пользователей определяют на DHCP-сервере, назначая ему идентификатор и набор параметров. Затем определяются клиентские компьютеры, принадлежащие классу, командой Ipconfig /setclassid. Когда впоследствие такие клиенты обращаются к DHCP-серверам, они объявляют свой идентификатор класса и получают соответствующие параметры.

Нестандартный класс пользователей полезен, когда нужно присвоить особые параметры определенной группе клиентских компьютеров. Например, если клиентам с разрешением обходить брандмауэр компании, создается класс, которому назначается уникальный основной шлюз. Затем настроить параметры так, чтобы уникальный основной шлюз назначался классу пользователей с особой категорией доступа.

Для создания нового класса пользователей щелкните правой кнопкой значок DHCP-сервера в консоли *DHCP* и выберите **Определить классы пользователей (Define User Classes)** (рис. 7-11).

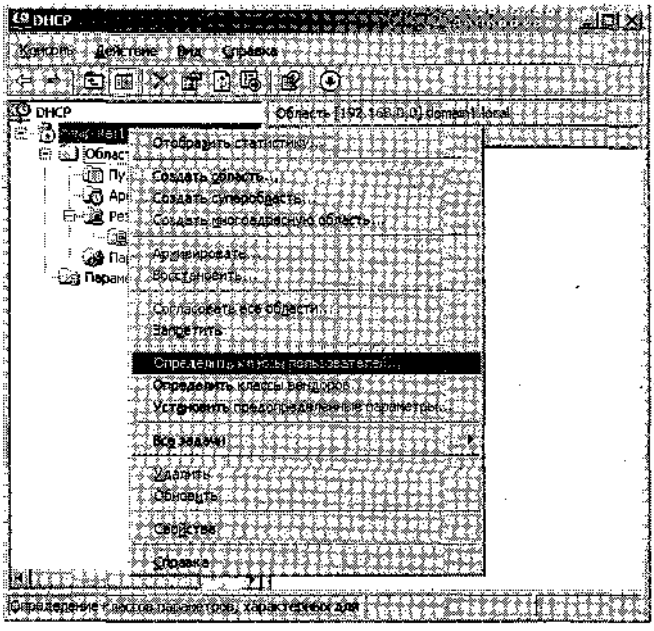


Рис. 7-11. Создание нового класса пользователей

Затем нужно ввести строку идентификатора класса. Идентификатор присваивается классу при его создании в консоли DHCP (рис. 7-12). После определения нового класса и присвоения ему идентификатора определяют нужные параметры класса.

Наконец, чтобы выбранным компьютерам назначались параметры нового класса, нужно задать на них идентификатор класса, соответствующий идентификатору, определенному на DHCP-сервере. Можно использовать команду ipconf ig /setclassid — она

выполняется на каждом клиентском компьютере. Клиенту разрешается назначать только один идентификатор, то есть клиентский компьютер может быть членом только одного класса пользователей, определенного на DHCP-сервере.

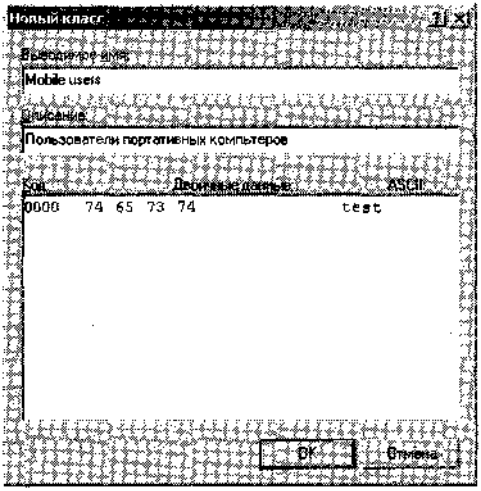


Рис. 7-12. Присвоение идентификатора новому классу

Создание нового класса пользователей или поставщиков

1. В дереве консоли *DHCP* выбелите нужный DHCP-сервер.
2. В меню **Действие (Action)** выберите одну из команд:
   - для создания нового класса пользователей — **Определить классы пользователей (Define User Classes);**
   - а для создания нового класса поставщиков — **Определить классы вендоров (Define Vendor Glasses).**
3. Щелкните **Добавить (Add).** Откроется диалоговое окно **Новый класс (New Class)** или **Классы вендоров DHCP (DHCP Vendor Classes).**
4. **В** поле **Выводимое имя (Display Name)** введите понятное имя класса. При необходимости заполните поле **Описание (Description).**
5. В текстовое поле **Код** (ID) введите в двоичном или ASCII-формате ту же строку, которая соответствует идентификатору класса DHCP, устанавливаемому для клиентов-членов класса.
6. Щелкните **ОК,** а затем **Закрыть (Close),** чтобы вернуться в консоль *DHCP.*

- **Настройка идентификатора класса на клиентском компьютере**

1. На клиентском компьютере со службой DHCP под управлением Windows 2000/XP/Server 2003 откройте окно командной строки.
2. Командой ipconfig /setclassid назначьте идентификатор класса DHCP, который клиент должен предъявлять при получении в аренду адреса от DHCP-сервера.

Вот использования команды, в котором ASCII строка *(MyNewClassId)* устанавливается в качестве идентификатора класса DHCP для подключения по локальной сети:

```
C:\>ipconfig /setclassid "Local Area Connection" MyNewClassId

Windows IP Configuration

Successfully set the class id for adapter Local Area Connection,
```

Примечание Можно использовать команду ipconfig /setclassid *<номер адаптера>* для отображения идентификаторов классов, разрешенных DHCP-сервером для любого сетевого адаптера компьютера.

Лабораторная работа 1. **Архивирование базы данных DHCP-сервера вручную**

На это лабораторной работе вы создадите архив базы данных DHCP.

Упражнение. Сохранение базы данных DHCP

Вы заархивируете базу данных DHCP, а затем проверите успешность создания резервной копии.

1. С Computerl войдите в *Domain!* как *Администратор* (Administrator).
2. В дереве консоли *DHCP* правой кнопкой щелкните узел DHCP-сервера *(Computer!.domain!.local)* и выберите **Архивировать (Backup).** Откроется окно **Обзор папок (Browse For Folder).** Папка по умолчанию для архивной копии базы данных *Windows\System32\Dhcp\Backup*.
3. Щелкните OK, принимая значение по умолчанию.
4. В *Проводнике* найдите папку *Windows\System32\Dhcp\Backup,* а в ней файл *DhcpCfg* — архивную копию базы данных DHCP.
5. Щелкните файл *DhcpCfg* правой кнопкой и выберите **Свойства (Properties).** Откроется окно **Свойства: DhcpCfg (DhcpCfg Properties).** Время и дата, указанные в строке **Изменен (Modified),** указывают, что файл недавно изменен, то есть архивирование прошло успешно.
6. Щелчком OK закройте окно **Свойства: DhcpCfg (DhcpCfg Properties).**

Лабораторная работа 2. **Создание новой суперобласти**

На этой лабораторной работе вы создадите суперобласть.

Упражнение. Создание суперобласти и ее дочерних областей

1. С Computerl войдите в *Domain!* как *Администратор* (Administrator).
2. В дереве консоли *DHCP* щелкните значок сервера правой кнопкой и выберите **Создать суперобласть (New Superscope).**
3. На первой странице **Мастера создания суперобласти (New Superscope Wizard)** щелкните **Далее (Next).**
4. На странице **Имя суперобласти (Superscope Name)** в поле **Имя (Name)** введите Superl и щелкните **Далее.**
5. На странице **Выберите области (Select Scopes)** в поле **Имеющиеся области (Available Scopes)** выберите одну область, имеющуюся в списке **[192.168.0.0] Test Scope,** и щелкните **Далее.**

6. На странице **Завершение мастера создания суперобласти (Completing The New Superscope Wizard)** щелкните **Готово (Finish). В** консоли *DHCP* появится новая суперобласть *Superl,* содержащая область *Test Scope.*
7. Раскройте папку **Суперобласть Superl (Superscope Superl).**
8. Щелкните папку **Суперобласть Superl (Superscope Superl)** правой кнопкой и выберите **Создать область (New Scope).** Откроется окно **Мастер создания области (New Scope Wizard).**
9. Используйте значения параметров из следующей таблицы для ответов на вопросы **Мастера создания области (New Scope Wizard).** Для всех параметров, не перечисленных в таблице, оставляйте значения по умолчанию.

Страница мастера создания области	**Значение параметра**
Имя области	*Имя (Name):* Test Scope2 *Начальный IP-адрес (Start IP address):* 192.168.1.11 *Конечный IP-адрес (End IP address):* 192.168.1.254 *Маска подсети (Subnet Mask):* 255.255.255.0 *Длина (Length):* 24
Добавление исключений	По умолчанию
Срок действия аренды	По умолчанию
Настройка параметров DHCP	По умолчанию
Маршрутизатор (основной шлюз)	По умолчанию
Имя домена и DNS-серверы	По умолчанию
WINS-серверы	По умолчанию
Активировать область	По умолчанию

По завершении мастера создания области вы увидите, что в суперобласть Superl теперь входят две области Test Scope 1 и Test Scope2.

10. Изучите полученную конфигурацию в консоли DHCP. В условиях реального предприятия здесь понадобился бы маршрутизатор для связи подсетей 192.168.0.0 и 192.168.1.0. Поскольку конфигурация данного примера не предусматривает маршрутизатор, а значит не сможет работать, суперобласть Superl и новую область Test Scope2 нужно удалить.

Внимание! Суперобласть всегда должна удаляться до удаления входящих в нее областей.

11. Щелкните папку **Суперобласть Superl (Superscope Superl)** правой кнопкой и выберите **Удалить (Delete).** В открывшемся окне с сообщением об удалении суперобласти, но не ее областей-потомков, щелкните Да (Yes).
12. В консоли *DHCP* щелкните папку **Область [192.168.1.0]Test Scope2 (Scope [192.168.1.0] Test Scope2)** правой кнопкой и выберите **Удалить (Delete).** В окне подтверждения удаления щелкните Да (Yes).
13. Закройте консоль *DHCP.*
14. Выйдите из системы на Computerl.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. В единственной подсети планируется, чтобы 10 особых клиентов (из 150 клиентов сети) использовали тестовый DNS-сервер, который DHCP не назначает никаким другим компьютерам. Как лучше всего решить задачу?
2. Надо перенести подсеть в новую область. Создается новая область, а затем деактивируется старая. Какая из перечисленных операций выполняется следующей?
   a. На каждом клиентском компьютере последовательно выполняются команды Ipconfig /release иIpconfig./renew.
   b. Перезагружается служба DHCP-сервера.
   c. Удаляется старая область.
   d. Авторизуется DHCP-сервер.
3. Назовите три этапа перемещения базы данных DHCP на другой сервер.
4. В единственном физическом сегменте сети не хватает адресов текущей области 207.46.159.0/24 для обслуживания всех DHCP-клиентов. Как при наличии одного DHCP-сервера ввести новые адреса в подсети, сохраняя адреса существующих клиентов?

Резюме

- *Суперобласть* (superscope) — это группа областей, объединенная в единый объект администрирования, которая используется для поддержки *мультисетей,* то есть нескольких логических подсетей в едином логическом сегменте сети.
- При переходе на совершенно новую область сначала создается и активируется новая, а затем деактивируется старая область. Перед удалением области надо убедиться, что прошло достаточно времени после деактивирования, чтобы клиенты переместились в новую область.
- Чтобы создать архив базы данных DHCP, щелкните значок DHCP-сервера в консоли *DHCP* правой кнопкой и выберите **Архивировать (Backup),** а для восстановления — **Восстановить (Restore).** Перемещая базу данных DHCP, ее архивируют, а затем восстанавливают на другом сервере.
- Утилита Jetpack.exe используется для сжатия базы данных DHCP в оффлайновом режиме.
- При наличии на сервере класса параметров клиенты класса получают особую конфигурацию DHCP, предназначенную только для данного класса. При создании класса задается его идентификатор (ID). DHCP-клиент присоединяется к классу командой Ipconfig /setclassid.

Занятие 3. Настройка DHCP-серверов для динамического обновления в DNS

По умолчанию DHCP-серверы взаимодействуют с DNS-серверами, выполняя динамическое обновление записей ресурсов PTR от имени DHCP-клиентов, которые также , являются DNS-клиентами. Такой порядок можно изменить, настраивая параметры на DHCP- и DNS-клиентах и на DHCP-сервере.

Изучив материал этого занятия, вы сможете:

- описать клиентские параметры DHCP по умолчанию на DNS-клиентах и DHCP-серверах;
- настроить динамическое обновление в DNS для DNS-клиентов;
- настроить динамическое обновление в DNS для DHCP-серверов;
- рассказать о целях, преимуществах и недостатках использования группы безопасности *DNSUpdateProxy*.

Продолжительность занятия - около 25 минут.

Настройка динамических обновлений средствами DHCP

По умолчанию DHCP-клиенты в версиях Windows, выпущенных после Windows 2000, пытаются выполнять динамические обновления своих записей ресурсов узлов (A) в DNS при любом событии, связанном с адресом (например обновлении). Однако эти же клиенты не пытаются динамически обновлять записи ресурсов-указателей (PTR), а вместо этого направляют запрос на DHCP-сервер, чтобы он от их имени выполнил обновление их PTR-записей

Стандартная настройка динамического обновления в DNS на DHCP-серверах

По умолчанию DHCP-сервер регистрирует записи ресурсов от имени DHCP-клиентов только по их запросу. Таким образом, поскольку по умолчанию DHCP-клиент посылает DHCP-серверу запрос на обновление сервером только записи ресурса PTR, DHCP-сервер выполняет только этот вид обновления. Однако сервер поддерживает обновление записей A и PTR независимо от запроса клиента. Эта функция настраивается на вкладке **DNS** окна свойств DHCP-сервера (рис. 7-13).

Примечание Эту функцию также настраивают в диалоговых окнах свойств области и резервирования.

При установке флажка **Включить динамическое обновление DNS в соответствии с настройкой (Enable DNS dynamic updates according to the settings below)** (по умолчанию флажок установлен) активизируется динамическое обновление для DHCP-сервера. В этом случае есть два варианта: в первом (по умолчанию) DHCP-сервер обновляет записи ресурсов только по запросам клиентов (рис. 7-13), во втором DHCP-сервер обновляет клиентские записи ресурсов A и PTR при каждом событии, связанном с адресом, независимо от запроса клиента. Тем не менее, этот параметр актуален только для DHCP-клиентов, поддерживающих запросы на динамическое обновление, а это клиенты под управлением Windows 2000/XP/Server 2003.

При снятии флажка **Включить динамическое обновление DNS в соответствии с настройкой** DHCP-сервер никогда не станет выполнять динамические обновления от имени клиентов под управлением Windows 2000/XP/Server 2003.

Есть еще один параметр, который настраивается на вкладке **DNS** окна свойств DHCP-сервера: флажок **Удалять A- и PTR-записи при удалении аренды (Discard A and PTR records when lease is deleted).** По умолчанию этот флажок установлен, и DHCP-сервер удаляет записи ресурсов клиентов из DNS при удалении аренды адреса этих клиентов. Если снять этот флажок, DHCP-сервер не станет удалять записи ресурсов клиентов в DNS даже при отмене их аренды адреса в DHCP.

Последний параметр динамического обновления на этой вкладке определяет, должен ли DHCP-сервер выполнять динамическое обновление от имени DHCP-клиентов, не поддерживающих динамическое обновление, например компьютеров под управлением Microsoft Windows NT 4. По умолчанию DHCP-серверы в Windows Server 2003 не выполняют динамические обновления от имени таких клиентов. Чтобы изменить поведение сервера, отметьте соответствующий флажок (нижний) на вкладке DNS (рис. 7-13).

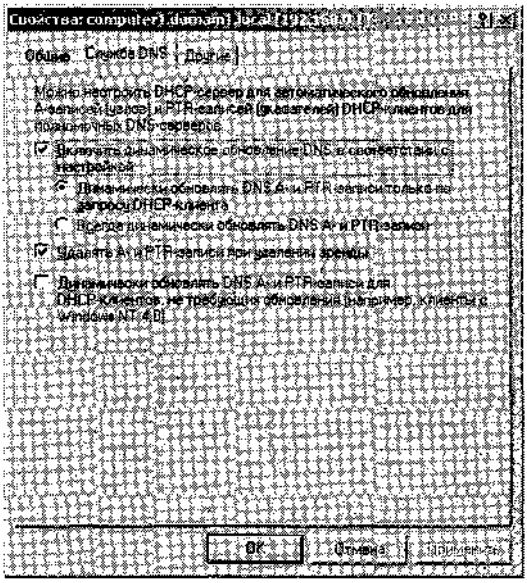


Рис. 7-13. Стандартная настройка DNS-клиента для DHCP-серверов

Группа безопасности *DnsUpdateProxy*

Ранее говорилось, что DHCP-сервер под управлением Windows Server 2003 можно настроить на динамическую регистрацию A- и PTR-записей ресурсов от имени DHCP-клиентов. Если при этом в системе поддерживаются безопасные динамические обновления на DNS-серверах под управлением Windows Server 2003, иногда могут появляться устаревшие записи ресурсов. Это обусловлено тем, что механизм безопасного обновления разрешает обновлять записи ресурса только владельцу, поэтому они часто не обновляются даже при изменениях конфигурации. Представьте себе такую последовательность событий.

1. В Windows Server 2003 DHCP-сервер (DHCP1) выполняет безопасное динамическое обновление DNS-имени одного из своих клиентов по его запросу.
2. Успешно обновив имя, DHCP1 становится его владельцем.
3. Раз DHCP1 стал владельцем имени клиента и связанных с ним записей ресурсов, то только DHCP1 сможет обновлять имя или IP-адрес этого клиента.

В некоторых ситуациях это вызывает проблемы. Допустим, через какое-то время сервер DHCP1 выходит из строя. Подключенный к сети второй резервный DHCP-сервер (DHCP2) не сможет обновлять записи ресурсов клиентов, так как не является их владельцем.

Вот еще сходный пример: DHCP1 зарегистрировал имя *host.examle.microsoft.com* от имени клиента под управлением версии Windows более ранней, чем Windows 2000. Затем администратор обновляет ОС клиентского компьютера до Windows XP Professional. Поскольку владелец имени— DHCP-сервер DHCP1, клиент после обновления ОС не сможет обновить запись ресурса в DNS.

Для решения несостыковок подобного рода Active Directory в Windows Server 2003 предусмотрена встроенная группа безопасности *DnsUpdateProxy*. Все объекты, созданные членами этой группы, не защищены. В результате у объекта нет владельца и, следовательно, даже в зонах с поддержкой безопасных обновлений его вправе обновить и DHCP-сервер, и клиент, которые его не создавали. Однако, как только запись обновит DHCP-сервер или клиент, не принадлежащие группе *DnsUpdateProxy,* он станет ее владельцем, и неприятностей с обновлением снова не избежать. Поэтому если все DHCP-серверы, регистрирующие записи ресурсов от имени клиентов под управлением ранних версий Windows будут членами упомянутой группы, а сами клиенты в нее входить не будут, проблема решится.

Добавление членов в группу DnsUpdateProxy

Глобальную группу безопасности *DnsUpdateProxy* настраивают посредством консоли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) (рис. 7-14).

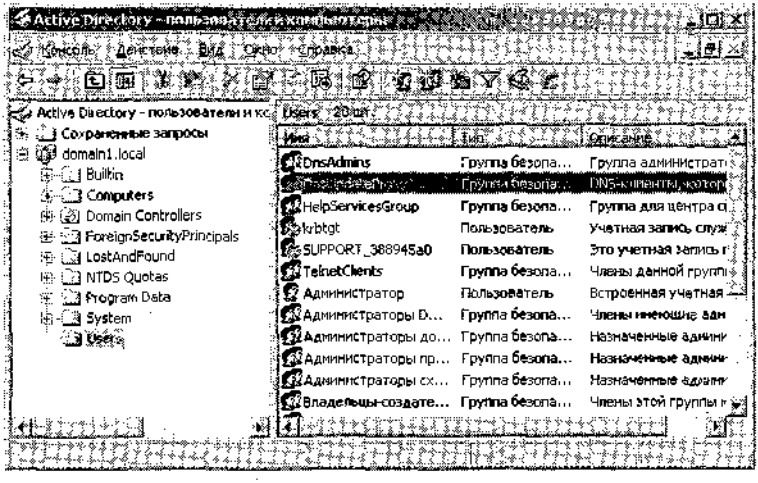


Рис. 7-14. Настройка группы *DnsUpdateProxy*

Внимание! Если для повышения отказоустойчивости используется несколько DHCP-серверов и в зонах, обслуживаемых этими серверами, требуются безопасные динамические обновления DNS, не забудьте ввести все компьютеры с DHCP-серверами Windows Server 2003 в состав глобальной группы безопасности *DnsUpdateProxy*.

Вопросы безопасности

Хотя присоединение всех DHCP-серверов к этой особой встроенной группе помогает решить некоторые проблемы безопасных обновлений DNS, такое решение создает определенную угрозу безопасности.

В частности, любые доменные имена DNS, зарегистрированные DHCP-сервером, не являются безопасными. Запись ресурса A для самого DHCP-сервера является примером такой записи. Для защиты от подобной угрозы можно вручную определить другого владельца всех записей ресурсов DNS, относящихся к самому DHCP-серверу.

Однако более сложная проблема возникает, когда DHCP-сервер, член группы *DnsUpdateProxy,* устанавливается на контроллере домена. В этом случае все записи ресурсов «служба» (SRV), «узел» (A) или «псевдоним» (CNAME), регистрируемые службой Netlogon для контроллера домена, не являются безопасными. Чтобы свести к минимуму риск, не стоит устанавливать DHCP-сервер на контроллере домена при наличии динамических обновлений.

Внимание! В Windows Server 2003 использование динамических обновлений может быть весьма опасным, когда DHCP-сервер установлен на контроллере домена, а служба DHCP настроена на регистрацию записей ресурсов DNS от имени DHCP-клиентов. Проблема устраняется разнесением DHCP-серверов и контроллеров доменов на разные компьютеры.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Как настроить DHCP-сервер на обновление записей ресурсов A и PTR от имени клиентов под управлением Windows NT 4?
   a. Ничего не нужно предпринимать.
   b. На вкладке **DNS** окна свойств DHCP-сервера отметить флажок **Динамически обновлять DNS A- и PTR-записи для DHCP-клиентов, не требующих обновления (Dynamically update DNS A and PTR records for DHCP clients that do not request updates).**
   c. На вкладке **DNS** окна свойств DHCP-сервера отметить флажок **Всегда динамически обновлять DNS A- и PTR-записи (Always dynamically update DNS A and PTR records).**
   d. Зарегистрировать клиента как динамический узел с помощью DHCP-сервера.
2. При настройке DNS значения по умолчанию на DHCP-клиенте и сервере не изменялись. Какая запись (или записи) ресурсов клиента в DNS будет обновлена DHCP-сервером? (Предполагается, что клиент работает под управлением Windows XP.)
   a. PTR.
   b. A.
   c. A И PTR.
   d. Ни A, ни PTR.
3. В зоне, где разрешены только безопасные динамические обновления, DHCP-сервер настроен на выполнение динамических обновлений от имени клиентов Windows NT. Все другие параметры DNS на DHCP-сервере настроены по умолчанию. После обновления ОС клиентов до Windows XP клиентские записи ресурсов A перестали обновляться. Какова наиболее вероятная причина неполадки?
4. При каких условиях считается небезопасным размещать DHCP-сервер на контроллере домена? Почему?

Резюме

- По умолчанию DHCP-сервер обновляет записи ресурсов PTR для DHCP-клиентов под управлением Windows 2000/XP/Server 2003, что эквивалентно выполнению динамических обновлений по запросам клиентов.
- Порядок динамического обновления DHCP-сервером определяется на вкладке DNS окна свойств сервера. Можно определить: выполнение динамического обновления всегда (независимо от запросов клиента), отменить динамическое обновление для клиентов под управлением версий Windows, предшествующих Windows 2000, а также настроить удаление записей ресурсов клиентов из DNS при удалении аренды адреса.
- Если в системе поддерживаются безопасные динамические обновления на DNS-серверах под управлением Windows Server 2003, иногда могут появляться устаревшие записи ресурсов. Это обусловлено тем, что механизм безопасного обновления разрешает обновлять записи ресурса только владельцу, поэтому они часто не обновляются даже при изменениях конфигурации.
- Все записи, созданные членами группы *DnsUpdateProxy,* не защищены. В результате у объекта нет владельца и, следовательно, даже в зонах с поддержкой безопасных обновлений его вправе обновить'и DHCP-сервер, и клиент, которые его не создавали.
- Как только запись обновляет DHCP-сервер или клиент, не принадлежащий группе *DnsUpdateProxy,* он становится ее владельцем. После этого только этот владелец может обновлять запись в зонах, требующих безопасных обновлений.

Пример из практики

Вы администратор сети в издательской компании Proseware, Inc, размещенной в одном здании в г. Канзас-Сити, штат Миссури. В компании 200 сотрудников на полной ставке, работающих на ПК, и 100 «контрактников», использующих ноутбуки. Контрактники часто перемещаются по зданию, подключаясь к разным стыковочным станциям, и работают в офисе не менее одного дня в неделю.

Вам поручили решить несколько проблем с сетью. Ответьте на следующие вопросы, порекомендовав наиболее эффективные действия.

1. Адресного пространства организации (207.46.1.21—207.46.1.254) недостаточно для обслуживания всех 300 сотрудников одновременно, поэтому в сети часто не хватает свободных адресов, предоставляемых в аренду службой DHCP. Вместе с тем в каждый отдельно взятый день в офисе работает не более 30 контрактников. Как максимально эффективно использовать имеющееся адресное пространство и обеспечить всех сотрудников адресами?
   a. Присвоить всем ноутбукам адрес альтернативной конфигурации внутри совместимого адресного пространства.
   b. Создать для контрактников отдельный класс, в котором установить срок аренды адреса равным одному дню.
   c. Увеличить число попыток обнаружения конфликтов на DHCP-сервере, чтобы предотвратить конфликты адресов.
   d. Присвоить контрактникам адреса в одном из частных диапазонов адресов.
2. На DHCP-сервере произошел сбой, и вернуть его в рабочее состояние невозможно. Последнее архивирование выполнялось четыре дня назад. Как лучше сохранить текущее адресное пространство без перезагрузки всех компьютеров компании?

a. Развернуть новый DHCP-сервер в той же области адресов и увеличить число попыток обнаружения конфликтов до 3.

b. Развернуть новый DHCP-сервер в той же области адресов и увеличить новый срок аренды до 15 дней.

c. Восстановить из архива базу данных DHCP.

d. Выполнить команду Ipconfig /renew на всех компьютерах.

3. DNS -домен *proseware. local* интегрирован в Active Directory, в которой поддерживаются только безопасные динамические обновления. DHCP-сервер настроен на регистрацию записей DNS для клиентов с устаревшими ОС и не является членом группы *DnsUpdateProxy*. Операционная система пятидесяти клиентских компьютеров недавно обновлена с Windows NT 4 до Windows XP Professional. После обновления пользователи начали жаловаться на отсутствие доступа к некоторым сетевым ресурсам. Какой из вариантов действий позволит решить проблему с минимумом усилий?

a. Остановить и перезагрузить обновленные клиентские компьютеры.

b. Выполнить на всех клиентских компьютерах сначала команду Ipconfig / renew, а затем Ipconfig /registerdns.

c. Активизировать механизм устаревания и очистки в зоне *proseware.local,* а затем уменьшить интервалы блокирования и обновления при настройке свойств очистки для зоны.

d. Присоединить DHCP-сервер к группе *DNSUpdateProxy*.

Практикум по устранению неполадок

На этом практикуме вы устраните неполадки разрешения имен.

1. С Computer2 войдите в *Domain 1* как *Администратор* (Administrator).
2. Вставьте в дисковод прилагаемый к книге компакт-диск.
3. Найдите файл *\70-291\labs\Chapter07\Ch7a.bat* и дважды щелкните его.
4. В окне командной строки выполните команду Ipconfig /renew. Через несколько секунд появится сообщение об ошибке превышения времени ожидания. Это говорит либо об отсутствии связи с сервером, либо о запрете доступа.
5. Воспользуйтесь командой Ipconfig, чтобы определить текущий IP-адрес Computer2. Если Computer2 присвоил себе адрес альтернативной конфигурации 192.168.0.2, перейдите к п. 6. В противном случае снова выполните команду Ipconfig /renew и убедитесь, что альтернативный адрес 192.168.0.2 успешно присвоен, а затем перейдите к п. 6.
6. Выполните команду netsh dhep server 192.168.0.1 show all.
   Вы получите описание конфигурации и состояния сервера.
7. Изучите полученную информацию и на ее основании ответьте на вопрос. Работает ли служба DHCP-сервера?
8. Выполните команду netsh dhep server 192.168.0.1 show scope.
   Вы получите сведения о конфигурации настроенной на сервере области.
9. Ответьте на вопрос: каково состояние описанной области?

10. Выполните следующие команды:

```
netsh dhcp server 192.168.0.1 scope 192.168.0.0 set state 1
```

и

```
netsh dhcp server 192.168.0.1 show scope
```

Теперь область описывается как **Активированная (Active).**

11. **В** командной строке выполните Ipconfig /renew. Произойдет успешное обновление адреса.
12. Выйдите из системы на Computer2.

Резюме главы

- В сетях с Active Directory DHCP-серверы должны обязательно проходить авторизацию.
- Область DHCP — это непрерывный диапазон IP-адресов, определенных в единой логической подсети, которые DHCP-сервер предоставляет клиентам. После определения и настройки области ее надо активировать — только после этого DHCP-сервер сможет обслуживать клиенты.
- Диапазон исключений — это набор из одного или нескольких IP-адресов в пределах диапазона заданной области, которые не предоставляются в аренду клиентам. Для постоянного выделения адреса в аренду применяется резервирование.
- Вместе с арендуемым адресом DHCP-сервер предоставляет клиентам другие параметры, в том числе адреса основного шлюза или DNS-сервера.
- *Суперобласть* — это группа областей, объединенная в единый объект администрирования, которая используется для поддержки *мультисетей,* то есть нескольких логических подсетей в едином логическом сегменте сети.
- При наличии на сервере класса параметров, клиенты класса получают особую конфигурацию DHCP, предназначенную только для данного класса. При создании класса задается его идентификатор (ID). DHCP-клиент присоединяется к классу командой Ipconfig /setclassid.
- По умолчанию DHCP-сервер обновляет PTR-записи для DHCP-клиентов под управлением Windows 2000, Windows XP и Windows Server 2003. Это эквивалентно выполнению динамических обновлений по запросам клиентов. Можно настроить DHCP-сервер на постоянное динамическое обновление записей ресурсов A и PTR на вкладке **DNS** окна свойств DHCP-сервера.
- Все записи, созданные членами группы *DnsUpdateProxy*, не защищены. В результате у объекта нет владельца и, следовательно, даже в зонах с поддержкой безопасных обновлений его вправе обновить и DHCP-сервер, и клиент, которые его не создавали.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Разберитесь с DHCP-областями, исключениями и резервированиями.
- Запомните, как предоставляется аренда в DHCP и команды для освобождения и обновления арендуемых адресов.
- Запомните, зачем нужны суперобласти.
- Выучите, для чего используются классы параметров.
- Запомните, как DHCP-серверы настраиваются для выполнения динамических обновлений в DNS.

Основные термины

Мультисеть ~ multinet — несколько логических подсетей в одном физическом сегменте сети. Подсети в мультисетевой конфигурации взаимодействуют между собой через маршрутизаторы.

Jetpack — утилита для сжатия баз данных Jet.

Ложный сервер ~ rogue server — изолированный DHCP-сервер, развернутый в сети с Active Directory.

Вопросы и ответы

Занятие 1. Лабораторная работа. Упражнение 4

6. Сколько активных арендованных адресов теперь отображается в правой панели консоли DHCP? Какому компьютеру присвоен адрес?

   Правильный ответ: один, присвоенный компьютеру *computer2.domainl.local*.

Занятие 1. Закрепление материала

1. Вы настроили область с диапазоном адресов 192.168.0.11—192.168.0.254. Однако DNS-серверу в той же подсети уже присвоен статический адрес 192.168.0.200. Как проще всего обеспечить совместимость адреса DNS-сервера и службы DHCP в данной подсети?

   Правильный ответ: исключение адреса 192.168.0.200 легко обеспечит совместимость между DNS-сервером и текущей настройкой DHCP-области.

2. Какой из перечисленных серверов должен стать первым DHCP-сервером в сети? (Выберите все подходящие варианты).
   a. Контроллер домена Windows Server 2003 в сети с Active Directory.
   b. Сервер рабочей группы Windows Server 2003 в сети, где нет доменов.
   c. Сервер рабочей группы Windows Server 2003 в сети с Active Directory.
   d. Рядовой сервер Windows 2000 Server в сети с Active Directory.

   Правильные ответы: a, b, d.

3. DHCP-область настроена с параметром *003 Маршрутизатор* (003 Router), который определяет адрес основного шлюза на клиентах. Однако после выполнения команды Ipconfig /all на клиенте Clientl обнаруживается, что клиент получает IP-адрес из назначенной области, но ему не назначается адрес основного шлюза. Какая самый вероятная причина неполадки?

a. Client 1 отключился от сети.
b. IP-адрес для Clientl предоставлен в рамках резервирования.
c. На уровне сервера не определены параметры области.
d. Область не активирована.

Правильный ответ: Ь.

4. Назовите две группы безопасности, кроме *Администраторы* (Administrators), которым предоставлено право управления DHCP-серверами.

   Правильный ответ: Администраторы предприятия (Enterprise Admins,) и Администраторы DHCP (DHCP Administrators).

5. **В** процессе работы *Мастера создания области* (New Scope Wizard) вы отказались от настройки каких-либо параметров DHCP. Впоследствии обнаруживается, что DHCP-сервер не присваивает адреса в заданной области. Какова наиболее вероятная причина неполадки?

   Правильный ответ: область не активирована.

Занятие 2. Закрепление материала

1. **В** единственной подсети планируется, чтобы 10 особых клиентов (из 150 клиентов сети) использовали тестовый DNS-сервер, который DHCP не назначает никаким другим компьютерам. Как лучше всего решить задачу?

   Правильный ответ: лучше всего создать новый класс пользователей, настроить для этого класса параметр 006 DNS-серверы (006 DNS Servers), определив в нем IP-адрес тестового DNS-сервера, а затем определить этот класс на каждом из 10 клиентов командой ipconfig /setclassid.

2. Надо перенести подсеть в новую область. Создается новая область, а затем деактивируется старая. Какая из перечисленных операций выполняется следующей?
   a. На каждом клиентском компьютере последовательно выполняются команды Ipconfig /release иIpconfig /renew.
   b. Перезагружается служба DHCP-сервера.
   c. Удаляется старая область.
   d. Авторизуется DHCP-сервер.

   Правильный ответ: а.

3. Назовите три этапа перемещения базы данных DHCP на другой сервер.
   Правильный ответ: 1) архивирование базы данных; 2) копирование архива на новый сервер; 3) восстановление конфигурации из архива на новом сервере.

4. В единственном физическом сегменте сети не хватает адресов текущей области 207.46.159.0/24 для обслуживания всех DHCP-клиентов. Как при наличии одного DHCP-сервера ввести новые адреса в подсети, сохраняя адреса существующих клиентов?

   Правильный ответ: создать и активировать суперобласть, которая включает в качестве дочерней текущую активную область. Получить у интернет-провайдера второй идентификатор сети. Создать, настроить и активировать дополнительную область с диапазоном адресов новой логической подсети. Добавить новую область в суперобласть. Для соединения двух логических подсетей в единой физической сети использовать маршрутизатор.

Занятие 3. Закрепление материала

1. Как настроить DHCP-сервер на обновление записей ресурсов A и PTR от имени клиентов под управлением Windows NT 4?
   a. Ничего не нужно предпринимать.
   b. На вкладке **DNS** окна свойств DHCP-сервера отметить флажок **Динамически обновлять DNS A- и PTR-записи для DHCP-клиентов, не требующих обновления (Dynamically Update DNS A And PTR Records For DHCP Clients That Do Not Request Updates).**
   c. На вкладке **DNS** окна свойств DHCP-сервера отметить флажок **Всегда динамически обновлять DNS A- и PTR-записи (Always Dynamically Update DNS A And PTR Records).**
   d. Зарегистрировать клиента как динамический узел с помощью DHCP-сервера.

   Правильный ответ: Ь.
2. При настройке DNS значения по умолчанию на DHCP-клиенте и сервере не изменялись. Какая запись (или записи) ресурсов клиента в DNS будет обновлена DHCP-сервером? (Предполагается, что клиент работает под управлением Windows **XP).**
   a. **PTR.**
   b. A.
   c. A и PTR.
   d. Ни A, ни PTR.

   Правильный ответ: a.
3. **В** зоне, где разрешены только безопасные динамические обновления, DHCP-сервер настроен на выполнение динамических обновлений от имени клиентов Windows NT. Все другие параметры DNS на DHCP-сервере настроены по умолчанию. После обновления ОС клиентов до Windows XP клиентские записи ресурсов A перестали обновляться. Какова наиболее вероятная причина неполадки?

   Правильный ответ: DHCP-сервер не является членом группы безопасности DnsUpdateProxy.
4. При каких условиях считается небезопасным размещать DHCP-сервер на контроллере домена? Почему?

   Правильный ответ: размещение DHCP-сервера на контроллере домена в зоне DNS, поддерживающей только безопасные динамические обновления, небезопасно, если сервер является членом группы DnsUpdateProxy. В этом случае все записи ресурсов, созданные службой Netlogon для контроллера домена, являются небезопасными.
   По этой же причине в зоне DNS, допускающей безопасные и небезопасные обновления, размещение DHCP-сервера на контроллере домена всегда опасно.

Пример из практики

Вы администратор сети в издательской компании Proseware, Inc, размещенной в одном здании в г. Канзас-Сити, штат Миссури. В компании 200 сотрудников на полной ставке, работающих на ПК, и 100 «контрактников», использующих ноутбуки. Контрактники часто перемещаются по зданию, подключаясь к разным стыковочным станциям, и работают в офисе не менее одного дня в неделю.

Вам поручили решить несколько проблем с сетью. Ответьте на следующие вопросы, порекомендовав наиболее эффективные действия.

1. Адресного пространства организации (207.46.1.21—207.46.1.254) недостаточно для обслуживания всех 300 сотрудников одновременно, поэтому в сети часто не хватает свободных адресов, предоставляемых в аренду службой DHCP. Вместе с тем в каждый отдельно взятый день в офисе работает не более 30 контрактников. Как максимально эффективно использовать имеющееся адресное пространство и обеспечить всех сотрудников адресами?
   a. Присвоить всем ноутбукам адрес альтернативной конфигурации внутри совместимого адресного пространства.
   b. Создать для контрактников отдельный класс, в котором установить срок аренды адреса равным одному дню.
   c. Увеличить число попыток обнаружения конфликтов на DHCP-сервере, чтобы предотвратить конфликты адресов.
   d. Присвоить контрактникам адреса в одном из частных диапазонов адресов.

   Правильный ответ: b.
2. На DHCP-сервере произошел сбой, и вернуть его в рабочее состояние невозможно. Последнее архивирование выполнялось четыре дня назад. Как лучше сохранить текущее адресное пространство без перезагрузки всех компьютеров компании?
   a. Развернуть новый DHCP-сервер в той же области адресов и увеличить число попыток обнаружения конфликтов до 3.
   b. Развернуть новый DHCP-сервер в той же области адресов и увеличить новый срок аренды до 15 дней.
   c. Восстановить из архива базу данных DHCP.
   d. Выполнить команду Ipconfig /renew на всех компьютерах.

   Правильный ответ: a.
3. DNS-домен *proseware.local* интегрирован в Active Directory, в которой поддерживаются только безопасные динамические обновления. DHCP-сервер настроен на регистрацию записей DNS для клиентов с устаревшими ОС и не является членом группы *DnsUpdateProxy*. Операционная система пятидесяти клиентских компьютеров недавно обновлена с Windows NT 4 до Windows XP Professional. После обновления пользователи начали жаловаться на отсутствие доступа к некоторым сетевым ресурсам. Какой из вариантов действий позволит решить проблему, затратив минимум усилий?
   a. Остановить и перезагрузить обновленные клиентские компьютеры.
   b. Выполнить на всех клиентских компьютерах последовательность команд Ipconfig /renew, а затем Ipconfig /registerdns.
   c. Активизировать механизм устаревания и очистки в зоне *proseware. local,* а затем уменьшить интервалы блокирования и обновления при настройке свойств очистки для зоны.
   d. Присоединить DHCP-сервер к группе *DNSUpdateProxy*.

   Правильный ответ: c.

Практикум по устранению неполадок

7. Изучите полученную информацию и на ее основании ответьте на вопрос. Работает ли служба DHCP-сервера?

   Правильный ответ: Работает (Running).
9. Ответьте на вопросы: каково состояние описанной области?

   Правильный ответ: Отключено (Disabled).

Наблюдение и устранение неполадок DHCP

Темы экзамена

- Устранение неполадок DHCP:
  - диагностика и устранение неполадок авторизации в DHCP;
  - проверка резервирований DHCP-клиентов;
  - проверка системного журнала событий и журналов аудита DHCP;
  - диагностика и устранение неполадок настройки DHCP-сервера и параметров областей;
  - а проверка целостности базы данных.

В этой главе

Здесь описывается механизм обмена сообщениями DHCP, а также их запись и анализ с помощью утилиты *Сетевой монитор* (Network Monitor). Далее вы познакомитесь с форматом и содержимым записей журнала DHCP-сервера. Наконец, в главе описаны основные способы обнаружения и устранения неполадок протокола DHCP в сети.

Прежде всего

Для изучения материала данной главы вам потребуется:

- два объединенных в сеть компьютера (Computerl и Computer2) под управлением Windows Server 2003. Компьютеру Computerl надо назначить статический адрес 192.168.0.1/24 и адрес основного DNS-сервера— 192.168.0.1. Computer2 нужно настроить на автоматическое получение собственного адреса и адреса DNS-сервера, а также определить альтернативную конфигурацию с адресом 192.168.0.2/24;
- установить на Computerl DNS-сервер и развернуть на нем основную зону прямого просмотра *domain 1.local,* настроенную для поддержки динамического обновления;
- повысить Computerl до контроллера нового домена в новом лесу Active Directory с именем *domain 1.local.* Computer2 надо присоединить к этому домену в качестве рядо-

вого члена. После установки Active Directory DNS-зона *domainl.local* настраивается как зона, интегрированная с Active Directory и поддерживающая только безопасные динамические обновления;

- удалить все подключения удаленного доступа, ранее определенные на Computer 1;
- установить DHCP-сервер на Computerl. DHCP-сервер должен обслуживать область Test Scope с диапазоном IP-адресов 192.168.0.11/24-192.168.0.254/24. В области надо установить флажки **003 Маршрутизатор (003 Router)** и **006 DNS-серверы (006 DNS Servers)** с одинаковыми IP-адресами 192.168.0.1. Параметр **015 DNS-имя доиена (015 DNS Domain Name)** надо настроить на уровне области с основным DNS-суффиксом *domainl.local.* Computer2 должен получать IP-адрес от DHCP-сервера, а запись ресурса А для Computer2 в зоне *domainl.local* должна отражать IP-адрес, присвоенный DHCP-сервером;
- установить на обоих компьютерах *Средства поддержки Windows* (Windows Support Tools);
- установить на обоих компьютера *Средства сетевого монитора* (Network Monitor Tools) *Сетевой монитор* (Network Monitor)' нужно настроить на прослушивание подключения по локальной сети.

Занятие 1. **Анализ DHCP-трафика**

Для эффективного устранения неполадок DHCP нужно уметь записывать и анализировать сетевой DHCP-трафик, то есть уметь «читать» и понимать сообщения, которыми обмениваются DHCP-клиенты и серверы в процессе выделения адресов.

Изучив материал этого занятия, вы сможете:

- *S* описать этапы процесса предоставления адреса в аренду службой DHCP;
- *S* распознавать и читать различные DHCP-сообщения, записанные с помощью *Сетевого монитора* (Network Monitor).

Продолжительность занятия — около 60 минут.

Получение конфигурационной информации DHCP-клиентами

Есть два метода получения DHCP-клиентами IP-адреса и параметров конфигурации от DHCP-сервера. Первый— процесс инициализации, который происходит при запуске клиентского компьютера и его попытке присоединения к сети, а второй — обновление аренды, когда клиенту надо обновить аренду уже имеющегося адреса.

Первичная аренда

При первом запуске DHCP-клиент автоматически пытается получить адрес в аренду от DHCP-сервера (рис. 8-1).

1. DHCP-клиент направляет в локальную подсеть широковещательный запрос-поиск DHCP-сервера (DHCP Discover).
2. DHCP-сервер отвечает сообщением DHCP Offer с предлагаемым IP-адресом.
3. В случае отсутствия отклика DHCP-сервера возможны два варианта дальнейшего развития событий:

- клиент под управлением Microsoft Windows 2000 автоматически присваивает себе APIPA-адрес;
- клиент под управлением Microsoft Windows XP/Server 2003 присваивает себе альтернативный адрес (если он задан). Если же статический альтернативный адрес не определен, клиент присваивает себе APIPA-адрес.

Клиентам под управлением ОС Windows версии, предшествующей Windows 2000, и тем, у которых отсутствует альтернативный статический адрес и запрещена автоматическая настройка IP, не удается начать работу в сети. Тем не менее они продолжают периодически отправлять сообщения-запросы DHCP-сервера 4 раза каждые 5 минут.

4. Получив предложение DHCP-сервера клиент принимает предложенный адрес, отвечая серверу сообщением-запросом DHCP Request. Обычно после этого сервер отвечает сообщением-подтверждением (DHCP ACK) аренду. (В этом сообщении содержится информация о параметрах DHCP.)
5. Получив подтверждение, клиент принимает предложенные параметры протокола TCP/IP и подключается к сети.

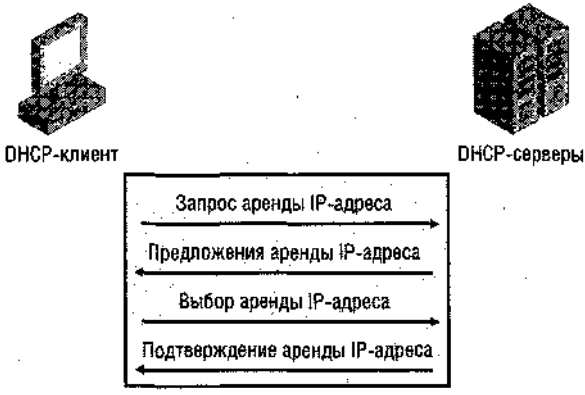


Рис. 8-1. Процесс получения DHCP-конфигурации в аренду

Обновление аренды

После перезагрузки DHCP-клиент обычно получает в аренду тот же IP-адрес, что он использовал до этого. Аренда также успешно обновляется по истечении половины срока аренды (по умолчанию 4 дня) и при выполнении на клиентском компьютере команды Ipconfig /renew, которая работает в такой последовательности.

1. Клиент направляет сообщение-запрос на обновление и продление аренды напрямую серверу, предоставившему ему конфигурацию.
2. Если сервер доступен, он обычно возвращает сообщение-подтверждение продления аренды (DHCP ACK).

   Как и при первичной аренде в ответе сервера содержится вся конфигурационная информация DHCP. Если в параметрах что-то изменилось, клиент сможет обновить свою конфигурацию.
3. Если клиент не может связаться с исходным DHCP-сервером, он ждет наступления *состояния повторной привязки* (rebiding state), которое по умолчанию наступает через 7 дней с момента последнего обновления. С этого момента клиент пытается обновить текущую аренду, обращаясь к любым доступным DHCP-серверам.

4. Получив от сервера предложение DHCP Offer, клиент обновляет аренду с предложенными параметрами и продолжает работу в сети.
5. Если же срок аренды истек и клиенту не удается связаться ни с одним DHCP-сервером, он должен немедленно прекратить использовать арендованный IP-адрес.
6. После этого клиент инициируется процесс аналогичный получения адреса в первичную аренду.

Примечание В некоторых случаях на этапе 2 DHCP-сервер отвечает клиенту не сообщением-подтверждением (ACK), а отказом (DHCP NACK), означающим, что возобновление указанного IP-адреса невозможно. Эта происходит, когда клиент пытается арендовать неверный или уже существующий в сети адрес. В такой ситуации обновление аренды невозможно, и клиент должен начать процесс получения первичной аренды.

Анализ DHCP-сообщений

Все связанные с арендой DHCP-сообщения можно увидеть и проанализировать, записав их с помощью утилиты *Сетевой монитор* (Network Monitor). Мы расскажем о структуре некоторых DHCP-сообщений, чтобы вы могли их легко распознать в общем потоке трафика, которым обмениваются DHCP-серверы и клиенты.

На рис. 8-2 представлена общая структура DHCP-кадра. Заголовок состоит из 15 разделов, в том числе раздел переменной длины Options. Тип DHCP-сообщения определяется параметром Option 53 — он обязателен для всех DHCP-сообщений.

В табл. 8-1 описаны значения каждого из полей.

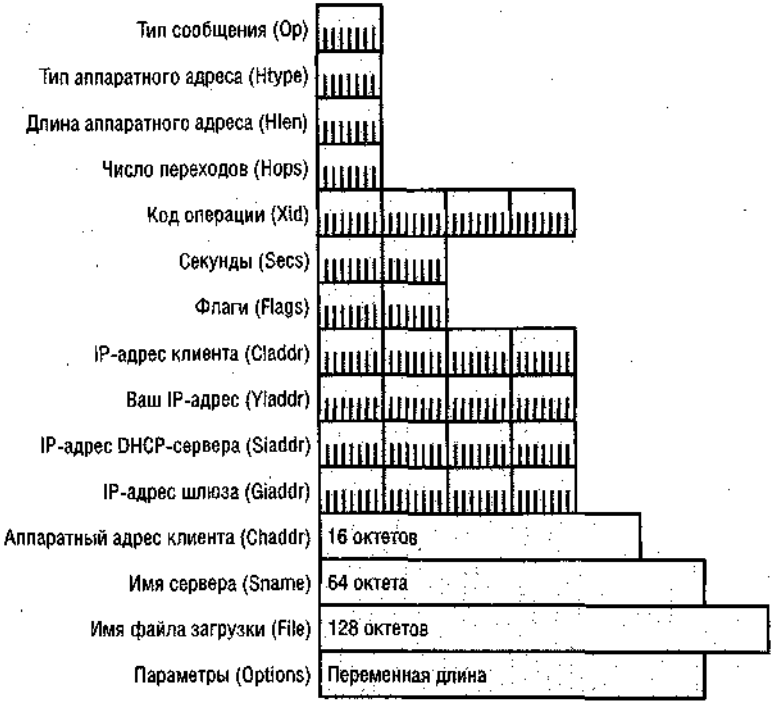


Рис. 8-2. Структура DHCP-кадра

Табл. 8-1. Поля заголовка DHCP-сообщения

Поле	Описание
Тип сообщения (Message Type) (Op)	Тип сообщения
Тип аппаратного адреса (Hardware Adress Type) (Htype)	Тип аппаратного адреса согласно разделу, посвященному протоколу ARP, в RFC 1700 (например, 0x1 означает Ethernet 10 Мбит)
Длина аппаратного адреса (Hardware Adress Length) (Hlen)	Длина аппаратного адреса в октетах (например, 0x6 для обычного 6-байтного Ethernet-адреса)
Число переходов (Hops)	Поле, указывающее на происхождение сообщения — из удаленной или локальной подсети. Значение этого поле инкрементируется DHCP-агентами пересылки и маршрутизаторами, удовлетворяющими требованиям RFC 1542
Код операции (Transaction ID) (Xid)	Случайное число для обозначения транзакции между DHCP-клиентом и DHCP-сервером (например получение адреса в аренду)
Секунды (Seconds) (Sees)	Время в секундах, прошедшее с момента начала процесса получения адреса службой DHCP-клиента. Заполняется DHCP-клиентом
Флаги (Flags)	Флаги, устанавливаемые клиентом. В RFC 2131 определен только один флаг Broadcast. DHCP-клиент, которому не удается получить одноадресную IP-дейтаграмму, устанавливает это флаг Broadcast, пока не получит IP-адрес
IP-адрес клиента (Client IP Address) (Ciaddr)	Адрес DHCP-клиента. Он нулевой, пока у клиента нет IP-адреса и он не в состоянии отвечать на ARP-запросы
Ваш IP-адрес (Your IP Address) (Yiaddr)	Адрес, предоставленный клиенту DHCP-сервером
IP-адрес DHCP-сервера (DHCP Server IP Address) (Siaddr)	IP-адрес DHCP-сервера, предлагающего аренду адреса (возвращенный в сообщении-предложении DHCP Offer)
IP-адрес шлюза [Relay (Gateway) IP Address] (Giaddr)	IP-адрес DHCP-агента ретрансляции или маршрутизатора, совместимого с требованиями RFC 1542. Поле используется при загрузке через DHCP-агент пересылки или маршрутизатор, совместимый с RFC 1542
Аппаратный адрес клиента (Client Hardware Address) (Chaddr)	Аппаратный адрес клиента
Имя сервера (Server Host Name) (Sname)	64-байтное поле, зарезервированное для имени узла сервера. Не используется в Windows XP и Windows Server 2003
Имя файла загрузки (Boot File Name) (File)	Имя файла, содержащего образ загрузки для клиентов протокола BOOTP (Boot Protocol)
Параметры (Options)	Набор полей переменной длины, соответствующих параметрам DHCP. Параметр **Option 53** должен присутствовать в каждом сообщении, так как определяет тип сообщения. Другие часто используемые параметры: **Интервал обновления аренды (Lease Renewal Time)** и **Интервал повторной привязки аренды (Lease Rebinding Time)**

Сообщение DHCP Discover. Ниже приведен отрывок записи, сделанной с помощью утилиты *Сетевой монитор* (Network Monitor), в котором показаны относящиеся к IP и DHCP части пакета DHCP, Discover. В разделе IP видны адрес назначения 255.255.255.255 (широковещание) и адрес источника 0.0.0.0. Раздел DHCP определяет пакет как сообщение Discover и в двух местах идентифицирует клиента, указывая физический адрес сетевого адаптера: значения полей Client Ethernet Address (Chaddr) и DHCP: Client Identifier идентичны.

```
IP: ID = 0x0; Proto = UDP; Len: 328
    IP: Version = 4 (0x4)
    IP: Header Length = 20 (0x14)
    IP: Service Type = 0 (0x0)
        IP: Precedence = Routine
        IP: ...0____'= Normal Delay
        IP: ....0... = Normal Throughput
        IP;. . . . .0.. = Normal Reliability
    IP: Total Length = 328 (0x148)
    IP: Identification = 0 (0x0)
    IP: Flags Summary = 0 (0x0)
        IP:. . . . . .0 = Last fragment in datagram
        IP:. . . . . .0.= May fragment datagram if necessary
    IP: Fragment Offset = 0 (0x0) bytes
    IP: Time to Live = 128 (0x80)
    IP: Protocol = UDP - User Datagram
    IP: Checksum = Ox33A6
    IP: Source Address = 0.0.0.0
    IP: Destination Address = 255.255.255.255
    IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: Discover                (xid=21274A1D)
    DHCP: Op Code             (op)     = 1 (0x1)
    DHCP: Hardware Type       (htype)  = 1 (0x1) 10Mb Ethernet
    DHCP: Hardware Address Length (hlen) = 6 (0x6)
    DHCP: Hops                (hops)   = 0 (0x0)
    DHCP: Transaction ID      (xid)    = 556223005 (0x21274A1D)
    DHCP: Seconds             (sees)   = 0 (0x0)  •
    DHCP: Flags               (flags)  = 0 (0x0)
        DHCP: 0. . . . . .= No Broadcast
    DHCP: Client IP Address (ciaddr) = 0.0.0.0
    DHCP: Your IP Address (yiaddr) = 0.0.0.0
    DHCP: Server IP Address (siaddr) =0.0.0.0
    DHCP: Relay IP Address (giaddr) = 0.0.0.0
    DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
    DHCP: Server Host Name (sname) = <Blank>
    DHCP: Boot File Name (file) = <Blank>
    DHCP: Magic Cookie = [OK]
    DHCP: Option Field (options)
        DHCP: DHCP Message Type = DHCP Discover
```

```
      DHCP: Client-identifier = (Type: 1) 08 00 2b 2e d8 5e
      DHCP: Host Name = CLIENT1
      DHCP: Parameter'Request. List = (Length-: 7) 01 Of 03 2c 2e 2f 06
      DHCP: End of this option field
```

Сообщение DHCP Offer. В IP-разделе в качестве адреса источника теперь выступает IP-адрес DHCP-сервера, а адрес назначения — широковещательный (255.255.255.255). В разделе DHCP пакет определяется как сообщение-предложение. В DHCP-поле Your IP Address (Yiaddr) указан IP-адрес сервера, предлагающего аренду клиенту. Обратите внимание, что поле DHCP: Client Ethernet Address (Chaddr) все еще содержит физический адрес клиента. Кроме того, в поле DHCP Option представлены различные параметры, пересылаемые сервером вместе с IP-адресом: маска подсети, стандартный шлюз (маршрутизатор), срок аренды, адрес WINS-сервера и тип NetBIOS-узла.

```
IP: ID = Ox3C3O; Proto = UDP; Len: 328
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Service Type = 0 (0x0)
      IP: Precedence = Routine
      IP: . . ,0____= Normal Delay
      IP: ....0... = Normal Throughput
      IP:. . . .0.. = Normal Reliability
   IP: Jotal Length' = 328 (0x148)
   IP: Identification = 15408 (Ox3C3O)
   IP: Flags Summary = 0 (0x0)
      IP:. . . . . .0 = Last fragment in datagram
      IP:. . . . .0. = May fragment datagram if necessary
   IP: Fragment Offset = 0 (0x0) bytes
   IP: Time to Live = 128 (0x80)
   IP: Protocol = UDP - User Datagram
   IP: Checksum = 0x2FA8
   IP: Source Address = 10.54.48.151
   IP: Destination Address = 255.255.25 5.255
   IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: Offer (xid=21274ATD)
   DHCP: Op Code (op) = 2 (0x2)
   DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
   DHCP: Hardware Address Length (hlen) = 6 (0x6)
   DHCP: Hops (hops) = 0 (0x0)
   DHCP: Transaction ID (xid) =556223005 (0x21274A1D)
   DHCP: Seconds (sees) = 0 (0x0) .
   DHCP: Flags (flags) = 0 (0x0)
      DHCP: 0. . . . . .= No Broadcast
   DHCP: Client IP Address (ciaddr) = 0.0.0.0
   DHCP: Your IP Address (yiaddr) = 10.54.50.5
   DHCP: Server IP Address (siaddr) = 0.0.0.0
   DHCP: Relay IP Address (giaddr) =0.0.0.0
   DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
```

```
DHCP: Server Host Name (sname) = <Blank>
DHCP: Boot File Name (file) = <Blank>
DHCP: Magic Cookie = [OK]
DHCP: Option Field (options) ..
   DHCP: DHCP Message Type = DHCP Offer
   DHCP: Subnet Mask = 255.255.240.0
   DHCP: Renewal'Time Value (T1) = 8 Days, 0:00:00
   DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
   DHCP: IP Address Lease Time = 16 Days, 0:00:00
   DHCP: Server Identifiers 10.54.48.151
   DHCP: Router = 10.54.48.T
   DHCP: NetBIOS Name Service = 10.54.16.154
   DHCP: NetBIOS Node Type = (Length: 1) 04
   DHCP: End of this option field
```

Сообщение-запрос DHCP Request. Клиент отвечает на пакет DHCP Offer отправкой сообщения DHCP Request. В разделе IP нижеследующей записи адрес источника клиента все еще 0.0.0.0, а адрес назначения пакета — 255.255.255.255. Адрес клиента нулевой, поскольку он ещё не получил подтверждение от сервера и не вправе использовать предложенный адрес. Адрес назначения остался широковещательным, поскольку клиенту может ответить и зарезервировать адрес не один DHCP-сервер.

Широковещательная рассылка одного конкретного запрошенного адреса позволяет остальным откликнувшимся DHCP-серверам освободить предложенные адреса и вернуть их в пул доступных адресов. Раздел DHCP идентифицирует пакет как запрос и подтверждает предложенный адрес, указывая его в поле DHCP: Requested Address. Поле DHCP: Server Identifier в области DHCP: Option содержит IP-адрес DHCP-сервера, предложившего аренду.

```
IP: ID = 0x100; Proto = UDP; Len: 328
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Service Type = 0 (0x0)
      IP: Precedence = Routine
      IP: ...0_____= Normal Delay
      IP: ....0... =.Normal Throughput
      IP:. . . .0.. = Normal Reliability
   IP: Total Length = 328 (0x148)
   IP: Identification = 256 (0x100)
   IP: Flags Summary = 0 (0x0)
      IP:. . . . . .0 = Last fragment in datagram
      IP:. . . . . .0. = May fragment datagram if necessary
   IP: Fragment Offset = 0 (0x0) bytes
   IP: Time to Live = 128 (0x80)
   IP: Protocol = UDP - User Datagram
   IP: Checksum = 0x38A6
   IP: Source Address =0.0.0.0
   IP: Destination Address = 255.255.255.255
   IP: Data: Number of data bytes remaining = 308 (0x0134)
```

```
DHCP: Request (xid=21274A1D)
    DHCP: Op Code (op) = 1 (0x1)
    DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
    DHCP: Hardware Address Length (hlen) = 6 (0x6)
    DHCP: Hops (hops) = 0 (0x0)
    DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
    DHCP: Seconds (sees) = 0 (0x0)
    DHCP: Flags (flags) = 0 (0x0)
        DHCP: 0. . . . . .= No Broadcast
    DHCP: Client IP Address (ciaddr) = 0.0.0.0
    DHCP: Your IP Address (yiaddr) = 0.0.0.0
    DHCP: Server IP Address (siaddr) = 0.0.0.0
    DHCP: Relay IP Address (giaddr) = 0.0.0.0
    DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
    DHCP: Server Host Name (sname) = <Blank>
    DHCP: Boot File Name (file) = <Blank>
    DHCP: Magic Cookie = [OK]
    DHCP: Option Field (options) •
        DHCP: DHCP Message Type = DHCP Request
        DHCP: Client Identifier = (Type: 1) 08 00 2b 2e d8 5e
        DHCP: Requested Address = 10.54.50.5
        DHCP: Server Identifier = 10.54.48.151
        DHCP: Host Name = CLIENT1
        DHCP: Dynamic DNS updates = (Length: 26) 00 00 00 63 6f 6d ...
        DHCP: Client Class information = (Length: 8) 4d 53 46 54 20 35 2e 30
        DHCP: Parameter Request List = (Length: 7) 01 Of 03 2c 2e 2f 06
        DHCP: End of this option field
```

Если у клиента до этого был присвоенный DHCP-сервером адрес, при перезапуске он в первую очередь запрашивает аренду именно этого адреса пакетом DHCP Request. Клиенты Microsoft указывают в поле DHCP: Requested Address ранее назначенный адрес. Строго поддерживающие спецификацию RFC клиенты указывают в поле DHCP: Client IP Address (Ciaddr) запрашиваемый адрес. DHCP-сервер принимает любой из этих адресов. Если сервер считает, что клиент вправе продолжить использование адреса, он либо не отвечает вовсе, либо отправляет сообщение ACK или DHCP Request. Если же использование указанного адреса невозможно, сервер отвечает сообщением NACK.

Подготовка к экзамену DHCP Request — это сообщение с запросом динамического обновления у DHCP-сервера. Обычно в сообщении-запросе указывается полное доменное имя (FQDN) клиента, что позволяет DHCP-серверу также обновить соответствующую клиенту запись ресурса **PTR.**

Сообщение DHCP ACK. DHCP-сервер обычно отвечает на сообщение-запрос DHCP Request подтверждением DHCP ACK, которое завершает цикл получения аренды. Это сообщение содержит IP-адрес, предоставляемый клиенту на установленный срок, а также другие параметры.

Адрес источника в следующей ниже записи — это IP-адрес DHCP-сервера, а адрес назначения все еще 255.255.255.255. В разделе DHCP определен тип пакета: ACK. Поле

DHCP: Your IP Address (Yiaddr) содержит адрес клиента, а поле **DHCP:** Client Ethernet Address **(Chaddr)** — физический адрес сетевой карты клиента, отправившего запрос.

```
IP: ID = 0x3030; Proto = UDP; Len: 328
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Service Type = 0 (0x0)
      IP: Precedence = Routine
      IP: ...0_____= Normal Delay
    ' IP: ...,0... = Normal Throughput
      IP:. . . .0.. = Normal Reliability
   IP: Total Length = 328 (0x148)
   IP: Identification = 15664 (0x3D30)
   IP: Flags Summary = 0 (0x0)
      IP:. . . . . .0 = Last fragment in datagram
      IP:. . . . . .0. = May fragmentd datagram if necessary
   IP: Fragment Offset = 0 (0x0) bytes
   IP: Time to Live = 128 (0x80)
   IP: Protocol = UDP - User Datagram
   IP: Checksum = 0x2EA8
   IP: Source Address = 10. 54.48.151
   IP: Destination Address = 255. 255.^255. 255
   IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: ACK (xid=21274A1D)
   DHCP: Op Code (op) = 2 (0x2)
   DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
   DHCP: Hardware Address Length (hlen) = 6 (0x6)
   DHCP: Hops (hops) = 0 (0x0)
   DHCP: Transaction ID (xid) = 556223005 (0x21274A1D)
   DHCP: Seconds (sees) = 0 (0x0)
   DHCP: Flags (flags) = 0 (0x0)
      DHCP: 0. . . . . .= No Broadcast
   DHCP: Client IP Address (ciaddr) = 0.0.0.0
   DHCP: Your IP Address (yiaddr) = 10.54.50.5
  ' DHCP: Server IP Address (siaddr) =0.0.0.0 •
   DHCP: Relay IP Address (giaddr) = 0.0.0.0
   DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
   DHCP: Server Host Name (sname) = <Blank>
   DHCP: Boot File Name (file) = <Blank>
   DHCP: Magic Cookie = [OK]
   DHCP: Option Field (options)
      DHCP: DHCP Message Type = DHCP ACK
      DHCP: Renewal Time Value (T1) =8 Days, 0:00:00
      DHCP: Rebinding Time Value (T2) = 14 Days, 0:00:00
      DHCP: IP Address Lease Time = 16 Days, 0:00:00
      DHCP: Server Identifier = 10.54.48.151
      DHCP: Subnet Mask = 255.255.240.0
```

```
      DHCP; Router = 10.54,48.1
      DHCP: NetBIOS Name Service = 10.54.16.154
      DHCP: NetBIOS Node Type = (Length: 1) 04
      DHCP: End of this option field
```

Сообщение-отказ DHCP NACK. Чаще всего такое сообщение клиент получает при физическом перемещении в другую сеть, однако оно может также указывать на окончание срока аренды адреса. Вот листинг сообщения.

```
IP: ID = 0x3F1A; Proto = UDP; Len: 328
   IP: Version = 4 (0x4)
   IP: Header Length = 20 (0x14)
   IP: Service Type = 0 (0x0)
      IP: Precedence = Routine
      IP: ...0____= Normal Delay                                    -    •
      IP: ....0... = Normal Throughput
      IP: .....0.. = Normal Reliability
   IP: Total Length = 328 (0x148)
   IP: Identification = 16154 (0x3F1A)
   IP: Flags Summary = 0 (0x0)
      IP:. . . . . .0 = Last fragment in datagram
      IP:. . . . . .0. = May fragment datagram if necessary
   IP: Fragment Offset = 0 (0x0) bytes
   IP: Time to Live = 128 (0x80)
   IP: Protocol = UDP - User Datagram
   IP: Checksum = 0x2CBE
   IP: Source Address = 10.54.48.151
   IP: Destination Address = 255.255.255.255
   IP: Data: Number of data bytes remaining = 308 (0x0134)

DHCP: NACK (xid=74A005CE)
   DHCP: Op Code (op) = 2 (0x2)
   DHCP: Hardware Type (htype) = 1 (0x1) 10Mb Ethernet
   DHCP: Hardware Address Length (hlen) = 6 (0x6)
   DHCP: Hops (hops) = 0 (0x0)
   DHCP: Transaction ID (xid) = 1956644302 (0x74A005CE)
   DHCP: Seconds (sees) = 0 (0x0) /
   DHCP: Flags (flags) = 0 (0x0)
      DHCP: 0. . . . . .= No Broadcast
   DHCP: Client IP Address (ciaddr) = 0.0.0.0
   DHCP: Your IP Address (yiaddr) = 0.0.0.0
•  DHCP: Server IP Address (siaddr) = 0.0.0.0
   DHCP: Relay IP Address (giaddr) = 0.0.0.0
   DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
   DHCP: Server Host Name (sname) = <Blank>
   DHCP: Boot File Name (file) = <Blank>
   DHCP: Magic Cookie = [OK]
   DHCP: Option Field (options)
```

```
DHCP: DHCP Message Type = DHCP NACK
DHCP: Server Identifier = 10.54.48.151
DHCP: End of this option field
```

Получив NACK, клиент начинает процесс получения аренды с самого начала. Однако на этот раз выполняется попытка получить в аренду тот же адрес, в котором ему только что было отказано (см. поле DHCP: Requested Address в приведенном ниже сообщении DHCP Discover). В ответном сообщении DHCP Offer сервер предлагает адрес, который не обязательно совпадает с запрошенным.

```
DHCP: Discover (xid=3ED14752)
   DHCP: Op Code (op) = 1 (0x1)                              \
   DHCP: Hardware Type (htype)= 1 (0x1) 10Mb Ethernet
   DHCP: Hardware Address Length (hlen) = 6 (0x6)
   DHCP: Hops (hops) = 0 (0x0)
   DHCP: Transaction ID (xid) = 1053902674 (0x3ED14752)
   DHCP: Seconds (sees) = 0 (0x0)
   DHCP: Flags (flags) = 0 (0x0)
      DHCP: 0.............= No Broadcast
   DHCP: Client IP Address (ciaddr) = 0.0.0.0,
   DHCP: Your IP Address (yiaddr) = 0.0.0.0
   DHCP: Server IP Address (siaddr) = 0.0.0.0  .
   DHCP: Relay IP Address (giaddr) = 0.0.0.0
   DHCP: Client Ethernet Address (chaddr) = 08002B2ED85E
   DHCP: 'Server Host, Name (sname) = <Blank>
   DHCP: Boot File Name (file) = <Blank>
   DHCP: Magic Cookie = [OK]
   DHCP: Option Field (options)
      DHCP: DHCP Message Type = DHCP Discover
      DHCP: Client Identifier = (Type: 1) 08 00 2b 2e d8 5e
      DHCP: Requested Address = 10.54.51.5
      DHCP: Host Name = CLIENT1
      DHCP: Parameter Request List = (Length: 7) 01 Of 03 2c 2e 2f 06
      DHCP: End of this, option field
```

Лабораторная работа. **Анализ DHCP-сообщений**

Вы проанализируете трафик как первичной, так и обновления DHCP-аренды.

Упражнение 1. Запись трафика первичной аренды

Вы освободите, а затем обновите IP-конфигурацию Computer2, запишете *Сетевым монитором* (Network Monitor), а затем изучите результаты.

1. На Computerl войдите в систему как *Администратор* (Administrator) в домене *Domain 1.*
2. Откройте окно **Сетевой монитор (Network Monitor)** и запустите запись, щелкнув кнопку **Начать запись данных (Start Capture).**
3. На Computer2 войдите в систему как *Администратор* (Administrator) в домене Domain 1.
4. Из командной строки исполните команду ipconfig /release. Через несколько секунд появится сообщение, что IP-адрес компьютера теперь *0.0.0.0.* Computer2 больше не подключен к сети.

5. Выполните команду ipconfig /renew.
6. Дождавшись отчета, остановите запись в окне **Сетевой монитор (Network Monitor)** на Computed, щелкнув кнопку **Закончить запись и отобразить данные (Stop and View Capture).**
7. **В** меню **Отображение (Display)** выберите **Фильтр (Filter).**
8. В открывшемся окне **Фильтр отображения (Display Filter)** дважды щелкните выражение **Protocol==Any.**
9. **В** окне **Выражение (Expression)** щелкните **Отключить все (Disable All).** Все протоколы переместятся в область **Отключенные протоколы (Disabled Protocols).**
10. **В** области **Отключенные протоколы** найдите и дважды щелкните протокол **DHCP.** Протокол DHCP переместится в область **Включенные протоколы (Enabled Protocols).** Щелкните OK.
11. В диалоговом окне **Фильтр отображения (Display Filter)** щелкните OK. Теперь в окне **Запись данных (Frame Viewer)** в окне **Сетевой монитор** отображаются только пять DHCP-кадров.
12. Сохраните запись в папке **Мои записи (My Captures)** под именем *DHCP Lease Initialization*. Не забудьте установить флажок **Фильтр (Filtered)** в окне **Сохранить как (Save As).**
13. Закройте окно **Сетевой монитор.**

Упражнение 2. Анализ записи первичной аренды

Вы проанализируете пять DHCP-кадров в файле записи *DHCP Lease Initialization.*

1. На Computerl войдите в систему как *Администратор* в домене Domain 1. В папке **Мои записи (My Captures)** дважды щелкните файл **DHCP Lease Initialization.** Запись откроется в окне **Сетевой монитор (Network Monitor).**
2. Ответьте на следующие вопросы.
   a. Как называются пять DHCP-сообщений? Запишите по порядку их названия, указанные в поле описания кадров.
   b. Какое из сообщений не является широковещательным? Почему?
   c. Из каких DHCP-сообщений состоит процесс получения первичной аренды?
   d. Изучите поле Options DHCP-сообщений. Какие два DHCP-сообщения включают параметры Domain Name, Router и Domain Name Server?
   e. Какой UDP-порт указывается как порт источника при отправке информации от DHCP-клиента и как порт назначения при получении информации DHCP-клиентом?
   f. Какой UDP-порт используется как порт источника при отправке информации от DHCP-сервера и как порт назначения при получении информации DHCP-сервером?
   g. Какое единственное из пяти DHCP-сообщений содержит раздел Dynamic DNS Updates в поле Options?
3. Выберите в этом сообщении раздел **Dynamic DNS Updates.** (Этот раздел можно увидеть в центральной панели, если раскрыть узел **DHCP Options.)** Данные, соответствующие разделу, при этом выделяются в нижней шестнадцатеричной панели.
4. Ответьте на следующие вопросы.

   Какая информация содержится в разделе **Dynamic DNS Updates?**

   Какую запись ресурса обновит DHCP-сервер на основе этой информации?
5. Закройте окно **Сетевой монитор.**

Упражнение 3. Запись трафика обновления аренды DHCP

Вы запишете трафик обновления аренды DHCP.

1. На Computerl войдите в систему как *Администратор* в домене Domainl.
2. Откройте окно **Сетевой монитор (Network Monitor)** и запустите запись, щелкнув кнопку **Начать запись данных (Start Capture).**
3. Перейдите к Computer2 и при необходимости войдите в систему под учетной записью *Администратор* (Administrator) домена Domainl.
4. Из командной строки исполните команду ipconfig /renew. Через несколько мгновений на экране появится информация об обновленной IP-конфигурации.
5. На Computerl в окне **Сетевой монитор** остановите запись, щелкнув кнопку **Закончить запись и отобразить данные (Stop And View Capture).**
6. Следуя указаниям из упражнения 1, задайте фильтр на отображение только DHCP-сообщений.
7. Сохраните запись в папке **Мои записи (My Captures)** под именем *DHCP Lease Renewal.* Не забудьте установить флажок **Фильтр (Filtered)** в окне **Сохранить как (Save As).**
8. Закройте **Сетевой монитор.**

Упражнение 4, Анализ записи обновления аренды

Вы проанализируете кадры, записанные в файле *DHCP Lease Renewal.*

1. Войдя в систему Computerl под учетной записью *Администратор* (Administrator) домена Domainl, дважды щелкните файл **DHCP Lease Renewal** в папке **Мои записи (My Captures).** Запись откроется в окне **Сетевой монитор (Network Monitor).**
2. Ответьте на следующие вопросы.
   a. Из скольких сообщений состоит процесс обновления аренды DHCP?
   b. Как называются записанные DHCP-сообщения? Запишите их по порядку в соответствии с информацией в поля описания кадров.
   c. Чем отличается набор этих сообщений и сообщений первичной аренды?
3. В обоих записанных кадрах найдите поля **Client IP Address** и **Your IP Address** и ответьте на следующие вопросы.
   a. При обновлении аренды запрашивает ли DHCP-клиент обновление конкретного IP-адреса?
   b. Какое конкретно поле какого DHCP-сообщения обновляет DHCP-параметы конфигурации клиента?
4. Закройте окно **Сетевой монитор.**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы развернули в подсети два DHCP-сервера — DHCP1 и DHCP2. Первый обслуживает адреса первых 80 % всего диапазона адресов области, а второй — остальные 20% диапазона. Компьютер ClientA получает свежий адрес от DHCP1, после чего DHCP1 немедленно отключается. Сколько времени пройдет, прежде чем ClientA попытается подучить новый адрес от DHCP2?

   a. 4 дня.

   ь. 5 дней.

c. 7 дней.
d. 8 дней.

2. Какое из следующих сообщений не используется в процессе получения первичной аренды DHCP?
   a. Renew.
   b. Request.
   c. ACK.
   d. Discover.
3. Какие два сообщения участвуют в процессе обновления аренды DHCP?
4. По истечении какого времени DHCP-клиент пытается обновить аренду IP-адреса?

Резюме

- Процесс получения первичной аренды адреса DHCP-клиент инициирует при первом подключении к сети. Он заключается в обмене четырьмя широковещательными сообщениями.
- Сначала DHCP-клиент пытается обнаружить DHCP-сервер в локальной сети, рассылая широковещательное сообщение DHCP Discover.
- Получив сообщение Discover, DHCP-сервер обычно отвечает широковещательным сообщением DHCP Offer с IP-адресом, предлагаемым клиенту.
- DHCP-клиент отвечает на DHCP Offer сообщением DHCP Request, содержащим запрос предложенного IP-адреса.
- Наконец, предложивший адрес сервер рассылает широковещательное сообщение DHCP ACK, которое подтверждает аренду адреса и сообщает клиенту параметры DHCP.

Занятие 2. Мониторинг DHCP с применением журнала аудита

По умолчанию работа DHCP-сервера регистрируется и ежедневно записывается в текстовый файл. Это называется *ведением журнала аудита* и позволяет наблюдать за работой DHCP-сервера и устранять его неполадки.

Изучив материал этого занятия, вы сможете:

- *S* находить и анализировать файлы журнала аудита в Windows Server 2003;
- *S* диагностировать и устранять неполадки авторизации в DHCP.

Продолжительность занятия — около 20 минут.

Ведение журнала аудита DHCP

По умолчанию служба DHCP-сервера ежедневно записывает файлы журнала аудита в папку *Windows\System32\Dhcp.* Они представляют собой текстовые файлы, в названии которых присутствуют названия дней недели. Например, *DhcpSrvLog-Mon* — файл журнала с информацией о деятельность DHCP-сервера в понедельник в период между 00:00 и 23:59, а в *DhcpSrvLog-Tue* — файл за вторник и т.д. Файлы журнала аудита обычно через неделю замещаются новыми с теми же именами.

Местоположение этих файлов можно изменить на вкладке **Другие (Advanced)** диалогового окна свойств DHCP-сервера (рис. 8-3), указав новый путь в поле **Журнал аудита (Audit Log File Path).**

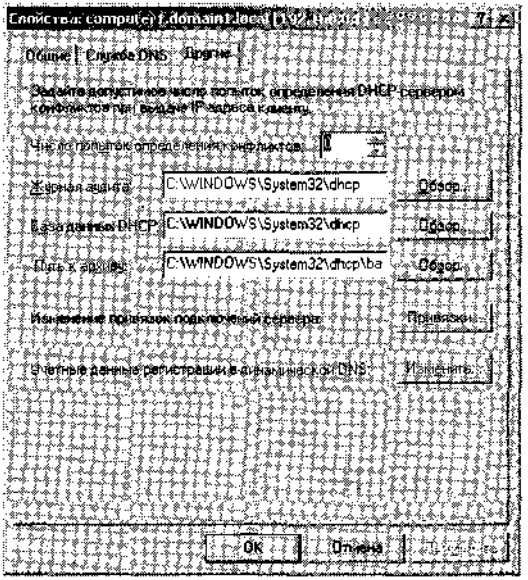


Рис. 8-3. Изменение расположения журнала аудита

Вкладка **Общие (General)** диалогового окна свойств DHCP-сервера в консоли *DHCP* позволяет полностью отключить ведение журнала аудита (рис. 8-4). Для этого нужно сбросить установленный по умолчанию флажок **Вести журнал аудита DHCP (Enable DHCP Audit Logging).**

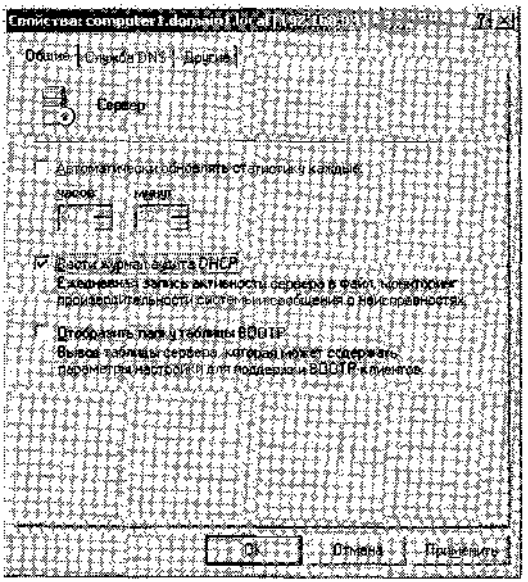


Рис. 8-4. Отключение ведения журнала аудита

По умолчанию максимальный размер текущего файла журнала аудита не превышает 1 Мб, а при сокращении свободного места на диске сервера до 20 Мб ведение журнала аудита прекращается и возобновляется при появлении свободного места.

Формат файла журнала аудита DHCP-сервера

Журналы DHCP-сервера — это текстовые файлы в формате с разделяющими запятыми, где каждая запись журнала представляет собой одну текстовую строку (рис. 8-5).

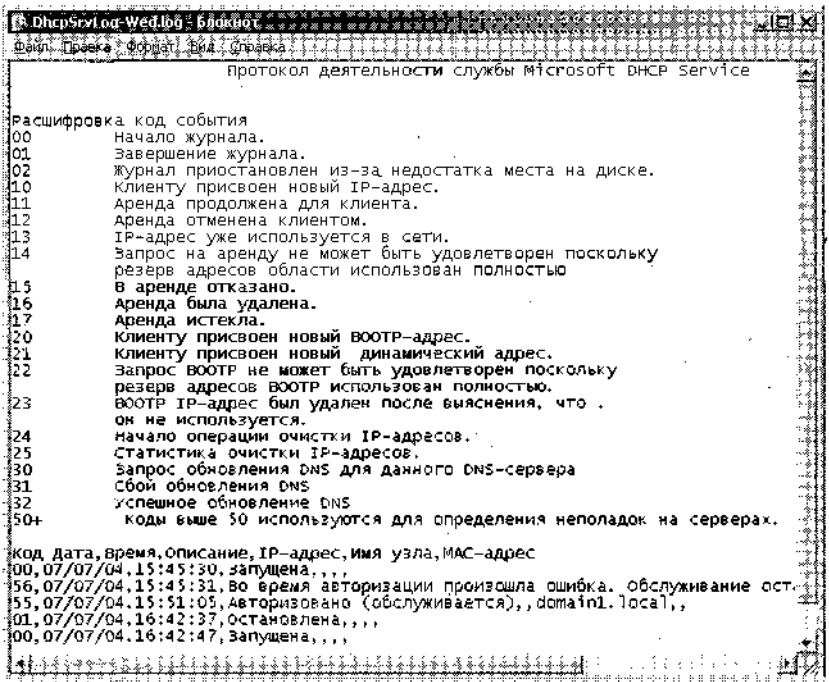


Рис. 8-5. Пример файла журнала аудита DHCP

Запись журнала содержит следующие поля: **Код (ID), Дата (Date), Время (Time), Описание (Description), IP-адрес (IP Address), Имя узла (Host Name)** и **MAC-адрес (MAC Address).** Все поля отделяются запятыми, в том числе и пустые. Например, в следующей записи две запятых подряд означают, что поля **IP-адрес** и **MAC-адрес** пусты.

```
55,06/03/03,09:08:57,Authorized(servicing), ,domain1. local, ,
```

В табл. 8-2 разъясняется значение полей журнала DHCP-сервера.

Табл. 8-2. Поля журнала DHCP-сервера

Поле	Описание
Код (ID)	Код события DHCP-сервера
Дата (Date)	Дата записи события в журнал DHCP-сервера
Время (Time)	Время записи события в журнал DHCP-сервера
Описание (Description)	Описание события DHCP-сервера
IP-адрес (IP Address)	IP-адрес DHCP-клиента
Имя узла (Host Name)	Имя узла DHCP-клиента
MAC-адрес (MAC Address)	Аппаратный MAC-адрес сетевого адаптера клиента

Коды стандартных событий

В журналах DHCP-сервера используются зарезервированные коды событий для информирования о типе события сервера или записываемой операции. События с кодами меньше 50 описаны в самом файле журнала, поэтому запоминать их нет никакой необходимости.

События авторизации сервера

В табл. 8-3 представлены коды и описания дополнительных кодов событий сервера. Эти коды отражают авторизацию DHCP-сервера при его развертывании в среде Active Directory. В отличие от ранее упоминавшихся, эти события не описаны в файле журнала, поэтому стоит запомнить коды этих событийлибо пользоваться справочной системой Windows Server 2003.

Табл. 8-3. События с кодами от 50 и выше

Код события	Описание
50	*Недостижимый домен.* DHCP-серверу не удается обнаружить домен, указанный в установке Active Directory
51	*Успешная авторизация.* DHCP-серверу разрешена работа в сети
52	*Операционная система обновлена до Windows Server 2003.* DHCP-сервер обновлен до Windows Server 2003 Standard Edition, поэтому функция выявления неавторизованного DHCP-сервера (используется для определения, был ли сервер авторизован в Active Directory) отключена
53	*Авторизация с кэшированными данными.* DHCP-сервер прошел авторизацию и использует ранее кэшированную информацию. На момент запуска сервера в сети Active Directory была недоступна
54	*Сбой авторизации.* DHCP-сервер не прошел авторизацию для работы в сети. После такого события сервер скорее всего останавливается
55	*Авторизация (обслуживание).* DHCP-сервер успешно прошел авторизацию для работы в сети
56	*Ошибка авторизации, обслуживание остановлено.* DHCP-сервер не прошел авторизацию для работы в сети и остановлен ОС Windows Server 2003. Необходимо авторизовать сервер в каталоге, а затем перезапустить
57	*В домене найден сервер.* Другой DHCP-сервер существует и авторизован для работы в текущем домене Active Directory
58	*Сервер не смог найти домен.* DHCP-сервер не смог обнаружить указанный домен Active Directory
59	*Сбой сети.* Ошибка в сети не позволяет серверу определить свое состояние: авторизован или нет
60	*Нет контроллера домена, поддерживающего службы каталога.* Не обнаружен контроллер домена (DC) Active Directory. Чтобы определения состояния авторизации сервера необходим контроллер домена, поддерживающий Active Directory
61	*Обнаружен сервер, принадлежащий к домену служб каталога (DS).* В сети найден другой сервер, принадлежащий к домену Active Directory.
62	*Обнаружен другой сервер.* В сети обнаружен другой DHCP-сервер

Табл. 8-3. *(окончание)*

Код события	Описание
63	*Перезапуск случайной проверки.* DHCP-сервер повторно пытается определить, был ли он авторизован для запуска и предоставления обслуживания в сети
64	*Отсутствуют интерфейсы, поддерживающие DHCP.* Привязки службы DHCP-сервера или его подключения настроены так, что не позволяют обеспечивать обслуживание. Обычно это происходит потому, что: • сетевые подключения сервера не установлены или неактивны; • не настроен хотя бы один статический IP-адрес для одного из установленных и активных сетевых подключений; • все статически настроенные сетевые подключения сервера отключены.

Фрагмент образца журнала аудита DHCP-сервера

В данном фрагменте записаны события обычного, без ошибок запуска и авторизации DHCP-сервера. Первые два события соответствуют успешной авторизации при запуске, а последние два соответствуют периодической ежечасной очистке базы данных DHCP.

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address
00,06/03/03,09:08:57,Started,
55, 06/03/03, 09:08:57, Authorized(servicing), ,domain2. local,-,
11,06/03/ 03,09:48:25,Renew,192.168.0.11,server2. domain2.local,0003FFBC3B46,
24,06/03/ 03,10:08:58,Database Cleanup Begin,,,,
25,06/03/ 03,10:08:58,0 leases expired and 0 leases deleted,,,,
```

В следующем фрагменте DHCP-серверу не удалось авторизоваться при запуске. Такая ситуация- может возникнуть при установке нового сервера. В этом примере DHCP-сервер авторизуется в Active Directory через 10 минут после запуска и уже после начинает обслуживать клиентов.

```
ID,Date,Time,Description,IP Address,Host Name,MAC Address
00,06/08/03,22:35:10,Started,
56,06/08/03,22:35:10,Authorization failure, stopped
servicing,,domainl.local,,
55,06/08/03,22:45:38,Authorized(servicing),,domainl.local,,
```

Совет Когда DHCP-сервер прекращает предоставлять адреса в аренду клиентам, нужно всегда в первую очередь проверить журнал на предмет сбоя авторизации.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. С понедельника стало невозможно получить эхо-ответ Ping от некоторых сетевых клиентов. В журнале DHCP-сервера за понедельник обнаружилась следующая запись:

```
54,6/09/ 03,06:47:29,Authorization failed,,domainl.local,,
```

Какая операция скорее всего стала источником неполадок? Кто ее выполнил? (Предполагается, что до сбоя авторизации в журнале нет никаких сообщений о неполадках DHCP-сервера.)

2. Каковы наиболее вероятные причины ошибки, описанной в следующей записи журнала аудита DHCP?

   00,5/24/03,08:21:57,Started,
   54,5/24/ 03,08:21:58,Authorization failed,,domainl.local,,

   a. Сервер запускается в первый раз.
   b. Сервер не может подключиться к сети.
   c. Администратор сети отменил авторизацию сервера.
   d. Сервер работает под управлением ОС, отличной от Windows Server 2003.

3. Как долго по умолчанию сохраняются записанные события в журналах DHCP-сервера?
   a. 1 день.
   b. 1 неделю.
   c. 1 месяц.
   d. Пока размер журнала не превысит 1 Мб.

Резюме

- Функция ведения журнала аудита используется для ежедневной записи действий DHCP-сервера в текстовые файлы в формате с разделяющими запятыми. По умолчанию файлы журнала DHCP-сервера располагаются в папке *Wmdows\Sysiem32\Dhcp*.
- Файлы журнала DHCP-сервера содержат название дня недели, в который он записывается, например *DhcpSrvLog-Mon* (понедельник) и *DhcpSrvLog-Tue* (вторник). Каждую неделю файлы перезаписываются.
- События в файлах журнала DHCP-сервера определяются кодом события. События с кодами меньше 50 описываются в самом файле журнала, поэтому их не нужно запоминать. События с кодами от 50 и выше относятся к состоянию авторизации Active Directory. Нужно либо запомнить эти события, либо узнавать их значения в справочной системе ОС.
- Когда DHCP-сервер перестает выделять адреса в аренду клиентам, нужно всегда в первую очередь проверить в журнале DHCP, не произошел ли сбой авторизации или неполадки.

Занятие 3. **Устранение неполадок DHCP**

Здесь представлены последовательности операций по устранению неполадок DHCP-сервера. Как и в большинстве подобных руководств, порядок рекомендуемых процедур изменяют в соответствии с конкретной ситуацией. Тем не менее, описанные в этом занятии схемы наверняка будут полезны в будущем для организации устранения неполадок DHCP.

Изучив материал этого занятия, вы сможете:

диагностировать ошибки настройки DHCP;
устранять неполадки авторизации в DHCP;
устранять неполадки, обусловленные неправильной настройкой областей.

Продолжительность занятия — около 45 минут.

Проверка настройки клиента

Один из первых сигналов отказа DHCP — потеря связи с ресурсами сети или неспособность новых клиентов подключиться к сети. В таких случаях нужно выяснить, обусловлена ли проблема неполадками на самом клиенте или в сети.

Начните с команды Ipconfig, чтобы выяснить, получил ли DHCP-клиент адрес в аренду. Если да, то в листинге работы команды Ipconfig /all должна присутствовать информация о нормальной работе DHCP, а IP-адрес должен описываться как **IP-адрес (IP Address),** а не **IP-адрес автонастройки (Autoconfiguration IP Address).** Есть еще способ: проверить тип адреса на вкладке **Поддержка (Support)** диалогового окна состояния подключения (рис. 8-6). Это окно можно открыть, дважды щелкнув соответствующее подключение в папке **Сетевые подключения (Network Connections).** Когда IP-адрес присваивается DHCP-сервером, на вкладке **Поддержка (Support)** он помечается, как **Присвоен DHCP (Assigned By DHCP).**

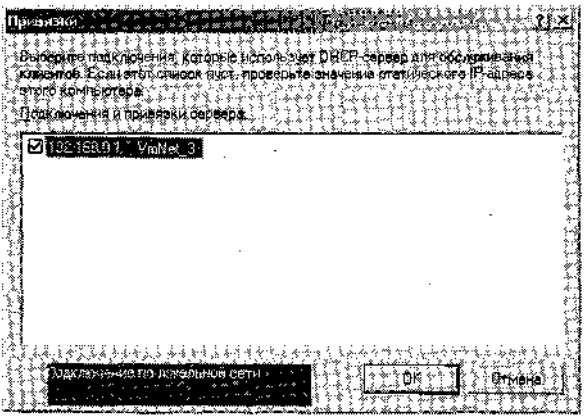


Рис. 8-6. Проверка типа адреса

Если клиент получил от DHCP-сервера адрес, разрешенный в данной сети, и не появилось никаких предупреждающих сообщений о конфликте адресов, следует думать, что неполадки не связаны с ошибкой адресации локального клиента.

Конфликты адресов

Если клиентский компьютер получил адрес, который уже используется другим компьютером данной сети, на системной панели появится предупреждение о конфликте адресов. Информация о конфликте также есть в журнале **Система (System)** в окне **Просмотр событий (Event Viewer)** (рис. 8-7).

Если при получении предупреждающего сообщения о конфликте адресов установлено.- что клиент получил IP-адрес от DHCP-сервера, конфликт может быть признаком конкуренции DHCP-серверов или реорганизации DHCP-областей. .

Обнаружить конкуренцию DHCP-серверов позволяет утилита Dhcpioc.exe из Состава *Средств поддержки Windows* (Windows Support Tools). Она находит в сети неавторизованные DHCP-серверь/. После удаления таких серверов надо позаботиться, чтобы оставшиеся DHCP-серверы *ti$* предоставляли в аренду адреса из пересекающихся диапазонов.

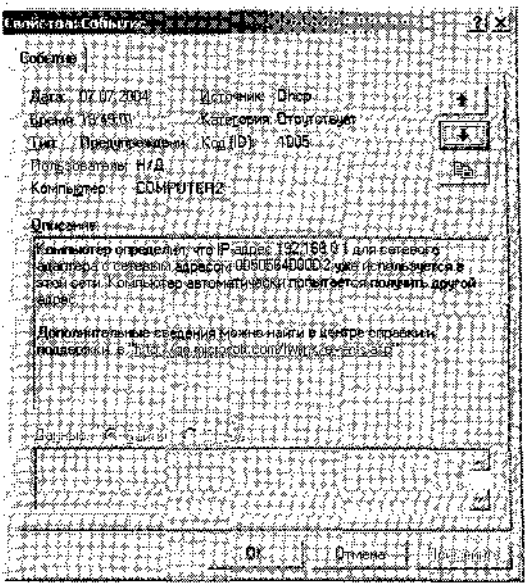


Рис. 8-7. Предупреждающее сообщение о конфликте адресов в окне *Просмотр событий*

Чтобы предотвратить неполадки и корректно выполнить реорганизацию областей, сначала увеличьте число попыток определения конфликтов серверов, а затем обновите аренду адресов клиентами. Для обновления аренды адреса клиентом используйте либо команду Ipconfig /renew, либо кнопку **Исправить (Repair)** в диалоговом окне состояния соответствующего подключения. Если необходимо обновить аренду адресов многими клиентами, можно воспользоваться командой Shutdown /i — она перезапускает многие удаленные компьютеры.

Примечание При выполнении команды Shutdown /i открывается окно, где можно выбрать удаленные компьютеры, которые надо остановить.

Кнопка *Исправить*

По щелчку кнопки **Исправить (Repair)** на вкладке **Поддержка (Support)** диалогового окна состояния подключения (рис. 8-6) последовательно выполняются шесТ2г операций.

1. Отправка широковещательного сообщения DHCP Request для обновления текущего IP-адреса клиента. (Эта операция выполняется только по отношению к DHCP-клиентам.) При этом происходит практически то же, что и при выполнении команды Ipconfig /renew, но в последнем случае запрос на обновление активного в данный момент IP-адреса выполняется в одноадресном порядке в адрес DHCP-сервера, выделившего адрес, а не по методу широковещания. Если у клиента нет адреса (0.0.0.0), первой операцией, выполняемой по щелчку кнопки **Исправить** (как и в команде Ipconfig /renew), будет рассылка в сети широковещательного пакета DHCP Discover.
2. Сброс кэша протокола ARP. Эта операция эквивалентна выполнению команды arp -d *. .

3. Сброс кэша NetBIOS. Тот же эффект достигается командой nbtstat -R.
4. Сброс кэша DNS. Равнозначен выполнению команды ipconf ig /flushdns.
5. Перерегистрация NetBIOS-имени клиента и его IP-адреса на WINS-сервере. Тоже, что команда nbtstat -RR.
6. Перерегистрация имени компьютера клиента и IP-адреса в DNS. Этот этап функционально эквивалентен выполнению ipconfig /registerdns.

Подготовка к экзамену Нужно знать, какие операции выполняются по щелчку кнопки **Исправить** и какие команды им соответствуют.

Сбой получения IP-адреса от DHCP-сервера

Когда при выполнении команды ipconf ig /a11 или в диалоговом окне состояния подключения выясняется, что адрес клиента присвоен APIPA или является адресом альтернативной конфигурации, следует прежде всего обновить IP-конфигурацию командой ipconfig /renew либо щелчком кнопки **Исправить (Repair)** в окне состояния подключения.

Если это не устраняет неполадку, причина может быть в отсутствии DHCP-сервера или агента ретрансляции в диапазоне адресов широковещания, физическом повреждении соединения или ошибке DHCP-сервера или области. Если DHCP-сервер или агент ретрансляции гарантировано присутствует в диапазоне широковещания, убедитесь, что не повреждено физическое соединение. Имейте в виду, что для успешной проверки связи с DHCP-сервером или агентом ретрансляции командой Ping может понадобиться вручную присвоить клиенту временный адрес в той же логической подсети, что и его шлюз по умолчанию.

Совет Если вам не известно местоположение, адрес или имя DHCP-сервера в сети, выполните команду netsh dhcp show server: она вернет имена и адреса всех серверов, авторизованных в Active Directory.

После устранения физического повреждения связи, а также проблем настройки или состояния агента ретрансляции DHCP (в случае его использования), переходят к проверке DHCP-сервера и области. Связанная с невозможностью клиента получить IP-адрес проверка DHCP-сервера включает проверку полноты установки, а также корректности настройки и авторизации. Также проверятся область: нужно убедиться, что она активна и не все возможные адреса предоставлены в аренду другим клиентам. (В разделе «Проверка конфигурации сервера» более подробно говорится об устранении подобных неполадок сервера и области.)

Адрес некорректной области

Если при выполнении команды ipconf ig /a11 в диалоговом окне состояния подключения обнаруживается, что адрес клиента получен от DHCP-сервера, но принадлежит некорректной области, первым делом проверяют, нет ли в сети конкурирующих серверов. Для этого можно воспользоваться утилитой Dhcploc.exe, чтобы определить, не занимаются ли неавторизованные DHCP-серверы распределением IP-адресов. Если неавторизованных серверов нет, убедитесь, что все диапазоны адресов, предоставляемых авторизованными DHCP-серверами, не перекрываются.

Корректный DHCP-сервер может предоставить адрес из некорректной области. Один DHCP-сервер может обслуживать многие области; адреса областей, не относящихся к собственной подсети сервера, выделяются удаленным клиентам. Однако DHCP-сервер в состоянии соотнести удаленные клиенты с правильной областью, только если поддерживающему спецификацию RFC 1542 маршрутизатору или агенту ретрансляции, через который происходит взаимодействие с клиентом, назначен правильный адрес. В такой ситуации, когда удаленный клиент получает от DHCP-сервера некорректный адрес, надо проверять корректность адреса DHCP-агента ретрансляции или маршрутизатора, пересылающего DHCP-сообщения.

Примечание В сообщения DHCP Request есть поле Giaddr, которое информирует DHCP-сервер о подсети, откуда исходит запрос. Если поле пусто, клиент получает адрес из локальной области. Если поле Giaddr содержит адрес, как в приведенном ниже примере, DHCP-сервер присваивает клиенту адрес из области, соответствующей этому адресу:

```
DHCP: Relay  IP Address (giaddr) = 192.168.2.1
```

Проверка конфигурации сервера

Обычно начинают с адреса DHCP-сервера. Чтобы предоставлять в аренду адреса клиентам из локальной сети, компьютер DHCP-сервера должен получить адрес с идентификатором сети, относящимся к этой логической подсети. Кроме того, служба DHCP-сервера должна иметь привязку к подключению к этой подсети. Чтобы проверить привязки DHCP-сервера, на вкладке **Другие (Advanced)** окна свойств сервера щелкните кнопку **Привязки (Bindings).** Откроется окно **Привязки (Bindings)** (рис. 8-8).

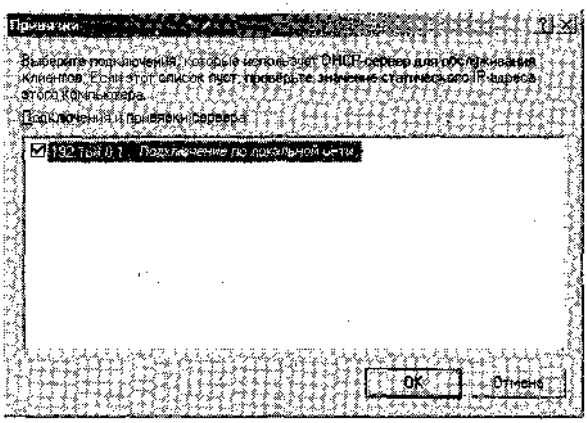


Рис. 8-8. Привязки DHCP-сервера

После проверки правильности адреса DHCP-сервера и его привязок проверяют авторизацию DHCP-сервера в Active Directory. Иногда отсутствие авторизации выявляется очень просто: значок сервера в консоли *DHCP* отмечен направленной вниз красной стрелкой в кружке, авторизованные — направленной вверх зеленой стрелкой.

Проверка конфигурации области

Проверку конфигурации области начинают с выяснения, активизирована ли она. Активизированные и неактивизированные области обозначаются такими же стрелками, как и авторизованные и неавторизованные серверы.

Затем проверяют правильность настройки диапазона адресов области. В области, обеспечивающей адреса для компьютеров в локальном сегменте сети и логической подсети, проверьте, совпадает ли сетевой идентификатор области с сетевым идентификатором DHCP-сервера. Это просто, когда используются стандартные маски подсети, но когда в локальной сети или в области маска отлична от /8, /16 или /24, приходится прибегать'к калькулятору и вычислять «логическое И» (AND), чтобы убедиться в совпадении сетевого идентификатора в адресе сервера и диапазоне адресов области.

Проверив диапазон адресов, убедитесь, что в области остались свободные и доступные для аренды адреса. Есть несколько способов увеличить число доступных для аренды адресов. Во-первых, расширить диапазон адресов области, если есть такая возможность. Во-вторых, можно переопределить область, Задав укороченную маску подсети (например /23 вместо /24), а затем заменить маску на всех компьютерах локальной сети. Наконец, можно воспользоваться мультисетевой конфигурацией с множеством областей и маршрутизатором.

Альтернативный вариант решения задачи поддержки большего количества компьютеров в рамках имеющегося адресного пространства заключается в сокращении срока аренды. При этом быстрее освобождаются адреса компьютеров, которые отключаются или временно удаляются из сети.

Подготовка к экзамену Следите за задачами, в которых имеет смысл сократить срок аренды в области, чтобы обслуживать больше пользователей в том же пространстве адресов. Обычно это бывает, когда в сети много пользователей с ноутбуками и пользователей, подключающихся по модему.

Продолжая проверку конфигурации области, проверьте исключения, определенные в пуле адресов. Убедитесь, что исключены все статические адреса, попадающие в диапазон адресов области. Убедитесь также в том, что сделаны только необходимые исключения.

Затем проверьте настроенные резервирования клиентов. Если клиенты с зарезервированными адресами не получают аренду, проверьте, не исключены ли эти адреса, и убедитесь, что зарезервированные адреса принадлежат диапазону адресов области. Наконец, следует проверить, правильно ли зарегистрированы MAC-адреса, соответствующие зарезервированным адреса.

Затем на DHCP-серверах, обслуживающих многие области, в том числе в удаленных подсетях, тщательно проверьте правильность определения каждой области. При обслуживании удаленной подсети диапазон адресов области должен соответствовать сетевому идентификатору DHCP-агента ретрансляции или поддерживающего спецификацию RFC 1542 маршрутизатора этой подсети.

Наконец, в сетях с несколькими DHCP-серверами в пределах досягаемости широковещания проверяют наличие и настройку суперобластей. Также следует убедиться, что диапазоны адресов, предоставляемых в аренду каждым из серверов, исключены на всех остальных DHCP-серверах.

Получение и проверка MAC-адресов для резервируемых адресов

Чтобы зарезервировать адрес, нужно знать аппаратный адрес компьютера, а узнать его можно так: на локальном компьютере — в окне состояния подключения по локальной сети, а на удаленном — в окне удаленного рабочего стола (Remote Desktop). На вкладке **Поддержка (Support)** щелкните кнопку **Подробности (Details).** Откроется диалоговое окно **Детали сетевого подключения (Network Connection Details)** с информацией, в том числе MAC-адресом компьютера и его IP-адресом, адресами DHCP- и DNS-серверов. MAC-адрес локального компьютера также выдает команда Ipconfig /all.

Это неплохие способы, но узнать MAC-адрес локального или удаленного компьютера можно значительно быстрее, воспользовавшись утилитой Getmac из состава *Средств поддержки Windows* (Windows Support Tools). Надо выполнить команду Getmac /s. Возвращенный MAC-адрес можно через буфер обмена скопировать прямо в окно **Создать резервирование (New Reservation).**

Например, выполните следующую команду:

```
getmac/s computer2 | clip.
```

Затем откройте *Блокнот* (Notepad) и нажмите Ctrl+V. При этом выполняется вставка из буфера результатов, загруженных туда утилитой Getmac. Далее из *Блокнота* аппаратный адрес Computer2 копируют и вставляют в соответствующее поле окна **Создать резервирование.**

Согласование базы данных DHCP

Если обнаруживается, что информация базы данных DHCP отсутствует либо противоречива, выполняют согласование данных отдельных или всех областей.

Информация об аренде IP-адресов хранится в базе данных службы DHCP-сервера в двух видах: подробном и сводном. При согласовании областей подробные и сводные записи сравниваются на предмет несоответствий.

Если выбрать режим устранения несоответствий, обнаруженных в процессе согласования, DHCP-сервер либо возвращает адреса, вызывающие сомнение, первоначальным владельцам, либо создает временные резервирования для этих адресов. Эти резервирования останутся в силе на весь срок аренды, установленный для области. По истечении этого срока адреса возвращаются в пул свободных адресов.

- Согласование базы данных DHCP выполняется так.

1. В дереве консоли *DHCP* выберите нужный DHCP-сервер.
2. В меню **Действие (Action)** щелкните **Согласовать все области (Reconcile All Scopes).**
3. **В** окне **Согласование всех областей (Reconcile All Scopes)** щелкните кнопку **Проверить (Verify).** Информация об обнаруженных несоответствиях появится в окне состояния.
4. Если обнаружится, что база данных непротиворечива, щелкните OK. В противном случае щелкните адреса, которые нужно согласовать, а затем — кнопку **Согласование (Reconcile).**

При согласовании отдельной области порядок действий такой же, но в п. 1 нужно выбрать не сервер, а конкретную область.

Проверка журналов в окне *Просмотр событий*

При сбое службы DHCP рекомендуется изучить журнал событий на предмет ошибок — это позволит более осмысленно подойти к решению проблемы. Откройте окно **Просмотр событий (Event Viewer)** и выберите в дереве консоли журнал **Система (System).** DHCP-сообщения, записываемые в журнал от имени DHCP-серверов, обозначаются в поле **Источник (Source)** ключевым словом DHCPServer (рис. 8-9).

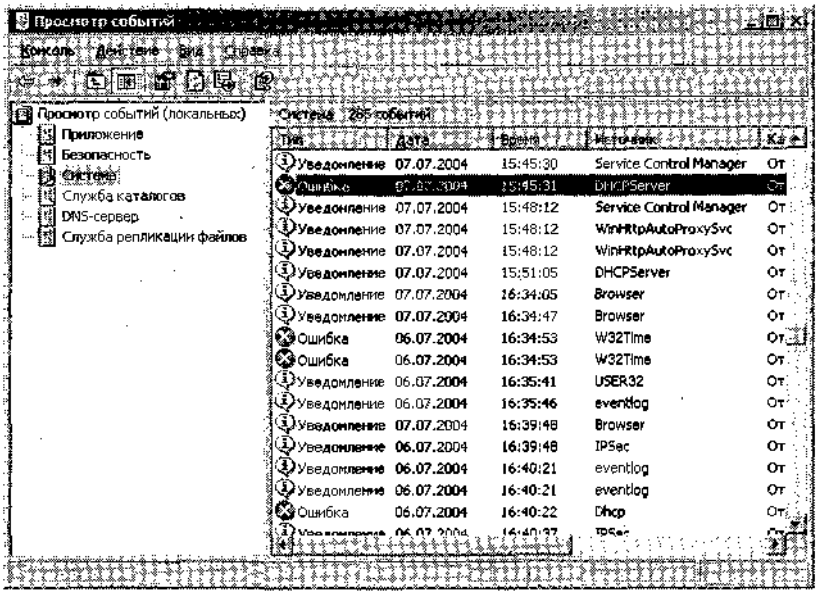


Рис. 8-9. Ошибки DHCP-сервера

Дважды щелкните событие с признаком DHCPServer и изучите связанное с ним сообщение. Ниже приведен пример сообщения об ошибке DHCP-сервера из журнала событий.

В русской версии Windows Server 2003 подобное сообщение выглядит так:

Служба DHCP/BINL на локальном компьютере, входящем в административный домен Windows "domain1.local", определила, что она не авторизована для запуска. Обслуживание клиентов остановлено. Возможными причинами могли стать:

Эта машина является частью предприятия службы каталогов и авторизована в том же домене. (Для получения дополнительной информации обратитесь к справке по программе "Управление службой DHCP").

Эта машина не может обнаружить предприятие службы каталогов и она обнаружила службу DHCP на другой машине в сети, принадлежащей предприятию службы каталогов, в котором этот компьютер не может авторизоваться.

Произошли непредвиденные ошибки сети.

а в англоязычной так:

The DHCP/BINL service on the local machine, belonging to the Windows Administrative domain domain"!, local, has determined'that it is not authorized

to start. It has stopped servicing clients. The following are some possible reasons for this:

This machine is part of a directory service enterprise and is not authorized in the same domain. (See help on the DHCP Service Management Tool for "additional information.)

This machine cannot reach its directory service enterprise and it has encountered another DHCP service on the network belonging to a directory service enterprise on which the local machine is not authorized.

Some unexpected network error occurred.

Журнал **Система** в окне **Просмотр событий** можно также использовать для обнаружения ошибок DHCP-клиентов. События, записанные в системный журнал от имени DHCP-клиентов, отмечаются в поле **Источник** ключевым словом Dhcp.

Вот пример ошибки DHCP-клиента, зафиксированной в журнале событий:

русская версия Windows:

Аренда IP-адреса 192.168.0.11 для сетевой карты с сетевым адресом 00D05380B7F6 отменена DHCP-сервером 192.168,0.1 (DHCP-сервер отправил сообщение DHCPNACK).

англоязычная версия Windows:

The IP address lease 192.168.0.11 for the Network Card with network address 00D05380B7F6 has been denied by the DHCP server 192.168.0.1 (The DHCP Server sent a DHCPNACK message)..

Примечание Больше информации о поведении DHCP-сервера можно найти в журнале аудита сервера (см. занятие 2).

Проверка базы данных Jet в окне *Просмотр событий*

При повреждении базы данных DHCP-сервера в журнале **Система** могут обнаружиться следующие сообщения службы DHCP (табл. 8-4).

Табл. 8-4. Ошибки повреждения базы данных DHCP

Код события	Источник	Описание
1014	DhcpServer	База данных JET выдает следующую ошибку: - 510
1014	DhcpServer	База данных JET выдает следующую ошибку: - 1022
1014	DhcpServer	База данных JET выдает следующую ошибку: - 1850

При обнаружении подобных сообщений рекомендуется вручную в оффлайновом режиме выполнить сжатие базы данных DHCP с помощью утилиты Jetpack. Если это не решает проблему, придется восстановить базу данных DHCP-сервера средствами консоли DHCP. (Обе процедуры описаны в занятии 2 главы 7.) Еще один способ восстановления базы данных DHCP-сервера — выполнить следующую команду:

```
netsh dhcp server set databaserestoreflag 1
```

При этом устанавливается флаг восстановления, который позволит при повторной инициализации службы DHCP-сервера загрузить копию базы данных DHCP из стандартного архивного каталога.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы отвечаете за развертывание DHCP согласно официальному плану сети компании. В соответствии со схемой, DHCP-серверу надо присвоить адрес 207.46.47.150, кроме того, он должен предоставлять в аренду адреса в локальном сегменте сети из области 207.46.48.0, однако в схеме не указана маска подсети для сервера и области. Какую маску подсети нужно присвоить серверу и области, чтобы DHCP-сервер и клиенты располагались в одной логической подсети, и при этом минимальное количество бит задействовалось под сетевой идентификатор узла?
2. В компании нужно предоставлять в аренду адреса 280 пользователям, но в наличии 254 адреса. Из всех 280 пользователей 50 подключаются к офисной сети лишь раз в две недели по VPN-подключениям. Что сделать, чтобы адресов хватило всем?
3. Когда нужно увеличивать число попыток обнаружения конфликтов на DHCP-сервере?

Резюме

и При устранении неполадок DHCP сначала нужно локализовать неполадку: клиент, физическая сеть или сервер.

- Используйте окно состояния подключения или результат команды Ipconfig /all для выяснения: корректен ли адрес клиента и получен ли он у DHCP-сервера.
- Убедитесь, что все клиенты попадают в диапазон широковещания настроенного DHCP-сервера, DHCP-агента ретрансляции или поддерживающего спецификацию RFC 1542 маршрутизатора.
- При проверке конфигурации DHCP-сервера проверьте корректность установки, авторизации и привязки сервера.
- При проверке конфигурации области убедитесь, что она активизирована,, а также проверьте диапазон адресов, маску подсети, исключения, резервирования и суперобласти.

Пример из практики

Вы администратор сети компании Forth Coffee в г. Ратленде, штат Вермонт. Компания недавно приобрела 60 новых клиентских компьютеров и планирует присоединить их к уже имеющимся 245. Сеть состоит из одного сегмента с единственным DHCP-сервером. До подключения 60 новых компьютеров DHCP-сервер предоставлял в аренду адреса из единственной области 10.0.0.0/24.

Вам поручили подключить 60 новых компьютеров и устранить все неполадки, которые при этом могут возникнуть. Ответьте на следующие вопросы и определите оптимальный способ решения каждой из поставленных задач.

1. Как с наименьшими усилиями предоставить достаточное количество адресов 290 клиентам, поддерживающим динамическую адресацию, сохранив при этом связь между компьютерами сети? (Выберите только один ответ.)
   a. Создать новую суперобласть и добавить в нее области 10.0.0.0/24 и 10.0.1.0/24.
   b. Перенастроить существующую область как 10.0.0.0/23 и установить для количества попыток обнаружения конфликтов значение 3. Затем перезагрузить все компьютеры командой Shutdown /i.
   c. Добавить в сегмент второй DHCP-сервер, предоставляющий в аренду адреса из области 10.0.1.0/24.
   d. Добавить в сегмент второй DHCP-сервер, предоставляющий в аренду адреса из области 10.0.0.0/24. Перезагрузить все компьютеры командой Shutdown /i.
2. Начальство потребовало зарезервировать 20 компьютеров в специальной подсети 192.168.0.0/24 и разместить их в том же сегменте, что и остальные компьютеры. Вы развернули новый DHCP-сервер, который предоставляет в аренду адреса из диапазона 192.168.0.0/24, и создали 20 резервированных адресов для новых компьютеров. Однако после развертывания нового DHCP-сервера в области аренда адресов недоступна несмотря на то, что область активизирована. В чем может быть причина?
   a. Не выполнено согласование областей на новом DHCP-сервере.
   b. Не проверена база данных на предмет непротиворечивости.
   c. Не исключен диапазон адресов, обслуживаемый первым DHCP-сервером.
   d. Новому DHCP-серверу не присвоен адрес из диапазона 192.168.0.0/24.
3. После активизации новых областей некоторые пользователи стали жаловаться, что доступ к сетевым ресурсам невозможен. В журналах аудита DHCP-сервера вы обнаружили несколько сообщений NACK. Как устранить неполадку? (Выберите все подходящие варианты.)
   a. Создать на каждом DHCP-сервере суперобласть, состоящую из активных областей данного сегмента сети.
   b. Создать резервирования для всех нужных клиентов на первом DHCP-сервере.
   c. На первом DHCP-сервере полностью исключить весь диапазон адресов специальной подсети 192.168.0.0/24.
   d. На новом DHCP-сервере полностью исключить диапазон адресов, поддерживаемых первым DHCP-сервером.

Практикум по устранению неполадок

На этом практикуме вы устраните неполадки службы DHCP.

1. На Computer2 войдите в систему под учетной записью *Администратор* (Administrator) домена Domainl.
2. Вставьте в дисковод Computer2 прилагаемый компакт-диск и двойным щелчком запустите командный файл *\70-291\labs\Chapter08\Ch8a.bat*.
3. На Computer2 выполните команду ipconfig /renew. Обновление не произойдет.
4. Проверьте физическое соединение обоих компьютеров с сетью. Используя команду Netsh или консоль *DHCP,* убедитесь, что сервер авторизован, область активизирована, а DHCP-серверу назначен корректный адрес. Затем проверьте область, то есть

правильность определения: диапазонов исключений, резервирования, параметров области.

5. После всех этих проверок ответьте, почему DHCP-сервер не предоставляет в аренду адреса?
6. После обнаружения ошибки выполните команду Ipconfig, чтобы убедиться, что Computer2 автоматически назначил себе альтернативный адрес 192.168.0.2. Если отображается адрес 0.0.0.0, выполните команду ipconfig /renew.
7. После того как вы удостоверитесь, что Computer2 действительно принял адрес альтернативной конфигурации 192.168.0.2, запустите с прилагаемого компакт-диска командный файл *\70-291\labs\Chapter08\Ch8b.bat*. Он восстановит корректные параметры DHCP-сервера, при этом исправит только некорректные параметры, а правильные оставит без изменений.
8. На Computer2 выполните команду ipconfig /renew. Computer2 получит новый IP-адрес от DHCP-сервера.
9. Завершите сеанс на Computerl и Computer2.

Резюме главы

- Процесс инициализации DHCP-клиента выполняется при первом запуске клиентского компьютера и его попытке подключиться к сети. Этот процесс состоит из обмена четырьмя широковещательными сообщениями: поиска — Discover, предложения — Offer, запроса — Request и подтверждения — ACK.
- Журнал аудита позволяет ежедневно регистрировать все операции DHCP-сервера в тестовых файлах в формате с разделяющими запятыми. По умолчанию файлы журналов DHCP-сервера хранятся в папке *Windows\System32\Dhcp*.
- События в файлах журнала DHCP-сервера идентифицируются кодом события. События с кодами менее 50 описаны в файле журнала, и их не обязательно запоминать. События с кодами 50 и выше относятся к обнаружению неавторизованного сервера (состоянию авторизации Active Directory). Нужно либо запомнить эти события, либо обращаться к справочной подсистеме для расшифровки их значения.
- Когда DHCP-сервер перестает предоставлять адреса в аренду, прежде всего нужно просмотреть журнал DHCP на предмет неполадок авторизации.
- При устранении неполадок DHCP в первую очередь надо локализовать неполадку, то есть определить, где причина: на клиенте, в физической сети или на сервере.
- При проверке конфигурации сервера проверяют правильность установки, авторизации и привязки сервера.
- При проверке конфигурации области надо убедиться, что область активизирована, а также проверить диапазон адресов, маску подсети, исключения, резервирования и суперобласти.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Разберитесь в типах и предназначении различных DHCP-сообщений.
- Изучите разные способы обновления аренды адреса: команда Ipconfig /renew, кнопка **Исправить (Repair)** и перезапуск клиентского компьютера.
- Необходимо четко понимать функции журнала аудита DHCP и уметь читать сообщения в этом журнале.
- Надо знать, что дает увеличение числа попыток обнаружения конфликтов на DHCP-сервере.
- Следует разобраться в достоинствах и недостатках увеличения и уменьшения срока аренды.
- Нужно уметь распознавать ошибки настройки DHCP-сервера и области.

Основные термины

DHCP Discover — широковещательное DHCP-сообщение, отправляемое DHCP-клиентом, позволяющее клиенту найти DHCP-сервер.

DHCP NACK — сообщение, отправляемое DHCP-сервером клиенту, которое указывает, что запрошенный клиентом IP-адрес неверен для локальной сети, обслуживаемой DHCP-сервером.

Giaddr — поле в DHCP-сообщении, содержащее адрес агента ретрансляции или RFC 1542-совместимого маршрутизатора. Это поле позволяет DHCP-серверу правильно присваивать адреса клиентам из удаленных подсетей.

Флаг восстановления базы данных ~ database restore flag — заставляет службу DHCP-сервера при повторной инициализации загрузить копию базы данных DHCP из стандартного архивного каталога. По умолчанию этот флаг установлен в 0, и при запуске службы архивная копия не загружается.

Вопросы и ответы

Занятие 1. Лабораторная работа. Упражнение 2

2. Ответьте на следующие вопросы:

   a. Как называются пять DHCP-сообщений? Запишите по порядку их названия, указанные в поле описания кадров.

   Правильный ответ: Release, Discover, Offer, Request, ACK.

   b. Какое из сообщений не является широковещательным? Почему?

   Правильный ответ: Release. Это сообщение не является широковещательным, поскольку в момент его отправки местоположение сервера известно и для завершения освобождения адреса клиенту не нужно обращаться к другим DHCP-серверам. Местоположение сервера известно, так как клиент уже обнаружил его, получив до этого в аренду адрес, освобождаемый данным сообщением.

   c. Из каких DHCP-сообщений состоит процесс получения первичной аренды?

   Правильный ответ: Discover, Offer, Request, ACK.

   d. Изучите поле Options DHCP-сообщений. Какие два DHCP-сообщения включают параметры: Domain Name, Router и Domain Name Server?

   Правильный ответ: Offer и ACK.

e. Какой UDP-порт указывается как порт источника при отправке информации от DHCP-клиента и как порт назначения при получении информации DHCP-клиентом?

Правильный ответ: 68.

f. Какой UDP-порт используется как порт источника при отправке информации от DHCP-сервера и как порт назначения при получении информации DHCP-сервером?

Правильный ответ: 67.

g. Какое единственное из пяти DHCP-сообщений содержит раздел Dynamic DNS Updates в поле Options?

Правильный ответ: DHCP Request.

4. Ответьте на следующие вопросы.

Какая информация содержится в разделе Dynamic DNS? Какую запись ресурса обновит DHCP-сервер на основе этой информации?

Правильный ответ: раздел содержит полное имя компьютера (имя узла и доменное имя) DHCP-клиента. На основе этой информации DHCP-сервер обновляет запись ресурса PTR.

Занятие 1. Лабораторная работа. Упражнение 4

2. Ответьте на следующие вопросы.

a. Из скольких сообщений состоит процесс обновления аренды DHCP?

Правильный ответ: из двух.

b. Как называются записанные DHCP-сообщения? Запишите их по порядку в соответствии с информацией в поля описания кадров.

Правильный ответ: Request, ACK.

c. Чем отличается набор этих сообщений и сообщений первичной аренды?

Правильный ответ: эти сообщения не являются широковещательными и отправляются прямо DHCP-серверу или клиенту.

3. **В** обоих записанных кадрах найдите поля **Client IP Address** и **Your IP Address** и ответьте на следующие вопросы.

a. При обновлении аренды запрашивает ли DHCP-клиент обновление конкретного IP-адреса?

Правильный ответ: да.

b. Какое конкретно поле какого DHCP-сообщения обновляет DHCP-параметы конфигурации клиента?

Правильный ответ: поле Option (Параметры) сообщения ACK.

Занятие 1. Закрепление материала

1. Вы развернули в подсети два DHCP-сервера — DHCP1 и DHCP2. Первый обслуживает адреса первых 80 % всего диапазона адресов области, а второй — остальные 20 % диапазона. Компьютер ClientA получает свежий адрес от DHCP1, после чего DHCP1 немедленно отключается. Сколько времени пройдет, прежде чем ClientA попытается получить новый адрес от DHCP2?

a. 4 дня.
b. 5 дней,
c… 7 дней.
d. 8 дней.

Правильный ответ: с.

2. Какое из следующих сообщений не используется в процессе получения первичной аренды DHCP?
   a. Renew.
   b. Request.
   c. ACK.
   d. Discover.

   Правильный ответ: а.
3. Какие два сообщения участвуют в процессе обновления аренды DHCP?

   Правильный ответ: Request и ACK.
4. По истечении какого времени DHCP-клиент пытается обновить аренду IP-адреса?

   Правильный ответ: через 4 дня.

Занятие 2. Закрепление материала

1. С понедельника стало невозможно получить эхо-ответ Ping от некоторых сетевых клиентов. В журнале DHCP-сервера за понедельник обнаружилась следующая запись:

   54,6/09/ 03,06:47:29, Authorization failed, , domain1, local, ,

   Какая операция скорее всего стала' стала источником неполадок? Кто ее выполнил? (Предполагается, что до сбоя авторизации в журнале нет никаких сообщений о неполадках DHCP-сервера.)

   Правильный ответ: сервер потерял авторизацию в Active Directory. Отменить авторизацию мог только пользователь из группы Администраторы предприятия (Enterprise Admins).
2. Каковы наиболее вероятные причины ошибки, описанной в следующей записи журнала аудита DHCP?

   00,5/24/03,08:21:57,Started,,,,
   54,5/24/ 03,08:21:58,Authorization failed,,domainl.local,,

   a. Сервер запускается в первый раз.
   b. Сервер не может подключиться к сети.
   c. Администратор сети отменил авторизацию сервера.
   d. Сервер работает под управлением ОС, отличной от Windows Server 2003.

   Правильный ответ: а.
3. Как долго по умолчанию сохраняются записанные события в журналах DHCP-сервера?
   a. 1 день.
   b. 1 неделю.
   c. 1 месяц.
   d. Пока размер журнала не превысит 1 Мб.

   Правильный ответ: Ъ.

Занятие 3. Закрепление материала

1. Вы отвечаете за развертывание DHCP согласно официальному плану сети компании. В соответствии со схемой, DHCP-серверу надо присвоить адрес 207.46.47.150, кроме того, он должен предоставлять в аренду адреса в локальном сегменте сети из области 207.46.48.0, однако в схеме не указана маска подсети для сервера и области. Какую маску подсети нужно присвоить серверу и области, чтобы DHCP-сервер и клиенты располагались в одной логической подсети, и при этом минимальное количество бит задействовалось под сетевой идентификатор узла?

   Правильный ответ: 255.255.224.0.

2. **В** компании нужно предоставлять в аренду адреса 280 пользователям, но в наличии 254 адреса. Из всех 280 пользователей 50 подключаются к офисной сети лишь раз в две недели по VPN-подключениям. Что сделать, чтобы адресов хватило всем?

   Правильный ответ: уменьшить срок аренды по умолчанию.

3. Когда нужно увеличивать число попыток обнаружения конфликтов на DHCP-сервере?

   Правильный ответ: при реорганизации области в то время, когда адреса арендуются сетевыми компьютерами.

Пример из практики

1. Как с наименьшими усилиями предоставить достаточное количество адресов 290 клиентам, поддерживающим динамическую адресацию, сохранив при этом связь между компьютерами сети? (Выберите только один ответ).
   a. Создать новую суперобласть и добавить в нее области 10.0.0.0/24 и 10.0.1.0/24.
   b. Перенастроить существующую область как 10.0.0.0/23 и установить для количества попыток обнаружения конфликтов значение 3. Затем перезагрузить все компьютеры командой Shutdown /i.
   c. Добавить в сегмент второй DHCP-сервер, предоставляющий в аренду адреса из области 10.0.1.0/24.
   d. Добавить в сегмент второй DHCP-сервер, предоставляющий в аренду адреса из области 10.0.0.0/24. Перезагрузить все компьютеры командой Shutdown /i.

   Правильный ответ: Ь.

2. Начальство потребовало зарезервировать 20 компьютеров в специальной подсети 192.168.0.0/24 и разместить их в том же сегменте, что и остальные компьютеры. Вы развернули новый DHCP-сервер, который предоставляет в аренду адреса из диапазона 192.168.0.0/24, и создали 20 резервированных адресов для новых компьютеров. Однако после развертывания нового DHCP-сервера в области аренда адресов недоступна несмотря на то, что область активизирована. В чем может быть причина?
   a. Не выполнено согласование областей на новом DHCP-сервере.
   b. Не проверена база данных на предмет непротиворечивости.
   c. Не исключен диапазон адресов, обслуживаемый первым DHCP-сервером.
   d. Новому DHCP-серверу не присвоен адрес из диапазона 192.168.0.0/24.

   Правильный ответ: d.

3. После активизации новых областей некоторые пользователи стали жаловаться, что доступ к сетевым ресурсам невозможен. В журналах аудита DHCP-сервера вы обнаружили несколько сообщений NACK. Как устранить неполадку? (Выберите все подходящие варианты.)

a. Создать на каждом DHCP-сервере суперобласть, состоящую из активных областей данного сегмента сети.
b. Создать резервирования для всех нужных клиентов на первом DHCP-сервере.
c. На первом DHCP-сервере полностью исключить весь диапазон адресов специальной подсети 192.168.0.0/24.
d. На новом DHCP-сервере полностью исключить диапазон адресов, поддерживаемых первым DHCP-сервером.

Правильные ответы: a, c и d.

Практикум по устранению неполадок

5. После всех этих проверок ответьте, почему DHCP-сервер не предоставляет в аренду адреса?

Правильный ответ: не задан диапазон адресов обслуживаемой DHCP-сервером области.

ГЛАВА 9

Маршрутизация в Windows Server 2003

Темы экзамена

- Управление интерфейсами маршрутизации и удаленного доступа.
- Управление фильтрами пакетов.
- Управление маршрутизацией TCP/IP:
  - управление протоколами маршрутизации;
  - управление таблицами маршрутизации;
  - управление портами маршрутизации.
- Устранение неполадок маршрутизации вызовов по требованию.
- Устранение неполадок подключения к Интернету.
- Проверка корректности работы агента DHCP-ретрансляции.

В этой главе

Здесь рассказывается о настройке и управлении множеством функций, предоставляемых службой *Маршрутизация и удаленный доступ* (Routing and Remote Access, RRAS) в Windows Server 2003, в том числе *преобразованием сетевых адресов* (Network Address Translation, NAT), маршрутизацией вызовов по требованию и фильтрами пакетов.

Прежде всего

Для изучения материалов этой главы вам потребуются:

- два физически объединенных в сеть компьютера с именами Computerl и Computer2 под управлением Windows Server 2003. Компьютеру Computerl надо назначить стати-

ческий адрес 192.168.0.1/24, а Computer2 нужно настроить на автоматическое получение адреса, а также задать на Computer2 альтернативную конфигурацию с адресом 192.168.0.2/24;

- модемное подключение компьютеров по отдельным (это обязательное требование) телефонным линиям;
- установленные на обоих компьютерах DNS-серверы. На Computerl надо разместить основную зону domainl.local, принимающую только безопасные динамические обновления, а на Computer2 — стандартную дополнительную зону domainl.local и делегированный поддомен sub.domainl.local в качестве стандартной основной зоны. Computerl поддерживает стандартную зону-заглушку sub.domainl.local;
- Computerl, сконфигурированный как контроллер домена смешанного режима domainl.local, а Computer2 — как член этого домена;
- установленный на Computerl DHCP-сервер, являющийся уполномоченным в данном домене и поддерживающий область Test Scope с диапазоном IP-адресов 192.168.0.11—192.168.0.254. В параметрах DHCP определены адреса: маршрутизатора (шлюза) — 192.168.0.1, DNS-сервера — 192.168.0.1 и имя DNS-домена domainl.local;
- установленный на обоих компьютера пакет *Средства поддержки Windows* (Windows Support Tools);
- установленный на обоих компьютера *Сетевой монитор* (Network Monitor);
- отсутствие любых телефонных подключений (все подобные подключения надо удалить) на обоих компьютерах.

Занятие 1. Настройка Windows Server 2003 для маршрутизации в локальной сети

В Windows Server 2003 маршрутизация обеспечивается службой *Маршрутизация и удаленный доступ* (Routing and Remote Access, RRAS), которая устанавливается, но не активизируется. По существу, эта служба представляет собой программный маршрутизатор, который при необходимости настраивается для обеспечения связи сетевых сегментов.

Изучив материал этого занятия, вы сможете:

- *V* конфигурировать Windows Server 2003 как сетевой маршрутизатор;
- *V* конфигурировать и управлять функциями маршрутизации в службе *Маршрутизация и удаленный доступ;*
- *V* просматривать и обслуживать таблицы маршрутизации;
- *V* конфигурировать и обслуживать статические маршруты.

Продолжительность занятия — около 90 минут.

Основные сведения о маршрутизации

Маршрутизация (routing) — это процесс пересылки данных между локальными вычислительными сетями (ЛВС). В отличие от *моста* (bridge), который обеспечивает связь сетевых сегментов и совместный доступ к трафику с использованием аппаратных адре-

сов, маршрутизатор принимает и пересылает трафик, ориентируясь на программные адреса. Поэтому мосты, действующие на втором (канальном) уровне модели OSI, иногда называют устройствами «уровня 2», а маршрутизаторы, функционирующие на третьем (сетевом) уровне — устройствами «уровня 3».

В IP-сетях маршрутизация выполняется по таблицам IP-маршрутизации, которые есть на всех IP-узлах. IP-маршрутизаторы отличаются от узлов тем, что используют таблицы маршрутизации для пересылки трафика, полученного от других маршрутизаторов или узлов (рис. 9-1).

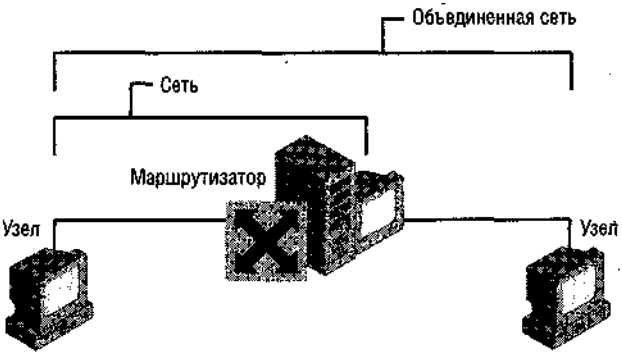


Рис. 9-1. Локальные сети, объединенные маршрутизатором

Использование службы *Маршрутизация и удаленный доступ*

Служба *Маршрутизация и удаленный доступ* (Routing and Remote Access, RRAS) в Windows Server 2003 представляет собой программный многопротокольный маршрутизатор, который легко объединяется с другими функциями Windows, такими как учетные записи безопасности и групповые политики. Служба поддерживает маршрутизацию между разными ЛВС, между ЛВС и WAN-каналами, VPN- и NAT-маршрутизацию в IP-сетях. Кроме того, службу можно сконфигурировать для особых видов маршрутизации: многоадресных IP-рассылок, маршрутизации вызовов по требованию, ретрансляции DHCP и фильтрации пакетов. Наконец, она поддерживает протоколы динамической маршрутизации — RIP (Routing Information Protocol version 2) и OSPF (Open Shortest Path First).

Примечание Windows Server 2003 также поддерживает маршрутизацию AppleTalk. Однако из-за того, что IPX-маршрутизация (Internetwork Packet Exchange) поддерживается Microsoft Windows 2000, компьютеры под управлением Windows Server 2003 не могут функционировать как IPX-маршрутизаторы.

На аппаратных маршрутизаторах много встроенных портов, каждый из которых обычно подключается к отдельному сетевому сегменту. Аппаратный маршрутизатор способен пересылать трафик между любыми двумя портами, однако число поддерживаемых службой *Маршрутизация и удаленного доступа* сетевых сегментов ограничено количеством сетевых интерфейсов компьютера. Например, на компьютере под управлением Windows Server 2003 с двумя сетевыми платами и модемом эта служба сможет организовать обмен трафиком между тремя сетями.

На рис. 9-2 показан компьютер под управлением Windows Server 2003 с четырьмя сетевыми адаптерами. Здесь служба со службой *Маршрутизация и удаленного доступа* управляет IP-трафиком между четырьмя локальными сетями.

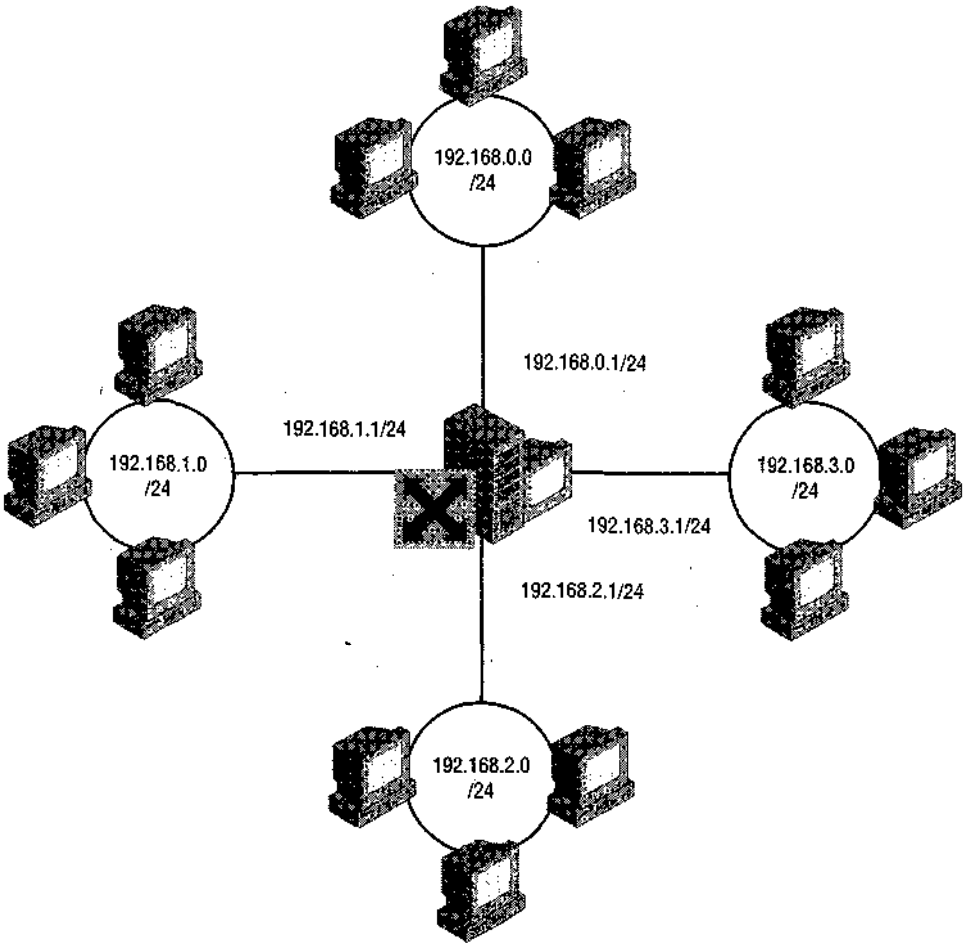


Рис. 9-2. Маршрутизатор на базе Windows с четырьмя сетевыми адаптерами

Активизация службы *Маршрутизация и удаленный доступ*

Во вновь установленной копии Windows Server 2003 служба *Маршрутизация и удаленный доступ* отключена — ее активизируют с помощью *Мастера настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard). Следует иметь в виду, что, если сервер, на котором надо сконфигурировать службу, является рядовым членом домена Active Directory, надо присоединить его к группе *Серверы RAS и LAS* (RAS and IAS Servers). Только после этого сервер сможет работать как маршрутизатор. Контроллер локального домена в дополнительной настройке не нуждается, так как автоматически присоединяется к этой группе.

Консоль *Маршрутизация и удаленный доступ*

Консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access) — это стандартный графический пользовательский интерфейс пользователя для управления маршрутизацией в Windows Server 2003. В конфигурации по умолчанию служба *Маршрутизация и удаленный доступ* поддерживает маршрутизацию только в ЛВС, а одноименная консоль содержит два основных узла — **Интерфейсы сети (Network Interfaces)** и **IP-маршрутизация (IP Routing)** (рис. **9-3).**

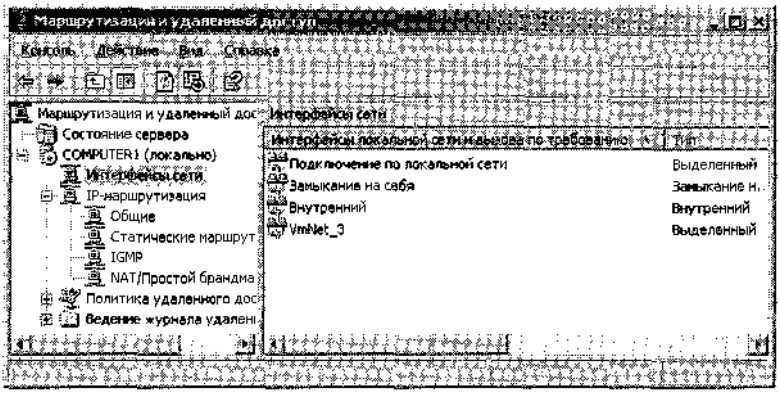


Рис. 9-3. Консоль *Маршрутизация и удаленный доступ*

Создание новых интерфейсов

В консоли **Маршрутизация и удаленный доступ** *сетевой интерфейс* (network interface) представляет собой программный компонент, подключаемый к физическому устройству, например модему или сетевой плате. В процессе настройки маршрутизации в этой консоли прежде всего надо позаботиться, чтобы в узле **Интерфейсы сети (Network Interfaces)** указывались все программные интерфейсы, через которые надо маршрутизировать трафик.

Обычно *Мастер настройки сервера маршрутизации и удаленного доступа* (Routing And Remote Access Server Setup Wizard) обнаруживает все сетевые адаптеры, перечисляет их в виде сетевых интерфейсов в узле **Интерфейсы сети** и позволяет далее настраивать их в консоли **Маршрутизация и удаленный доступ.**

Однако существующие подключения по телефонным линиям не отображаются в консоли *Маршрутизация и удаленный доступ*. Если надо сконфигурировать маршрутизацию через подключение по требованию или постоянное подключение по телефонной линии, VPN- или PPPoE-подключение (Point-to-Point Protocol over Ethernet), придется сделать это вручную в узле **Интерфейсы сети** консоли *Маршрутизация и удаленный доступ*. Совместно все три указанных типа подключений называются *интерфейсами вызова по требованию* (demand-dial interfaces). Только после добавления интерфейса вызова по требованию в консоль **Маршрутизация и удаленный доступ** его можно настраивать для поддержки функций маршрутизации, таких как NAT, статические маршруты или *DHCP-ретрансляция* (DHCP relay).

Примечание Помните, что интерфейс вызова по требованию не обязательно подключение по телефонной линии, это может быть VPN- или PPPoE-подключение по выделенной линии.

Подключение по телефонной линии, VPN- или PPPoE-подключение добавляется так.

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **Интерфейсы сети (Network Interfaces)** правой кнопкой и выберите **Создать новый интерфейс вызова по требованию (New Demand-Dial Interface).**
2. Следуйте инструкциям *Мастера интерфейса вызова по требованию* (Demand Dial Interface Wizard).

Единственное исключение, когда интерфейс создается вручную, — при добавлении нового сетевого адаптера уже после настройки и запуска службы *Маршрутизация и удаленный доступ*.

Новый интерфейс создают в подузле интерфейсов узла **IP-маршрутизация (IP Routing).**

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **Общие (General)** правой кнопкой и выберите **Новый интерфейс (New Interface).**
2. В открывшемся окне выберите добавляемый интерфейс и щелкните OK.
3. При необходимости в дополнительных окнах определите конфигурацию интерфейса.

Узел *IP-маршрутизация*

Узел **IP-маршрутизация (IP Routing)** консоли *Маршрутизация и удаленный доступ* служит для настройки основных параметров маршрутизации по протоколу IP. По умолчанию он содержит три подузла: **Общие (General), Статические маршруты (Static Routes)** и **NAT/Простой брандмауэр (NAT/Basic Firewall)** (рис. 9-3).

Настройка параметров службы *Маршрутизация и удаленный доступ*

Параметры службы *Маршрутизация и удаленный доступ* настраиваются в окне свойств узла сервера в консоли *Маршрутизация и удаленный доступ*. К этим параметрам относятся: маршрутизация, вызов по требованию, включение поддержки удаленного доступа, конфигурация аутентификации, назначение адресов пользователей, протокол PPP (Point-to-Point Protocol) и особенности входа в систему.

Вкладка *Общие*

Вкладка **Общие (General)** (рис. 9-4) служит для настройки службы *Маршрутизация и удаленный доступ* для выполнения функции маршрутизатора ЛВС, маршрутизатора вызовов по требованию, сервера удаленного доступа или всех трех функций. Например, если выбрать вариант **Только локальной сети [Local area network (LAN) routing only]** и не установить флажок **Сервер удаленного доступа (Remote access server),** не будут доступны ни маршрутизация вызовов по требованию, ни удаленный доступ. До создания любых интерфейсов вызовов по требованию следует установить в консоли *Маршрутизация и удаленный доступ* флажок **Локальной сети и вызова по требованию (LAN and demand-dial routing).** Точно так же, чтобы позволить удаленным клиентам подключаться к локальному серверу надо установить флажок **Сервер удаленного доступа.**

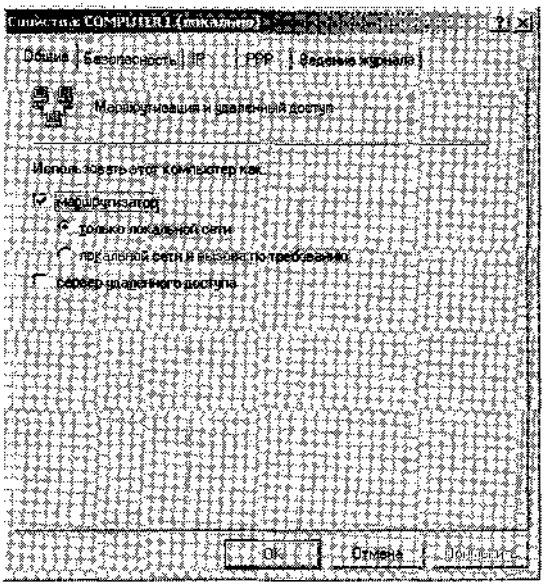


Рис. 9-4. Вкладка *Общие* окна свойств службы *Маршрутизация и удаленный доступ*

Вкладка *Безопасность*

Вкладка **Безопасность (Security)** *(рис.* 9-5) служит для настройки методов аутентификации, записи информации о запросах на подключение и *предварительных ключей* (preshared keys) протокола IPSec (Internet Protocol Security). Эти параметры безопасности применяются как к клиентам удаленного доступа, так и к маршрутизаторам вызовов по требованию.

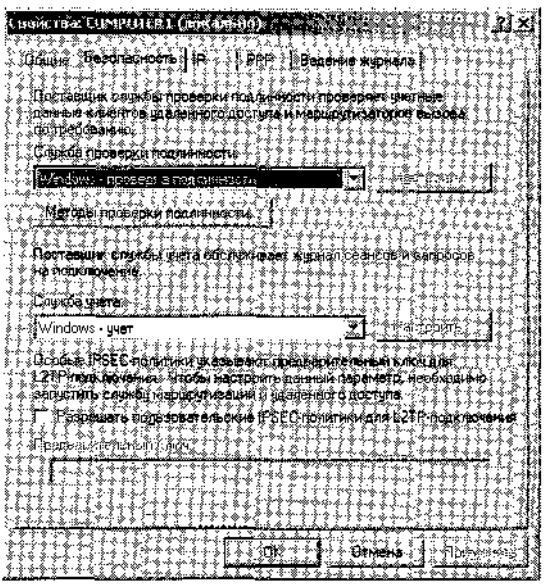


Рис. 9-5. Вкладка *Безопасность* окна свойств службы *Маршрутизация и удаленный доступ*

Вкладка *IP*

Вкладка **IP** (рис. 9-6) позволяет настроить службу *Маршрутизация и удаленный доступ* на маршрутизацию IP-пакетов по ЛВС и подключениям вызова по требованию или по телефонной линии. Параметры на вкладке **Общие** относятся к порядку маршрутизации, вызову по требованию и службе удаленного доступа вообще, а роль вкладки **IP** — настроить IP-трафик по подключениям различных типов. Поэтому для успешной настройки IP-маршрутизации и удаленного доступа надо указать соответствующие параметры на обеих вкладках — **Общие** и **IP.**

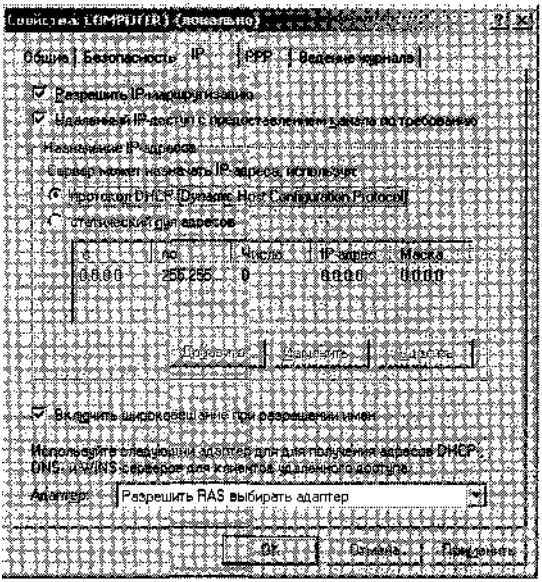


Рис. 9-6. IP-свойства маршрутизатора

В области **Назначение IP-адресов (IP Address Assignment)** определяется порядок назначения сервером IP-адресов клиентам удаленного доступа. При выборе варианта **Протокол DHCP (Dynamic Host Configuration Protocol) [Dynamic Host Configuration Protocol (DHCP)]** клиенты удаленного доступа получают адреса от DHCP-сервера. Если функцию последнего выполняет не сама служба *Маршрутизация и удаленный доступ,* DHCP-серверы надо подключить к интерфейсу удаленного доступа с помощью агента ретрансляции DHCP.

С другой стороны, при выборе варианта **Статический пул адресов (Static address pool)** функции DHCP-сервера берет на себя служба *Маршрутизация и удаленный доступ*. В этом случае надо вручную определить диапазон адресов, назначаемых клиентам.

Наконец, на вкладке **IP** есть флажок **Включить широковещание при разрешении имен (Enable broadcast name resolution),** при установке которого клиенты удаленного доступа получают возможность разрешать имена компьютеров всех сетевых сегментов, напрямую подключенных к компьютеру со службой *Маршрутизация и удаленный доступ* — даже в отсутствие DNS-или WINS-серверов. По существу, эта включенная по умолчанию функция позволяет маршрутизатору пересылать направляемые клиентом удаленного доступа широковещательные сообщения NetBT (NetBIOS поверх TCP/IP) во все сетевые сегменты, подключенные к маршрутизатору (рис. 9-7).

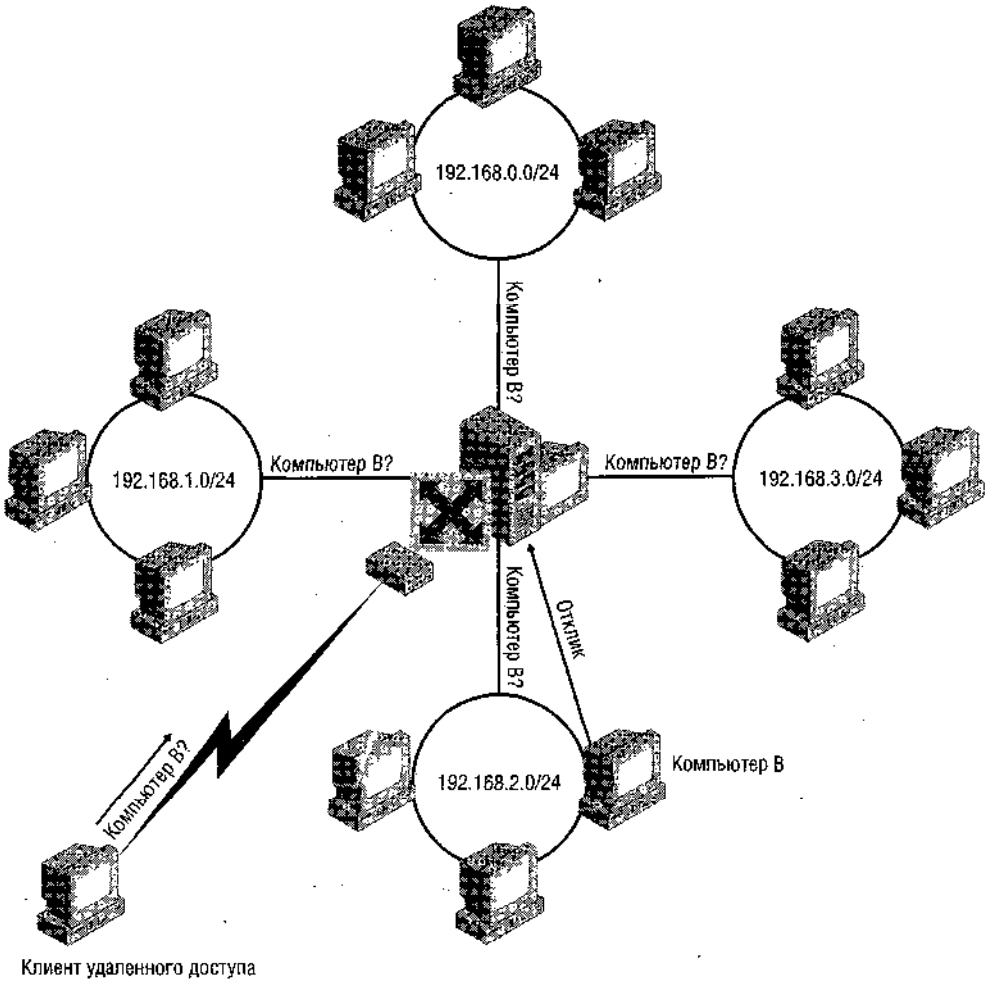


Рис. 9-7. Широковещание запросов на разрешение имен в службе *Маршрутизация и удаленный доступ* разрешено

Вкладка *PPP*

Вкладка **PPP** (рис. 9-8) применяется для согласования и аутентификации подключений по телефонной линии. На вкладке четыре относящихся к: PPP флажка: **Многоканальные подключения (Multilink connections), Дин. управление пропускной способностью (BAP/BACP) (Dynamic bandwidth control using BAP or BACP), Расширения протокола управления связью (LCP) [Link control protocol (LCP) extensions]** и **Программное сжатие данных (Software Compression).** Все они по умолчанию установлены.

Многоканальные подключения — при установке этого флажка служба *Маршрутизация и удаленный доступ* поддерживает многоканальные подключения от клиентов удаленного доступа. В этом случае несколько физических подключений работают как единое логическое подключение для приема и отправки данных. Таким образом клиенты PPP способны увеличить собственную полосу пропускания за счет объединения нескольких подключений к серверу удаленного доступа в один канал связи (при этом требуется определенным образом сконфигурировать клиент).

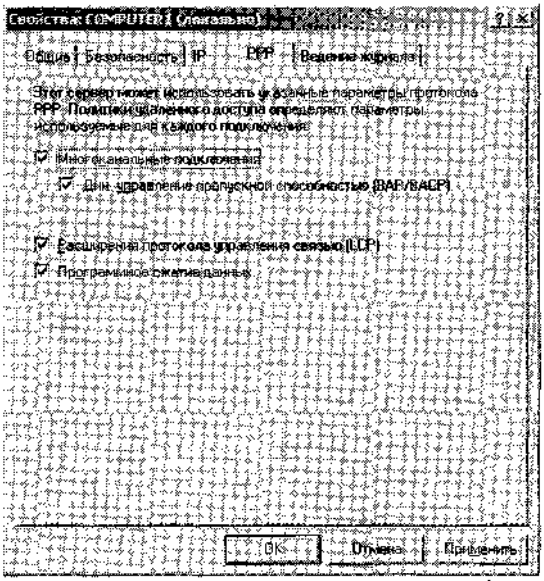


Рис. 9-8. Свойства PPP в службе *Маршрутизация и удаленный доступ*

Дин. управление пропускной способностью (BAP/BACP) — при установке этого флажка в многоканальных подключениях автоматически увеличивается/уменьшается число дополнительных PPP-подключений в соответствии с расширением/сужением доступной пропускной способности. Такая функция — она называется *пропускная способность по требованию,* или BOD (bandwidth on demand), — обеспечивается за счет взаимодействия двух протоколов: BAP (Bandwidth Allocation Protocol) и BACP (Bandwidth Allocation Control Protocol).

Расширения протокола управления связью (LCP) — флажок необходим для поддержки некоторых дополнительных возможностей PPP, например *обратного вызова* (callback). Этот флажок должен быть установлен — исключение составляет ситуация, когда клиенты не в состоянии подключиться по PPP. Отключение этого флажка также необходимо при неполадках «устаревших» клиентов, не поддерживающих эти расширения.

Программное сжатие данных — этот флажок позволяет службе *Маршрутизация и удаленный доступ* выполнять сжатие данных PPP на программном уровне. Оставьте этот флажок включенным, если модем PPP-клиента поддерживает эту функцию на аппаратном уровне.

Вкладка *Ведение журнала* .

На вкладке **Ведение журнала (Logging)** определяют порядок регистрации событий службы *Маршрутизация и удаленный доступ*. По умолчанию служба сконфигурирована для регистрации только ошибок и предупреждений. На рис. 9-9 показаны другие параметры записи событий. Обратите внимание, что вкладка позволяет сконфигурировать регистрацию дополнительной информации для целей отладки.

Управление общими свойствами IP-маршрутизации

Некоторые функции службы *Маршрутизация и удаленный доступ* (Routing and Remote Access относятся в целом к IP и управляются только в окне свойств подузла **Общие (General)** узла **IP-маршрутизация (IP Routing)** в консоли **Маршрутизация и удаленный доступ.**

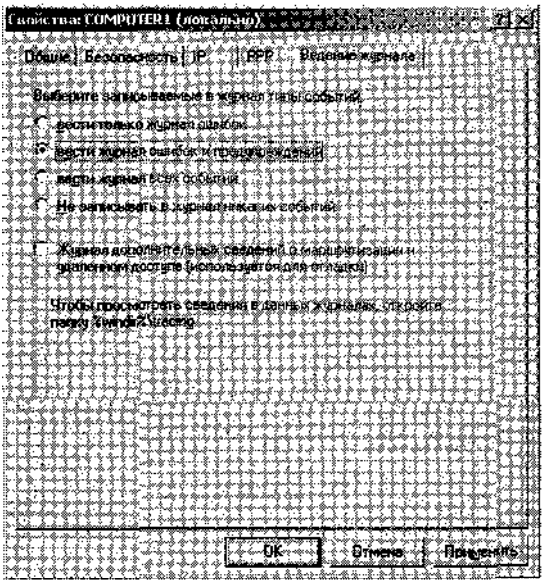


Рис. 9-9. Параметры регистрации событий службы *Маршрутизация и удаленный доступ*

Чтобы открыть окно **Свойства: Общие (General Properties),** щелкните правой кнопкой подузел **Общие (General)** узла **IP-маршрутизация (IP Routing)** в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) и выберите **Свойства (Properties).** Окно содержит три вкладки: **Ведение журнала (Logging), Уровни предпочтений (Preference Levels)** и **Многоадресные области (Multicast Scopes).** (Поскольку знание многоадресных рассылок на экзамене не проверяется, мы поговорим только о первых двух вкладках.)

Вкладка *Ведение журнала*

На этой вкладке (рис. 9-10) определяют, какие события IP-маршрутизации регистрируются в журнале событий. По умолчанию записывается только информация об ошибках, но вы вправе выбрать более подробный уровень — **Вести журнал ошибок и предупреждений (Log errors and warnings)** или **Вести журнал всех событий (Log the maximum amount of information)** — или вовсе отключить запись в журнал, выбрав вариант **Отключить журнал событий (Disable event logging).**

Вкладка *Уровни предпочтений*

Вкладка **Уровни предпочтений** (рис. 9-11) служит для определения приоритетов маршрутов IP-маршрутизации, информация о которых поступает из различных источников. Когда два источника предоставляют противоречивые маршруты, в таблицу маршрутизации записывается только маршрут с более высоким уровнем предпочтения. Таким образом, уровни предпочтений заменяют собой любые метрики маршрутов.

Уровни предпочтений перечисляются в определенном порядке. Первый (верхний) источник маршрута обладает наивысшим приоритетом и самый низким рангом (1), а источник маршрутов с наименьшим приоритетом имеет самый низкий приоритет и самый высокий номер ранга (120). Корректируют ранг источника маршрутов, выбрав его в списке и щелкая кнопки **Повысить уровень (Move Up)** или **Понизить уровень (Move Down)** нужное число раз.

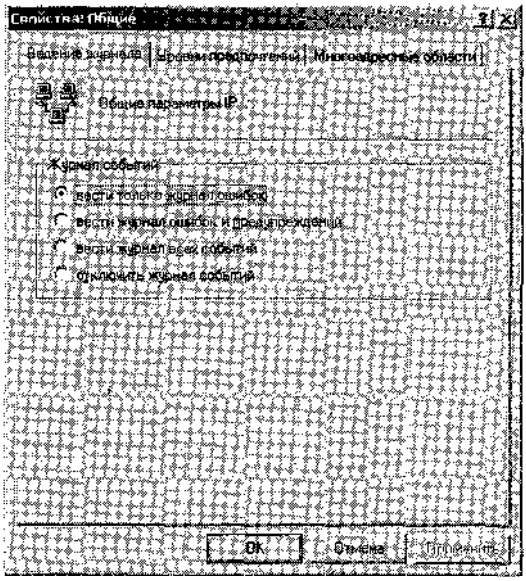


Рис. 9-10. Параметры записи журнала событий IP-маршрутизация

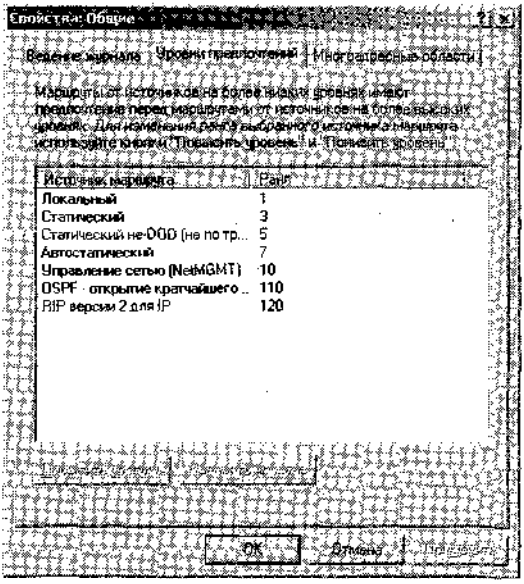


Рис. 9-11. Уровни предпочтений IP-маршрутизации

Управление таблицами маршрутизации

Маршрутизаторы считывают адреса назначения пакетов и переправляют пакеты в соответствии с информацией, хранящейся в таблицах маршрутизации. На рис. 9-12 показан пример таблицы маршрутизации.

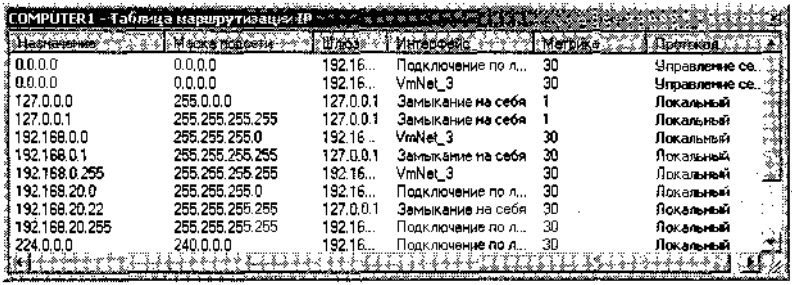


Рис. 9-12. Таблица IP-маршрутизации

Отдельные записи таблицы маршрутизации называются *маршрутами* (routes) — они содержат ссылки на сети и узлы-адресаты. Существуют три типа маршрутов.

- **Маршрут узла** (host route) — определяет ссылку на определенный узел или широковещательный адрес. В таблицах маршрутизации IP такие маршруты обозначаются маской подсети 255.255.255.255.
- **Маршрут сети** (network route) — определяет маршрут к определенной сети, а соответствующее поле в таблицах IP-маршрутизации может содержать любую маску подсети из диапазона 0.0.0.0-255.255.255.255.
- **Маршрут по умолчанию** (default route) — один маршрут, по которому «уходят» все пакеты, чей адрес назначения не совпадает ни с одним адресом таблицы маршрутизации. В таблицах IP-маршрутизации такому маршруту соответствует адрес 0.0.0.0 и маска подсети 0.0.0.0.

Просмотр таблицы IP-маршрутизации

Увидеть таблицу IP-маршрутизации можно в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) или в командной строке.

В консоли *Маршрутизация и удаленный доступ* разверните узел **IP-маршрутизация (IP Routing),** щелкните правой кнопкой узел **Статические маршруты (Static Routes)** и выберите **Отобразить таблицу IP-маршрутизации (Show IP Routing Table)** (рис. 9-1.)

В командной строке таблица маршрутизации отображается командой `route print` (рис. 9-13).

Чтение таблицы 1P-маршрутизации

Маршрутизаторы используют таблицы маршрутизации для определения, куда отправлять пакеты. Приняв IP-пакет, маршрутизатор считывает адрес назначения и сравнивает его с записями таблицы маршрутизации, чтобы определить, какой интерфейс использовать для пересылки пакета и на какой шлюз.

Каждая запись таблицы маршрутизации содержит 5 полей (рис. 9-13).

Столбец **Сетевой адрес (Network Destination)** содержит информацию, с которой маршрутизатор сравнивает адрес назначения каждого полученного IP-пакета. Несколько значений этого поля совпадают в большинстве таблиц маршрутизации. Например, 0.0.0.0 представляет маршрут по умолчанию — он используется, когда не удается найти соответствия в других записях. Значение 127.0.0.0 указывает на *адрес замыкания.на себя* (loopback address), то есть на локальную машину. Кроме того, каждая из записей со значением 224.0.0.0 в этом поле относится к отдельному многоадресному маршруту. Записи со значением последнего октета 255 представляют широковещательный адрес. Такие адреса содержат конкретные адреса подсети, в которой должно выполняться широковещание, например 192.168.1.255, и зарезервированный широковещательный адрес 255.255.255.255, общий для всех сетей и маршрутизаторов.

```
C:\Documents and Settings\Администратор.COMPUTER1>route print

IPv4 таблица маршрута
===========================================================================
Список интерфейсов
0x1 ........................... MS TCP Loopback interface
0x2 ...00 50 ba 40 5c 73 ...... D-Link DFE-530TX+ PCI Adapter
0x10003 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
0x20004 ...00 53 45 00 00 00 ...... WAN (PPP/SLIP) Interface
===========================================================================
===========================================================================
Активные маршруты:
Сетевой адрес           Маска сети      Адрес шлюза       Интерфейс  Метрика
          0.0.0.0          0.0.0.0    207.46.252.3   207.46.252.88       1
        127.0.0.0        255.0.0.0      127.0.0.1      127.0.0.1        1
      192.168.1.0    255.255.255.0    192.168.1.1    192.168.1.1        1
      192.168.1.1  255.255.255.255      127.0.0.1      127.0.0.1        1
    192.168.1.31  255.255.255.255      127.0.0.1      127.0.0.1       50
    192.168.1.255  255.255.255.255    192.168.1.1    192.168.1.1        1
     207.46.252.3  255.255.255.255  207.46.252.88  207.46.252.88        1
    207.46.252.88  255.255.255.255      127.0.0.1      127.0.0.1       50
   207.46.252.255  255.255.255.255  207.46.252.88  207.46.252.88       50
        224.0.0.0        240.0.0.0    192.168.1.1    192.168.1.1        1
        224.0.0.0        240.0.0.0  207.46.252.88  207.46.252.88       50
  255.255.255.255  255.255.255.255    192.168.1.1    192.168.1.1        1
Основной шлюз:        207.46.252.3
===========================================================================
Постоянные маршруты:
  Отсутствует

C:\Documents and Settings\Администратор.COMPUTER1>
```

Рис. 9-13. Таблица маршрутизации, отображенная средствами командной строки

Значение поля **Маска сети (Netmask)** определяет, какая часть адреса назначения сравнивается со значениями поля **Сетевой адрес.** Эта информация важна, так как определяет маршрут или строку таблицы, которая применяется для перенаправления пакета.

Допустим, маршрутизатор с таблицей маршрутизации, показанной на рис. 9-13, получает два пакета: первый направлен по адресу 192.168.1.1, а второй — 192.168.1.2. Оба пакета соответствуют условиям третьей строки таблицы, так как маска подсети 255.255.255.0 указывает на сравнение первых трех октетов с идентификатором сети, то есть с 192.168.1.0. С другой стороны, только первый пакет отвечает условиям четвертой записи (сетевая маска 255.255.255.255, и все четыре октета совпадают с адресом подсети 192.168.1.1). Таким образом, четвертая запись применяется для маршрутизации первого пакета, потому что именно она максимально соответствует параметрам пакета. А третья запись используется для перенаправления второго пакета, так как она одна отвечает условиям пакета (конечно же, за исключением маршрута по умолчанию).

Поле **Адрес шлюза (Gateway)** определяет следующий адрес, или *переход* (hop), по которому направляется пакет. Например, согласно таблице маршрутизации на рис. 9-13, IP-пакет с адресатом 206.73.118.5 (он соответствует только маршруту по умолчанию — 0.0.0.0) перенаправляется по адресу шлюза 207.46.252.3. Обратите внимание, что адрес шлюза маршрута по умолчанию совпадает с адресом основного шлюза, определенного в свойствах TCP/IP.

Важно понять одно: адрес шлюза должен отличаться от адреса сети назначения, указанного в той же сроке таблицы маршрутизации, даже если сеть назначения находится в пределах широковещательного диапазона маршрутизатора. Например, на рис. 9-13 шестая запись указывает на адрес 207.46.252.0/24 одной из двух подсетей, с которыми напрямую подключен маршрутизатор, (Другая подсеть — 192.168.1.0/24.)

Несмотря на прямое подключение к подсети 207.46.252.0/24, маршрутизатор принимает пакеты, направленные в эту подсеть только через интерфейс192.168.1.1. (Кстати, пакеты, поступающие из подсети 207.46.252.0/24, не нуждаются в том, чтобы маршрута-

затор возвращал их обратно в ту же подсеть.) Таким образом, следующий переход для пакетов из одной из локальных подсетей маршрутизатора — другой интерфейс маршрутизатора. Поэтому в качестве шлюза в таблице маршрутизации указан интерфейс маршрутизатора в этой целевой подсети (207.46.252.88).

Совет Другой способ разобраться в причине отличий между адресом шлюза и адресом целевой сети — взглянуть на каждую запись таблицы маршрутизации как на указание направления (интерфейс и шлюз) для доставки пакета нужному адресату. Теперь понятно, почему записи не дадут направления, если будут просто дублировать адресат. (Как попасть в 192.168.1.5? Да просто отправляйтесь по адресу 192.168.1.5 — тавтология!) Таким образом, когда целевая сеть находится в пределах широковещательного диапазона маршрутизатора, таблица маршрутизации направляет не напрямую в целевую сеть, а на локальный адрес собственного интерфейса маршрутизатора, который подключен к целевой подсети. Поэтому адрес шлюза совпадает с адресом интерфейса. Аналогично, когда адресат — один из собственных адресов маршрутизатора, в таблице маршрутизации указывается другой адрес в качестве шлюза и интерфейса — адрес замыкания на себя, или 127.0.0.1.

После выбора маршрута (записи таблицы) значение поля **Интерфейс (Interface)** определяет, на который из интерфейсов локальной сети перенаправить пакет. Например, на рис. 9-13 IP-пакет на адрес 131.107.23.101 отвечает только маршруту по умолчанию. Согласно таблице маршрутизации, такой пакет направляется через интерфейс 207.46.252.88 по адресу основного шлюза.

Поле **Метрика (Metric)** указывает на стоимость маршрута. Если IP-пакету соответствуют несколько маршрутов (записей), метрика определяет, какой из них выбрать. Чем меньше метрика, тем предпочтительнее маршрут.

В протоколе маршрутизации RIP метрика определяет числом переходов до целевой сети. Однако при настройке маршрута вручную назначать метрики допускается по любому удобному алгоритму.

Статическая и динамическая маршрутизация

На каждом узле и маршрутизаторе протокол IP автоматически строит простую таблицу маршрутизации с минимально необходимыми целевыми сетями. Существует восемь типов таких адресов: адрес по умолчанию, адрес замыкания на себя, основной шлюз, локальные адреса, адреса локальных подсетей, широковещательные адреса локальных подсетей, ограниченные широковещательные адреса и адреса многоадресной рассылки на каждом адаптере.

Все эти восемь типов записей описывают маршруты, напрямую связанные с IP-узлом или маршрутизатором. Такая схема работает только в простых ситуациях, а в сложной сети маршрутизатору надо четко указать, на который их множества его интерфейсов отправлять пакеты, адресованные в неизвестные (не соседние) сети.

Поддержка трафика на узлы, расположенные за пределами широковещательного диапазона, обеспечивается одним из двух способов. Во-первых, путем определения маршрутов вручную, командой route add, или в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access). Так определяют порядок *статической маршрутизации* (static routing). Второй вариант: сконфигурировать динамический протокол маршрутизации, например RIP или OSPF, который позволит маршрутизаторам обмениваться ин-

формацией таблиц маршрутизации. Такой процесс называется *динамической маршрутизацией* (dynamic routing).

В табл. 9-1 приводятся основные различия между статической и динамической маршрутизацией.

Табл. 9-1. Сравнение статической и динамической маршрутизации

Статическая маршрутизация	Динамическая маршрутизация
Функция IP	Функция протоколов маршрутизации, например RIP или OSPF
Маршрутизаторы не обмениваются информацией о маршрутизации	Маршрутизаторы автоматически обмениваются информацией маршрутизации
Таблицы маршрутизации создаются и поддерживаются вручную	Таблицы маршрутизации строятся и поддерживаются динамически

Примеры организации маршрутизации в ЛВС

Маршрутизаторы применяются в самых различных топологиях и конфигурациях сети. В процессе настройки сервера со службой *Маршрутизация и удаленный доступ* обычно определяют следующее:

- маршрутизируемые протоколы (IP или AppleTalk);
- маршрутизируемые протоколы маршрутизации (RIP или OSPF);
- среду связи в ЛВС или WAN-линиях (сетевые адаптеры, модемы и другое оборудование).

Простой вариант маршрутизации

На рис. 9-14 показана простая сетевая конфигурация с сервером со службой *Маршрутизация и удаленный доступ,* соединяющим два сегмента локальной сети (сеть А и сеть В). В такой конфигурации протоколы маршрутизации не нужны; также не нужно определять вручную статические маршруты, потому что маршрутизатор напрямую связан со всеми сетями, которые обслуживает.

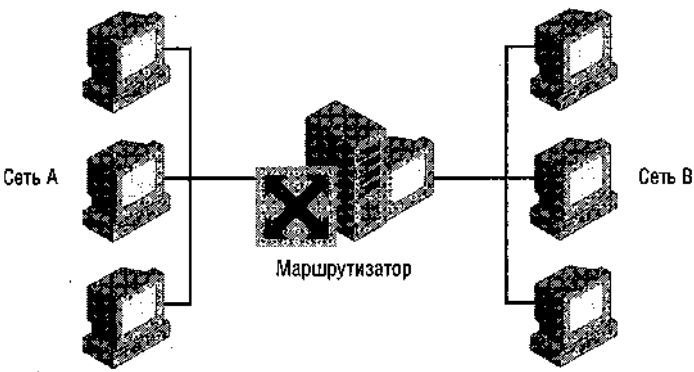


Рис. 9-14. Локальная маршрутизация без протоколов маршрутизации и статических маршрутов

Вариант со многими маршрутизаторами

На рис. 9-15 показана более сложная конфигурация маршрутизаторов. Здесь три сети (A, B и C) связаны двумя маршрутизаторами (1 и 2). Маршрутизатор 1 напрямую связан с сетями A и B, а маршрутизатор 2 — с сетями B и C. Маршрутизатор 1 должен уведомить Маршрутизатор 2 о достижимости сети A через Маршрутизатор 1, а Маршрутизатор 2 — уведомить Маршрутизатор 1, что сеть C доступна через Маршрутизатор 2. Обмен этой информацией происходит автоматически — по протоколу маршрутизации RIP или OSPF. Когда пользователь сети A направляет пакет пользователю в сети C, с компьютера первого пользователя пакет попадает на Маршрутизатор 1, который переправляет его на Маршрутизатор 2, а тот, в свою очередь, пересылает пакет на компьютер пользователя в сети C.

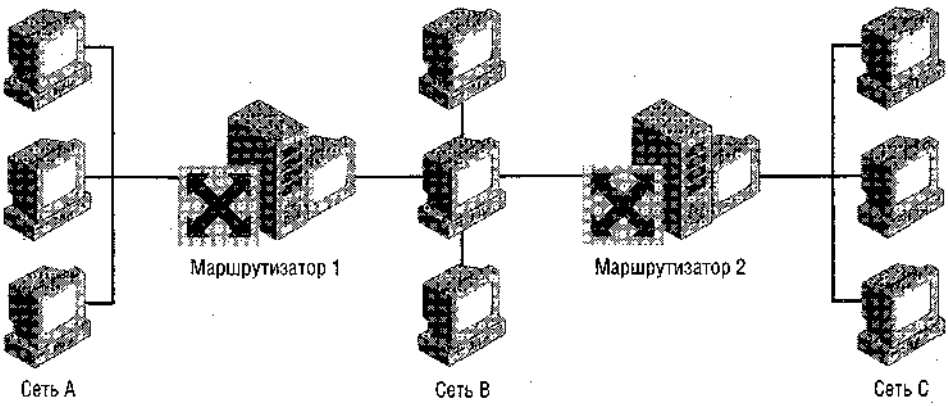


Рис. 9-15. Маршрутизация с использованием протоколов маршрутизации или статических маршрутов

В отсутствие протоколов маршрутизации сетевому администратору придется вручную определять статические маршруты в таблицах маршрутизации маршрутизаторов 1 и 2. Статические маршруты прекрасно работают в простых сетях, но в сложных ими очень трудно управлять. Кроме того, статические маршруты автоматически не изменяются в соответствии с изменениями топологии сети.

Основные сведения о статических маршрутах

В сетях со статической маршрутизацией не используются протоколы маршрутизации, например RIP или OSPF, для обмена информацией маршрутизации между маршрутизаторами. Такое решение больше всего подходит для мелких, статических сетей с одним маршрутом. Лучше всего, когда сеть состоит не более чем из 10 подсетей. Кроме того, эти подсети должны размещаться последовательно (в линию) — это обеспечит максимальную предсказуемость пути прохождения трафика. И еще: топология сетей со статической маршрутизацией не должна изменяться со временем.

В примере на рис. 9-16 маршрутизатор «C-B» «видит» все компьютеры подсетей C и B. Получив пакет, не адресованный в одну их этих подсетей, он пересылает его по маршруту по умолчанию на маршрутизатор «B-A». Поскольку все компьютеры, внешние по отношению к подсетям B *и* C, находятся в направлении маршрута по умолчанию, в таблицу маршрутизации на маршрутизаторе «C-B» не надо добавлять дополнительные статические маршруты.

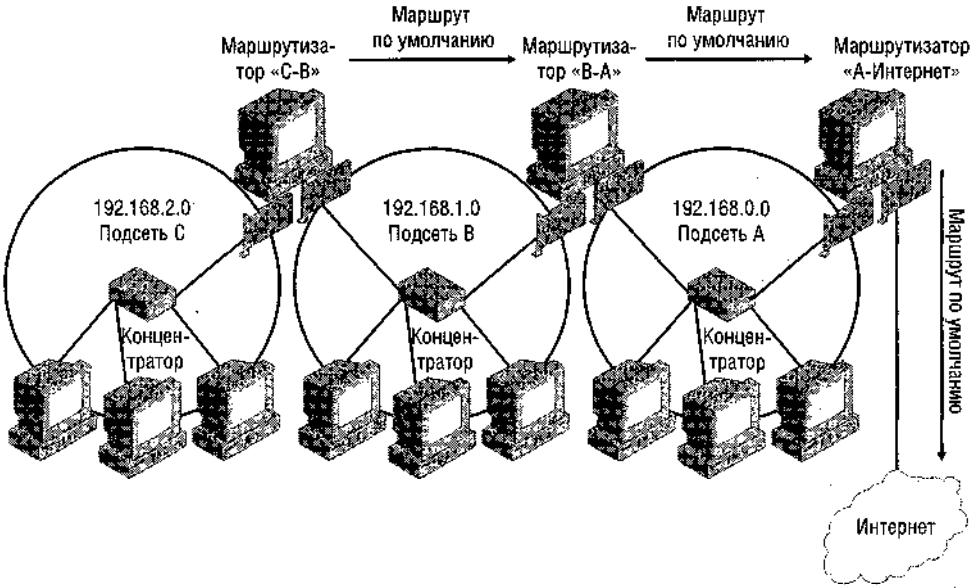


Рис. 9-16. Пример сети, подходящей для статической маршрутизации

Хотя маршрутизатор «B-A» и «видит» все компьютеры подсетей B и A, компьютер! подсети C не лежат в направлении определенного на нем маршрута по умолчанию. Есл] его не проинструктировать должным образом, маршрутизатор, получив пакет в подсеть C ошибочно переправит его вперед на маршрутизатор «A-Интернет». Дополнительный ста тический маршрут в таблице маршрутизатора «B-A» (рис. 9-17) позволит ему правильна направлять трафик в подсеть C, то есть пересылать его на маршрутизатор «C-B».

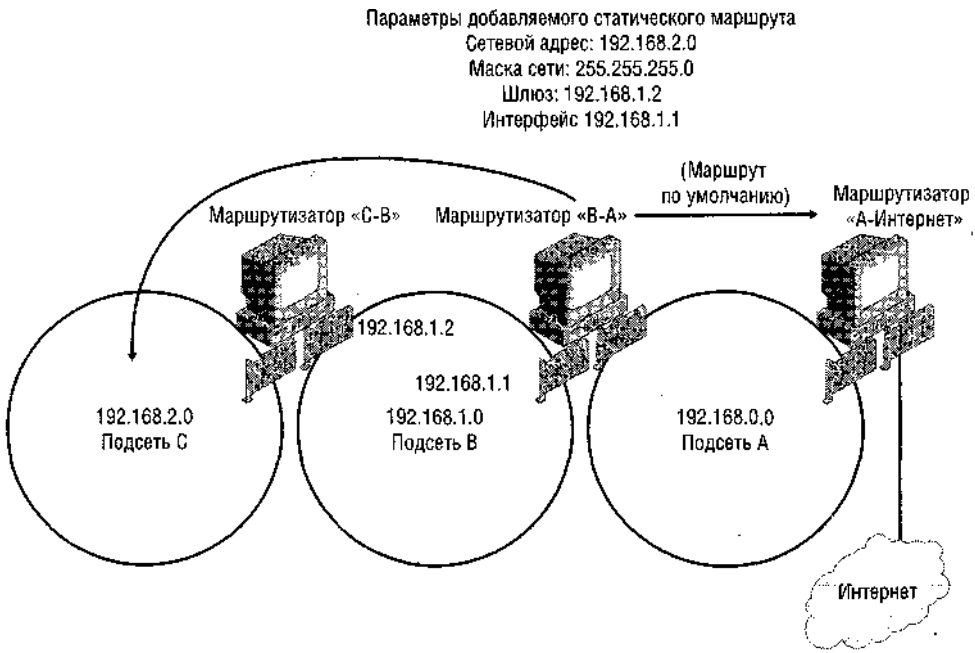


Рис. 9-17. Создание статического маршрута

Вместе с тем, маршрутизатору «А-Интернет» видны компьютеры подсети А и вышестоящий компьютер интернет-провайдера. Поскольку маршрут по умолчанию направляет трафик в Интернет, в отсутствие статических маршрутов пакеты, направленные в подсети С и В, ошибочно переправляются в Интернет. На рис. 9-18 показано, как определить эти маршруты. Заметьте: статическому маршруту в подсеть С достаточно указывать только на соседний маршрутизатор «В-А», который сам не видит подсеть С, но направленные в нее пакеты все равно попадают по назначению за счет статического маршрута, сконфигурированного на маршрутизаторе «В-А», который в свою очередь пересылает их на маршрутизатор «С-В».

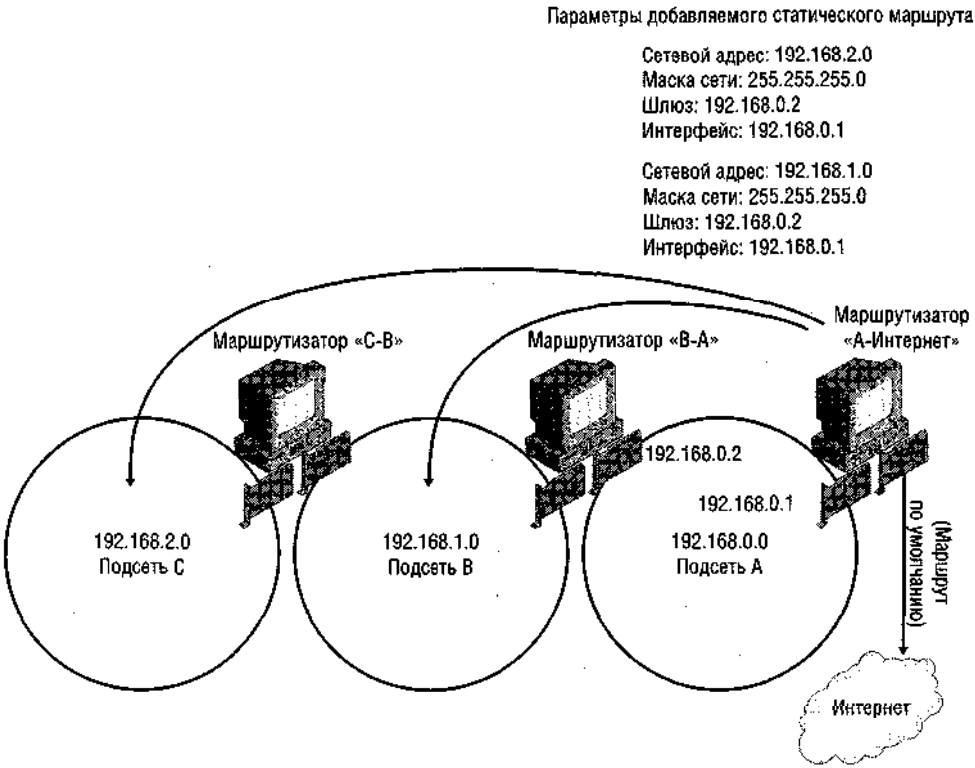


Рис. 9-18. Создание дополнительных статических маршрутов

Создание статических маршрутов

Статические маршруты создаются в консоли *Маршрутизация и удаленный доступ* или посредством утилит командной строки.

- **Создание статического маршрута в консоли *Маршрутизация и удаленный доступ***

1. **В** дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните подузел **Статические Маршруты (Static Routes)** узла **IP-маршрутизация (IP Routing)** правой кнопкой и выберите **Новый статический маршрут (New static route).**

2. В окне **Статический маршрут (Static Route)** укажите значения полей **Интерфейс (Interface), Назначение (Destination), Маска подсети (Network mask), Шлюз (Gateway)** и **Метрика (Metric).**

Примечание Статические маршруты, созданные посредством консоли *Маршрутизация и удаленный доступ,* являются *постоянными* (persistent) и остаются активными даже после перезагрузки компьютера.

В командной строке статический IP-маршрут создается следующей командой:

route add <*адресат*> **mask** <*маска подсети*> <*шлюз*> **metric** <метрика> if <*интерфейс*>

Указывать метрику не обязательно, да и интерфейс выбирается автоматически, если его не указать. Например, чтобы добавить статический маршрут в сеть 10.0.0.0 с маской подсети 255.0.0.0 и шлюзом 192.168.0.1, достаточно такой команды:

```
route add 10.0.0.0 mask 255.0.0.0 192.168.0.1
```

При использовании команды route следует учесть ряд моментов.

- Команда route создает непостоянные статические маршруты, если не задать параметр -p. Чтобы в указанном примере маршрут остался после перезагрузки компьютера, надо выполнить следующую команду:

  ```
  route add -p 10.0.0.0 mask 255.0.0.0 192.168.0.1
  ```

- Команда route delete служит для удаления маршрута. Ей достаточно информации, которая однозначно определяет удаляемый маршрут, например:

  ```
  route delete 10.0.0.0
  ```

- Статические маршруты, добавленные командой route, не отображаются в узле **Статические маршруты** консоли *Маршрутизация и удаленный доступ* — их можно увидеть наряду с другими маршрутами при выборе команды **Отобразить таблицу IP-маршрутизации (Show IP Routing Table)** в контекстном меню.
- Интерфейсы в результате работы команды route обозначаются шестнадцатеричным номером, а не адресом интерфейса..

```
C:\>route print

IPv4 Route Table

Interface List
0x1. . . . . .MS TCP Loopback interface
0x2 ...00 50 ba 40 5c 73. . . . . .D-Link DFE-530TX+ PCI Adapter
0x10003 ...00 53 45 00 00 00 . .. :. . WAN (PPP/SLIP) Interface
0x20004 . .'.00 53 45 00 00 00. . . . . WAN (PPP/SLIP) Interface
```

Для ссылки на один из этих интерфейсов надо ввести либо шестнадцатеричный номер (включая префикс «0x»), либо его десятичный эквивалент. Обратите внимание, что шестнадцатеричные значения из диапазона 0x1—0x9 эквивалентны десятичным числам диапазона 1—9.

Таким образом, следующие две команды добавляют один и тот же маршрут:

```
route add 192.168.2.0 mask 255.255.255.0 192.168.1.2 IF 0x2
route add 192.168.2.0 mask 255.255.255.0 192.168.1.2 IF 2
```

А вот еще две равносильные команды (шестнадцатеричное число 0x10003 эквивалентно десятичному 65539):

```
route add 207.46.2.0 mask 255.255.255.0 207.46.1.2 IF 0x10003
route add 207.46.2.0 mask 255.255.255.0 207.46.1.2 IF 65539
```

Преимущества статической маршрутизации

Статическая маршрутизация удобна в маленьких сетях, где проще определить несколько статических маршрутов и не заниматься сложной процедурой настройки протокола динамической маршрутизации.

Другое преимущество статической маршрутизации — меньшая нагрузка на ресурсы, чем в протоколах динамической маршрутизации. Она не требует «общения» между маршрутизаторами, что делает статические маршруты предпочтительными при использовании малопроизводительных WAN-каналов.

Последнее преимущество статической маршрутизации — поддержка *ненумерованных подключений* (unnumbered connection), то есть таких, в которых у одного или обоих соединяющихся логических интерфейсов (обычно это подключение вызова по требованию) отсутствует IP-адрес. Как правило, маршрутизация вызовов по требованию выполняется с использованием нумерованных подключений, то есть запрашивающий и отвечающий маршрутизаторы получают IP-адреса друг друга и назначают их логическим конечным точкам прямого подключения.

При сбое этого процесса в Windows Server 2003 связывающиеся логические интерфейсы обычно получают APIPA-адреса (Automatic Private IP Addressing). Таким образом, ненумерованные подключения возникают, только когда какой-то из маршрутизаторов не поддерживает APIPA.

Недостатки статической маршрутизации

Главный недостаток статической маршрутизации — ее применимость только в мелких сетях. По мере увеличения сети затраты на администрирование растущего по экспоненте количества статических маршрутов быстро перевешивают стоимость развертывания и поддержки протокола динамической маршрутизации.

Второй недостаток — отсутствие поддержки отказоустойчивости. В случае ошибки в маршруте связь теряется, пока администратор не обнаружит и не устранит неполадку.

На заметку На экзамене вам наверняка предложат варианты локальных сетей со статическими маршрутами, но в реальности они используются только в отсутствие других вариантов, так как поддержка таких сетей — утомительное, отнимающее массу времени и неблагодарное занятие. Статические маршруты надо не только создавать, но постоянно обновлять и устранять неполадки, и все это вручную.

С другой стороны, протокол динамической маршрутизации RIP выполняет ту же функцию — создает статические маршруты, но зато прост в установке и практически не требует сопровождения. В крупных сетях, где статическая маршрутизация просто неприменима, требуется другой протокол динамической маршрутизации — OSPF.

В сущности, единственная ситуация, в которой нужны статические маршруты, а не RIP или OSPF, — когда подключение к удаленному маршрутизатору неустойчиво. В таких обстоятельствах протокол динамической маршрутизации не работает, так как требует регулярного обмена информации между маршрутизаторами — каждые 30 сек в RIP и 10 сек в OSPF.

Вопросы проектирования среды со статической маршрутизацией

Во избежание возможных неполадок при реализации статической маршрутизации не обходимо учитывать следующие моменты.

Конфигурация периферийного маршрутизатора

У *периферийных маршрутизаторов* (peripheral routers) по определению есть только один соседствующий маршрутизатор. Находясь на периферии сети, они подключают внешние подсети организации к ее магистральной сети. Для упрощения конфигурации обычно на периферийном маршрутизаторе задают маршрут по умолчанию, указывающий на соседствующий маршрутизатор. Пример такого маршрутизатора — маршрутизатор «С-В ; на рис. 9-16. Его маршрут по умолчанию указывает на соседствующий маршрутиза тор «В-А».

Маршруты по умолчанию и циклические маршруты

Рекомендуется не задавать на двух соседствующих маршрутизаторах маршруты по умол чанию друг к другу. Маршрут по умолчанию передает весь трафик, не предназначенные для непосредственно подключенной сети, на указанный маршрутизатор. Два маршру тизатора, заданные в маршрутах по умолчанию друг друга, могут образовывать циклы маршрутизации, делая невозможной доставку трафика узлам назначения

Лабораторная работа. **Включение и настройка службы *Маршрутизация и удаленный доступ***

Вы воспользуетесь *Мастером настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard) на Computerl, чтобы сконфигурироват; службу *Маршрутизация и удаленный доступ* (Routing and Remote Access) для маршрута зации в локальной сети.

Упражнение. Выполнение *Мастера настройки сервера маршрутизации и удаленного доступа*

Вы сконфигурируете и запустите службу *Маршрутизация и удаленный доступ* на Computerl

1. С Computerl войдите в домен Domainl *как Администратор* (Administrator).
2. Откройте консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access) выбрав **Пуск (Start)\Администрирование (Administrative TooЬД\Маршрутизация и уда ленный доступ (Routing and Remote Access).**
3. **В** дереве консоли *Маршрутизация и удаленный доступ* щелкните узел **COMPUTER (локально) [COMPUTER1 (Local)]** правой кнопкой и выберите **Настроить и включит маршрутизацию и удаленный доступ (Configure and Enable Routing And Remote Access)**
4. **В** окне **Мастер настройки сервера маршрутизации и удаленного доступа (Routing am Remote Access Server Setup Wizard)** щелкните **Далее** (Next).
5. На странице **Конфигурация (Configuration)** ознакомьтесь со списком возможных ва риантов. Выберите вариант **Особая конфигурация (Custom configuration)** и щелкнит **Далее.**

6. На странице **Особая конфигурация (Custom configuration)** ознакомьтесь со списком возможных вариантов и ответьте на вопрос: сколько базовых функций маршрутизации позволяет сконфигурировать данный мастер?
7. Установите флажок **Маршрутизация ЛВС (Routing LAN)** и щелкните Далее.
8. На странице **Завершение мастера сервера маршрутизации и удаленного доступа (Completing the Routing and Remote Access Server Setup Wizard)** щелкните **Готово (Finish).**
9. **В** информационном окне с предложением запустить службу *Маршрутизация и удаленный доступ* щелкните Да (Yes).
10. Выйдите из системы Computerl.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — • в разделе «Вопросы и ответы» в конце главы.

1. ИТ-отдел подключен к Интернету по *цифровой абонентской линии* (Digital Subscriber Line, DSL), которой также пользуются остальные подразделения организации. Однако вскоре отдел получил более быстрое подключение к Интернету по линии T1, которую решили использовать исключительно для нужд ИТ-отдела. DHCP-сервер предоставляет всем пользователям IP-конфигурацию, но компьютеры сотрудников ИТ-отдела распределены в тех подсетях, что и компьютеры обычных сотрудников. Как обеспечить, чтобы только сотрудники ИТ-отдела получили доступ к Интернету по новой линии T1? Причем требуется сконфигурировать эту возможность лишь раз с тем, чтобы потом ничего не пришлось изменять.
2. Вам не удается подключиться ни к одному компьютеру за пределами локальной подсети. Результат выполнения команды `route print` приведен ниже. В чем наиболее вероятная причина неполадки?

Network Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.1

3. После создания постоянного статического маршрута командой `route` он не обнаруживается в результатах работы команды `route print` на локальной машине. Маршруту назначена метрика 1. Предполагается, что команда выполнена успешно. В чем может быть причина неполадки?
4. Какие протоколы используются для поддержки многоканальных подключений и добавления/отключения подключений по телефонной линии по мере необходимости?

Резюме

- Служба *Маршрутизация и удаленный доступ* (Routing and Remote Access) в Windows Server 2003 — это многопротокольный программный маршрутизатор, который легко интегрируется с другими функциями Windows, например подсистемой безопасности и групповыми политиками. Консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access) — основной инструмент конфигурирования и управления этой службой.
- Маршрутизаторы считывают адреса назначения пакетов и переправляют пакеты в соответствии с информацией, хранящейся в таблицах маршрутизации. В Windows Server 2003 увидеть таблицу IP-маршрутизации можно в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) или с использованием команды `route print`.

- Приоритеты маршрутов определяются в окне **Свойства: Общие (General Properties),** которое открывается по щелчку команды **Свойства (Properties)** в контекстном меню подузла **Общие (General)** узла **IP-маршрутизация (IP Routing).** Приоритеты определяют, какие маршруты используются, если несколько источников предоставляют информацию о перекрывающихся маршрутах.
- Для подключения к не-соседним подсетям, когда нет протоколов динамической маршрутизации, а сами подсети располагаются в направлении, отличном от маршрута по умолчанию, на маршрутизаторе надо настроить статические маршруты.
- Статические маршруты создаются в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) или с использованием команды route add. Параметр -p в команде route add делает статический маршрут постоянным, то есть маршрут сохраняется даже после перезагрузки маршрутизатора.

Занятие 2. Настройка маршрутизации вызовов по требованию

Интерфейсы вызовов по требованию часто применяются для создания подключения между удаленными маршрутизаторами, известного как *маршрутизация вызовов по требованию* (demand-dial routing). Обычно она используется, когда цена создания выделенной линии связи между двумя маршрутизаторами неоправданно высока или когда подключение по выделенной линии используется достаточно редко и не оправдывает затраченных на него средств.

Изучив материал этого занятия, вы сможете:

V сконфигурировать маршрутизацию вызовов по требованию;

V управлять интерфейсами вызовов по требованию;

V устранять неполадки марпгоутизации вызовов по требованию.

Продолжительность занятия — около 60 минут.

Настройка интерфейсов вызовов по требованию

Первым делом при развертывании маршрутизации вызовов по требованию конфигурируют интерфейс вызовов по требованию на всех компьютерах, которые должны функционировать как маршрутизаторы таких вызовов. Это делается с помощью *Мастера интерфейса вызова по требованию* (Demand-Dial Interface Wizard). Причем этот мастер выполняется либо в процессе работы *Мастера настройки сервера маршрутизации и удаленного доступа* (Routing And Remote Access Server Setup Wizard), либо после настройки и запуска службы *Маршрутизация и удаленный доступ*.

Если служба *Маршрутизация и удаленный доступ* настроена и запущена без поддержки вызовов по требованию, эту функцию надо включить до создания каких бы то ни было интерфейсов вызовов по требованию. Для этого устанавливают флажок **Локальной сети и вызова по требованию (LAN and demand-dial routing)** на вкладке **Общие (General)** окна свойств службы *Маршрутизация и удаленный доступ* (рис. 9-19).

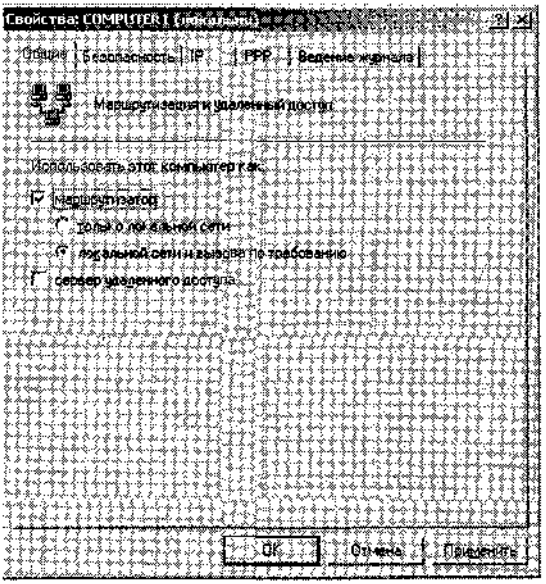


Рис. 9-19. Включение маршрутизации вызовов по требованию

Теперь можно запустить *Мастер интерфейса вызова по требованию,* щелкнув правой кнопкой узел **Интерфейсы сети (Network Interfaces)** в дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) и выбрав *Создать новый интерфейс вызова по требованию* (New Demand-Dial Interface). Мастер позволяет сконфигурировать базовые параметры интерфейса.

После создания и настройки основных свойств интерфейса вызовов по требованию переходят к более детальному конфигурированию в консоли *Маршрутизация и удаленный доступ*. Управление интерфейсами здесь делится на четыре области: команды контекстного меню, свойства интерфейса сети, свойства портов и свойства интерфейса IP-маршрутизации.

Команды контекстного меню

Команды контекстного меню интерфейса вызовов по требованию отображаются по щелчку правой кнопки интерфейса в правой панели консоли *Маршрутизация и удаленный доступ*. Интерфейсы отображаются в правой панели, когда в дереве консоли выбран узел **Интерфейсы сети (Network Interfaces)** (рис. 9-20). Заметьте, что помимо описанных ниже функций управления это контекстное меню позволяет устанавливать/разрывать связь через интерфейс вызовов по требованию или включать/отключать его.

Далее описаны четыре команды, характерные только для контекстного меню интерфейса вызовов по требованию.

- **Установить учетные данные (Set credentials)** служит для определения имени пользователя и пароля, используемого интерфейсом для подключения к удаленному маршрутизатору.
- **Причина недостижимости (Unreachability reason)** поясняет, в чем причина сбоя последней попытки подключения.

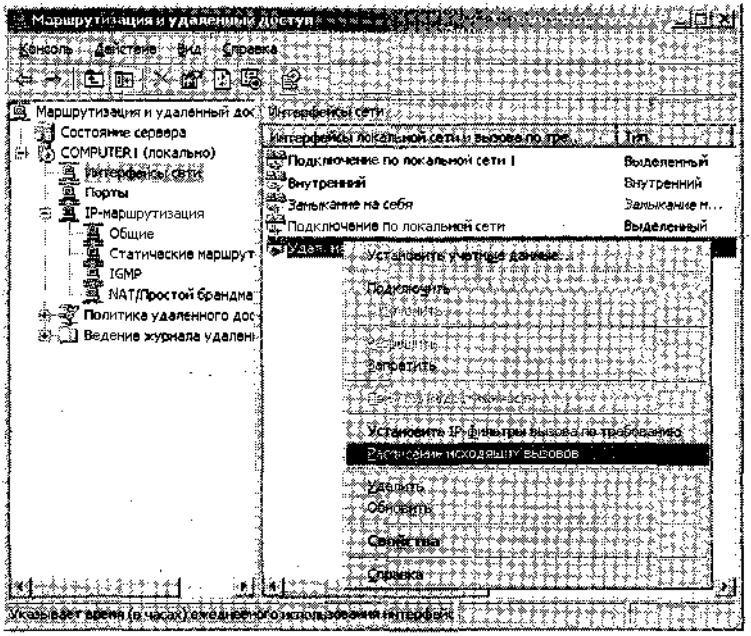


Рис. 9-20. Функции управления в контекстном меню

- **Установка IP-фильтров вызова по требованию (Set IP demand-dial filters)** служит для ограничения видов трафика, который инициирует подключение вызова по требованию через данный интерфейс. Подключения могут ограничиваться (фильтроваться) по исходному адресу, адресу назначения и протоколу.
- **Расписание исходящих вызовов (Dial-out hours)** позволяет задать часы, когда разрешен доступ к интерфейсу вызовов по требованию.

Свойства интерфейса сети

Когда выбран узел **Интерфейсы сети,** эти параметры можно конфигурировать в окне свойств интерфейса вызова по требованию. Окно содержит четыре вкладки.

Вкладка **Общие (General)** позволяет скорректировать параметры модема и задать основной номер телефона, относящийся к интерфейсу вызовов по требованию. Кнопка **Другие (Alternates)** служит для настройки списка дополнительных номеров телефона, по которым осуществляется вызов, если основной номер недоступен. Вы вправе также включить автоматическую настройку списка так, что «удачным» номерам назначается более высокий приоритет.

Вкладка **Параметры (Options)** (рис. 9-21). В области **Тип подключения (Connection Type)** интерфейс настраивается как **Вызов по требованию (Demand Dial)** или **Постоянное подключение (Persistent connection).** Интерфейсы первого типа подключаются по требованию, а второго — при потере связи. При выборе интерфейса вызовов по требованию на этой вкладке можно задать время простоя, по истечении которого подключение автоматически разъединяется.

В области **Политика набора номера (Dialing policy)** определяется число попыток повторного набора и интервала между ними.

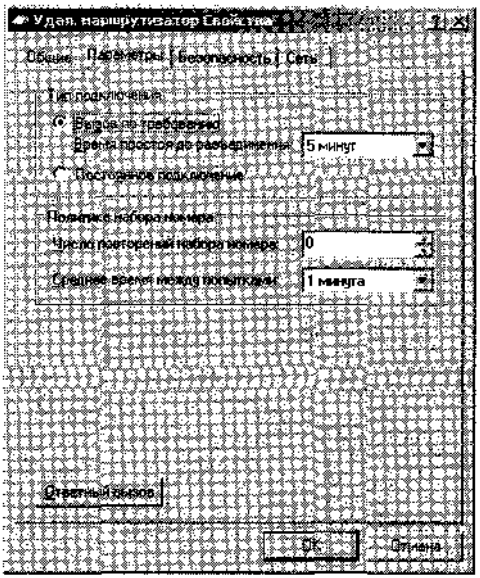


Рис. 9-21. Параметры интерфейса вызовов по требованию

Кнопка **Ответный вызов (Callback)** позволяет настроить параметры обратного вызова. Эта функция предусматривает, что после получения запроса сервер разрывает подключение и немедленно подключается по заданному номеру, так обеспечивается безопасность подключения, то есть его доступность только уполномоченным клиентам.

Кнопка **X.25** служит для конфигурирования интерфейса для поддержки сетей X.25.

На вкладке **Безопасность (Security)** при необходимости определяется пароль и/или включается шифрование данных в подключении вызова по требованию. Дополнительные параметры позволяют определить набор допустимых протоколов аутентификации, по которым интерфейс принимает реквизиты пользователя. По умолчанию в качестве протоколов аутентификации выбраны CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft CHAP) и MS-CHAP v2 (Microsoft CHAP version 2). (Подробнее о протоколах аутентификации и шифровании — в главе 10.) Наконец, эта вкладка позволяет задать сценарий входа в систему, используемый интерфейсом вызова по требованию.

Вкладка **Сеть (Networking)** нужна для привязки и конфигурирования стандартных элементов сетевого подключения, в том числе таких компонентов, как **Протокол Интернета (TCP/IP) [Internet Protocol (TCP/IP)], Служба доступа к файлам и принтерам сетей Microsoft (File and printer sharing for Microsoft networks)** и **Клиент для сетей Microsoft (Client for microsoft networks).**

Свойства портов и устройств

Чтобы открыть окно **Свойства: Порты (Ports Properties)** (рис. 9-22), в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **Порты (Ports)** правой кнопкой и выберите **Свойства (Properties).**

Выбрав модем, используемый в подключении вызова по требованию, щелкните кнопку **Настроить (Configure),** откроется окно **Настройка устройства (Configure Device)** (рис. 9-23). Оно позволяет настроить модем: только для входящих или входящих и исхо-

дящих подключений. Здесь же указывается номер телефона для устройства. Этот номер может считываться вызывающим интерфейсом и использоваться в политике удаленного доступа, в которой задействован атрибут Called-Station-Id. Он требуется для подключений с поддержкой BAP — его использует клиент, когда ему нужны дополнительные подключения.

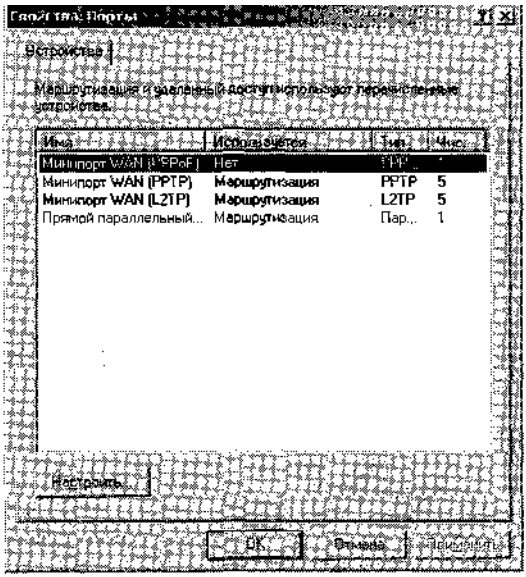


Рис. 9-22. Окно свойств портов

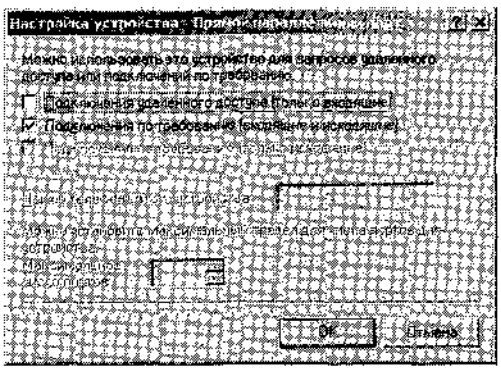


Рис. 9-23. Конфигурирование устройства вызовов по требованию

И последняя особенность управления, связанная с узлом **Порты,** — окно **Состояние порта (Port Status).** При выборе узла **Порты** в консоли *Маршрутизация и удаленный доступ* в правой панели отображается список портов подключения, в котором кроме прочего указаны доступные модемы или устройства. Подробности состояния можно увидеть в окне **Состояние порта,** которое открывается двойным щелчком значка модема или устройства, содержит статистику (когда устройство активно) и позволяет сбросить модемное подключение.

Особенности интерфейса IP-маршрутизации

Эти функции управления доступны в подузле **IP-маршрутизация (IP Routing)** узла консоли *Маршрутизация и удаленный доступ.* При выборе подузла **Общие (General)** в узле **IP-маршрутизация** в правой панели отображаются сконфигурированные на сервере интерфейсы. Контекстное меню интерфейса вызовов по требованию содержит различные команды управления вызовами по требованию и устранения неполадок (рис. 9-24).

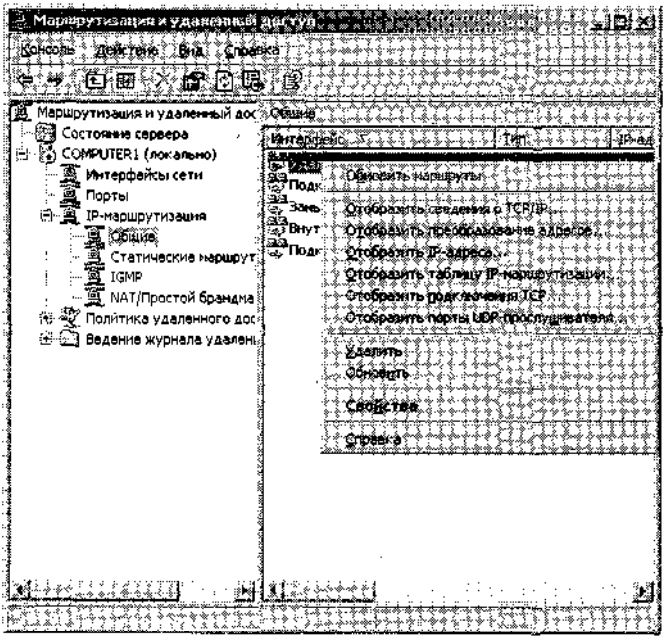


Рис. 9-24. Команды интерфейса IP-маршрутизации вызовов по требованию

Команда **Обновить маршруты (Update Routes)** отображается в контекстном меню интерфейса IP-маршрутизации вызовов по требованию. Когда эта команда выполняется при наличии протокола маршрутизации RIP, она автоматически обновляет статические маршруты интерфейса вызовов по требованию. Статические маршруты, обновленные этой командой, не требуют никакого дальнейшего конфигурирования и называются *автостатическими* (autostatic). По причине непостоянного характера подключений вызова по требованию вместо нормальных межмаршрутизаторных связей по протоколу RIP используются автостатические маршруты. Важно, что такие маршруты можно автоматически обновлять, настроив сценарий, периодически выполняемый службой *Планировщик заданий* (Task Scheduler).

Команда **Отобразить сведения о TCP/IP (Show TCP/IP information)** позволяет получить информацию о TCP/IP, обычно предоставляемую утилитами командной строки Ipconfig, Route Print и Netstat. Эти сведения об активных TCP- и UDP-подключениях, отправленных байтах и назначенных IP-адресах используются для проверки и устранения неполадок связи по сети.

Команда **Сведения (Properties)** открывает окно свойств интерфейса вызовов по требованию (рис. 9-25), которое отличается от подобного окна, доступного при выбранном узле **Интерфейсы сети (Network Interfaces).** Окно содержит три вкладки: **Общие (General),**

Границы многоадресной области (Multicast Boundaries) и **Пульс многоадресной рассылки (Multicast Heartbeat).** Поскольку знание многоадресных рассылок на экзамене не проверяется, поговорим только о вкладке **Общие.**

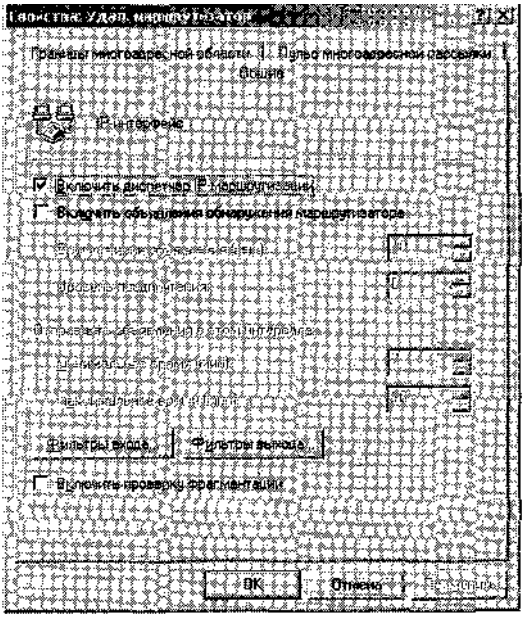


Рис. 9-25. Свойства интерфейса IP-маршрутизации

На вкладке **Общие** по умолчанию установлен флажок **Включить диспетчер IP-маршрутизации (Enable IP router manager).** Диспетчер IP-маршрутизации — это компонент службы *Маршрутизация и удаленный доступ,* отвечающий за многие функции маршрутизации, в том числе фильтрацию пакетов, преобразование сетевых адресов и динамическую маршрутизацию. При необходимости временного отключения IP-маршрутизации можно сбросить этот флажок.

Флажок **Включить объявления обнаружения маршрутизатора (Enable router discovery advertisements)** по умолчанию сброшен. Он управляет функцией, известной как *обнаружение маршрутизатора* (router discovery), которая требует настройки не только машрутизатора, но и узлов. Сетевые узлы направляют *запросы на обнаружение маршрутизатора* (solicitations), на которые те отвечают периодическими *объявлениями* (advertisements). Это позволяет выявить в сети «живые» маршрутизаторы. Запросы и объявления выполняются по протоколу ICMP (Internet Control Message Protocol).

Кнопки **Фильтры входа (Inbound Filters)** и **Фильтры выхода (Outbound Filters)** служат для управления фильтрацией пакетов (см. занятие 5), то есть разрешением/запрещением пакетов на основании основе источника, адресата или типа протокола (TCP или UDP).

Сброшенный по умолчанию флажок **Включить проверку фрагментации (Enable fragmentation checking)** также относится к фильтрации пакетов. Если заблокировать пакеты с определенного адреса, то при установленном флажке блокируются также фрагменты пакетов, поступающие с того же адреса.

Развертывание среды вызовов по требованию

Хотя принцип маршрутизации вызовов по требованию прост, его реализация — дело непростое из-за большого числа функций, требующих настройки.

Адресация конечной точки подключения

Подключение должно выполняться по сетям передачи данных общего пользования, например по телефонной сети общего пользования (PSTN). Конечная точка подключения должна обозначаться определенным идентификатором, например номером телефона.

Аутентификация и авторизация вызывающего маршрутизатора

Для маршрутизации вызовов по требованию в сетях Windows Server 2003 нужны по крайней мере два маршрутизатора со службой *Маршрутизация и удаленный доступ* — вызывающий и вызываемый. Оба конфигурируются для выполнения обеих функций, но в каждом процессе подключения вызывающий маршрутизатор должен проходить процедуру аутентификации и авторизации.

Аутентификация выполняется на основе реквизитов вызывающего маршрутизатора, передаваемых в процессе создания подключения. Они должны соответствовать пользовательской учетной записи. Авторизация выполняется в рамках разрешений пользователя для подключения по телефонной линии и политик удаленного доступа.

Различие между клиентами и маршрутизаторами удаленного доступа

Обе службы — маршрутизации и удаленного доступа — сосуществуют на одном сервере со службой *Маршрутизация и удаленный доступ*. И клиенты удаленного доступа, и маршрутизаторы способны звонить по одному номеру телефона. Поэтому отвечающий на запрос сервер со службой *Маршрутизация и удаленный доступ* должен «уметь отличать» клиенты удаленного доступа от маршрутизаторов, обращающихся за созданием подключения вызова по требованию.

Чтобы отличить пользователя удаленного доступа от маршрутизатора вызовов по требованию, имя пользователя в аутентификационных реквизитах, предоставляемых вызывающим маршрутизатором, должно совпадать с именем интерфейса вызовов по требованию на вызываемом маршрутизаторе. В противном случае считается, что соединение является подключением удаленного доступа.

Настройка на обоих концах подключения

Обязательно сконфигурировать оба конца подключения, даже если подключение вызова по требованию инициируется только в один конец. Если настроить только одну сторону подключения, пакеты смогут проходить только в одном направлении, а для нормальной работы нужна двусторонняя связь.

Определение статических маршрутов

Протоколы динамической маршрутизации хороши для постоянных подключений по телефонными линиям, но неприменимы для обслуживания временных подключений вызовов по требованию, в которых нужно создавать в таблице маршрутизации статические маршруты к сетям, нуждающимся в интерфейсе вызовов по требованию.

Также следует иметь в виду, что для инициирования подключения вызовов по требованию надо выбрать один статический маршрут. Для этого должен быть установлен

флажок **Использовать этот маршрут для подключений по требованию (Use this route to initiate demand-dial connections)** в окне свойств соответствующего статического маршрута (рис. 9-26).

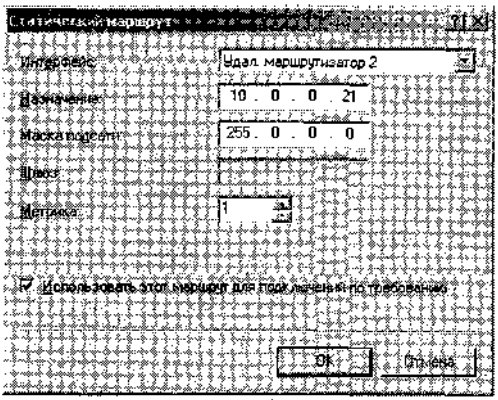


Рис. 9-26. Использование статического маршрута для поддержки подключения вызова по требованию

Устранение неполадок маршрутизации вызовов по требованию

В приведенном ниже списке представлены основные моменты развертывания маршрутизации вызовов по требованию и связанные с ними возможные точки сбоя. Ознакомьтесь с последовательностью настройки и обращайтесь к списку по мере необходимости при устранении неполадок маршрутизации через интерфейсы вызовов по требованию.

1. Для нормальной работы подключения маршрутизации вызовов по требованию на обоих его концах надо настроить ряд функций. Прежде всего убедитесь, что на обоих серверах установлена служба *Маршрутизация и удаленный доступ* (Routing and Remote Access). Во-вторых, удостоверьтесь, что на обоих серверах активизирована поддержка маршрутизации локальных вызовов и вызовов по требованию в консоли *Маршрутизация и удаленный доступ*. Затем проверьте, активизирована ли IP-маршрутизация. И, наконец, убедитесь, что необходимые интерфейсы вызовов по требованию не отключены.
2. Для маршрутизации вызовов по требованию необходимо наличие статических маршрутов на обоих концах подключения. Проверите корректность настройки этих маршрутов. Убедитесь, что в свойствах нужного подключения установлен флажок **Использовать этот маршрут для подключений по требованию (Use this route to initiate demand-dial connections).**
3. Чтобы подключение функционировало как связь в маршрутизируемой сети, подключение вызовов по требованию не должно интерпретироваться как подключение удаленного доступа. Для этого убедитесь, что имя пользователя в реквизитах вызывающего маршрутизатора совпадает с именем интерфейса вызовов по требованию на вызываемом маршрутизаторе. Позаботьтесь, чтобы реквизиты вызывающего маршрутизатора, состоящие из имени пользователя, пароля и имени домена, были правильными и вызываемый маршрутизатор был в состоянии их проверить.

4. Вызываемые маршрутизаторы должны быть авторизованы для работы в доменах Active Directory. Учетная запись компьютера вызываемого маршрутизатора — члена домена Active Directory должна быть членом группы безопасности *Серверы RAS и IAS* (RAS and IAS Servers).
5. Маршрутизируемые подключения аутентифицируются и шифруются (см. главу 10). Убедитесь, что политика удаленного доступа предусматривает по крайней мере один общий метод аутентификации и шифрования для вызывающего и вызываемого маршрутизаторов.
6. На каждом интерфейсе вызовов по требованию можно настроить ограничения в виде разрешенных часов и фильтров. Проверьте, не конфликтуют ли эти ограничения на обоих интерфейсах, не позволяя создать подключение.
7. Интерфейсы вызовов по требованию «общаются» через порты, которые могут блокироваться для входящего или исходящего трафика в консоли *Маршрутизация и удаленный доступ*. Если на каком-то из подключении вызова по требованию не удается установить связь, проверьте, на всех ли используемых портах разрешена маршрутизация вызовов по требованию (входящих и исходящих).
8. Фильтры пакетов могут блокировать доступ за пределы конечной точки подключения. Если не удается получить доступ к ресурсами за пределами вызываемого маршрутизатора, убедитесь, что ни на одном из интерфейсов вызовов по требованию нет фильтров пакетов, запрещающих нужный трафик. (Подробнее о фильтрации пакетов — в занятии 5.)

Лабораторная работа. **Настройка маршрутизации вызовов по требованию**

«Настоящую» маршрутизацию невозможно продемонстрировать лишь на двух компьютерах, тем не менее в задании 1 показано, как сконфигурировать два маршрутизатора для создания подключения TCP/IP по телефонной сети общего пользования. Вы создадите необходимые для подключения интерфейсы вызовов по требованию, учетные записи пользователей и статические маршруты. Затем вы проверите подключение, открыв Web-страницу, размещенную на удаленном компьютере.

Упражнение 1. Установка IIS-сервера на Computer2

Вы установите IIS (Internet Information Services) на Computer2 и создадите на Web-сайте страницу по умолчанию. Перед выполнением задания вставьте в дисковод Computer2 установочный компакт-диск Windows Server 2003.

1. С Computer2 войдите в Domain 1 как *Администратор* (Administrator).
2. В окне **Установка и удаление программ (Add or Remove Programs)** щелкните кнопку **Установка компонентов Windows (Add/Remove Windows Components).** Откроется окно **Мастер компонентов Windows (Windows Components Wizard).**
3. В списке компонентов выберите **Сервер приложений (Application Server)** (не отмечайте его флажком!) и щелкните кнопку **Состав (Details).**
4. В окне **Сервер приложений (Application Server)** установите флажок **Службы IIS [Internet Information Services (IIS)].** Одновременно установится флажок **Поддержка доступа по протоколу COM+ (Enable Network COM+ Access).** Щелкните OK.
5. На странице **Компоненты Windows (Windows Components)** щелкните **Далее** (Next).
6. Откроется страница **Настройка компонентов (Configuring Components)** и начнется установка выбранных компонентов Windows. По завершении установки откроется стра-

ница **Завершение мастера компонентов Windows (Completing the Windows Components Wizard).** Щелкните **Готово (Finish).**

7. . Скопируйте следующий текст в *Блокнот* (Notepad):

```
<html>
<head>
<title>Welcome</title>
</head>
<h1>Sample Web Page</h'1>
<body>
Welcome to the Web page on Computer 2
</body>
</html>
```

и сохраните файл как *Default.htm* в папке *C:\Inetpub\Wwwroot*.

Упражнение 2. Настройка службы *Маршрутизация и удаленный доступ* для поддержки маршрутизации вызовов по требованию

С помощью *Мастера настройки сервера маршрутизации и удаленного доступа* (Routing And Remote Access Server Setup Wizard) вы сконфигурируете Computerl для поддержки маршрутизации вызовов по требованию. В этом задании необходимо подключить Computerl и Computer2 через модемы к двум отдельным телефонным линиям.

1. Войдите в систему Computerl *как Администратор* (Administrator).
2. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **COMPUTER1** правой кнопкой и выберите **Отключить маршрутизацию и удаленный доступ (Disable routing and remote access).** Подтвердите отключение щелчком кнопки Да (Yes). *Мастер настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard) работает, только если служба *Маршрутизация и удаленный доступ* отключена.
3. Щелкните узел **COMPUTER1** правой кнопкой и выберите **Настроить и включить маршрутизацию и удаленный доступ (Configure and enable routing and remote access).**
4. **В** окне **Мастер настройки сервера маршрутизации и удаленного доступа (Routing And Remote Access Server Setup Wizard)** щелкните **Далее** (Next).
5. На странице **Конфигурация (Configuration)** выберите вариант **Безопасное соединение между двумя частными сетями (Secure connection between two private networks)** и щелкните **Далее.**
6. На странице **Подключения по требованию (Demand-Dial Connections)** оставьте вариант по умолчанию — Да (Yes).
7. На странице **Назначение IP-адресов (IP Address Assignment)** выберите вариант **Из заданного диапазона адресов (From a specified range of addresses)** и щелкните **Далее.**
8. На странице **Назначение диапазонов IP-адресов (Address Range Assignment)** щелкните кнопку **Создать (New).**
9. **В** открывшемся окне **Новый диапазон адресов (New Address Range)** в поле **Начальный IP-адрес (Start IP address)** введите 10.0.0.11, ав поле **Конечный IP-адрес (End IP address)** - 10.0.0.20. Щелкните OK.
10. На странице **Назначение диапазонов IP-адресов** щелкните **Далее.**
11. На странице **Завершение мастера сервера маршрутизации и удаленного доступа (Completing the Routing and Remote Access Server Setup Wizard)** щелкните **Готово (Finish).**

Откроется окно **Мастер интерфейса вызова по требованию (Demand-Dial Interface Wizard).** Щелкните **Далее.**

12. На странице **Имя интерфейса (Interface Name)** оставьте имя по умолчанию — **Удал, маршрутизатор (Remote Router)** и щелкните **Далее.**
13. На странице **Тип подключения (Connection Type)** оставьте вариант по умолчанию — **Подключаться используя модем, адаптер ISDN или другое устройство (Connect using a modem, ISDN adapter, or other physical device)** и щелкните **Далее.**
14. На странице **Выберите устройство (Select a Device)** выберите нужный модем и щелкните **Далее.**
15. На странице **Номер телефона (Phone Number)** в текстовом поле **Номер телефона или адрес (Phone number or address)** введите номер телефона линии подключения к другому компьютеру и щелкните **Далее.**
16. На странице **Протоколы и безопасность (Protocols and Security)** установите флажок **Добавить учетную запись для входящих звонков удаленного маршрутизатора (Add a user account so a remote router can dial in).** Оставьте установленным флажок **Перенаправлять пакеты IP на этот интерфейс (Route IP packets on this interface).** Щелкните **Далее.**
17. На странице **Статические маршруты для удаленных сетей (Static Routes for Remote Networks)** щелкните кнопку **Добавить (Add).**
18. **В** окне **Статический маршрут (Static Route)** в поле **Назначение (Destination)** введите 10.0.0.0, а в поле **Маска сети (Network mask)** укажите 255.0.0.0. В поле **Метрика (Metric)** оставьте значение 1. Щелкните OK.
19. На странице **Статические маршруты для удаленных сетей** щелкните **Далее.**
20. Ознакомьтесь с текстом на странице **Учетные данные входящего подключения (Dial In Credentials). В** полях **Пароль (Password)** и **Подтверждение (Confirm Password)** введите пароль учетной записи *Domainl\Administrator* и щелкните **Далее.**
21. На странице **Учетные данные исходящего подключения (Dial Out Credentials):**
    - в поле **Имя пользователя (User Name)** введите Удал, маршрутизатор (Remote router);
    - p поле **Домен (Domain)** оставьте пустым;
    - в полях **Пароль (Password)** и **Подтверждение (Confirm Password)** введите пароль учетной записи *Domain 1 \Administrator*.
22. Щелкните **Далее.**
23. На странице **Завершение мастера интерфейса вызова по требованию (Completing The Demand- Dial Interface Wizard)** щелкните **Готово** (Finish).
24. Выполните пп. 3–23 на Computer2, но в п. 9 назначьте диапазон адресов 10.0.0.21—10.0.0.30.

Упражнение 3. Проверка конфигурации

Вы проверите способность созданного подключения поддерживать трафик между маршрутизаторами .

1. С Computerl войдите в Domainl как *Администратор* (Administrator).
2. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) выберите узел **Интерфейсы сети (Network Interfaces).**
3. **В** правой панели щелкните интерфейс **Удал, маршрутизатор (Remote Router)** правой кнопкой и выберите **Подключить (Connect).** Откроется окно **Подключение интерфейса (Interface Connection).** Computer2 отвечает на звонок двух сигналов.

4. Когда состояние подключения сменится на **Подключено (Connected),** перейдите к Computer2 и войдите в систему как *Администратор* (Administrator).
5. На Computer2 из командной строки исполните ipconfig /all.
6. Запишите адрес, назначенный интерфейсу **PPP Adapter RAS Server (Dial In) Interface.**
7. На Computer!, откройте окно Internet Explorer и в адресной строке введите http://*<IP-адрес>,* где *<IP-адрес>* — адрес, записанный в п. 6. Например, если это 10.0.0.21, то в поле адреса надо ввести: http://10.0.0.21. Нажмите Enter.
   Проигнорируйте все предупреждения Internet Explorer. Откроется страница с текстом **Welcome to the Web page on Computer 2.** Интерфейс вызовов по требованию Computerl успешно подключился к Web-сайту на Computer2 через интерфейс вызовов по требованию на Computer2.
8. В консоли *Маршрутизация и удаленный доступ* компьютера Computerl щелкните правой кнопкой узел локального сервера и выберите **Отключить маршрутизацию и удаленный доступ (Disable Routing And Remote Access).**
9. Подтвердите отключение щелчком кнопки Да (Yes).
10. На Computer2 повторите пп. 8 и 9.
11. Перезагрузите оба компьютера.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Используя службу *Маршрутизация и удаленный доступ,* вы сконфигурировали маршрутизацию вызовов по требованию, чтобы подключить филиал к корпоративной ЛВС. Однако даже при наличии протокола RIP маршруты не обновляются по WAN-каналам. Почему это происходит и как организовать обновление маршрутов?
2. Связь с филиалом обеспечивается по подключению вызовов по требованию. Как надежнее всего запретить пользователям подключаться к филиалу на время обеда?
3. Филиал подключен к сети штаб-квартиры по *цифровой сети с комплексными услугами* (Integrated Services Digital Network, ISDN) с использованием подключения вызова по требованию. Надо заблокировать открытие подключения HTTP-запросами. Как это сделать?
4. Штаб-квартира подключена к филиалу с применением маршрутизации вызовов по требованию. Каждый из маршрутизаторов сконфигурирован на инициирование и прием вызовов. Однако финансовый отдел потребовал, чтобы большую долю расходов на телефонную связь между маршрутизаторами вызовов по требованию несла штаб-квартира. Как решить эту задачу?

Резюме

- Маршрутизация вызовов по требованию — это процесс пересылки трафика с одного маршрутизатора на другой по телефонной линии. Такое телефонное подключение может-создаваться по мере необходимости, то есть «вызываться по требованию», или быть постоянным.
- В каждом процессе подключения по требованию вызывающий маршрутизатор должен проходить процедуру аутентификации и авторизации. Аутентификация выполняется на основе реквизитов вызывающего маршрутизатора, передаваемых в про-

цессе создания подключения. Они должны соответствовать пользовательской учетной записи. Авторизация выполняется в рамках разрешений пользователя для подключения по телефонной линии и политик удаленного доступа.

- Чтобы отличить пользователя удаленного доступа от маршрутизатора вызовов по требованию, имя пользователя в аутентификационных реквизитах, предоставляемых вызывающим маршрутизатором, должно совпадать с именем интерфейса вызовов по требованию на вызываемом маршрутизаторе. В противном случае считается, что соединение является подключением удаленного доступа.
- В процессе реализации маршрутизации вызовов по требованию надо определить статический маршрут, по которому инициируется подключение вызова по требованию.
- Служба *Маршрутизация и удаленный доступ* (Routing and Remote Access) позволяет настроить дополнительные функции маршрутизации вызовов по требованию: обратный вызов, фильтры вызовов по требованию, фильтры пакетов и часы исходящих вызовов.

Занятие 3. Настройка NAT

Компонент преобразования сетевых адресов (Network Address Translation, NAT) службы *Маршрутизация и удаленный доступ* (Routing and Remote Access) в Windows Server 2003 позволяет не только маршрутизировать IP-пакеты, проходящие между локальной сетью и Интернетом, но и изменять их адрес назначения (переадресовывать). Такая переадресация позволяет обеспечить доступ в Интернет многим клиентским компьютерам, используя один *общий* (public) адрес или ограниченный пул таких адресов. NAT дает возможность назначить всем внутренним клиентам *частные* (private) адреса, причем общий адрес нужен только внешнему интерфейсу NAT-сервера.

Изучив материал этого занятия, вы сможете:

- V настроить NAT в сети Windows Server 2003;
- V рассказать о различии между *общим подключением к Интернету* (Internet Connection Sharing, ICS) и NAT;
- V устранять неполадки NAT.

Продолжительность занятия — около 45 минут.

Основные сведения о NAT

NAT — это служба маршрутизатора, которая изменяет информацию заголовка IP-дейтаграмм перед пересылкой их адресату. Она позволяет узлам подключаться к Интернету, совместно используя один или несколько общих зарегистрированных IP-адресов на компьютере со службой NAT. Компьютер с NAT действует как преобразователь сетевых адресов, упрощенный DHCP-сервер, DNS- и WINS-прокси (рис. 9-27).

NAT конфигурируется на интерфейсе вызовов по требованию или на постоянном подключении. Интерфейс вызовов по требованию подключается только по требованию клиента. Постоянное подключение — это выделенная линия, например DSL или T1, или интерфейс телефонного вызова, автоматически восстанавливающий подключение в случае потери связи.

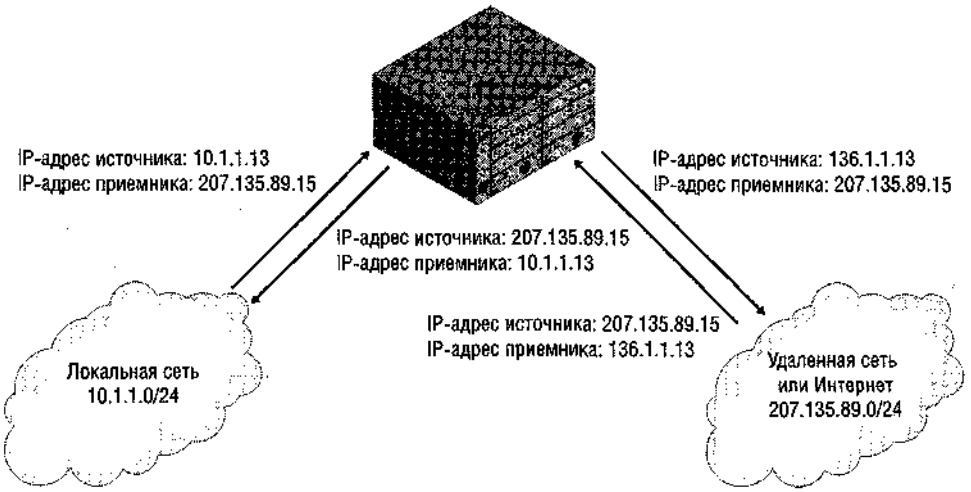


Рис. 9-27. Преобразование сетевых адресов

Различие между NAT и ICS

Как и NAT, встроенная в Windows служба *общего доступа к Интернету* (Internel Connection Sharing, ICS) обеспечивает подключение к Интернету через единственный интерфейс (по телефонной линии или постоянный) Windows-компьютера. ICS также позволяет внутренним клиентам сохранять свои частные IP-адреса при подключении в общим внешними адресами. Наконец, NAT содержит компонент *Простой брандмауэр* (Basic Firewall), который блокирует любой входящий трафика за исключением ответо! на запросы из локальной сети. Он аналогичен службе *Брандмауэр подключения к Интернету* (Internet Connection Firewall), выполняющей идентичные функции в ICS.

Главное различие между NAT и ICS — гибкость конфигурации. ICS жестко сконфигурирована и автоматически назначает компьютеру, обеспечивающему общий доступ, внутренний адрес 192.168.0.1. Все внутренние клиенты размещаются в одной физической подсети, получают адреса из диапазона 192.168.0.0/24 и используют для разрешенш имен только DNS-сервер, размещенный на компьютере с ICS. Внешнему общему интерфейсу назначается единственный общий адрес Интернета.

С другой стороны, NAT позволяет выбрать любой частный IP-адрес в качестве внутреннего адреса NAT-сервера, есть возможность отключить DHCP-сервер и DNS-прокси. Например, если в сети уже есть службы DHCP или DNS, их можно отключить пр* настройке NAT. При настройке NAT для предоставления услуг DHCP внутренним клиентам можно задавать любые диапазоны адресов. Кроме того, в отличие от ICS, NAT поддерживает множественные внутренние интерфейсы (впрочем, адреса, назначаемы* внутренним клиентам этими интерфейсами, должны все принадлежать одной логической подсети).

И последнее: NAT позволяет сконфигурировать внешний совместно используемы! интерфейс с одним или несколькими общими адресами. Множественные общие адрес, полезны, например, когда определенным внутренним серверам надо назначить различные общие IP-адреса.

Подготовка к экзамену При назначении IP-адресов ICS не выполняет проверку на предмет конфликтов со статическими адресами, уже существующими в сети. Поэтому не следует развертывать ICS в сетях, где критически важным серверам назначены статические адреса из начала диапазона 192.168.0.0/24. Следует также знать, что если критически важным серверам назначены статические адреса в другом логическом адресном пространстве (например, 192.168.1.0/24), после развертывая ICS такие серверы могут стать недоступными. Поэтому если в описанной на экзамене ситуации после установки ICS важные сетевые службы перестают работать, надо подумать о замене ICS на NAT.

В табл. 9-2 сравниваются функции и возможности ICS и NAT в Windows Server 2003.

Табл. 9-2. Сравнение ICS и NAT

Общий доступ к Интернету (ICS)	**Преобразование сетевых адресов (NAT)**
Конфигурирование установкой единственного флажка	Настройка вручную
Единственный общий IP-адрес	Один или несколько общих IP-адресов
Фиксированный диапазон адресов (192.168.0.0/24), назначаемых внутренним узлам	Свободно определяемый интервал адресов для внутренних узлов
Единственный внутренний интерфейс, подключенный к единственной логической подсети	Один или несколько внутренних интерфейсов, подключенных к единственной логической подсети
Настраивается в окне **Сетевые подключения (Network Connections)**	Настраивается в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access)
Microsoft Windows 98 Second Edition или более поздняя ОС	Windows 2000 Server или Windows Server 2003
Брандмауэр подключения к Интернету (Internet Connection Firewall)	Простой Брандмауэр (Basic Firewall)

Входящие запросы и NAT

ICS имеет одну приятную особенность, которой нет в NAT: при настройке на подключение по телефонной линии ICS никогда не отвечает на входящие вызовы. А если сконфигурировать в NAT интерфейс вызовов по требованию, он заставляет модем отвечать на входящие вызовы сразу после второго звонка. Это ограничение может раздражать, особенно когда одна телефонная линия попеременно используется для подключения к Интернету и для речевого общения. В этом случае если не снять трубку сразу после первого звонка, модем скорее всего испортит приятный разговор своим скрипучим «голосом».

Если выбора нет и приходится использовать ICS вместе с обычными телефонными звонками, рекомендуется отредактировать реестр, чтобы модем принимал вызов после бо'лыпего числа сигналов. Откройте редактора реестра и добавьте параметр NumberOfRirigs типа REG_DWORD в следующий раздел:

HKEY_LOCAL__MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters

Разрешенное значение (число сигналов до приема вызова) этого параметра — от 0 до 20. В будущем значение 0 будет вообще запрещать модему отвечать на вызов, но пока оно аналогично значению 2. Если нужно запретить модему «поднимать трубку», лучшее, что можно сделать, — задать значение 20. Это не идеальное решение, тем не менее хам, дождавшийся 20-го сигнала вполне заслуживает скрипучего голоса модема.

Устранение неполадок NAT

В приведенном ниже списке представлены основные моменты развертывания NAT и связанных с этим возможных точек сбоя. Ознакомьтесь с последовательностью настройки и обращайтесь к списку по мере необходимости при устранении неполадок NAT.

1. NAT требует, чтобы все нужные внешние (общие) и внутренние (частные) интерфейсы добавлялись в протокол NAT в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access). Обычно внутренний интерфейс создан по умолчанию, но внешние интерфейсы часто перед добавлением, приходится создавать вручную. После добавления интерфейсов обоих видов надо убедиться, что общий интерфейс [для подключений вызовов по требованию получающий по умолчанию имя *Удал, маршрутизатор* (Remote Router)] обозначен в окне свойств как общий в узле **NAT/Простой брандмауэр (NAT/Basic Firewall).** Точно так же частный интерфейс должен назначаться таковым в своем окне свойств в этом же узле.
2. NAT требует определения статического маршрута по умолчанию в консоли *Маршрутизация и удаленный доступ*. В этом маршруте адресату и сетевой маске должно присваиваться значение 0.0.0.0, шлюзу — значение None, и интерфейс должен соответствовать общему (внешнему) интерфейсу, подключенному к Интернету.
3. Для NAT нужно, чтобы служба DHCP была должным образом сконфигурирована для обслуживания внутренних клиентов. Если DHCP-сервера нет, позаботьтесь о включении *DHCP-распределителя* (DHCP allocator) на вкладке **Назначение адресов (Address Assignment)** окна свойств узла **NAT/Простой брандмауэр (NAT/Basic Firewall).**
4. Для нормальной работы NAT с разрешением DNS-имен надо настроить DNS-сервер на компьютере с NAT или определить через DNS-прокси в NAT. Последнее выполняется на вкладке **Разрешение имен в адреса (Name Resolution)** окна свойств узла **NAT/Простой брандмауэр (NAT/Basic Firewall).**
5. Некоторые функции NAT требуют более сложной настройки. Если внешнему интерфейсу назначен пул адресов, надо позаботиться о корректной настройке адреса и маски. На специальных портах надо проверить конфигурацию общих и частных адреса и порта.

Лабораторная работа. Установка и настройка NAT

Вы развернете NAT на новом интерфейсе вызовов по требованию, а затем проверите функции управления NAT.

Внимание! Для выполнения некоторых из следующих упражнений придется подключаться ко внешним Web-сайтам, работая в системе как *Администратор* (Administrator). В реальной среде надо избегать подключения к Интернету компьютера, когда на нем открыт сеанс учетной записи *Администратор*. В качестве альтернативы предлагается выполнять административные задачи, используя команду Runas из сеанса пользователя, не имеющего административных полномочий.

Упражнение 1. Настройка NAT через интерфейс вызовов по требованию

- **Настройка NAT через интерфейс вызовов по требованию**

1. С Computerl войдите в Domainl *как Администратор* (Administrator).
2. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **COMPUTER1 (локально) [COMPUTER1 (Local)]** правой кнопкой и выберите **Настроить и включить маршрутизацию и удаленный доступ (Configure And Enable Routing And Remote Access). В** окне **Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard)** щелкните **Далее** (Next).
3. На странице **Конфигурация (Configuration)** выберите вариант **Преобразование сетевых адресов (NAT) [Network Address Translation (NAT)]** и щелкните **Далее.**
4. **На** странице **Подключение к Интернету на основе NAT (NAT Internet Connection)** выберите **Создать интерфейс для нового подключения вызова по требованию к Интернету (Create a new demand-dial interface to the Internet)** и щелкните **Далее.**
5. На странице **Выбор сети (Network Selection)** выберите **Подключение по локальной сети (Local Area Connection)** и щелкните **Далее.**
6. На странице **Готово к применению выбранного (Ready to Apply Selection)** щелкните **Далее.** Откроется окно **Мастер интерфейса вызова по требованию (Demand-Dial Interface Wizard).** Щелкните **Далее.**
7. На странице **Имя интерфейса (Interface Name)** оставьте имя по умолчанию **Удал, маршрутизатор (Remote Router)** и щелкните **Далее.**
8. На странице **Тип подключения Connection Type)** оставьте вариант по умолчанию **Подключаться используя модем, адаптер ISDN или другое устройство (Connect using a modem, ISDN adapter, or other physical device)** и щелкните **Далее.**
9. На странице **Выберите устройство (Select a Device)** выберите нужный модем и щелкните **Далее.**
10. На странице **Номер телефона (Phone Number)** в поле **Номер телефона или адрес (Phone number or address)** введите номер телефона линии подключения к другому компьютеру и щелкните **Далее.**
11. На странице **Протоколы и безопасность (Protocols and Security)** оставьте установленным флажок **Перенаправлять пакеты IP на этот интерфейс (Route IP packets on this interface)** и щелкните **Далее.**
12. На странице **Учетные данные исходящего подключения (Dial Out Credentials)** в соответствующих полях введите имя пользователя и пароль (в двух полях) для интернет-провайдера. Обратите внимание, что у большинства провайдеров поле **Домен (Domain)** должно оставаться пустым. Щелкните **Далее.**
13. На странице **Завершение мастера интерфейса вызова по требованию (Completing The Demand-Dial Interface Wizard)** ознакомьтесь со сводкой. Обратите внимание, что NAT и простой брандмауэр настроены для нового интерфейса вызовов по требованию. Также обратите внимание, что мастер обнаружил DNS- и DHCP-серверы на локальном компьютере и автоматически сконфигурировал NAT для использования этих внешних служб. Если таких серверов не было бы, мастер предложил бы сконфигурировать DHCP-распределитель и DNS-прокси.
14. Щелкните **Готово (Finish).**

- **Проверка новой конфигурации NAT**

1. С Computer2 войдите в Domain 1 как *Администратор* (Administrator).
2. На Computer2 откройте Internet Explorer и в поле адреса введите `http: //www. windows-update, com`. Проигнорируйте предупреждения браузера. Интерфейс вызовов по требованию на Computerl с именем *Удал, маршрутизатор* (Remote Router) подключается по телефонной линии к интернет-провайдеру. После создания подключения благодаря службе NAT на Computerl Internet Explorer получает возможность подключиться к Интернету через Computer2.

   Примечание На Computer2 время ожидания Internet Explorer может истечь до подключения интерфейса вызовов по требованию на Computerl через интернет-провайдера. Поэтому, получив сообщение в Internet Explorer о невозможности отобразить страницу, щелкните кнопку **Обновить (Refresh),** чтобы повторить попытку.

3. На Computerl щелкните правой кнопкой значок **NAT/Простой брандмауэр (NAT/Basic Firewall)** — появится контекстное меню, позволяющее: добавить в NAT другой интерфейс, отобразить сведения DHCP-распределителя или DNS-прокси.
4. В контекстном меню выберите **Свойства (Properties).** Откроется окно **Свойства: NAT/Простой брандмауэр (NAT/Basic Firewall Properties)!**
5. Перейдите на вкладку **Назначение адресов (Address Assignment)** и ответьте на вопрос: какая служба NAT настраивается на этой вкладке?
6. Перейдите на вкладку **Разрешение имен в адреса (Name Resolution)** и ответьте на вопрос: какая служба NAT настраивается на этой вкладке?
7. Щелкните **Отмена (Cancel)** в окне **Свойства: NAT/Простой брандмауэр.**

Упражнение 2. Просмотр и настройка параметров NAT

Вы проанализируете функции и параметры конфигурации NAT, в том числе статический маршрут по умолчанию, сопоставление адресов, конфигурацию фильтров пакетов, пулов адресов, специальных портов и ICMP-фильтров.

- **Просмотр маршрута NAT по умолчанию**

1. С Computerl войдите в Domainl как *Администратор* (Administrator).
2. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) последовательно разверните узлы **COMPUTER1 (локально) [COMPUTER1 (Local)]** и **IP-маршрутизация (IP Routing).**
3. Выберите узел **Статические маршруты (Static Routes).** В правой панели отображается один статический маршрут — заданный по умолчанию. Для нормальной работы NAT надо настроить этот маршрут по умолчанию.

   Внимание! Этот статический маршрут по умолчанию надо создать вручную, если служба NAT настраивалась не в *Мастере настройки сервера маршрутизации и удаленного доступа* (Routing And Remote Access Server Setup Wizard).

4. Маршрут по умолчанию задается конкретным адресом назначения и маской сети. Запишите их.

- **Проверка сопоставлений NAT**

1. С Computer2 войдите в Domainl как *Администратор* (Administrator).
2. В командной строке выполните команду ipconfig, чтобы определить IP-адрес, назначенный подключению по локальной сети. Запишите этот адрес.
3. Откройте Internet Explorer и перейдите по адресу внешнего Web-сайта, например *http://www.windowsupdate.com*.
4. На Computer! в дереве консоли *Маршрутизация и удаленный доступ,* выберите узел **NAT/Простой брандмауэр (NAT/Basic Firewall),** в правой панели щелкните значок **Удал, маршрутизатор (Remote Router)** правой кнопкой и выберите **Отображение сопоставлений (Show Mappings).** Откроется **Таблица сопоставления сеанса преобразования сетевых адресов (NAT) - COMPUTER1 (COMPUTER1 - Network Address Translation Session Mapping Table).**
5. **В** списке отображений в таблице выберите запись, чей частный адрес соответствует адресу Computer2, а удаленный порт — порту для Web-трафика (80).
6. Запишите общий адрес этого сопоставления сеанса.

   Какому физическому интерфейсу принадлежит общий адрес, сопоставленный службой NAT частному адресу Computer2?
7. Закройте окно **Таблица сопоставления сеанса преобразования сетевых адресов (NAT) - COMPUTER1.**

- **Просмотр функций NAT**

1. Не выходя из сеанса *Администратор* (Administrator) домена Domainl на Computerl, при выбранном узле **NAT/Простой брандмауэр (NAT/Basic Firewall)** в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните правой кнопкой значок Удал, **маршрутизатор (Remote Router)** и выберите **Свойства (Properties).** Откроется окно **Свойства: >дал. маршрутизатор (Remote Router Properties)** на вкладке **NAT/Простой брандмауэр (NAT/Basic Firewall).** Здесь включают/отключают функцию **NAT/Простой брандмауэр (NAT and Basic Firewall).**
2. В области **Фильтры статических пакетов (Static Packet Filters)** прочтите предложение с описанием фильтрации пакетов. (Подробнее о фильтрах пакетов см. занятие 5.)
3. Перейдите на вкладку **Пул адресов (Address Pool).** Если интернет-провайдер выделил вам диапазон общих адресов, эта вкладка позволит назначить их внешнему интерфейсу;
4. Щелкните кнопку **Создать (Add).** Откроется окно **Добавление пула адресов (Add Address Pool)** с полями **Начальный адрес (Start address), Маска (Mask)** и **Конечный адрес (End address).**
5. Ответьте на следующие вопросы.
   a. Нужно ли при назначении этих параметров конфигурации, чтобы пул адресов, назначаемый внешнему интерфейсу, составлял непрерывное адресное пространство?
   b. Воспользовавшись калькулятором, определите, какую маску подсети надо назначитыгулу 207.46.200.0-207.46.207.255.
   c. Какое максимальное число адресов возможно в пуле с маской подсети 255.255.255.248?
6. Щелкните **Отмена (Cancel)** в окне **Добавление пула адресов.**
7. **В** области **Резервирование общих адресов (Reserve Public Addresses)** вкладки **Пул адресов** ознакомьтесь с описанием резервирования.

В каких ситуациях при конфигурировании свойств NAT используется кнопка Резер **вирование (Reservations}?**

8. Перейдите на вкладку **Службы и порты (Services and Ports). В** верхней части вкладки ознакомьтесь с описанием доступных функций.
9. В области **Службы (Services)** дважды щелкните **FTP-сервер (FTP Server).** Откроет! окно **Изменить службу (Edit Service).**
10. В верхней части окна ознакомьтесь с описанием доступных функций. Если есть вн шние пользователи, подключающиеся ко внутренним FTP-серверам, в этом ою можно сконфигурировать службу NAT для пересылки FTP-запросов на соответств ющий внутренний сервер. Пример такой ситуации приведен на рис. 9-28.

Подготовка к экзамену Вы должны знать, что настройка функций на вкладке **Службы порты** (рис. 9-28) известна как конфигурирование *специальных портов* (special port; Настроить специальный порт означает сопоставить внутреннюю службу (например Wet Telnet- или FTP-серверу) внешнему интерфейсу компьютера с NAT, что позволяет вн шние запросы служб внутренней сети направлять на соответствующий компьютер.

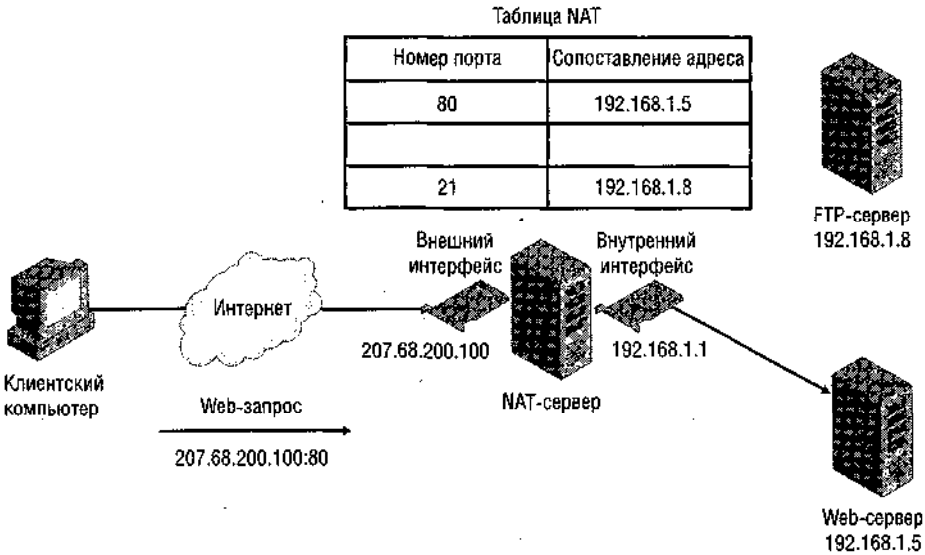


Рис. 9-28. Специальные порты NAT

11. Щелчком **Отмена (Cancel)** закройте окно **Изменить службу.**
12. **В** окне **Свойства: ЭДал. маршрутизатор** перейдите на вкладку **ICMP** и ознакомьтесь с описанием. Эта вкладка позволяет запрещать определенные типы 1CMP-сообщениий. Эти сообщения используются для поддержки различных сетевых функций, напр мер эхо-запроса Ping или ICMP-обнаружения маршрутизатора.

    Блокирует ли маршрутизатор по умолчанию ping-запросы внешнего интерфейса вне- шними клиентами? внутренними клиентами?
13. Щелчком **Отмена (Cancel)** закройте окно **Свойства: Удал, маршрутизатор.**
14. Выйдите из системы Computerl и Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В сети размещается новый компьютер для обеспечения подключения к Интернету сети, состоящей из одной подсети с клиентскими компьютерами, которым назначены статические адреса из диапазона 192.168.0.1—192.168.0.65, и критически важными серверами со статическими адресами из диапазона 192.168.0.100—192.168.0.120. На новом компьютере настроена служба ICS, но ни один из компьютеров сети не в состоянии подключиться к Интернету. Как проще всего решить проблему?
2. В сети размещены 11 критически важных серверов, которым назначены статические адреса из диапазона 192.168.0.1—192.168.0.20. После настройки ICS пользователи не в состоянии подключаться к сети, а сетевым компьютерам не удается найти контроллеры домена и подключиться к сетевыми объектам по их именам. Как устранить неполадку, если предполагается, что изменять адреса критически важных серверов нельзя?
3. В сети расположены критически важные серверы со статическими адресами из диапазона 10.0.0.1—10.0.0.20. Клиентским компьютерам назначены статические адреса из диапазона 10.0.0.21—10.0.0.100. Изменить назначенные сетевые адреса не представляется возможным. В сети устанавливается NAT-сервер, который должен распределять IP-адреса в этой же IP-подсети и обеспечивать подключение к Интернету. Однако компьютеры сети не в состоянии подключаться к Интернету. Какова наиболее вероятная причина неполадки?
4. NAT-сервер подключен к Интернету по DSL-линии. Интернет-провайдер предоставил блок из 8 адресов, которые надо назначить внешнему интерфейсу NAT-сервера. Как решить задачу?

Резюме

- *Компонент преобразования сетевых адресов* (Network Address Translation, NAT) службы *Маршрутизация и удаленный доступ* (Routing and Remote Access) в Windows Server 2003 позволяет не только маршрутизировать IP-пакеты, проходящие между локальной сетью и Интернетом, но и изменять их адрес назначения (переадресовывать). Такая переадресация обеспечивает доступ в Интернет многим клиентским компьютерам, используя один *общий* (public) адрес или ограниченный пул таких адресов.
- В службе *Маршрутизация и удаленный доступ* (Routing and Remote Access) NAT может выполнять функции DHCP-распределителя, DNS- или WINS-прокси.
- NAT можно рассматривать как полностью настраиваемую службу ICS.
- Для нормальной работы NAT надо задать маршрут по умолчанию без шлюза.
- На NAT-клиентах в одной подсети с NAT-сервером надо в качестве шлюза определить этот NAT-сервер.

Занятие 4. Настройка и управление протоколами маршрутизации

Протоколы динамической маршрутизации RIP и OSPF позволяют маршрутизаторам определять наиболее подходящие маршруты для пересылки трафика. *Агент DHCP-ретрансляции* (DHCP Relay Agent) в службе *Маршрутизация и удаленный доступ* (Routing and Remote Access) также считается протоколом маршрутизации; он позволяет DHCP-серверу предоставлять конфигурационные параметры IP компьютерам удаленных подсетей.

Изучив материал этого занятия, вы сможете:

- организовать маршрутизацию на основе RIP;
- определить, какой протокол больше всего подходит в конкретной ситуации — RIP или OSPF;
- установить *Агент DHCP-ретрансляции*.

Продолжительность занятия — около 40 минут.

Основные сведения о протоколах маршрутизации

В службе *Маршрутизация и удаленный доступ* (Routing and Remote Access), *протоколы маршрутизации* (routing protocols) обеспечивают связь между маршрутизаторами. Windows Server 2003 эта служба поддерживает четыре протокола маршрутизации: протоколы динамической маршрутизации RIP и OSPF, маршрутизатор и прокси протокола маршрутизации многоадрестных рассылок IGMP и *Агент DHCP-ретрансляции*.

Добавление и конфигурирование протоколов маршрутизации

До настройки протокола маршрутизации его надо добавить в консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access). Для этого щелкните подузел **Общие (General)** узла **IP-маршрутизация (IP Routing)** в консоли **Маршрутизация и удаленный** доступ правой кнопкой и выберите **Новый протокол маршрутизации (New Routing Protocol)** (рис. 9-29).

После определения в консоли *Маршрутизация и удаленный доступ* протокол надо включить на нужных сетевых интерфейсах. Для этого щелкните значок нового протокола в дереве консоли правой кнопкой и выберите Новый интерфейс (New **Interface).** После включения протокола на интерфейсах переходят к его настройке в окне свойств протокола или интерфейса.

Конфигурирование RIP

RIP — протокол динамической маршрутизации, позволяющий маршрутизаторам определять оптимальный путь для пересылки данных. Маршруты выбираются по принципу минимальной стоимости. По умолчанию стоимость определяется числом переходов, или маршрутизаторов, пересекаемых на пути между конечными точками, однако при необходимости стоимость маршрутов можно скорректировать.

Следует помнить, что RIP отбрасывает маршруты со стоимостью выше 15. Эта особенность ограничивает размер сети, поддерживаемой RIP. Другая важная особенность RIP — RIP-маршрутизаторы обмениваются полными таблицами маршрутизации каждые 30 сек, поэтому служба инициирует значительный сетевой трафик.

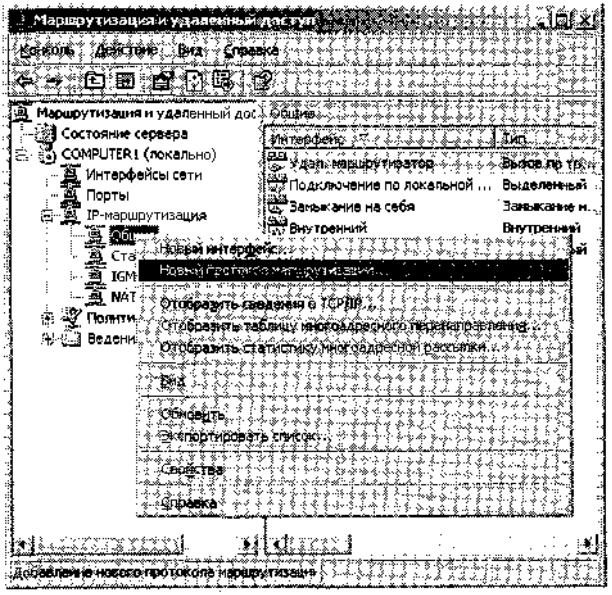


Рис. 9-29. Создание нового протокола маршрутизации

RIP-среда

RIP-маршрутизация больше всего подходит для мелких и средних динамичных объединенных многомаршрутных IP-сетей:

- *мелкие и средние* означает объединенные сети, состоящие из 10—50 сетей. Кроме того, «диаметр» RIP-сети не может превышать 15 маршрутизаторов;
- *многомаршрутные* (multipath) означает, что пакетам доступны несколько маршрутов для перемещения между двумя конечными точками объединенной сети;
- *динамическая* означает, что топология объединенной сети меняется во времени.

Преимущества и недостатки RIP

Главное преимущество RIP — простота развертывания, для которой достаточно включить протокол RIP на всех маршрутизаторах. Однако RIP плохо масштабируется до размера крупных сетей из-за ограничения в 15 переходов. К другим недостаткам RIP следует отнести большое время синхронизации в сетях среднего размера и неспособность учитывать другие параметры стоимости маршрутов кроме переходов (например загруженность и пропускную способность сети).

Управление безопасностью в RIP

RIP поддерживает ряд настраиваемых функций, в том числе аутентификацию, фильтрацию равных RIP-маршрутизаторов, фильтры маршрутов и соседи.

Подготовка к экзамену Вы должны хорошо знать эти функции безопасности RIP.

Аутентификация в RIP. Чтобы предотвратить искажение маршрутов RIP неправомочным RIP-маршрутизатором или злоумышленником, интерфейсы RIP-маршрутизаторов можно настроить на использование простой аутентификации на основе пароля. Объяв-

ления RIP, не соответствующие паролю, отбрасываются. Однако следует иметь в виду, что пароль пересылается открытым текстом, который легко перехватить *анализатором пакетов* (sniffer), например *Сетевом монитором* (Network Monitor).

Аутентификация RIP включается путем установки флажка **Проверять подлинность (Activate Authentication)** на вкладке **Общие (General)** окна свойств RIP-интерфейса (рис. 9-30).

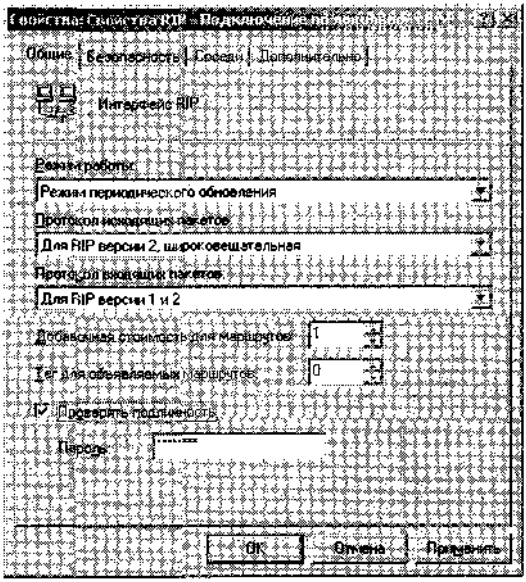


Рис. 9-30. Включение RIP-аутентификации

Фильтры равных RIP-маршрутизаторов (peer filtering). На каждом RIP-маршрутизаторе определяется список маршрутизаторов (точнее, их IP-адресов), с которых принимаются RIP-объявления. По умолчанию объявления принимаются со всех источников. Список равных RIP-маршрутизаторов позволяет не принимать объявления от посторонних (не указанных в списке) маршрутизаторов.

Список маршрутизаторов определяется на вкладке **Безопасность (Security)** окна свойств RIP (рис. 9-31).

Фильтры маршрутов (Route Filters) настраиваются при необходимости на любом интерфейсе RIP. Они служат для отбора только тех маршрутов, которые отражают идентификаторы только доступных сетей. Например, если в организации используется подсеть частной сети с идентификатором 10.0.0.0, фильтрация маршрутов может обеспечить блокирование всех RIP-маршрутизаторы за исключением тех, что находятся в рамках идентификатора сети 10.0.0.0.

Фильтры маршрутов определяются на вкладке **Безопасность (Security)** окна свойств RIP (рис. 9-32).

Соседи (Neighbors). По умолчанию RIP-объявления распространяются путем широковещания (RIP версии 1 или 2) или многоадресной рассылки (только RIP версии 2). Чтобы узлы принимали RIP-трафик только от своих прямых соседей-узлов, в службе *Маршрутизация и удаленный доступ* RIP-объявления организуются по методу одноадресной рассылки.

RIP-соседи определяются на вкладке **Соседи (Neighbors)** окна свойств RIP **(рис. 9-33).**

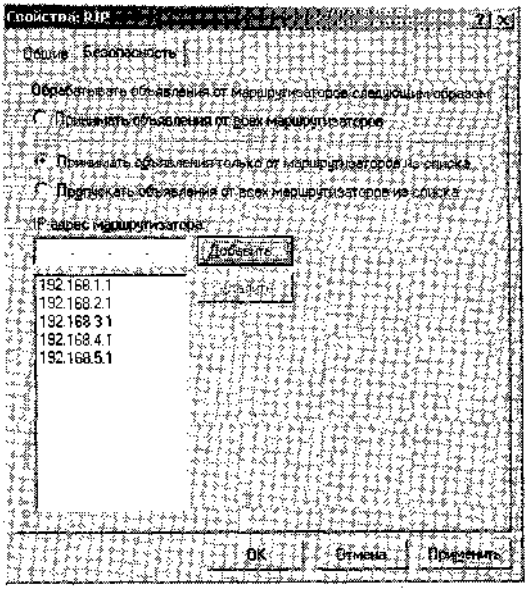


Рис. 9-31. Фильтры равных RIP-маршрутизаторов

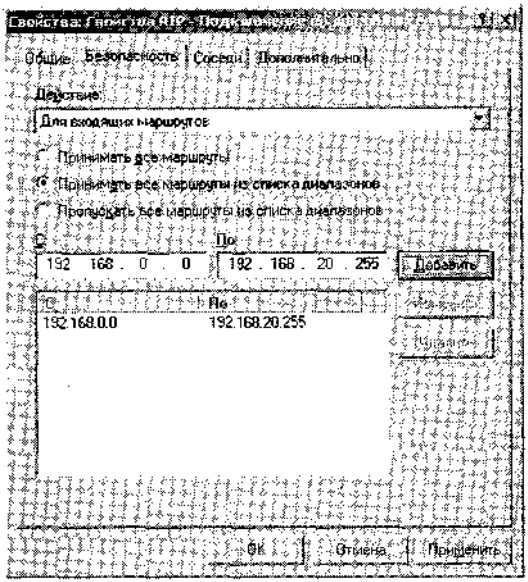


Рис. 9-32. Фильтры маршрутов в RIP

Общие сведения об OSPF

Протокол OSPF служит для обмена информацией о маршрутизации в крупных и очень крупных объединенных сетях.

Самое большое преимущество OSPF — его производительность; в процессе работы протокол создает минимальную нагрузку на сеть, даже обслуживая исключительно крупные сети. А самый большой недостаток OSPF — сложность; он требует предварительного планирования и сложен в конфигурировании и управлении.

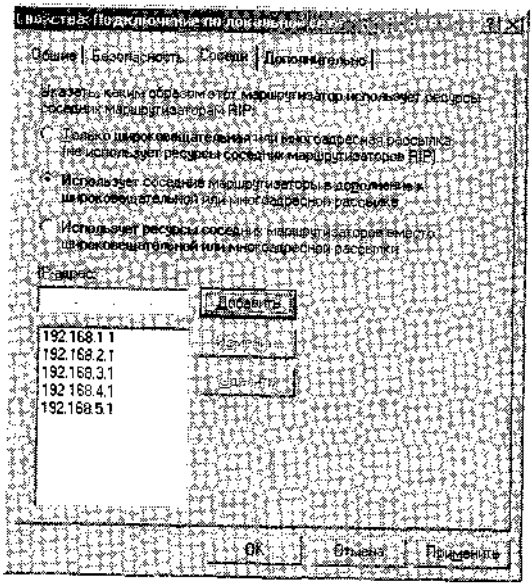


Рис. 9-33. Конфигурирование одноадресных приемников RIP-объявлений, или соседей

В OSPF используется алгоритм *отбора кратчайшего маршрута* (Shortest Path First, SPF) для определения самого «дешевого» пути между маршрутизатором и всеми сетями объединенной сети. В OSPF-маршрутах гарантированно отсутствуют циклы.

Вместо обмена записями таблиц маршрутизации (как это делают RIP-маршрутизаторы) OSPF-маршрутизаторы хранят схему объединенной сети, обновляя ее после каждого изменения топологии сети. Эта схема, называемая *базой данных состояния связей* (link state database), синхронизируется между всеми OSPF-маршрутизаторами и используется для вычисления маршрутов в таблице маршрутизации. Соседствующие OSPF-маршрутизаторы образуют *соседство* (adjacency) — логическую связь между маршрутизаторами для синхронизации базы данных состояния связей.

Изменения в топологии сети эффективно распространяются по всей объединенной сети, обеспечивая синхронизацию и точность базы данных состояния связей на всех маршрутизаторах. При любых изменениях базы данных состояния связей таблица маршрутизации пересчитывается.

По мере увеличения размера базы данных состояния связей возрастают требования к памяти, а также время на пересчет. Для решения этой проблемы масштабирования OSPF делит объединенную сеть на *области* (areas) (наборы соединенных сетей), которые связаны друг с другом через *магистральную область* (backbone area). Каждый маршрутизатор хранит базу данных состояния связей только тех областей, которые к нему подключены. *Маршрутизаторы на границах областей* (Area Border Routers, ABR) связывают магистральную область с другими областями.

Для дальнейшего уменьшения количества информации маршрутизации в отдельных областях протокол OSPF поддерживает изолированные области. *Изолированная область* (stub area) может содержать одну запись и точку выхода (один граничный маршрутизатор) или несколько граничных маршрутизаторов, когда любой из них может использоваться для достижения адреса назначения внешнего маршрута.

На рис. 9-34 показана схема объединенной OSPF-сети.

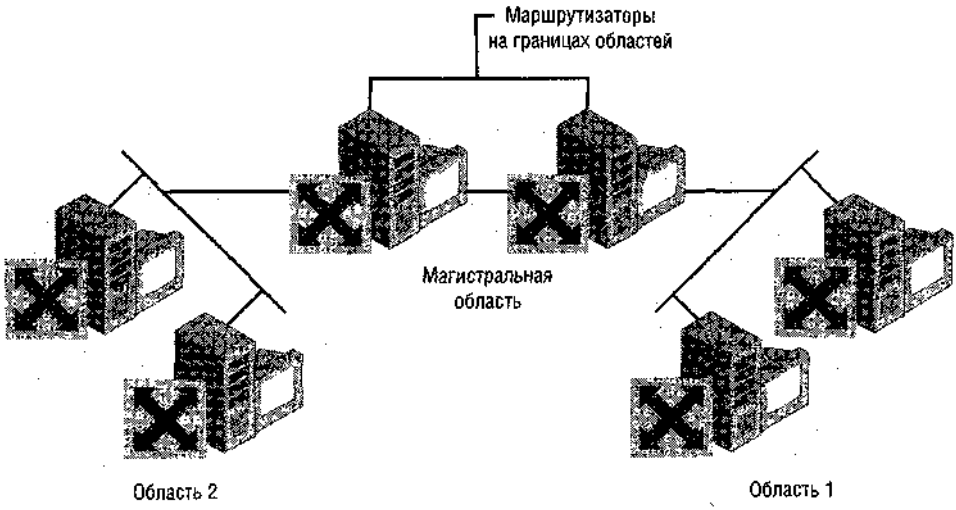


Рис. 9-34. Пример топология OSPF

OSPF и RIP

У OSPF следующие преимущества перед RIP:

- OSPF обеспечивает масштабируемость до размера крупных и крупных объединенных сетей;
- в OSPF отсутствует ограничение на число переходов;
- OSPF быстрее перестраивается при изменении сети;
- OSPF меньше нагружает сеть;
- в OSPF-маршрутах отсутствуют циклы (петли).

Основные сведения об агенте DHCP-ретрансляции

Агент DHCP-ретрансляции (DHCP Relay Agent) — это протокол маршрутизации, позволяющий клиентским компьютерам получать адреса у DHCP-сервера, расположенного в удаленной подсети. Как правило, DHCP-клиенты рассылают широковещательные пакеты DHCPDISCOVER, которые принимает и на которые отвечает DHCP-сервер в той же подсети. Поскольку маршрутизаторы блокируют широковещание, DHCP-клиенты и сервера должны располагаться в одной физической подсети.

Однако есть два метода, позволяющие обойти это ограничение. Во-первых, если маршрутизаторы, отделяющие DHCP-сервер и клиенты, поддерживают спецификацию RFC 1542, на маршрутизаторах можно настроить пересылку по протоколу BOOTP (Boot Protocol), которая позволяет широковещательному DHCP-трафику пересекать машрутизаторы и обеспечивает связь между клиентами и серверами. В такой ситуации DHCP-серверы успешно назначают адреса удаленным клиентам.

Второй способ удаленной связи между DHCP-серверами и клиентами.состоит в настройке агента DHCP-ретрансляции в подсети с удаленными клиентами. Агенты DHCP-ретрансляции перехватывают пакеты DHCPDISCOVER и пересылают их на предопределенный адрес удаленного DHCP-сервера. Хотя агент DHCP-ретрансляции и конфигурируется средствами консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access), компьютер на котором располагается агент не обязан выполнять роль маршрутизатора между двумя подсетями.

На рис. 9-35 показана топология сети с шестью подсетями.

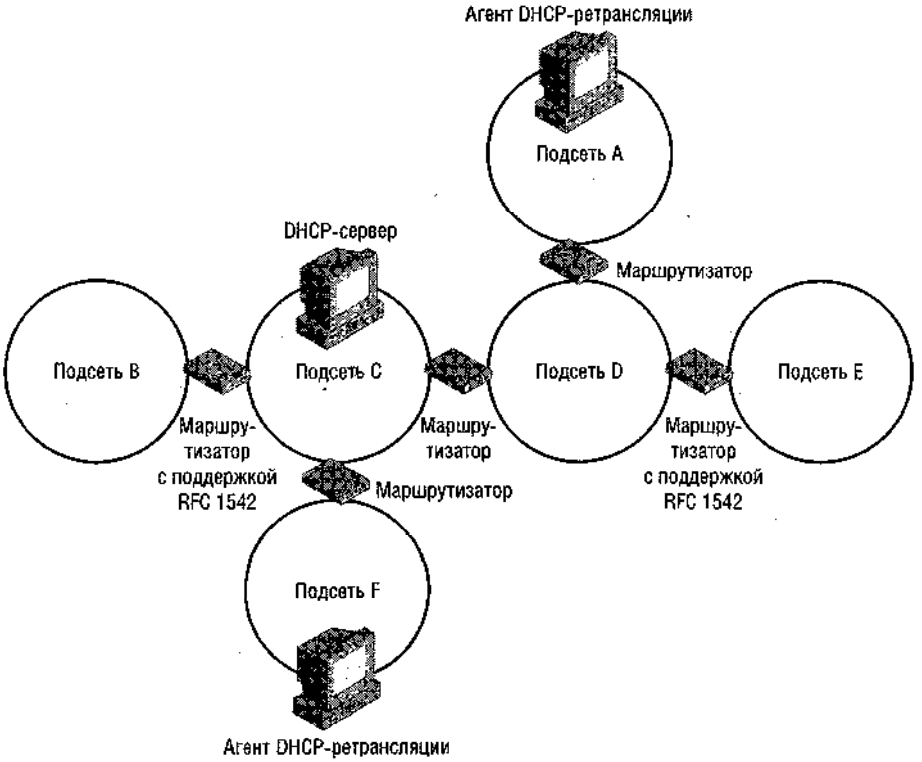


Рис. 9-35. Топология сети с агентом DHCP-ретрансляции

Подготовка к экзамену Будьте готовы к вопросам о топологии, в которой используется агент DHCP-ретрансляции и маршрутизаторы, поддерживающие спецификацию RFC 1542.

В такой сети клиенты всех подсетей кроме D и E смогут получать IP-адреса у DHCP-сервера подсети C.

- В подсети A есть агент DHCP-ретрансляции. Если агент DHCP-ретрансляции настроен на IP-адрес DHCP-сервера в подсети C, DHCP-клиенты подсети A смогут получить адрес у этого сервера.
- В подсети B нет DHCP-сервера или агента DHCP-ретрансляции. Однако широковещательные сообщения DHCPDISCOVER от клиентов подсети B без задержек проходят через поддерживающий спецификацию RFC 1542 маршрутизатор (при условии, что разрешена пересылка BOOTP). Таким образом, запросы DHCP-клиентов подсети B поступают на DHCP-сервер подсети C, который может отвечать, назначая клиентам адреса.
- В подсети C есть DHCP-сервер. Клиенты этой подсети взаимодействуют с DHCP-сервером напрямую.
- В подсети D нет DHCP-сервера или агента DHCP-ретрансляции. И хотя один из ее маршрутизаторов поддерживает спецификацию RFC 1542, что обеспечивает широковещание DHCP-запросов в другую подсеть, в этой подсети также нет ни того, ни другого, поэтому клиенты подсети D не способны получать адреса у DHCP-сервера подсети C.

- В подсети E также нет ни DHCP-сервера, ни агента DHCP-ретрансляции, и поддерживающий спецификацию RFC 1542 маршрутизатор не обеспечивает связь клиентов подсети E с DHCP-сервером.
- В подсети F есть агент DHCP-ретрансляции. Если он настроен на адрес DHCP-сервера подсети C, то обеспечит перехват запросов клиентов подсети F и их пересылку на DHCP-сервер.

Примечание Агент DHCP-ретрансляции нельзя устанавливать на компьютере со службой DHCP, компонентом протокола маршрутизации NAT с поддержкой автоматического назначения адресов или службой ICS.

Настройка агента DHCP-ретрансляции

До настройки агента DHCP-ретрансляции надо добавить одноименный протокол в консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access).

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните подузел **Общие (General)** узла **IP-маршрутизация (IP Routing)** правой кнопкой и выберите **Новый протокол маршрутизации (New Routing Protocol).**
2. **В** одноименном окне выберите **Агент DHCP-ретрансляции (DHCP Relay Agent)** и щелкните OK.

Далее сконфигурируйте агент DHCP-ретрансляции на адрес по крайней мере одного удаленного DHCP-сервера в окне **Свойства: Агент DHCP-ретрансляции (DHCP Relay Agent Properties)** (рис. 9-36). (Для обеспечения отказоустойчивости разрешается назначать несколько DHCP-серверов.)

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **Агент DHCP-ретрансляции (DHCP Relay Agent)** правой кнопкой и выберите **Свойства** (Properties).
2. На вкладке **Общие (General)** в поле **Адрес сервера (Server Address)** введите IP-адрес DHCP-сервера и щелкните Добавить **(Add).**
3. Повторите п. 2 для всех добавляемых DHCP-серверов и щелкните OK.

Далее включите протокол на интерфейсе(ах), указывающем на сетевой сегмент с DHCP-клиентами.

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните **Агент DHCP-ретрансляции (DHCP Relay Agent)** правой кнопкой и выберите **Новый интерфейс (New Interface).**
2. Выберите нужный интерфейс и щелкните OK.
3. Убедитесь, что в окне **Свойства DHCP-ретрансляции (DHCP Relay Properties)** на вкладке **Общие (General)** установлен флажок **Ретрансляция DHCP-пакетов (Relay DHCP packets).**
4. Если необходимо, стрелками задайте новые пороговые значения в полях числа переходов и времени ожидания.

Проверка работы агента DHCP-ретрансляции

Один из методов проверки агента DHCP-ретрансляции — использование консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access). Для этого выберите узел **Агент DHCP-ретрансляции (DHCP Relay Agent)** и в правой панели наблюдайте статистику работы. Здесь приводится информация о полученных и отброшенных запросах и ответах. Получение и запросов и ответов говорит о работе агента DHCP-ретрансляции.

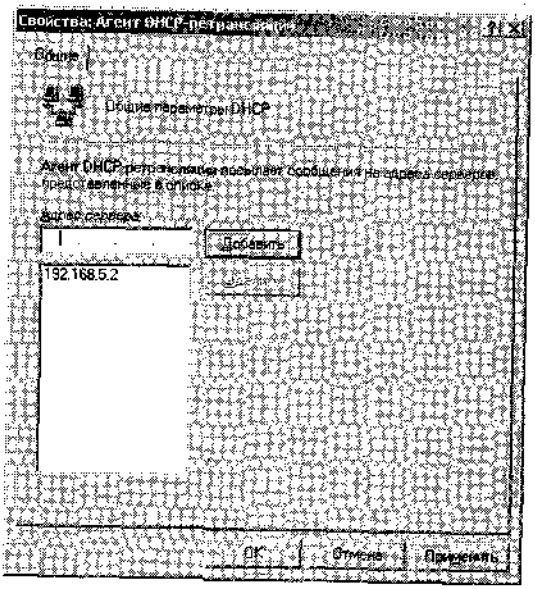


Рис. 9-36. Свойства агента DHCP-ретрансляции

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки - в разделе «Вопросы и ответы» в конце главы.

1. В чем недостаток RIP-аутентификации?
2. Какие методы помимо RIP-аутентификации позволяют предотвратить создание злоумышленниками неверных маршрутов на ШР-маршрутизаторах?
3. Перечислите пять преимуществ OSPF перед RIP
4. В сети, состоящей из двух подсетей, надо развернуть один DHCP-сервер. Опишите два метода, которые позволяют решить эту задачу?

Резюме

- RIP - протокол динамической маршрутизации, позволяющий маршрутизаторам определять оптимальный путь для пересылки данных. Маршруты выбираются по принципу минимальной стоимости. По умолчанию стоимость определяется числом переходов, или маршрутизаторов между конечными точками, однако в RIP число переходов ограничено — всего 15.
- RIP поддерживает ряд настраиваемых функций, в том числе аутентификацию фильтрацию равных RIP-маршрутизаторов, фильтры маршрутов и соседи.
- OSPF служит для обмена информацией о маршрутизации в крупных и очень крупных объединенных сетях. Хотя он сложен в развертывании, у него много преимуществ перед RIP, в том числе более высокая производительность, точность маштабируемость и способность настройки.
- Если надо обеспечить автоматическую поддержку адресации во всех подсетях надо в каждой подсети установить DHCP-сервер или *Агент DHCP-ретрансляции* (DHCP Relay Agent), указывающий на DHCP-сервер. В качестве альтернативы можно отде-

лить клиентов от подсетей с DHCP-сервером или агентом DHCP-ретрансляции маршрутизаторами, поддерживающими пересылку BOOTP-трафика (то есть поддерживающими спецификацию RFC 1542).

Занятие 5. Настройка фильтров пакетов

При включении *Простого брандмауэра* (Basic Firewall) на внешнем интерфейсе в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access), интерфейс начинает блокировать весь входящий незапрошенный трафик. Однако иногда требуется разрешить вполне определенные запросы определенной внутренней службы, например Web-сервера. В этом случае создают фильтры пакетов, которые блокируют весь трафик из внешней сети за исключением предназначенных определенной службе.

Изучив материал этого занятия, вы сможете:

V настроить фильтры пакетов, чтобы разрешить доступ к внутренним службам.

Продолжительность занятия — около 25 минут.

Основные сведения о фильтрах пакетов

Фильтры пакетов (packet filters) — это правила, определяемые на конкретном интерфейсе, которые разрешают или запрещают трафик по определенным признакам: по исходному адресу, адресу назначения, направлению или протоколу. Фильтры можно рассматривать как отдушины в брандмауэре, через которые клиентам позволено получить доступ к определенным внутренним службам. Без них брандмауэр жестко блокирует все запросы из внешней сети.

Функционирование фильтров в службе *Маршрутизация и удаленный доступ* (Routing and Remote Access) основано на исключениях. Фильтры назначаются интерфейсам и настраиваются в одном из двух режимов:

- пропуск всего трафика за исключением пакетов, запрещенных фильтрами;
- запрещение всего трафика за исключением пакетов, запрещенных фильтрами.

В Windows Server 2003 фильтры пакетов делятся на два типа: *входные* (input filters) и *выходные фильтры* (output filters). Первые ограничивают трафик, Поступающий на интерфейс из непосредственно подключенной к нему сети, а вторые — трафик, поступающий с интерфейса в сеть. На рис. 9-37 показан пример входного фильтра, блокирующего все пакеты за исключением направленных на TCP-порт 1723 и IP-адрес 207.46.22.1.

Подготовка к экзамену Будьте готовы к вопросам, в которых все фильтры пакетов определены правильно, но действие фильтра настроено некорректно.

Создание фильтров пакетов

Фильтры пакетов создаются в узле **IP-маршрутизация (IP Routing)** консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access). Они определяются в окне свойств узла **Общие (General)** или **NAT/Простой брандмауэр (NAT/Basic Firewall).** Следует иметь в виду, что последний позволяет создавать только фильтры на внешних интерфейсах, а первый — на любых.

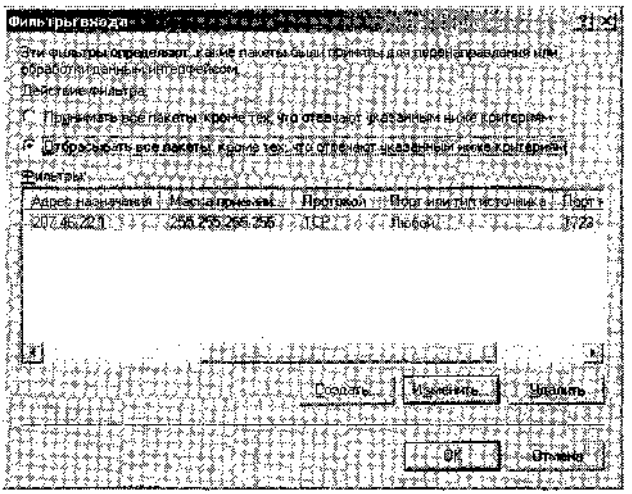


Рис. 9-37. Пример фильтра пакетов

- **Создание фильтра пакетов**

1. **В** дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) разверните узел **IP-маршрутизация (IP Routing)** и выберите **Общие (General).**
2. В правой панели щелкните правой кнопкой интерфейс, на котором надо задать фильтр, и выберите **Свойства (Properties).** Откроется окно свойств, показанное на рис. 9-38.

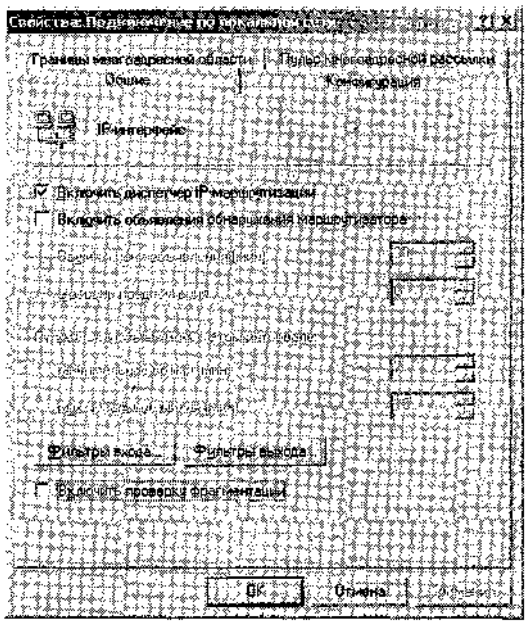


Рис. 9-38. Настройка фильтров пакетов

3. На вкладке **Общие** щелкните кнопку **Фильтры входа (Inbound Filters)** или **Фильтры выхода (Outbound Filters).**

4. В открывшемся одноименном окне щелкните **Создать** (New).
5. В окне **Добавление IP-фильтра (Add IP Filter)** введите параметры фильтра и щелкните OK.
6. В области **Действие фильтра (Filter Action)** выберите нужное действие фильтра и щелкните **OK.**

Примечание Фильтры пакетов можно определять в конфигурации политики удаленного доступа. Политика удаленного доступа (см. главу 10) позволяет назначать правила и ограничения на определенные подключения удаленного доступа. Комбинируя фильтры пакетов и уровень политик удаленного доступа, можно определять самые различные уровни ограничений доступа для различных пользователей.

Базовый сценарий фильтрации пакетов

В этом сценарии, реализованном в Windows Server 2003, на внешнем интерфейсе создаются два фильтра пакетов, которые разрешают незапрошенные подключения к Web-серверу (адрес 207.46.22.1), размещенному во внутренней сети (рис. 9-39).

Фильтр № 1 сконфигурирован как входной и определяет IP-адрес адресата 207.46.22.1 с маской 255.255.255.255. Кроме того, этот фильтр настроен на протокол TCP и предназначенный для Web порт 80. Действие фильтра в окне **Фильтры входа (Inbound Filters)** определено как **Отбрасывать все пакеты, кроме тех, что отвечают указанным ниже критериям (Drop all packets except those that meet the criteria below).**

Фильтр № 2 определен как выходной; в нем задан IP-адрес источника 207.46.22.1 с маской 255.255.255.255. Фильтр также настроен на протокол TCP и назначенный для Web порт 80. Действие фильтра в окне **Фильтры выхода (Outbound Filters)** также определено как **Отбрасывать все пакеты, кроме тех, что отвечают указанным ниже критериям.**

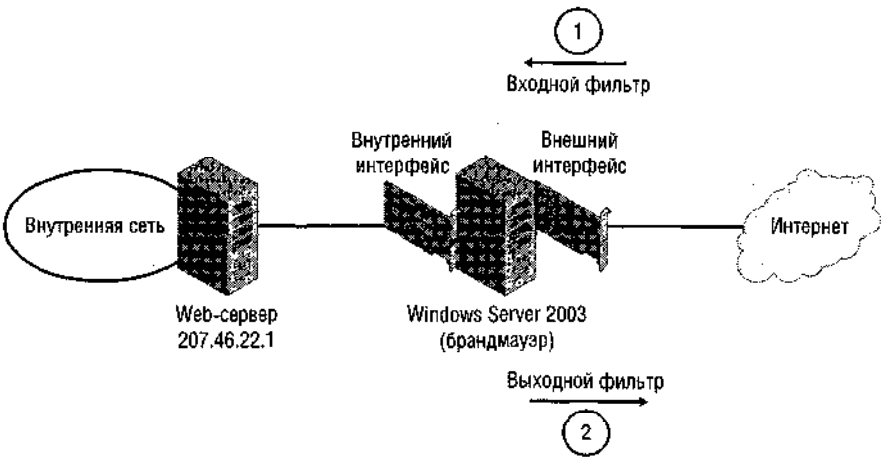


Рис. 9-39. Базовый сценарий фильтрации пакетов

Сценарий «блокирующей» фильтрации пакетов

В этом сценарии максимальной безопасности для доступа к службе создаются четыре фильтра. Как видно на рис. 9-40, один фильтр работает на всех четырех этапах связи.

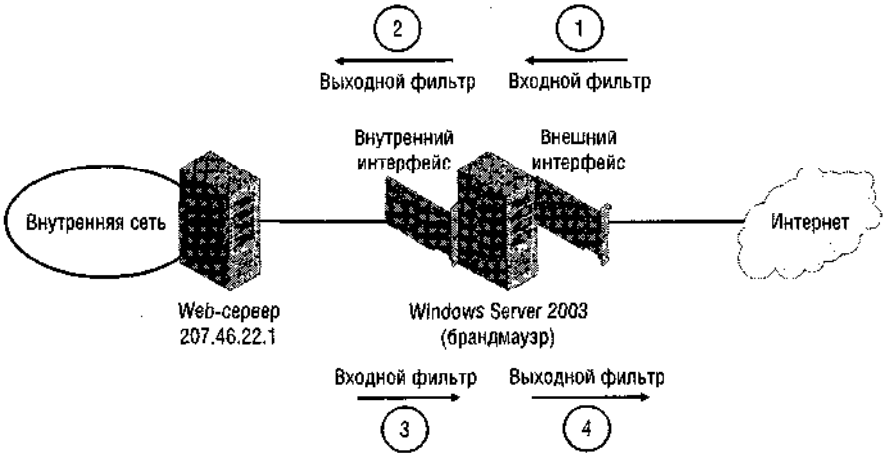


Рис. 9-40. Сценарий «блокирующей» фильтрации пакетов

В случае внутреннего Web-сервера во всех фильтрах определен протокол TCP и порт 80, а также IP-адрес Web-сервера (207.46.22.10) как источник или адресат, соответственно.

1. Внешний интерфейс, входной фильтр: сеть назначения— 207.46.22.10/32, протокол — TCP, порт — 80.
2. Внутренний интерфейс, выходной фильтр: сеть назначения— 207.46.22.10/32, протокол — TCP, порт — 80.
3. Внутренний интерфейс, входной фильтр: исходная сеть— 207.46.22.10/32, протокол - TCP, порт - 80.
4. Внешний интерфейс, выходной фильтр: исходная сеть — 207.46.22.10/32, протокол — TCP, порт - 80.

   Затем набор фильтров конфигурируется на запрещение любого другого трафика.

На заметку В плане фильтрации пакетов экзамен существенно отличается от реалий жизни. В действительности при организации доступа к определенной внутренней службе большинство администраторов просто устанавливает специализированный брандмауэр и определяет один двунаправленный фильтр на внешнем интерфейсе.

На экзамене вы, скорее всего, столкнетесь с вопросом о фильтрах пакетов с вариантами ответов, содержащими запутанный набор из четырех фильтров пакетов для каждого протокола. Как правило, по крайней мере два из предложенных ответов определяют правильные порты, поэтому вам достаточно определить, который из вариантов правильно определяет направление фильтра на интерфейсе. Такие вопросы непросты, но если вы в состоянии представить себе четыре этапа связи через внешние и внутренние интерфейсы, то наверняка осилите их.

Развитые сценарии фильтрации пакетов

В отличие от Web-серверов связь в других службах организована не по одному, а по нескольким каналам. Например, в протоколе PPTP (Point-to-Point Tunneling Protocol) задействованы TCP-порт 1723 — для создания и поддержки VPN-подключения и IP-протокол № 47 для пересылки данных по этому подключению. Таким образом для под-

держки подключения удаленных PPTP-пользователей к внутреннему VPN-серверу надо создать два набора фильтров: один — для TCP-порта 1723 и второй — для протокола с номером 47. Каждый набор фильтров действует по схеме, описанной на рис. 9-39 или 9-40.

Подготовка к экзамену Номер протокола обычно указывает на поток данных определенной службы. Чтобы создать фильтр пакетов для протокола с определенным номером, в окне **Добавление IP-фильтра (Add IP Filter)** в поле со списком **Протокол (Protocol)** выберите **Другой (Other)** и введите номер протокола в поле **Номер протокола (Protocol number).**

Другой VPN-протокол, L2TP/IPSec (Layer2 Tunneling Protocol/Internet Protocol Security), требует три набора фильтров. Здесь задействованы UDP-порты 500 и 4500 — для создания и поддержки подключения, — и IP-протокол 50 — для пересылки данных.

VPN, PPTP и L2TP/IPSec подробно обсуждаются в главе 10. Информацию о других номерах портов, связанных с различными службами TCP/IP, вы найдете в занятии 1 главы 2.

Подготовка к экзамену Запомните номера протоколов и портов, необходимых для работы PPTP и L2TP/IPSec.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В компании используется частный протокол XCA, работающий по двум отдельным TCP-портам. Вам поручили организовать связь внешних пользователей с пользователями внутренней сети по XCA. Каково минимальное число фильтров пакетов надо создать на сервере удаленного доступа с Windows Server 2003, чтобы обеспечить входящую и исходящую связь по XCA с внутренней сетью?
2. В сети установлен компьютер под управлением Windows Server 2003 со службой *Маршрутизация и удаленный доступ* (Routing and Remote Access), выполняющий функции простого брандмауэра. Сколько фильтров пакетов надо создать, чтобы обеспечить удаленный доступ к VPN-серверу по протоколу L2TP/IPSec? Предполагается, что требуется обеспечить самые жесткие ограничения безопасности.
3. Какие порты и протоколы надо открыть, чтобы обеспечить связь с VPN-сервером на основе PPTP, расположенным за брандмауэром, то есть во внутренней сети? Какие порты и протоколы надо открыть, чтобы обеспечить связь с VPN-сервером на основе L2TP/IPSec?

Резюме

- *Фильтры пакетов* (packet filters) — это правила, определяемые на конкретном интерфейсе, которые разрешают или запрещают трафик по определенным признакам: по исходному адресу, адресу назначения, направлению или протоколу. Без них брандмауэр просто блокирует все запросы из внешней сети.
- Когда внешним пользователям надо обеспечить доступ к серверу или службе внутренней сети, создают фильтры пакетов, которые блокируют весь трафик в/из внешней сети за исключением предназначенных определенной службе.

- В Windows Server 2003 каждый фильтр пакетов ограничивает трафик только в одном направлении. Чтобы обеспечить доступ извне к внутренней службе, обычно определяют один входной и один выходной фильтр на внешнем интерфейсе брандмауэра. На обоих фильтрах определяют протокол и адрес службы. Для укрепления защиты обычно конфигурируют аналогичный дополнительный набор фильтров на внутреннем интерфейсе брандмауэра.

Пример из практики

Вас пригласили в качестве консультанта в фармацевтическую компанию Fabrikam, Inc., специализирующуюся на выпуске «сердечных» лекарств. Fabrikam расположена в г. Итаке, штат Нью-Йорк; в ней работает более 600 ученых и исследователей, многие пришли из других фармацевтических компаний.

За прошедшие полтора года группа исследователей Fabrikam сделала ряд открытий, которые позволяют надеяться на революционные перемены в лечении инфаркта миокарда. Разделяя оптимизм исследователей, руководство компании также обеспокоено возможностью утечки информации и угрозой промышленного шпионажа.

Чтобы устранить возможность утечки информации, руководство решило хранить все данные исследований, связанных с научными открытиями, в новой защищенной подсети. В целом корпоративная сеть состоит из 12 подсетей (рис. 9-41), четыре из которых принадлежат научно-исследовательскому отделу. В компании используется маршрутизация на основе RIP, но руководство опасается, что хакеры смогут узнать маршруты к подсетям.

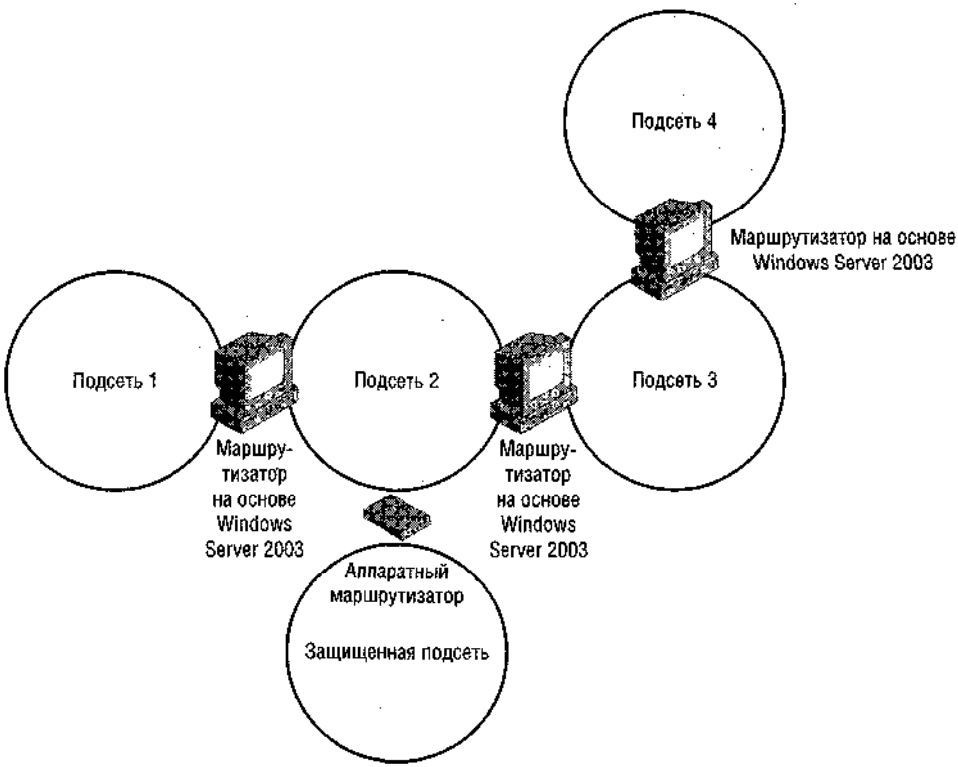


Рис. 9-41. Сеть научно-исследовательского отдела компании Fabrikam

В каждой из следующих ситуаций порекомендуйте оптимальный вариант решения.

1. Руководство компании требует улучшить защиту маршрутизации в сети и недвусмысленно выразило свое недовольство тем, что аутентификация маршрутизаторов выполняется паролем в виде открытого текста. Какие дополнительные меры можно предпринять для предотвращения перехвата информации о маршрутах и появления в сети подставных маршрутизаторов? (Выберите все подходящие варианты.)
   a. Развернуть службу каталогов Active Directory.
   b. Настроить в RIP поддержку автостатических маршрутов.
   c. Сконфигурировать соседей RIP.
   d. Создать фильтры равных RIP-маршрутизаторов.
   e. Организовать фильтрацию маршрутов.
2. Что нужно сделать, чтобы информация о маршруте к новой защищенной подсети была доступна только узлам подсети 2?
   a. Развернуть в сети протокол OSPF и сконфигурировать маршрутизатор, подключенный к защищенной подсети, как маршрутизатор границы области.
   b. Настроить фильтры равных RIP-маршрутизаторов на маршрутизаторе, подключенном к защищенной подсети.
   c. Обеспечить шифрование маршрутов по методу MPPE.
   d. Не развертывать протокол маршрутизации на маршрутизаторе, подключенном к защищенной подсети. Настроить на рабочих станциях подсети 2 статические маршруты в защищенную подсеть.
3. Группа из 20 ученых из Fabrikam проводила исследования в течение 10 месяцев в г. Оттаве, штат Онтарио. Они создали сеть и хотят, чтобы она периодически подключалась к штаб-квартире в Итаке. Как обеспечить, чтобы входящие вызовы, принимаемые сетевым маршрутизатором штаб-квартиры, действительно поступали с маршрутизатора временного офиса в Оттаве?
   a. Сконфигурировать принимающий маршрутизатор в Итаке на аутентификацию всех входящих вызовов.
   b. Настроить обратный вызов на принимающем маршрутизаторе в Итаке.
   c. Настроить обратный вызов на вызывающем маршрутизаторе в Оттаве.
   d. Отключить автостатические маршруты на обоих маршрутизаторах.

Практикум по устранению неполадок

Вам надо устранить неполадки NAT. Прежде всего проверьте, что на Computerl нет никаких других дополнительных интерфейсов вызовов по требованию помимо **Удал, маршрутизатор (Remote Router).**

1. С Computer2 войдите в Domain 1 как *Администратор* (Administrator).
2. Откройте Internet Explorer подключитесь к любому внешнему Web-сайту, например *http://www.windowsupdate.com*. Если интерфейс вызовов по требованию **Удал, маршрутизатор (Remote Router)** на Computerl еще не подключен, по истечении времени ожидания Internet Explorer сообщит о невозможности загрузить Web-страницу. В этом случае щелкните кнопку **Обновить (Refresh).**

3. После подключения к внешнему Web-сайту с Computer2 на Computerl войдите в Domainl -*как Администратор* (Administrator) и откройте окно командной строки.
4. Выполните команду: netsh ro ip na se in "r" p.
5. Вернитесь к Computer2 и попытайтесь открыть другой внешний сайт. Этого сделать не удастся.
6. На Computerl проверьте конфигурацию NAT в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access). В чем ошибка в конфигурации?
7. На Computerl выполните следующую команду:

```
netsh routing ip nat set interface "Remote Router" fullfirewall
```

8. Убедитесь, что теперь можно подключиться к внешним Web-сайтам с Computer2.
9. Выйдите из системы Computerl и Computer2.

Резюме главы

- Служба *Маршрутизация и удаленный доступ* (Routing and Remote Access) может выполнять функции программного маршрутизатора.
- Консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access) — основной инструмент конфигурирования и управления службой *Маршрутизация и удаленный доступ* (Routing and Remote Access).
- В Windows Server 2003 увидеть таблицу IP-маршрутизации можно в консоли *Маршрутизация и удаленный доступ* или исполнив команду route print.
- Для подключения к не-соседним подсетям, когда нет протоколов динамической маршрутизации, а сами подсети располагаются в направлении, отличном от маршрута по умолчанию, на маршрутизаторе надо настроить статические маршруты.
- Статические маршруты создаются в консоли *Маршрутизация и удаленный доступ* или командой route add. Параметр -p в команде route add делает статический маршрут постоянным, то есть он сохраняется даже после перезагрузки маршрутизатора.
- Маршрутизация вызовов по требованию — это процесс пересылки трафика с одного маршрутизатора на другой по телефонной линии. Такое телефонное подключение может создаваться по мере необходимости, то есть вызываться по требованию или быть постоянным.
- *Компонент преобразования сетевых адресов* (Network Address Translation, NAT) службы *Маршрутизация и удаленный доступ* в Windows Server 2003 позволяет не только маршрутизировать IP-пакеты, проходящие между локальной сетью и Интернетом, но и изменять их адрес назначения (переадресовывать). Такая переадресация позволяет обеспечить доступ в Интернет многим клиентским компьютерам по одному *общему* (public) адресу или ограниченному пулу таких адресов. NAT можно рассматривать как полностью настраиваемую службу ICS.
- RIP — протокол динамической маршрутизации, который прост в развертывании, но требует много ресурсов и не годится для очень больших сетей. OSPF — протокол динамической маршрутизации, который сложен в развертывании, но зато легко масштабируется, производителен и эффективен.
- *Агент DHCP-ретрансляции* (DHCP Relay Agent) — это протокол маршрутизации, позволяющий клиентским компьютерам получать адреса у DHCP-сервера, расположенного в удаленной подсети.

- Когда внешним пользователям надо обеспечить доступ к серверу или службе внутренней сети, создают фильтры пакетов, которые блокируют весь трафик в/из внешней сети за исключением предназначенных определенной службе.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Научитесь определять, в каких ситуациях необходимы статические маршруты.
- Научитесь читать таблицу маршрутизации.
- Запомните все варианты конфигурации интерфейсов вызовов по требованию.
- Научитесь сравнивать и противопоставлять ICS и NAT. Умейте определять, когда уместна та или иная служба.
- Будьте готовы сравнивать и противопоставить RIP и OSPF, а также определять, какой протокол нужен в той или иной ситуации.
- Научитесь выяснять на основании топологии сети, в каких подсетях нужен агент DHCP-ретрансляции.
- Запомните, какие фильтры пакетов надо настроить на брандмауэре, чтобы обеспечить внешним пользователям доступ к службам внутренней сети, например VPN- или Web-серверу.

Основные термины

Обратный вызов ~ callback — механизм, в котором отвечающий маршрутизатор немедленно по получении вызова по телефонной линии разрывает соединение и пытается подключиться по предопределенному номеру телефона.

Протоколы BAP/BACP (Bandwidth Allocation Protocol/Bandwidth Allocation Control Protocol) — протоколы, которые обеспечивают в многоканальных подключениях подключение/отключение дополнительных каналов связи в соответствии с расширение/сужением доступной пропускной способности.

Автостатические маршруты ~ autostatic routes — особенность RIP, при наличии которой по маршруту не направляются обычные объявления, а маршруты обновляются полуавтоматически: вручную или с использованием заданного сценария.

Обнаружение маршрутизатора ~ router discovery — функция, основанная на обмене ICMP-сообщениями, в которых инициируются запросы на обнаружение маршрутизатора, на которые те отвечают периодическими объявлениями, что позволяет клиенту обнаружить работоспособные маршрутизаторы.

Пересылка BOOTP ~ BOOTP forwarding — процесс пересылки широковещательных DHCP-сообщений между сетями маршрутизаторами, поддерживающими спецификацию RFC 1542.

Вопросы и ответы

Занятие 1. Упражнение

6. На странице **Особая конфигурация (Custom configuration)** ознакомьтесь со списком возможных вариантов и ответьте на вопрос: сколько базовых функций маршрутизации позволяет сконфигурировать данный мастер?
   Правильный ответ: 5.

Занятие 1. Закрепление материала

1. ИТ-отдел подключен к Интернету по *цифровой абонентской линии* (Digital Subscriber Line, DSL), которой также пользуются остальные подразделения организации. Однако вскоре отдел получил более быстрое подключение к Интернету по линии T1, которую решили использовать исключительно для нужд ИТ-отдела. DHCP-сервер предоставляет всем пользователям IP-конфигурацию, но компьютеры сотрудников ИТ-отдела распределены в тех подсетях, что и компьютеры обычных сотрудников. Как обеспечить, чтобы только сотрудники ИТ-отдела получили доступ к Интернету по новой линии T1? Причем требуется сконфигурировать эту возможность лишь раз с тем, чтобы потом ничего не пришлось изменять.

   Правильный ответ: используйте команду Route с параметром -p на компьютерах сотрудников ИТ-отдела, чтобы создать постоянный статический маршрут к линии T1. Параметр -p позволит создать постоянный маршрут.

2. Вам не удается подключиться ни к одному компьютеру за пределами локальной подсети. Результат выполнения команды `route print` приведен ниже. В чем наиболее вероятная причина неполадки?

Network Destination	Netmask	Gateway	Interface
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.1

   Правильный ответ: шлюз по умолчанию настроен на адрес локального компьютера.

3. После создания постоянного статического маршрута командой `route` он не обнаруживается в результатах работы команды `route print` на локальной машине. Маршруту назначена метрика 1. Предполагается, что команда выполнена успешно. В чем может быть причина неполадки?

   Правильный ответ: есть другой источник маршрута с более высоким приоритетом.

4. Какие протоколы используются для поддержки многоканальных подключений и добавления/отключения подключений по телефонной линии по мере необходимости?
   Правильный ответ: BAP и BACP.

Занятие 2. Закрепление материала

1. Используя службу *Маршрутизация и удаленный доступ,* вы сконфигурировали маршрутизацию вызовов по требованию, чтобы подключить филиал к корпоративной ЛВС. Однако даже при наличии протокола RIP маршруты не обновляются по WAN-каналам. Почему это происходит и как организовать обновление маршрутов?

Правильный ответ: RIP настроен на обновление автостатических маршрутов по подключениям вызовов по требованию. В узле Общие (General) консоли Маршрутизация и удаленный доступ (Routing and Remote Access), щелкните интерфейс вызовов по требованию правой кнопкой и выберите Обновить маршруты (Update Routes).

2. Связь с филиалом обеспечивается по подключению вызовов по требованию. Как надежнее всего запретить пользователям подключаться к филиалу на время обеда?

   Правильный ответ: настройте часы исходящих подключений на запрещение доступа в обеденные часы.

3. Филиал подключен к сети штаб-квартиры по *цифровой сети с комплексными услугами* (Integrated Services Digital Network, ISDN) с использованием подключения вызова по требованию. Надо заблокировать открытие подключения HTTP-запросами. Как это сделать?

   Правильный ответ: сконфигурируйте IP-фильтр вызовов по требованию на обоих маршрутизаторах так, чтобы подключения создавались для всего трафика за исключением направленного на TCP-порт 80.

4. Штаб-квартира подключена к филиалу с применением маршрутизации вызовов по требованию. Каждый из маршрутизаторов сконфигурирован на инициирование и прием вызовов. Однако финансовый отдел потребовал, чтобы большую долю расходов на телефонную связь между маршрутизаторами вызовов по требованию несла штаб-квартира. Как решить эту задачу?

   Правильный ответ: настройте обратный вызов на главном корпоративном маршрутизаторе так, чтобы приняв вызов по телефонной линии, маршрутизатор разрывал связь и сам подключался к маршрутизатору филиала.

Занятие 3. Упражнение 1

5. Перейдите на вкладку **Назначение адресов (Address Assignment)** и ответьте на вопрос: какая служба NAT настраивается на этой вкладке?

   Правильный ответ: DHCP-распределитель.

6. Перейдите на вкладку **Разрешение имен в адреса (Name Resolution)** и ответьте на вопрос: какая служба NAT настраивается на этой вкладке?

   Правильный ответ: DNS-прокси.

Занятие 3. Упражнение 2

6. Какому физическому интерфейсу принадлежит общий адрес, сопоставленный службой NAT частному адресу Computer2?

   Правильный ответ: модему на Computerl.

5. Ответьте на следующие вопросы.

   a. Нужно ли при назначении этих параметров конфигурации, чтобы пул адресов, назначаемый внешнему интерфейсу, составлял непрерывное адресное пространство?

   Правильный ответ: да.

   b. Воспользовавшись калькулятором, определите, какую маску подсети надо назначить пулу 207.46.200.0-207.46.207.255.

   Правильный ответ: 255.255.248.0.

   c. Какое максимальное число адресов возможно в пуле с маской подсети 255.255.255.248?

   Правильный ответ: 6.

7. Ответьте на вопрос: в каких ситуациях при конфигурировании свойств NAT используется кнопка **Резервирование (Reservations)?**

   Правильный ответ: кнопка Резервирование (Reservations) используется при наличии пула внешних адресов и необходимости сопоставить один адрес конкретному компьютеру внутренней сети.

12. Ответьте на следующие вопросы. Блокирует ли маршрутизатор по умолчанию ping-запросы внешнего интерфейса внешними клиентами? внутренними клиентами?

    Правильный ответ: да, нет.

Занятие 3. Закрепление материала

1. В сети размещается новый компьютер для обеспечения подключения к Интернету сети, состоящей из одной подсети с клиентскими компьютерами, которым назначены статические адреса из диапазона 192.168.0.1—192.168.0.65, и критически важными серверамисо статическими адресами из диапазона 192.168.0.100—192.168.0.120. На новом компьютере настроена служба ICS, но ни один из компьютеров сети не в состоянии подключиться к Интернету. Как проще всего решить проблему?

   Правильный ответ: настройте клиентские компьютеры на автоматическое получение адреса, а на критически важных серверах определите в качестве шлюза по умолчанию адрес 192.168.0.1.

2. В сети размещены 11 критически важных серверов, которым назначены статические адреса из диапазона 192.168.0.1—192.168.0.20. После настройки ICS пользователи не в состоянии подключаться к сети, а сетевым компьютерам не удается найти контроллеры домена и подключиться к сетевыми объектам по их именам. Как устранить неполадку, если предполагается, что изменять адреса критически важных серверов нельзя?

   Правильный ответ: для подключения к Интернету вместо ICS используйте NAT. Назначьте NAT-серверу свободный адрес из диапазона адресов критически важных серверов и настройте в качестве шлюза по умолчанию адрес NAT-сервера.

3. **В** сети расположены критически важные серверы со статическими адресами из диапазона 10.0.0.1—10.0.0.20. Клиентским компьютерам назначены статические адреса из диапазона 10.0.0.21—10.0.0.100. Изменить назначенные сетевые адреса не представляется возможным. В сети устанавливается NAT-сервер, который должен распределять IP-адреса в этой же IP-подсети и обеспечивать подключение к Интернету. Однако компьютеры сети не в состоянии подключаться к Интернету. Какова наиболее вероятная причина неполадки?

   Правильный ответ: надо настроить на сетевых компьютерах в качестве шлюза по умолчанию адрес NAT-сервера. (Не определяйте шлюз по умолчанию на самом NAT-сервере.)

4. NAT-сервер подключен к Интернету по DSL-линии. Интернет-провайдер предоставил блок из 8 адресов, которые надо назначить внешнему интерфейсу NAT-сервера. Как решить задачу?

   Правильный ответ: сконфигурируйте пул адресов на общем интерфейсе. Определите пул как диапазон адресов, полученных от интернет-провайдера.

Занятие 4. Закрепление материала

1. В чем недостаток RIP-аутентификации?

   Правильный ответ: пароли пересылаются по сети открытым текстом.

2. Какие методы помимо RIP-аутентификации позволяют предотвратить создание злоумышленниками неверных маршрутов на RIP-маршрутизаторах?

   Правильный ответ: настройка фильтрации равных RIP-маршрутизаторов.

3. Перечислите пять преимуществ OSPF перед RIP.

   Правильный ответ: масштабируемость, отсутствие ограничения в 15 переходов, более быстрая адаптация к изменениям сети, меньшая нагрузка на сеть и отсутствие циклов в маршрутах.

4. В сети, состоящей из двух подсетей, надо развернуть один DHCP-сервер. Опишите два метода, которые позволяют решить эту задачу?

   Правильный ответ: 1 — разделить две подсети маршрутизатором, поддерживающим спецификацию RFC 1542, и активизировать BOOTP-пересылку; 2 — сконфигурировать агент DHCP-ретрансляции в подсети, не имеющей собственного DHCP-сервера.

Занятие 5. Закрепление материала

1. **В** компании используется частный протокол XCA, работающий по двум отдельным TCP-портам. Вам поручили организовать связь внешних пользователей с пользователями внутренней сети по XCA. Каково минимальное число фильтров пакетов надо создать на сервере удаленного доступа с Windows Server 2003, чтобы обеспечить входящую и исходящую связь по XCA со внутренней сетью?

   Правильный ответ: 4.

2. **В** сети установлен компьютер под управлением Windows Server 2003 со службой *Маршрутизация и удаленный доступ* (Routing and Remote Access), выполняющий функции простого брандмауэра. Сколько фильтров пакетов надо создать, чтобы обеспечить удаленный доступ к VPN-серверу по протоколу L2TP/IPSec? Предполагается, что требуется обеспечить самые жесткие ограничения безопасности.

   Правильный ответ: 12.

3. Какие порты и протоколы надо открыть, чтобы обеспечить связь с VPN-сервером на основе PPTP, расположенным за брандмауэром, то есть во внутренней сети? Какие порты и протоколы надо открыть, чтобы обеспечить связь с VPN-сервером на основе L2TP/IPSec?

   Правильный ответ: для PPTP надо открыть TCP-порт 1723 и протокол с номером 47, а для L2TP /IPSec — UDP-порты 4500 и 500 и протокол 50.

Пример из практики

1. Руководство компании требует улучшить защиту маршрутизации в сети и недвусмысленно выразило свое недовольство тем, что аутентификация маршрутизаторов выполняется паролем в виде открытого текста. Какие дополнительные меры можно предпринять для предотвращения перехвата информации о маршрутах и появления в сети подставных маршрутизаторов? (Выберите все подходящие варианты.)

   a. Развернуть службу каталогов Active Directory.
   b. Настроить в RIP поддержку автостатических маршрутов.
   c. Сконфигурировать соседей RIP.
   d. Создать фильтры равных RIP-маршрутизаторов.
   e. Организовать фильтрацию маршрутов.

   Правильные ответы: a, c, d, e.

2. Что нужно сделать, чтобы информация о маршруте к новой защищенной подсети была доступна только узлам подсети 2?
   a. Развернуть в сети протокол OSPF и сконфигурировать маршрутизатор, подключенный к защищенной подсети, как маршрутизатор границы области.
   b. Настроить фильтры равных RIP-маршрутизаторов на маршрутизаторе, подключенном к защищенной подсети.
   c. Обеспечить шифрование маршрутов по методу MPPE.
   d. Не развертывать протокол маршрутизации на маршрутизаторе, подключенном к защищенной подсети. Настроить на рабочих станциях подсети 2 статические маршруты в защищенную подсеть.

   Правильный ответ: d.
3. Группа из 20 ученых из Fabrikam проводила исследования в течение 10 месяцев в г. Оттаве, штат Онтарио. Они создали сеть и хотят, чтобы она периодически подключалась к штаб-квартире в Итаке. Как обеспечить, чтобы входящие вызовы, принимаемые сетевым маршрутизатором штаб-квартиры, действительно поступали с маршрутизатора временного офиса в Оттаве?
   a. Сконфигурировать принимающий маршрутизатор в Итаке на аутентификацию всех входящих вызовов.
   b. Настроить обратный вызов на принимающем маршрутизаторе в Итаке.
   c. Настроить обратный вызов на вызывающем маршрутизаторе в Оттаве.
   d. Отключить автостатические маршруты на обоих маршрутизаторах.

   Правильный ответ: b.

Практикум по устранению неполадок

6. На Computerl проверьте конфигурацию NAT в консоли **Маршрутизация и удаленный доступ (Routing and Remote Access).** В чем ошибка в конфигурации?
   Правильный ответ: созданный для протокола NAT интерфейс вызовов по требованию, *Удал, маршрутизатор* (Remote Router), некорректно конфигурирован как подключенный к частной сети.

ГЛАВА 10

Настройка и управление удаленным доступом

Темы экзамена

- Настройка аутентификации пользователя в службе *Маршрутизация и удаленный доступ* (Routing and Remote Access):
  - настройка протоколов аутентификации при удаленном доступе;
  - настройка службы IAS (Internet Authentication Service) для аутентификации клиентов службы *Маршрутизация и удаленный доступ;*
  - настройка политик службы *Маршрутизация и удаленный доступ* для разрешения или запрещения доступа.
- Управление удаленным доступом:
  - управление интерфейсами маршрутизации службы *Маршрутизация и удаленный доступ;*
  - управление устройствами и портами;
  - управление протоколами маршрутизации;
  - управление клиентами службы *Маршрутизация и удаленный доступ;*
- Реализация безопасного доступа между частными сетями.
- Устранение неполадок доступа пользователя к службам удаленного доступа:
  - диагностика и устранение неполадок удаленного доступа по VPN;
  - диагностика и устранение неполадок при установке подключения удаленного доступа;
  - диагностика и устранение неполадок при доступе пользователей к ресурсам, обслуживаемым сервером удаленного доступа
- Устранение неполадок маршрутизации в службе *Маршрутизация и удаленный доступ:*
  - устранение неполадок межмаршрутизаторных VPN-подключений.

В этой главе

Здесь подробно рассказано о настройке удаленного доступа к сети по телефонной линии или с применением виртуальных частных сетей (VPN). Кроме того, вы узнаете о принципах и процедурах, лежащих в основе адресации удаленного доступа, аутентификации, авторизации и устранения неполадок, а также как обеспечить безопасность и управляемость удаленного доступа в корпоративной среде.

Прежде всего

Для изучения материалов этой главы вам потребуется:

- два объединенных в сеть компьютера Computerl и Computer2 под управлением Microsoft Windows Server 2003. Computerl надо присвоить статический адрес 192.168.0.1/24. Computer2 надо настроить на автоматическое получение адреса, а также определить для него альтернативную конфигурацию с адресом 192.168.0.2/24;
- отдельная телефонная линия для каждого компьютера (рекомендуется);
- две учетных записи у интернет-провайдера или одна учетная запись, позволяющая подключить к Интернету одновременно два разных компьютера (рекомендуется);
- установить на Computerl DNS-сервер для управления основной интегрированной с Active Directory областью *domain 1. local;*
- настроить Computer 1 в качестве контроллера домена смешанного режима *domain I. local,* а Computer2 присоединить к этому домену;
- установить на Computerl DHCP-сервер, который надо авторизовать в домене и назначить ему область Test Scope с диапазоном адресов IP 192.168.0.11—192.168.0.254. В параметрах DHCP следует назначить для области маршрутизатор (шлюз) с адресом 192.168.0.1, DNS-сервер с адресом 192.168.0.1 и DNS-имя домена *domain 1.local.* Область следует активизировать. Computer2 должен получить параметры IP у этого DHCP-сервера.

Занятие 1. Настройка подключений удаленного доступа

Чтобы пользователи смогли подключаться к удаленной сети (например, по телефонной линии), необходимо выполнить ряд условий, в том числе: организовать адресацию, позволяющую клиентам телефонного подключения связываться с удаленной сетью, и настроить аутентификацию пользователей, установив соответствующий протокол аутентификации.

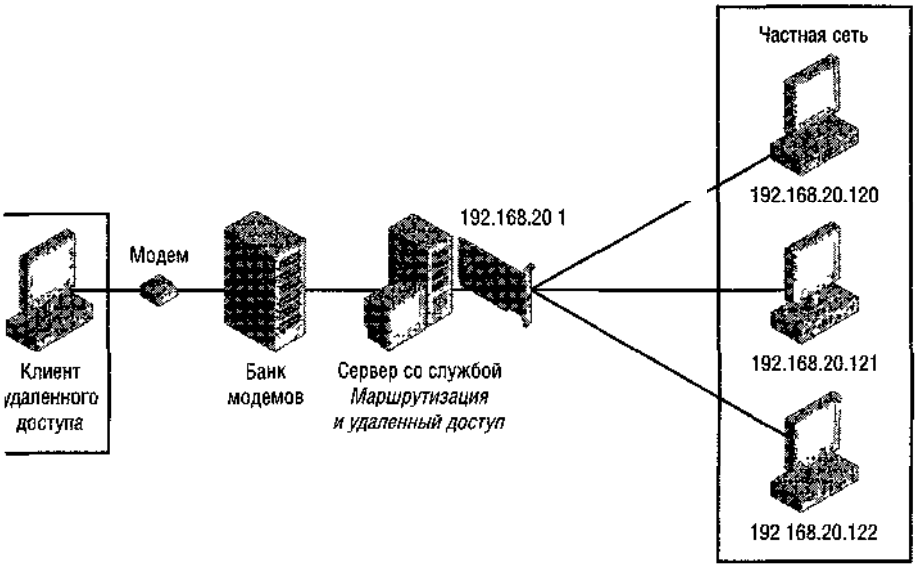
Изучив материал этого занятия, вы сможете:

- V настроить адресацию удаленного доступа;
- V настроить сервер удаленного доступа по телефонной линии;
- V настроить клиент удаленного доступа по телефонной линии;
- V настроить аутентификацию пользователей службы *Маршрутизация и удаленный доступ* (Routing And Remote Access);
- V настроить протоколы аутентификации удаленного доступа.

Продолжительность занятия — около 75 минут.

Удаленный доступ по телефонной линии

Обычно удаленный доступ осуществляется по телефонной линии либо по VPN-подключению. Здесь описан порядок настройки адресации и аутентификации удаленного доступа для подключения по телефонной линии (рис. 10-1).



ис. 10-1. Схема подключения к сети по телефонной линии

Клиент подключается по телефонной линии с использованием протокола PPP (Point-to-Point Protocol) к компьютеру с Windows Server 2003 и службой *Маршрутизация и удаленный доступ*. Обычно такое подключение устанавливается по линиям телефонной коммутируемой сети общего пользования, хотя возможен и другой вариант: цифровая сеть с комплексными услугами (ISDN) или сеть X.25.

Сервер удаленного доступа, или NAS-сервер (network access server), отвечает на телефонные вызовы клиента по отдельным модемам, которые устанавливаются в самостоятельном банке (рис. 10-1) или непосредственно на самом сервере.

Чтобы обеспечить удаленный доступ по телефонной линии, надо настроить и клиент, и сервер. На первом необходимо сконфигурировать подключение к серверу удаленного доступа с помощью *Мастера новых подключений* (New Connection Wizard). На втором настройка выполняется с помощью *Мастера настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard) или в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access).

Примечание *Мастер настройки сервера маршрутизации* и *Мастер удаленного доступа* можно использовать, лишь если на сервере еще не сконфигурирована служба *Маршрутизация и удаленный доступ*. Чтобы открыть окно мастера, в консоли *Маршрутизация и удаленный доступ* щелкните правой кнопкой значок сервера и выберите *Настроить и включить маршрутизацию и удаленный доступ* (Configure and Enable Routing and Remote Access).

Адресация клиентов удаленного доступа

Любому удаленному компьютеру, подключающемуся к серверу удаленного доступа по протоколу PPP, автоматически присваивается IP-адрес. Сервер удаленного доступа получает IP-адреса, которые затем распределяет среди клиентов удаленного доступа либо с DHCP-сервера, либо из статического набора IP-адресов.

Способ распределения IP-адресов определяется на странице **Назначение IP-адресов (IP Address Assignment)** *Мастера настройки сервера маршрутизации и удаленного доступа* (Ro and Remote Access Server Setup Wizard) (рис. 10-2) или в области **Назначение IP-адресов (IP Address Assignment)** окна свойств сервера маршрутизации и удаленного доступа (рис. 10-3).

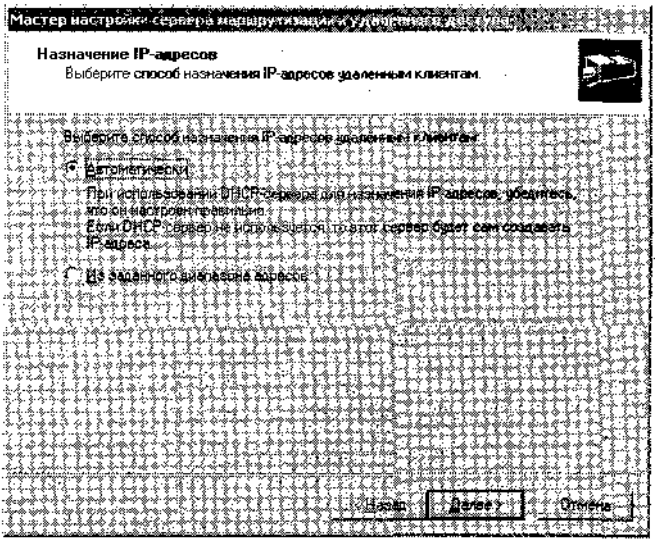


Рис. 10-2. Настройка адресации в *Мастере настройки сервера маршрутизации и удаленного доступа*

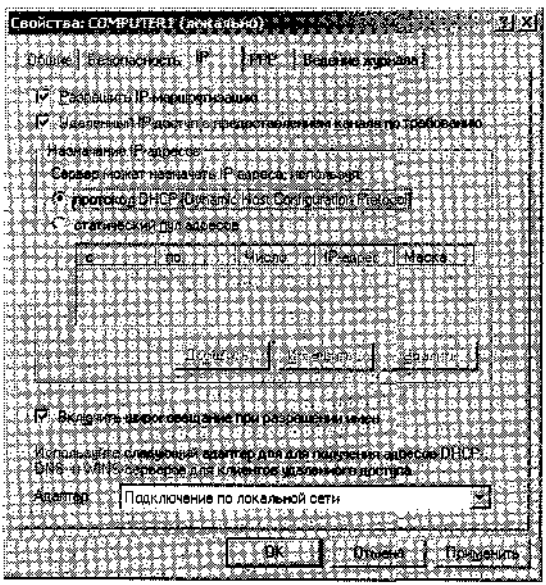


Рис. 10-3. Настройка адресации в окне свойств сервера

DHCP

При наличии в сети DHCP-сервера надо предусмотреть в конфигурации сервера удаленного доступа возможность выделения адресов этим DHCP-сервером, Если DHCP-сервер находится за пределами широковещательного диапазона сервера удаленного доступа, надо настроить агент ретрансляции DHCP на самом сервере удаленного доступа или в его сетевом сегменте.

Если получение адресов от DHCP-сервера уже включено, при запуске сервер удаленного доступа получает блок из 10 адресов, первый из которых достается самому серверу удаленного доступа, а остальные выделяются удаленным TCP/IP-клиентам по мере их подключения. Если этих IP-адресов не хватает, сервер удаленного доступа получает дополнительные адреса порциями по 10 штук. Если при запуске службы *Маршрутизация и удаленный доступ* DHCP-сервер недоступен, клиент удаленного доступа сам присваивает себе адрес из диапазона 169.254.0.1-169.254.255.254 по протоколу APIPA (Automatic Private IP Addressing). С таким адресом, как правило, нельзя получить удаленный доступ к сети.

Подготовка к экзамену На экзамене нужно знать, как служба *Маршрутизация и удаленный доступ* получает и распределяет IP-адреса, и что неполадки возникают, когда эта служба не получает от DHCP-сервера очередные 10 адресов. Типичным признаком отклонения от этой «нормы» является появление у клиента удаленного доступа APIPA-адреса. Помните, что APIPA-адрес может также информировать о необходимости настройки DHCP-сервера или агента ретрансляции DHCP в сегменте сети сервера удаленного доступа.

Статический пул адресов

Если в сети нет DHCP-сервера, сервер удаленного доступа обычно присваивает клиентам адреса, взятые из специального статического пула (рис. 10-4). Так называется особый набор адресов, логически связанный с диапазоном адресов, обслуживаемых сервером удаленного доступа, но не перекрывающий его. Например, если внутренний адрес сервера удаленного доступа 192.168.1.1/24, пул адресов можно описать как часть диапазона 192.168.1.0/24, из которого исключены адреса, уже присвоенные компьютерам внутренней сети.

Если статический пул адресов определен в виде отдельной подсети (или набора подсетей), логически не связанной с подсетями, к которым напрямую подключен сервер удаленного доступа, нужно обязательно указать новую подсеть в параметрах маршрутизаторов. Это все равно, что к физическому сетевому сегменту сервера удаленного доступа добавить логическую подсеть. Иначе говоря, маршрутизаторы сети должны пересылать адресованные удаленным клиентам пакеты в сегмент сети сервера удаленного доступа. О настройке протоколов маршрутизации и статических маршрутизаторов — в главе 9.

Настройка аутентификации при удаленном доступе

После вызова сервера удаленного доступа и получения необходимого IP-адреса выполняется аутентификация учетных данных, отправленных на сервер. *Аутентификация* (authentication) — это процесс подтверждения личности пользователя, при котором осуществляется проверка пароля или иных учетных данных, например сертификатов и смарт-карт. Аутентификация удаленного доступа предшествует аутентификации при входе в домен; если подключающийся по телефонной линии пользователь входит в домен, аутентификацию и авторизацию сначала проходит телефонное подключение, и только затем выполняется вход в домен.

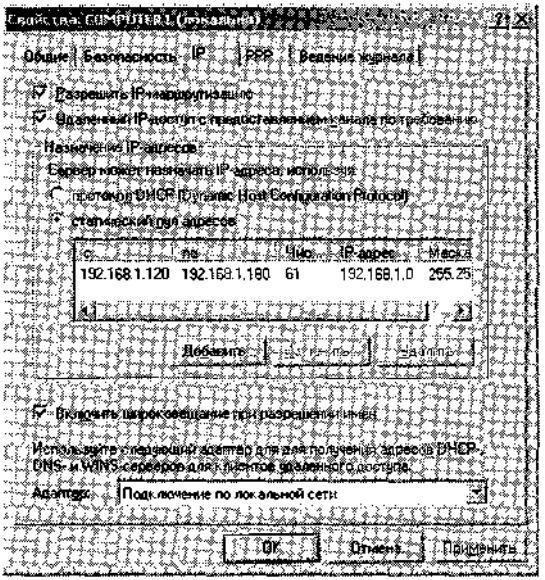


Рис. 10-4. Настройка пула адресов для клиентов удаленного доступа

Примечание В отличие от *аутентификации* — процесса подтверждения подлинности пользователя, *авторизация* (authorization) — это процесс получения разрешений на доступ к ресурсам. Вслед за аутентификацией удаленного доступа выполняется авторизация подключения удаленного доступа, то есть учетной записи пользователя предоставляется доступ к ресурсам, определенный в разрешениях и политиках удаленного доступа, применяемых к телефонному подключению. Подробнее о политике удаленного доступа и авторизации — в занятии 2.

Чтобы войти в домен посредством телефонного подключения, установите в диалоговом окне **Вход в Windows (Log On To Windows)** флажок **С использованием удаленного доступа (Log On Using Dial-Up Connection).** После ввода имени и пароля пользователя и щелчка OK откроется окно **Сетевые подключения (Network Connections).** Выберите в списке подключений сконфигурированное для удаленного доступа по телефонной линии и щелкните **Подключить (Connect).** После создания подключения выполняется аутентификация и авторизация удаленного доступа. Обычно имя пользователя, домен и пароль, заданные в свойствах подключения, совпадают с учетными данными, зарегистрированными в домене, однако оба набора учетных данных задаются и проверяются порознь.

Если учетные данные телефонного подключения подтверждены и получены необходимые разрешения, создается подключение удаленного доступа. Далее следует обычный вход в домен; учетные данные, введенные в окне **Вход в Windows,** передаются для аутентификации на контроллер домена.

Примечание При телефонном подключении к изолированному серверу удаленного доступа (не члену домена) пользователь должен прежде войти в систему своего локального компьютера или в локальный домен. В этом случае аутентификация ограничивается проверкой на удаленном компьютере только реквизитов телефонного подключения. Эти учетные данные должны быть заранее внесены в локальную базу SAM (Security Accounts Manager) на запрашиваемом сервере.

Выполнение аутентификации посредством RADIUS

Аутентификация удаленного доступа может выполняться как средствами Windows, так и при участии RADIUS-сервера (Remote Authentication Dial-In User Service). В первом случае пользователь пытается связаться по телефонной линии с компьютером рабочей группы, и аутентификация заключается в проверку имени пользователя и пароля в локальной базе данных безопасности сервера. Когда удаленный пользователь пытается дозвониться в домен, NAS пересылает запрос на аутентификацию контроллеру домена. Во втором случае NAS поручает аутентификацию и авторизацию центральному IAS-серверу. (Подробнее об аутентификации с применением RADIUS — в занятии 4.)

Метод аутентификации определяется на странице **Управление несколькими серверами удаленного доступа (Managing Multiple Remote Access Servers)** *Мастера настройки сервера маршрутизации и удаленного доступа* (рис. 10-5) или на вкладке **Безопасность (Security)** диалогового окна свойств сервера консоли *Маршрутизация и удаленный доступ* (рис. 10-6). Обратите внимание, что при необходимости Windows-аутентификации вместо RADIUS-сервера в мастере надо выбрать вариант **Нет, использовать маршрутизацию и удаленный доступ для проверки подлинности запросов на подключение (No, use Routing And Remote Access to authenticate connection requests).**

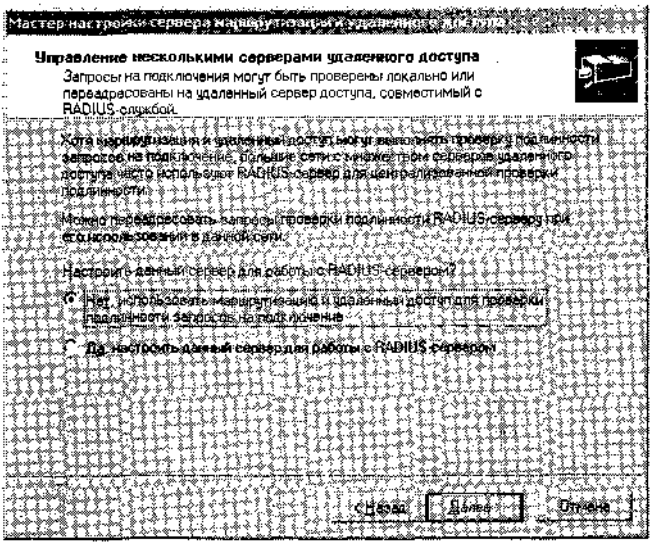


Рис. 10-5. Выбор метода аутентификации удаленного доступа

Выбор протокола аутентификации

Перед аутентификацией учетных данных телефонного подключения сервер удаленного доступа должен согласовать с клиентом удаленного доступа используемый протокол аутентификации. В большинстве таких протоколов есть средства, препятствующие перехвату реквизитов пользователя, и на серверах, и на клиентах под управлением Windows протоколам аутентификации присваивается приоритет, исходя из этого требования безопасности.

Всегда выбирается самый защищенный протокол аутентификации, поддерживаемый клиентом и сервером, и применяемая к подключению политика удаленного доступа. На всех клиентах и серверах удаленного доступа под управлением Microsoft Windows 2000/XP/Server 2003 по умолчанию применяется протокол MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol версии 2).

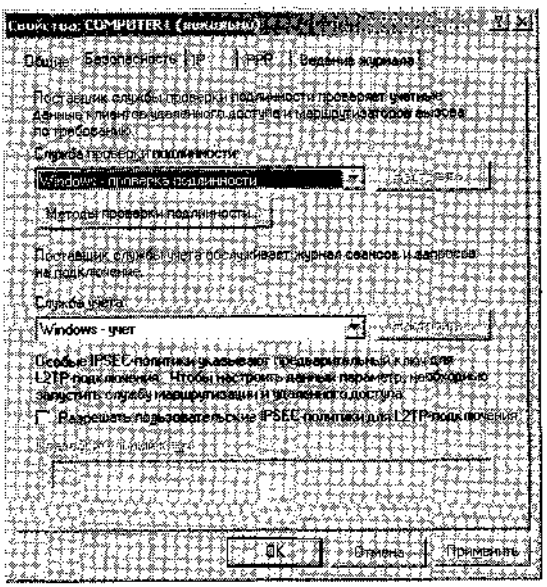


Рис. 10-6. Выбор метода аутентификации удаленного доступа

Ниже приводится полный список протоколов аутентификации, поддерживаемых в Microsoft Windows Server 2003 службой *Маршрутизация и удаленный доступ* (в порядке снижения уровня безопасности).

- **В EAP-TLS (Extensible Authentication Protocol-Transport Level Security)** аутентификация выполняется на основе обмена сертификатами и расширяемой инфраструктуры EAP, включающей новые методы аутентификации. Обычно применяется в сочетании со смарт-картами. Поддерживает шифрование данных аутентификации и подключения. Важно, что EAP-TLS не поддерживается на изолированных серверах; сервер удаленного доступа с Windows Server 2003 должен быть членом домена.
- **MS-CHAP** v2 — алгоритм взаимной аутентификации с шифрованием данных аутентификации и подключения. Для каждого подключения и направления пересылки данных создается свой криптографический ключ. По умолчанию этот метод применяется в Windows 2000/XP/Server 2003.
- **MS-CHAP v1** — алгоритм односторонней аутентификации с шифрованием данных аутентификации и подключения. Во всех подключениях используется один криптографический ключ. Применяется на клиентах ранних версий ОС — Microsoft Windows 95/98. (Полный список совместимости — в табл. 10-2.)
- **EAP-MD5 CHAP (Extensible Authentication Protocol-Message Digest 5 Challenge Handshake Authentication Protocol)** — разновидность метода CHAP, перенесенного в инфраструктуру EAP. Поддерживает шифрование данных аутентификации по алгоритму хеширования MD5. Обеспечивает совместимость с клиентами, не использующими Windows, такими как Mac OSX. Шифрование данных подключения не предусмотрено.
- **CHAP (Challenge Handshake Authentication Protocol)** — общий метод аутентификации, в котором пароль шифруется по алгоритму хеширования MD5. Обеспечивает совместимость с клиентами под управлением ОС, отличных от Windows. Групповая политика для учетных записей, применяющих этот метод аутентификации, должна предусматривать сохранение паролей с использованием *обратимого шифрования* (reversible encryption). (После применения новой политики требуется сброс паролей.) Шифрование данных подключения не поддерживается.

- **SPAP (Shiva Password Authentication Protocol)** — протокол аутентификации со слабым шифрованием. Применяется для взаимодействия с серверами удаленного доступа Shiva. Шифрование данных подключения не поддерживается.
- **PAP (Password Authentication Protocol)** — стандартный метод аутентификации без шифрования паролей, реквизиты передаются по сети открытым текстом. Шифрование данных подключения также не поддерживается.
- **Доступ без аутентификации (Unauthenticated access)** — это не аутентификационный протокол, который, будучи установлен на сервере удаленного доступа, позволяет удаленному клиенту установить подключение без передачи своих реквизитов, если к подключению применяется политика удаленного доступа. Может применяться для устранения неполадок и тестирования подключений удаленного доступа. Шифрование данных подключения не поддерживает.

В табл. 10-1 представлены сведения, облегчающие выбор протокола аутентификации, наиболее подходящего для конкретных целей.

Табл. 10-1. Критерии выбора протокола аутентификации

Требование	Наиболее подходящий вариант
Аутентификация с шифрованием для клиентов удаленного доступа под управлением Windows 95/98/Me/NT 4 (поддерживается изначально)	MS-CHAP v1
Аутентификация с шифрованием для клиентов удаленного доступа под управлением Windows 95/98/Me/NT 4 [с последним обновлением удаленного доступа к сети (Dial-Up Networking)]	MS-CHAP v2 (VPN только для Windows 95)
Аутентификация с шифрованием для инфраструктуры на основе сертификатов PKI (Public Key Infrastructure), а также смарт-карт (когда сервер удаленного доступа является членом домена Windows 2000 Server или Windows Server 2003)	EAP-TLS
Аутентификация с шифрованием для других клиентов удаленного доступа — под управлением Windows 2000/XP/Server 2003	MS-CHAP v2
Двусторонняя аутентификация (клиент и сервер выполняют взаимную проверку)	EAP-TLS, MS-CHAP v2
Шифрование данных подключения	MS-CHAP v1, MS-CHAP v2, EAP-TLS
Аутентификация с шифрованием для клиентов удаленного доступа под управлением других ОС	CHAP, EAP-MD5 CHAP
Аутентификация с шифрованием для клиентов удаленного доступа с Shiva LAN Rover	SPAP
Аутентификация без шифрования, когда клиенты удаленного доступа не поддерживают никакие другие протоколы	PAP
Удаленный клиент не предоставляет аутентификационных данных	Протокол без проверки

Подготовка к экзамену Будьте готовы ответить по крайней мере на следующие вопросы о возможностях и ограничениях протоколов аутентификации.

- Какой протокол требуется для смарт-карт?
- Какой протокол требует использования сертификатов?
- Каковы особые требования к настройке для нормальной работы CHAP?
- В каких ситуациях лучше всего подходит MS-CHAP vl?
- Когда лучше всего выбрать MS-CHAP v2?
- В чем разница между шифрованием аутентификационной информации и данных?
- Какие протоколы поддерживают шифрование данных?
- Какой протокол не поддерживает шифрование аутентификационных данных?
- Какой протокол поддерживает двустороннюю аутентификацию?
- Какой протокол нужно использовать для взамодействия с доменами службы каталогов Active Directory?

В табл. 10-2 представлен перечень протоколов аутентификации, поддерживаемых различными версиями Windows.

Табл. 10-2. Поддержка протоколов аутентификации

Клиент доступа по телефонной линии	Поддерживаемый протокол аутентификации	Неподдерживаемый протокол аутентификации
Windows Server 2003, Windows XP, Windows 2000	MS-CHAP, CHAP, SPAP, PAP,	MS-CHAPV2HEAP
Windows NT 4	MS-CHAP, CHAP, SPAP, PAP и MS-CHAP v2 (с пакетом исправлений Service Pack 4 для Windows NT 4.0 или более поздним)	EAP
Windows NT 3.5 и 3.51	MS-CHAP, CHAP, SPAP и PAP	MS-CHAP v2 и EAP
Windows Me, Windows 98	MS-CHAP, CHAP, SPAP, PAP и MS-CHAP v2 (с Service Pack 1 для Windows 98 или более поздним)	EAP
Windows 95	MS-CHAP, CHAP, SPAP и PAP (с обновлением Dial-Up Networking 1.3 Performance & Security Upgrade для Windows 95 или более поздним)	MS-CHAP v2 и EAP

Подготовка к экзамену Запомните, что Windows 95 не поддерживает MS-CHAPv2 для подключений по телефонным линиям, а EAP поддерживается только в Windows Server 2003/XP/2000.

Настройка протоколов аутентификации на стороне клиента

Для просмотра или изменения протокола аутентификации для телефонного подключения на стороне клиента удаленного доступа откройте окно свойств удаленного доступа и перейдите на вкладку **Безопасность (Security)** (рис. 10-7), где по умолчанию установлены переключатель **Обычные (рекомендуемые параметры) [Typical (Recommended Settings)]** и параметр **Небезопасный пароль (Allow Unsecured Password).** Если щелкнуть переключатель **Дополнительные (выборочные параметры) [Advanced (Custom Settings)],** а затем кнопку **Параметры (Settings),** откроется окно **Дополнительные параметры безопасности (Advanced Security Settings)** (рис. 10-7). Здесь в числе включенных в текущей конфигураций протоколов аутентификации указаны PAP (без шифрования) и SPAP. Последний хотя и шифрует данные аутентификации, но не считается безопасным, поскольку пересылаемый пароль кодируется по известному алгоритму обратимого шифрования. Ясно, что хакерам ничего не стоит его «взломать».

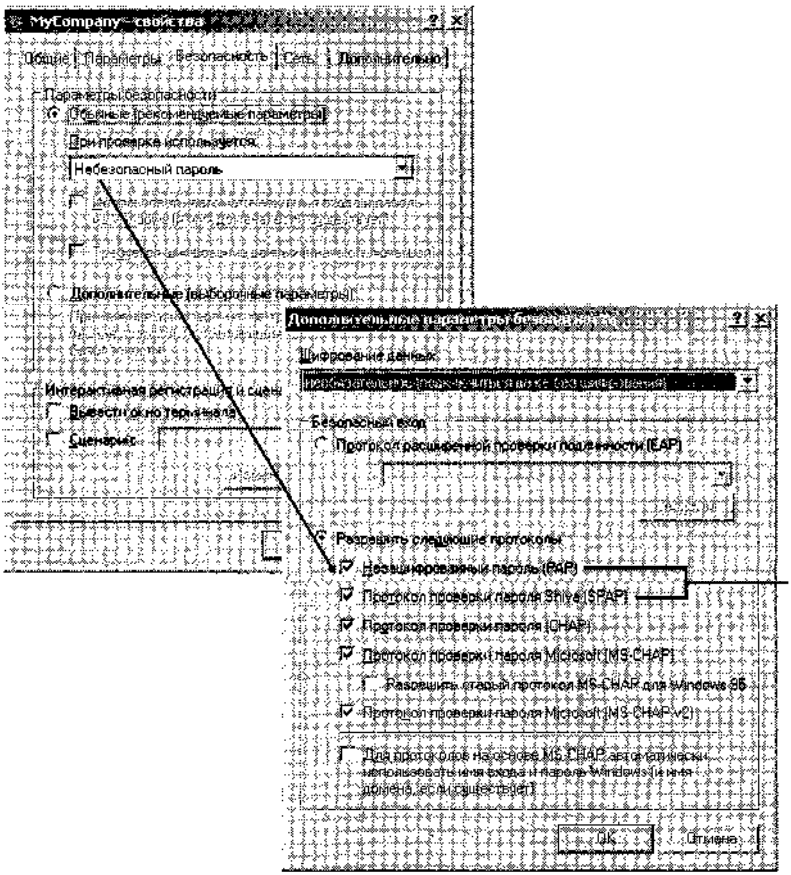


Рис. 10-7. Протоколы аутентификации, включенные по умолчанию на клиенте

Если на вкладке **Безопасность** выбрать параметр **Безопасный пароль (Require Secured Password)** (рис. 10-8), в диалоговом окне **Дополнительные параметры безопасности** изменяется состав активных протоколов аутентификации: остаются CHAP, MS-CHAP v1 и MS-CHAP v2. Менее безопасные PAP и SPAP отключаются.

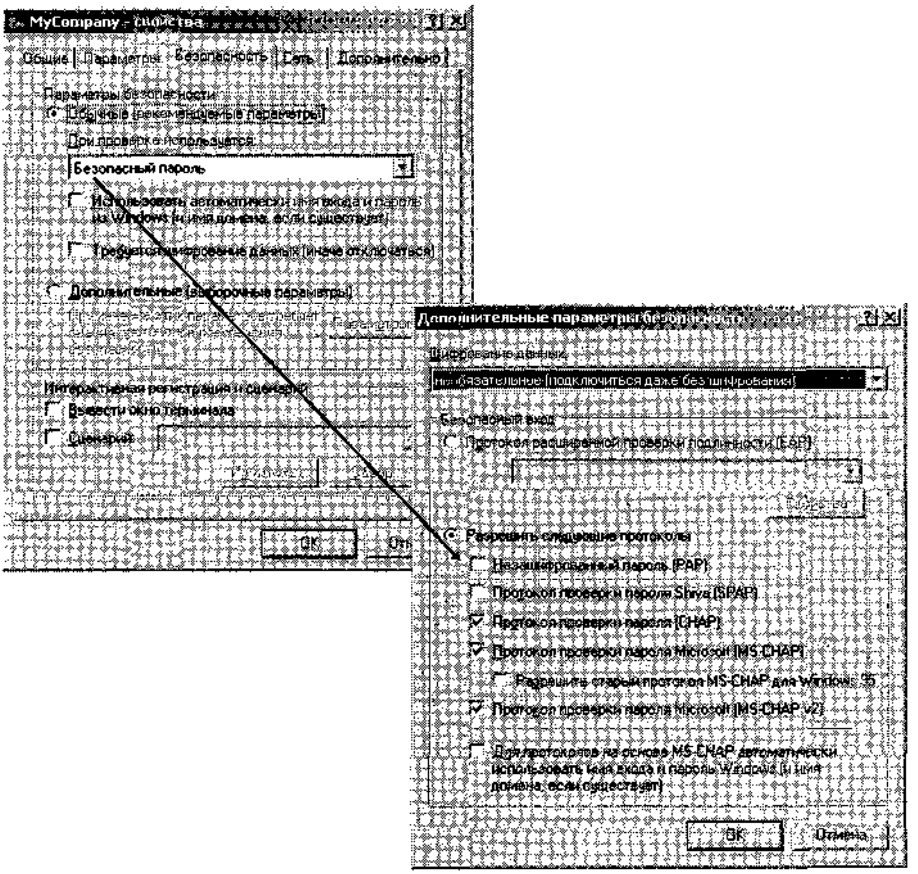


Рис. 10-8. Требование безопасных паролей на стороне клиента удаленного доступа

После установки флажка **Требуется шифрование данных (иначе отключаться) [Require Data Encryption (Disconnect If None)]** (рис. 10-9) включенных протоколов аутентификации становится меньше: остаются только MS-CHAP vl и MS-CHAP v2, а CHAP отключается. Во всех протоколах кроме PAP данные аутентификации (имя пользователя и пароль) шифруются. Протоколы MS-CHAP шифруют также данные PPP-подключения по протоколу MPPE (Microsoft Point-to-Point Encryption). Чтобы обеспечить шифрование данных подключения, необходимо настроить соответствующим образом политику, применяемую к подключению удаленного доступа. (В политике удаленного доступа шифрование данных активизировано по умолчанию.)

Примечание Протокол EAP-TLS также поддерживает шифрование данных PPP-подключения. Но этот протокол требует дополнительной настройки и при установке флажка **Требуется шифрование данных (иначе отключаться)** автоматически не включается.

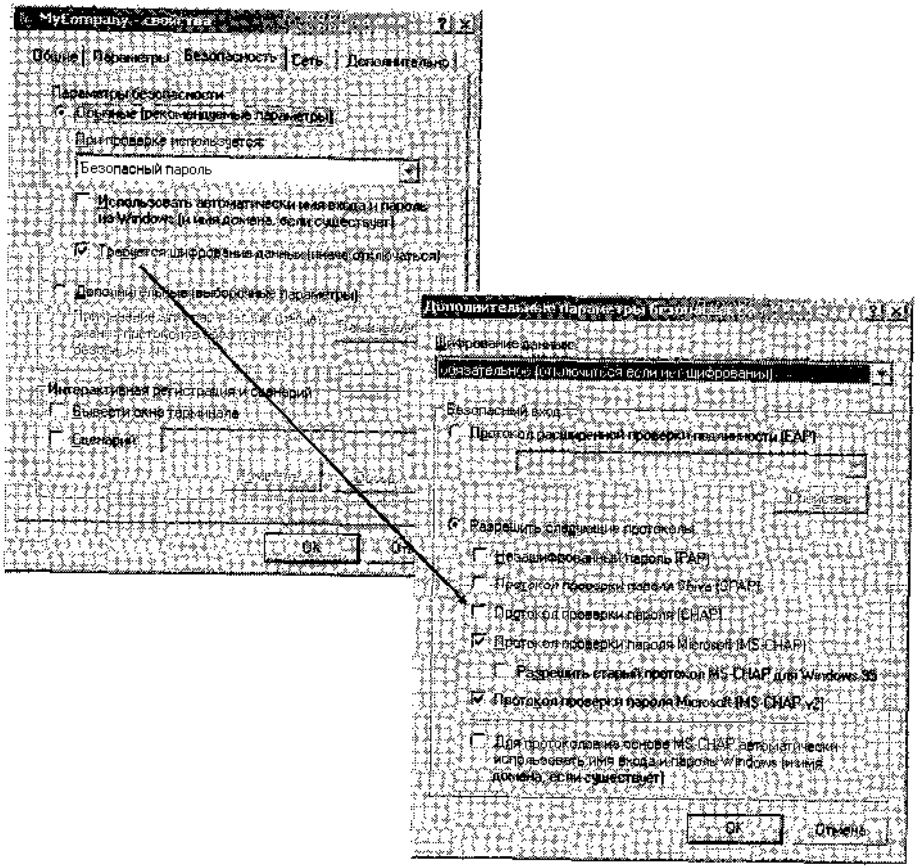


Рис. 10-9. Требование шифрования данных на стороне клиента удаленного доступа

И наконец, при выборе варианта **Смарт-карта (Use Smart Card)** (рис. 10-10) включается только EAP-TLS. В этом случае у параметра **Протокол расширенной проверки подлинности (EAP) [Use Extensible Authentication Protocol (EAP)]** устанавливается значение **Смарт-карта или иной сертификат (шифрование включено) [Smart Card or Other Certificate (Encryption Enabled)].**

Настройка протоколов аутентификации на стороне сервера

Для просмотра и изменения протокола аутентификации на сервере удаленного доступа в консоли *Маршрутизация и удаленный доступ* щелкните значок сервера правой кнопкой и выберите **Свойства (Properties).** На вкладке **Безопасность (Security)** окна свойств сервера щелкните кнопку **Методы проверки подлинности (Authentication Methods).** Откроется одноименное окно (рис 10-11).

И наконец, для просмотра и изменения протоколов аутентификации, установленных в политике удаленного доступа, выберите в консоли *Маршрутизация и удаленный доступ* узел **Политики удаленного доступа (Remote Access Policies),** щелкните дважды нужную политику, а затем в окне ее свойств щелкните кнопку **Изменить профиль (Edit Profile).** В диалоговом окне **Изменение профиля коммутируемых подключений (Edit Dial-In Profile)** перейдите не вкладку **Проверка подлинности (Authentication)** (рис. 10-12). Обратите внимание: по умолчанию EAP-методы отключены.

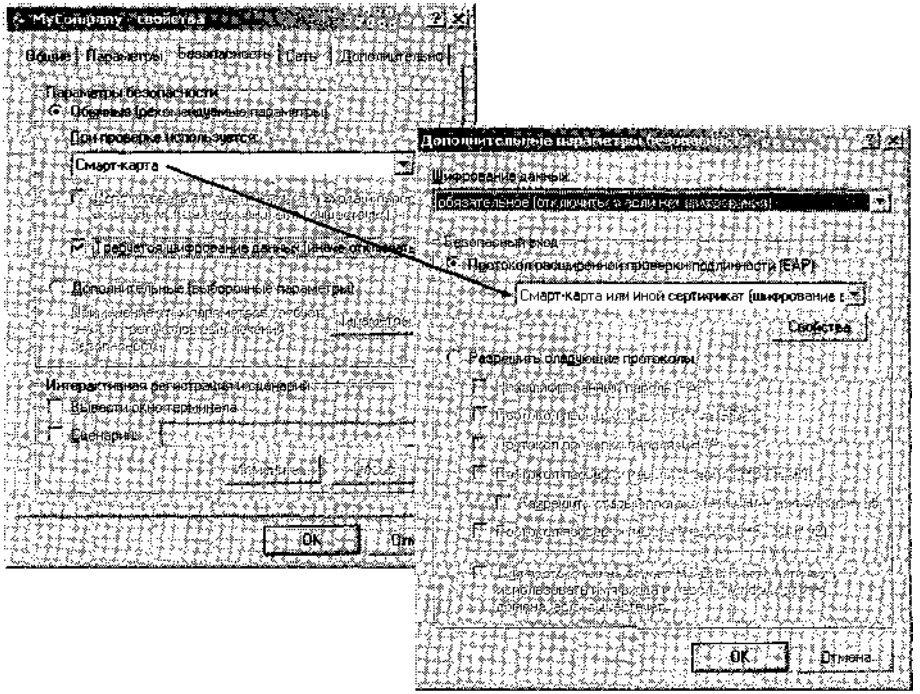


Рис. 10-10. Требование аутентификации с применением смарт-карты на стороне клиента удаленного доступа

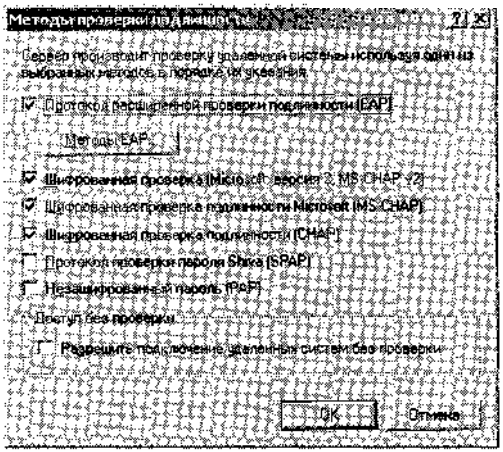


Рис. 10-11. Протоколы аутентификации в службе *Маршрутизация и удаленный доступ*

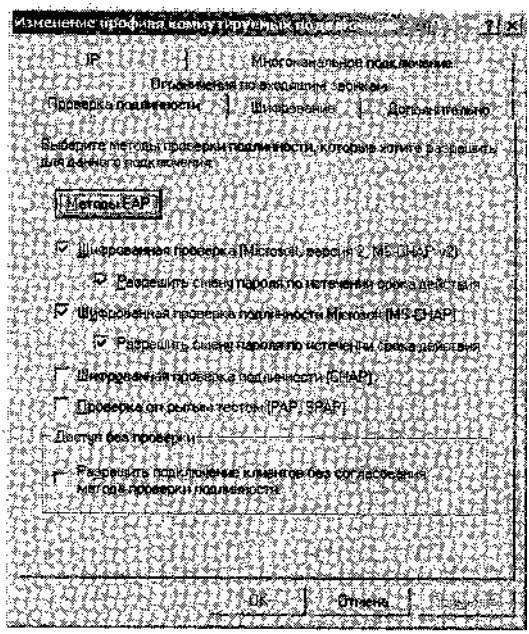


Рис. 10-12. Протоколы аутентификации в политике удаленного доступа

а В консоли *Служба проверки подлинности в Интернете* (Internet Authentication Service) разверните узел **Служба проверки подлинности в Интернете (Internet Authentication Service).**

2. **В** дереве консоли выберите **Политика удаленного доступа (Remote Access Policies)** и в правой панели дважды щелкните нужную политику.
3. В окне свойств щелкните кнопку **Изменить профиль (Edit Profile).**
4. На вкладке **Проверка подлинности (Authentication)** установите нужные параметры и щелкните OK.

Лабораторная работа. **Создание сервера удаленного доступа по телефонной линии**

На этой лабораторной работе вы настроите Computerl в качестве сервера удаленного доступа по телефонной линии с помощью *Мастера настройки сервера маршрутизации и удаленного доступа*.

Упражнение 1. Создание сервера доступа по телефонной линии с помощью *Мастера настройки сервера маршрутизации и удаленного доступа*

Вы войдете в систему Computerl и удалите в консоли *Маршрутизация и удаленный доступ* предыдущую конфигурацию. Затем запустите *Мастер настройки сервера маршрутизации и удаленного доступа* и настроите на Computerl удаленный доступ по телефонной линии.

1. На Computerl войдите в систему как *Администратор* (Administrator) в домене *Domainl.*

2. **В** меню **Пуск (Start)** выберите **Администрирование (Administrative Tools)\Маршрутизация и удаленный доступ (Routing And Remote Access).** Откроется консоль *Маршрутизация и удаленный доступ*.
3. В дереве консоли щелкните узел **COMPUTERl (Local)** правой кнопкой и выберите **Отключить маршрутизацию и удаленный доступ (Disable Routing And Remote Access).** Если эта команда недоступна, перейдите к п. 4.

   Появится информационное окно с предложением подтвердить отключение маршрутизатора. Щелкните Да (Yes). Появится сообщение об остановке службы *Маршрутизация и удаленный доступ*.
4. **В** дереве консоли щелкните узел **COMPUTER1 (Local)** правой кнопкой и выберите **Настроить и включить маршрутизацию и удаленный доступ (Configure and Enable Routing And Remote Access).**
5. В окне *Мастер настройки сервера маршрутизации и удаленного доступа* щелкните **Далее** (Next).
6. На странице **Конфигурация (Configuration)** примите вариант по умолчанию **Удаленный доступ (VPN или модем) [Remote Access (Dial-Up or VPN)]** и щелкните **Далее.**
7. На странице **Удаленный доступ (Remote Access)** установите флажок **Удаленный доступ (Dial-Up)** и щелкните **Далее.**
8. На странице **Выбор сети (Network Selection)** выберите вариант по умолчанию **Подключение по локальной сети (Local Area Connection)** (IP-адрес 192.168.0.1) и щелкните **Далее.**
9. На странице **Назначение IP-адресов (IP Address Assignment)** выберите вариант по умолчанию **Автоматически (Automatically)** и щелкните **Далее.**
10. На странице **Управление несколькими серверами удаленного доступа (Managing Multiple Remote Access Servers)** выберите вариант по умолчанию **Нет, использовать маршрутизацию и удаленный доступ... (No, use Routing and Remote Access...)** и щелкните **Далее.**
11. На странице **Завершение мастера сервера маршрутизации и удаленного доступа (Completing the Routing and Remote Access Server Setup Wizard)** щелкните **Готово (Finish).**
12. Если появится сообщение о необходимости настроить свойства *Агента DHCP-ретрансляции* (DHCP Relay Agent), щелкните **OK.** Появится окно с сообщением об успешном запуске службы *Маршрутизация и удаленный доступ,* а в окне консоли *Маршрутизация и удаленный доступ* под узлом сервера появится структура новой конфигурации.
13. Выйдите из системы Computer 1.

Упражнение 2. Настройка телефонного подключения к удаленному серверу

Вы настроите телефонное подключение на Computer2. Проследите, чтобы Computerl и Computer2 физически подключались к разным телефонным линиям. Настройкой удаленного доступа по телефонной линии к Computerl задача не заканчивается, продолжение — в лабораторной работе занятия 2.

1. На Computer2 войдите в систему как *Администратор* (Administrator) в домене *Domain 1.*
2. Откроите окно **Сетевые подключения (Network Connections).**
3. **В** меню **Файл (File)** щелкните **Новое подключение (New Connection).**
4. **В** окне **Мастер новых подключений (New Connection Wizard)** щелкните **Далее (Next).**

5. На странице **Тип сетевого подключения (Network Connection Type)** выберите вариант **Подключить к сети на рабочем месте (Connect to the network at my workplace)** и щелкните **Далее.**
6. На странице **Сетевое подключение (Network Connection)** оставьте вариант по умолчанию **Подключение удаленного доступа (Dial-Up Connection)** и щелкните **Далее.**
7. На странице **Имя подключения (Connection Name)** в поле **Организация (Company Name)** введите MyCompany и щелкните **Далее.**
8. На странице **Введите номер телефона (Phone Number to Dial)** в поле **Номер телефона (Phone Number)** введите номер телефонной линии, к которой подключен Computerl и щелкните **Далее.**
9. На странице **Доступность подключения (Connection Availability)** оставьте вариант по умолчанию — **Для всех пользователей (Anyone's Use)** и щелкните **Далее.**
   Появится страница **Завершение работы мастера новых подключений (Completing The New Connection Wizard).**
10. На странице **Завершение работы мастера новых подключений (Completing The New Connection Wizard)** щелкните **Готово (Finish).** Откроется окно **Подключение к MyCompany (Connect MyCompany).**
11. Щелкните кнопку **Свойства (Properties).** Отроется окно **MyCompany Свойства (MyCompany Properties).**
12. На вкладке **Параметры (Options)** установите флажок **Включать домен входа в Windows (Include Windows Logon Domain).**
13. Обратите внимание, что на вкладке **Безопасность (Security)** по умолчанию выбран вариант **Небезопасный пароль (Allow Unsecured Password).**
14. Установите переключатель **Дополнительные (выборочные параметры) [Advanced (Custom Settings)]** и щелкните кнопку **Параметры (Settings).** Появится окно **Дополнительные параметры безопасности (Advanced Security Settings).** Обратите внимание, что включены протоколы PAP, SPAP, CHAP, MS-CHAP и MS-CHAP v2.
15. Установите переключатель **Протокол расширенной проверки подлинности (EAP) [Use Extensible Authentication Protocol (EAP)]. В** ставшем доступным поле со списком выбран вариант **Смарт-карта или иной сертификат (шифрование включено) [Smart Card Or Other Certificate (Encryption Enabled)].** Он соответствует протоколу EAP-TLS. Применение смарт-карт по EAP-TLS — это самая безопасная форма аутентификации в сетях Windows Server 2003.
16. Раскройте список **Протокол расширенной проверки подлинности (EAP).** Обратите внимание, что в списке есть еще только один протокол EAP — **MDS-отклик (MD5-Challenge).** Это разновидность CHAP, в котором для передачи информации используются EAP-сообщения. Он задействован во всех реализациях EAP, но уровень обеспечиваемой им безопасности считается невысоким.
17. Закройте список и щелкните **Отмена (Cancel),** чтобы закрыть окно **Дополнительные параметры безопасности.**
18. На вкладке **Безопасность** выберите вариант **Обычные (рекомендуемые параметры) [Typical (Recommended Settings)]. В** списке способе проверки выбран вариант **Небезопасный пароль.**
19. Щелкните **OK,** чтобы закрыть окно **MyCompany Свойства.**
20. Щелкните **Отмена,** чтобы закрыть окно **Подключение к MyCompany.**
21. Выйдите из системы **Computer2.**

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Сервер удаленного доступа настроен на предоставление адресов клиентам удаленного доступа DHCP-сервером. Однако у некоторых клиентов удаленного доступа появляются APIPA-адреса. Назовите две возможные причины такого поведения.
2. Какой протокол аутентификации необходим для поддержки смарт-карт?
3. Какие протоколы аутентификации обеспечивают шифрование данных?

Резюме

- Служба *Маршрутизация и удаленный доступ* (Routing and Remote Access) назначает клиентам удаленного доступа IP-адреса, полученные либо от DHCP-сервера, либо из статического набора IP-адресов. Обычно клиенты получают адреса в той же логической подсети, что и компьютеры, обслуживаемые сервером удаленного доступа.
- Аутентификации удаленного доступа предшествует аутентификация входа в домен. , Прежде чем войти в домен по телефонной линии, подключение пользователя должно пройти аутентификацию и авторизацию.
- Протоколам аутентификации присваивается приоритет на основе уровня их безопасности. Подключение осуществляется по наиболее безопасному протоколу, поддерживаемому как клиентом, так и сервером, и разрешенному применяемой к подключению политикой удаленного доступа.

Занятие 2. Авторизация подключений удаленного доступа

После аутентификации реквизитов подключения удаленного доступа выполняется авторизация подключения, состоящая из двух процедур: сначала проверяются свойства входящих звонков учетной записи пользователя, представленные подключением удаленного доступа, а затем применяется первая подходящая политика удаленного доступа службы *Маршрутизация и удаленный доступ*.

Изучив материал этого занятия, вы сможете:

V настраивать политики службы *Маршрутизация и удаленный доступ* для разрешения или запрещения доступа;

V управлять клиентами службы *Маршрутизация и удаленный доступ;*

V диагностировать и устранять неполадки, связанные с созданием подключения удаленного доступа;

V диагностировать и устранять неполадки, связанные с предоставлением доступа к ресурсам через сервер удаленного доступа.

Продолжительность занятия — около 90 минут.

Настройка входящих звонков для учетной записи пользователя

Параметры входящих звонков, применяемые к телефонным и VPN-подключениям, задаются на вкладке Входящие звонки **(Dial-In)** окна свойств учетной записи пользователя (рис. 10-13). Учетная запись пользователя, которая необходима для подключения, создается в домене заранее, то есть параметры входящих звонков задаются в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Учетная запись пользователя, подключающегося к изолированному серверу, должна указываться в локальной базе (SAM) сервера. Параметры входящих звонков в этом случае задаются в подчиненной консоли *Локальные пользователи и группы* (Local Users and Groups) консоли *Управление компьютером* (Computer Management).

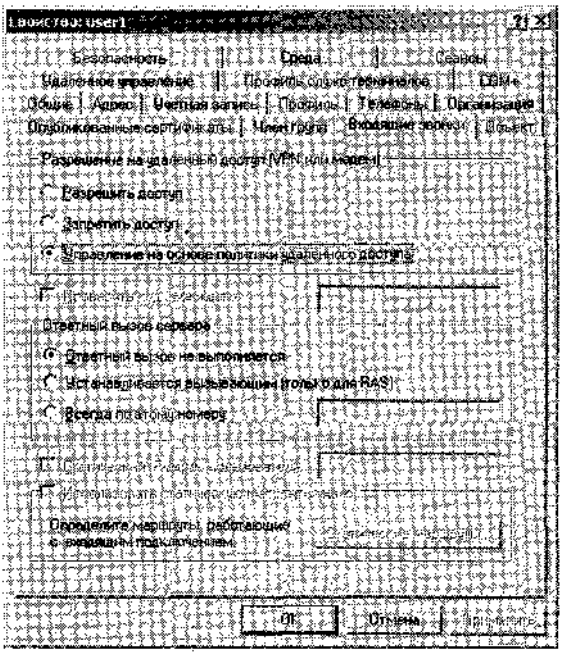


Рис. 10-13. Настройка параметров входящих звонков

Разрешение на удаленный доступ (VPN или модем)

Учетной записи пользователя можно предоставить одно из трех разрешений на удаленный доступ.

- Управление на основе политики удаленного доступа (Control Access **Through** Remote Access **Policy)** — этот вариант выбран по умолчанию во всех серверных средах за исключением доменов Active Directory смешанного режима в Windows 2000. Этот тип разрешения не ограничивает и не разрешает доступ удаленного пользователя напрямую, а определяется первой подходящей политикой удаленного доступа, применяемой к данному подключению. (Однако по умолчанию политики удаленного доступа блокируют все подключения удаленного доступа.)

- **Запретить доступ (Deny Access)** — в этом случае удаленный доступ по телефонной линии блокируется для данной учетной записи пользователя независимо от других параметров или политик, применяемых к данной учетной записи.
- **Разрешить доступ (Allow Access)** — при выборе этого варианта удаленный доступ разрешается, невзирая на ограничения, установленные в политиках удаленного доступа. Однако этот выбор не всегда гарантирует доступ, который может ограничиваться профилем политики удаленного доступа. Так, доступ можно ограничить, просто запретив в профиле политики подключение по телефонной линии в вечерние часы, даже если в свойствах телефонного вызова установлен параметр **Разрешить доступ.** Тем не менее, данный параметр обладает приоритетом перед параметром **Отказать в праве удаленного доступа (Deny Remote Access Permission)** политики удаленного доступа.

Внимание! По умолчанию в Windows Server 2003 домены Active Directory работают в смешанном режиме Windows 2000, допускающем только варианты **Запретить доступ** и **Разрешить доступ.** По умолчанию выбран последний вариант, эквивалентный варианту управления на основе политики удаленного доступа в других серверных средах. Разрешения удаленного доступа для конкретных пользователей имеют приоритет перед параметрами в политиках удаленного доступа.

Проверка идентификатора абонента

Если установлен флажок **Проверять код звонящего (Verity Caller ID),** подключение состоится только при совпадении телефонного номера абонента и идентификатора, заданного в данной конфигурации сервера.

Функция проверки номера абонента должна поддерживаться абонентом, телефонной системой, связывающей абонента с удаленным сервером, и самим сервером. На компьютере со службой *Маршрутизация и удаленный доступ* эта функция выполняется *коммутатором* (call answering equipment), предоставляющим сведения об абоненте и драйвер Windows, передающий эту информацию службе *Маршрутизация и удаленный доступ*.

Если проверка идентификатора абонента по телефонному номеру активизирована, а передача сведений о телефонном номере от абонента к службе *Маршрутизация и удаленный доступ* не поддерживается, попытки подключения будут отклоняться.

Параметры ответного вызова

По умолчанию сервер не выполняет обратных вызовов, так как выбран вариант **Ответный вызов не выполняется (No Callback).** Если же выбрать вариант **Устанавливается вызывающим (Set By Caller),** сервер будет перезванивать по номеру, указанному абонентом. Кроме того, номер обратного вызова можно зафиксировать, выбрав вариант **Всегда по этому номеру (Always Call Back To)** и указав номер.

Подготовка к экзамену Для поддержки ответного вызова необходимо, чтобы в свойствах сервера со службой *Маршрутизация и удаленный доступ* были включены расширения LCP (Link Control Protocol), впрочем они включаются по умолчанию.

Назначение статического IP-адреса

Чтобы при создании подключения удаленному пользователю присваивался определенный IP-адрес, его нужно указать в поле **Статический IP-адрес пользователя (Assign a static ip address).**

На заметку Именно параметр **Статический IP-адрес пользователя** задают интернет-провайдеры, предоставляя зарезервированные IP-адреса и взимая за это дополнительную плату. Теперь-то вы знаете, как легко им достаются эти деньги!

Применение статических маршрутизаторов

Установка флажка **Использовать статическую маршрутизацию (Apply Static Routes)** позволяет описать последовательность статических IP-маршрутов, добавляемых в таблицу маршрутов сервера *Маршрутизация и удаленный доступ* при создании подключения.

Основные сведения о политиках удаленного доступа

Политика удаленного доступа (remote access policy) — это набор разрешений и ограничений, применяемые к подключению удаленного доступа после его аутентификации сервером. На сервере аутентификации одновременно можно сконфигурировать несколько политик удаленного доступа, однако к подключению применяется только одна. Применяемые политики определяют, сопоставляя их конкретным подключениям. Применяется только первая отвечающая заданным условиям политика; если нет ни одной подходящей политики, подключение блокируется.

Чтобы узнать текущую конфигурацию политик удаленного доступа, выберите в дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) узел **Политики удаленного доступа (Remote Access Policies)** (рис. 10-14).

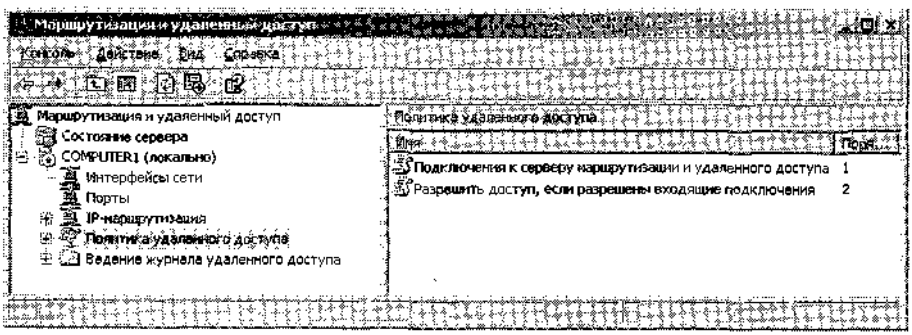


Рис. 10-14. Просмотр политик удаленного доступа

Политики удаленного доступа определяются для конкретного локального компьютера, а не для службы *Маршрутизация и удаленный доступ.* После создания политики обрабатываются либо службой *Маршрутизация и удаленный доступ,* либо RADIUS-сервером локального компьютера. Именно поэтому политики удаленного доступа нельзя удалить простым отключением службы *Маршрутизация и удаленный доступ.* Информация политик хранится на локальном" жестком диске и удаляется средствами консоли *Маршрутизация и удаленный доступ* или *Служба проверки подлинности в Интернете* (Internet Authentication Sendee) (средства администрирования RADIUS-серверов).

По умолчанию в Windows Server 2003 определены две политики удаленного доступа. Первая — *Подключения к серверу маршрутизации и удаленного доступа* (Connections to Microsoft Routing and Remote Access Server) — проверяет все подключения удаленного доступа к службе *Маршрутизация и удаленный доступ*. Когда же политику обрабатывает RADIUS-сервер, сетевой доступ не всегда обеспечивается ПО, разработанным Microsoft, поэтому в такой ситуации она может «не работать».

Вторая политика — *Подключения к другим серверам доступа* (Connections To Other Access Servers) — подходит всякому входящему подключению и любому типу сервера удаленного доступа, однако поскольку первая политика отбирает все подключения к службе *Маршрутизация и удаленный доступ,* до второй политики «добираются» только подключения, предназначенные для других серверов удаленного доступа. Если первая политика не удалена и сохранен исходный порядок следования политик, вторая оказывается доступной только RADIUS-серверами.

Параметры политики

Основой любой политики удаленного доступа являются условия, или параметры ее применения. Например, если в качестве условия политики определено, что атрибуту Windows-Groups должно соответствовать значение *DOMAIN1\Telecommuters,* такая политика применяется к подключению пользователя, члена глобальной Windows-группы безопасности Telecommuters (рис. 10-15).

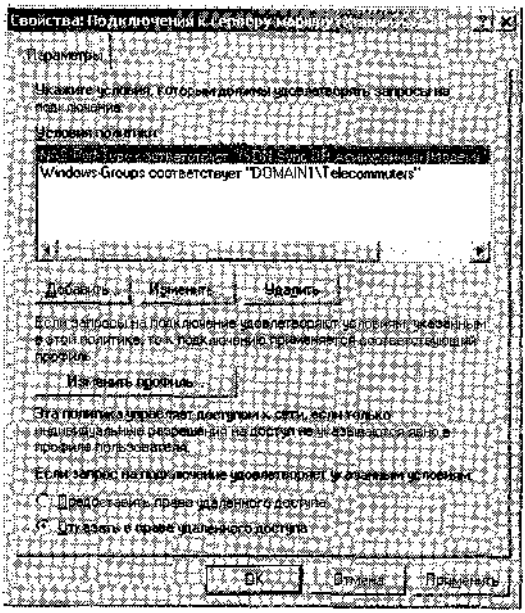


Рис. 10-15. Условия удаленного подключения для членов группы Telecommuters

Чтобы добавить новую категорию для условия политики удаленного доступа, щелкните в окне свойств политики кнопку **Добавить (Add).** Откроется окно **Выбор атрибута (Select Attribute),** в котором надо указать нужное условие. Так, атрибут **NAS-IP-Address** позволяет RADIUS-серверу отбирать клиентов удаленного доступа, подключающихся через конкретный удаленный сервер (заданный по IP-адресу).

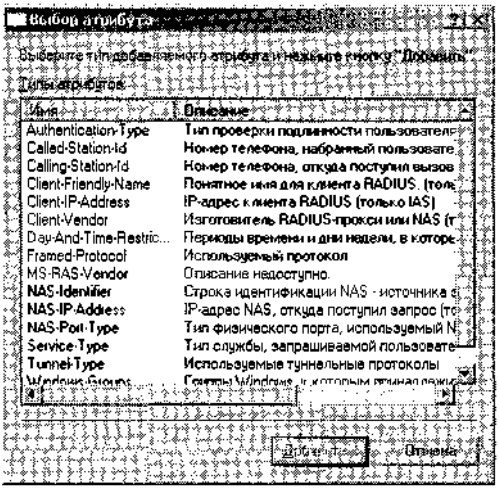


Рис. 10-16. Атрибуты условия политики

Щелкните кнопку **Добавить (Add)** в диалоговом окне **Выбор атрибута (Select Attribute),** чтобы в специальном диалоговом окне конкретизировать условие атрибута. Если, к примеру, выбрать атрибут **Authentication-Type,** откроется одноименное окно (рис. 10-17), в котором в качестве условия политики можно выбрать конкретные методы аутентификации. В приведенном примере политика подходит всем подключениям без проверки подлинности. Аналогично задаются характеристики любого атрибута, выбранного в качестве условия политики.

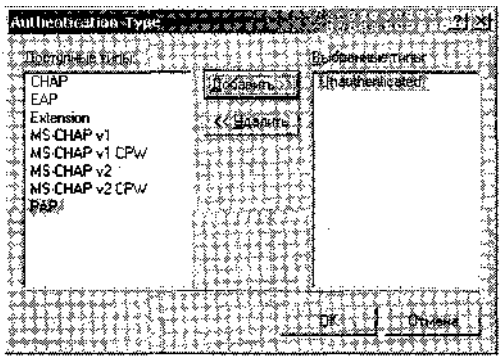


Рис. 10-17. Примеры элементов условия политики

Примечание Условием удаленной политики может являться только членство в глобальной группе безопасности. Нельзя в качестве условия политики удаленного доступа задавать членство в универсальных или локальных доменных группах безопасности.

Разрешение удаленного доступа

Политика удаленного доступа либо предоставляет, либо запрещает доступ подключению, удовлетворяющему ее условиям, согласно установленному в политике варианту: **Предоставить право удаленного доступа (Grant Remote Access Permission)** или

Отказать в праве удаленного доступа (Deny Remote Access Permission) соответственно (рис. 10-15). Помните, что этот параметр переопределяется параметрами **Разрешить доступ (Allow Access)** (кроме доменов смешанного режима Windows 2000) и **Запретить доступ (Deny Access)** свойств телефонного вызова конкретной учетной записи пользователя.

Профиль политики

Профиль политики удаленного доступа состоит из набора ограничений и свойств, применяемых к подключению. Настраивают профиль политики удаленного доступа в диалоговом окне **Изменение профиля входящего звонка (Edit Dial-In Profile)** (рис. 10-18), которое открывается по щелчку кнопки **Изменить профиль (Edit Profile)** в окне свойств политики (рис. 10-15). По умолчанию профиль политики не настроен, поэтому к подключениям не применяются никакие дополнительные ограничения.

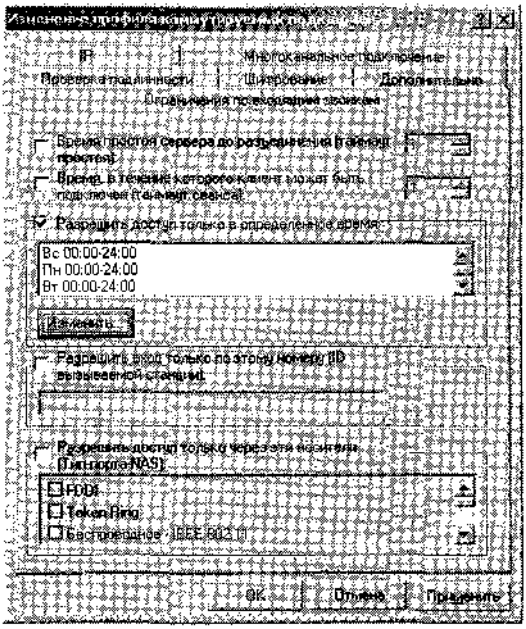


Рис. 10-18. Окно настройки профиля политики удаленного доступа по телефонной линии

В окне настройки профиля политики имеется шесть вкладок.

На вкладке **Ограничения по входящим звонкам (Dial-In Constraints)** задают следующие ограничения на входящие звонки:

- **Время простоя сервера до разъединения (Minutes server can remain idle before it is disconnected)** — время простоя в минутах, по прошествии которого связь принудительно разрывается;
- **Время, в течение которого клиент может быть подключен (Minutes client can be connected)** — максимальное время сеанса подключения в минутах;
- **Разрешить доступ только в определенное время (Allow access only on these days and at these times)** — дни и время, когда разрешается устанавливать подключение;

- **Разрешить доступ только к этому номеру (Allow access only to this number)** — номер телефона, по которому разрешается устанавливать подключение;
- **Разрешить доступ только через эти носители (Allow access only through these media)** — типы носителей (модемы, VPN и т. п.), с помощью которых клиенту разрешено подключаться.

На вкладке **IP** задается способ присвоения IP-адреса:

- **IP-адрес должен быть назначен сервером (Server must supply an IP address);**
- **Клиент может запросить IP-адрес (Client May Request An IP Address);**
- **IP-адрес определяют параметры сервера (Server Settings Determine IP Address Assignment)** (по умолчанию);
- **Статический IP-адрес пользователя (Assign A Static IP Address)** — присвоенный IP-адрес, как правило, применяется для добавления особых атрибутов поставщика IP-адресов.

На вкладке **IP** можно также описать фильтры для IP-пакетов, применяемые к трафику подключений удаленного доступа (подробнее о фильтрах пакетов — в занятии 5 главы 9).

Вкладка **Многоканальное подключение (Multilink)** позволяет включить многоканальные подключения и задать максимальное число портов (модемов), используемых при многоканальной связи. Кроме того, здесь настраивают политику протокола распределения пропускной способности BAP (Bandwidth Allocation Protocol). Эта политика определяет порядок работы протокола BAP и задает условия, при которых отключаются дополнительные линии. Параметры многоканальных подключений и протокола BAP нужны только службе *Маршрутизация и удаленный доступ*. По умолчанию многоканальные подключения и протокол BAP отключены.

Чтобы действовали определенные в профиле параметры многоканальных подключений, в службе *Маршрутизация и удаленный доступ* надо включить многоканальные подключения и протокол BAP.

На вкладке **Проверка подлинности (Authentication)** можно определить типы аутентификации, которые разрешено использовать в подключениях, а также выбрать и настроить определенный тип EAP. По умолчанию включены MS-CHAP и MS-CHAP v2. В Windows Server 2003 можно определить, разрешается ли пользователям менять устаревший пароль посредством протоколов MS-CHAP и MS-CHAP v2.

Чтобы заданные в профиле параметры аутентификации применялись, в службе *Маршрутизация и удаленный доступ* надо включить соответствующие методы проверки подлинности.

Вкладка **Шифрование (Encryption)** (рис. 10-19) служит для определения порядка поддержки шифрования. В Windows Server 2003 поддерживается два основных метода шифрования данных удаленного подключения: RSA (Rivest-Shamir Adleman) RC4 и DES (Data Encryption Standard). RSA RC4 — это семейство алгоритмов, применяемых в MPPE, способе шифрования, используемом совместно с протоколами MS-CHAP и EAP-TLS в телефонных и VPN-подключениях по протоколу PPTP (Point-to-Point Tunneling Protocol). DES — общая схема шифрования, наиболее часто используемая в стандарте безопасности IPSec (Internet Protocol Security), использующем для поддержки VPN протокол аутентификации L2TP (Layer 2 Tunneling Protocol). (Подробнее о VPN, PPTP, L2TP и IPSec — в занятии 3.)

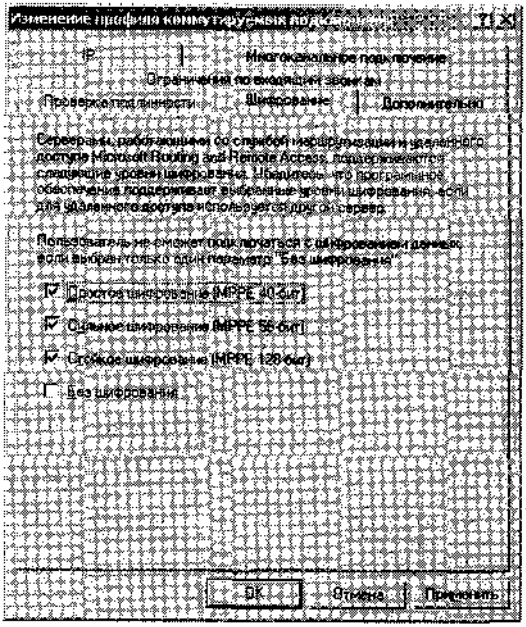


Рис. 10-19. Вкладка *Шифрование* окна профиля политики удаленного доступа

В табл. 10-3 представлены уровни шифрования, поддерживаемые MPPE и IPSec.

Табл. 10-3. Типы шифрования

Тип шифрования	Поддерживаемый уровень шифрования
Простое шифрование и сильное шифрование MPPE (MPPE Standard)	40-битный и 56-битный ключ
Стойкое шифрование MPPE (MPPE Strong)	128-битный ключ
IPSec DES	56-битный ключ
IPSec Triple DES	168-битный ключ

Вкладка **Шифрование** позволяет установить уровни шифрования без указания конкретного типа шифрования, однако его надежность определяется применяемой схемой:

- **Основное шифрование (MPPE 40-бит) [Basic Encryption (MPPE 40-Bit)]** — для телефонных и VPN-подключений по протоколу PPTP используется шифрование по MPPE с 40-битным ключом, а по протоколу L2TP/IPSec — 56-битное шифрование DES;
- **Сильное шифрование (MPPE 56-бит) [Strong Encryption (MPPE 56-Bit)]** — для телефонных и VPN-подключений по протоколу PPTP используется 56-битное шифрование MPPE, а по протоколу L2TP поверх IPSec — 56-битное шифрование DES;
- **Стойкое шифрование (MPPE 128-бит) [Strongest Encryption (MPPE 128-bit)]** — для телефонных и VPN-подключений по протоколу PPTP используется 128-битное шифрование MPPE, а для VPN-подключений по протоколу L2TP/IPSec — шифрование по алгоритму Triple DES (3DES) с 168-битным ключом;
- **Без шифрования (No Encryption)** — отключение шифрования подключения. Если шифрование обязательно, этот флажок следует сбросить.

Подготовка к экзамену Хорошо разберитесь во всех нюансах настройки шифрования. Например, надо знать, что для телефонных и PPTP-подключений вариант **Основное шифрование (Basic Encryption)** означает 40-битное шифрование по методу MPPE, а для Ь2ТР/1Р8ес-подключений — 56-разрядное шифрование по методу DES.

Вкладка **Дополнительно (Advanced)** служит для определения набора атрибутов RADIUS, возвращаемых для проверки LAS-сервером NAS-серверу или RADIUS-клиенту. Эти параметры используются только RADIUS-серверами и игнорируются службой *Маршрутизация и удаленный доступ*.

Обзор возможных вариантов авторизации при удаленном доступе

Здесь рассказывается о процессе авторизации при удаленном доступе на конкретных примерах. В представленных сценариях пользователь Userl, член группы Telecommuters, пытается установить подключение по телефонной линии при различных параметрах авторизации, определенных на сервере удаленного доступа. На рис. 10-20 показан порядок обработки политик удаленного доступа сервером.

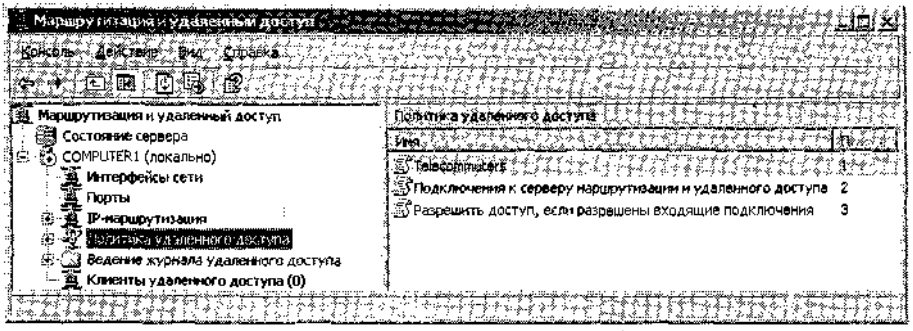


Рис. 10-20. Список политик удаленного доступа на сервере

Примечание Во всех случаях предполагается, что установлен режим домена, отличный от смешанного режима Windows 2000.

В каждой попытке подключения применяется до трех наборов разрешений и параметров в следующем порядке.

1. Свойства телефонного вызова учетной записи пользователя, определенные в подключении.
2. Разрешения доступа, описанные в первой подходящей политике удаленного доступа.
3. Параметры профиля, соответствующего первой подходящей политике удаленного доступа.

В первом примере (рис. 10-21) в свойствах учетной записи Userl оставлено определенное по умолчанию разрешение на удаленный доступ — **Управление на основе политики удаленного доступа (Control Access Through Remote Access Policy).** Поэтому к подключению применяется разрешение удаленного доступа первой политики удаленного доступа — Telecommuters, предоставляющей доступ группе безопасности Telecommuters.

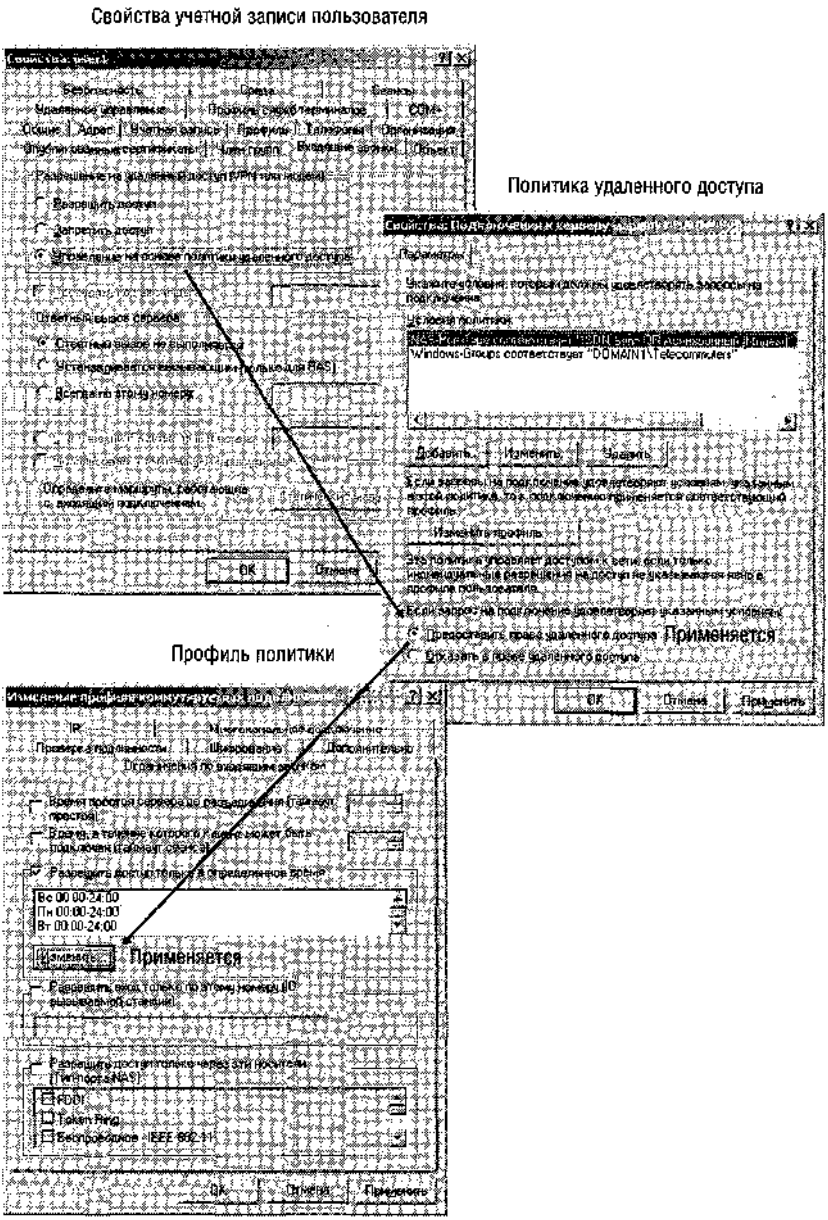


Рис. 10-21. Первый сценарий авторизации при удаленном доступе

После применения определенного политикой разрешения проверяется профиль политики. В данном примере профиль политики Telecommuters разрешает доступ в любой день недели за исключением воскресенья. В итоге Userl сможет получить доступ в любое время кроме воскресенья.

Во втором примере (рис. 10-22) в свойствах учетной записи Userl также оставлено разрешение удаленного доступа по умолчанию. Поэтому разрешения на удаленный доступ опять определяется политикой удаленного доступа. Однако в этом примере поли-

тика Telecommuters запрещает доступ для группы Telecommuters. В итоге попытка подключения Userl блокируется, и до обработки профиля политики дело не доходит.

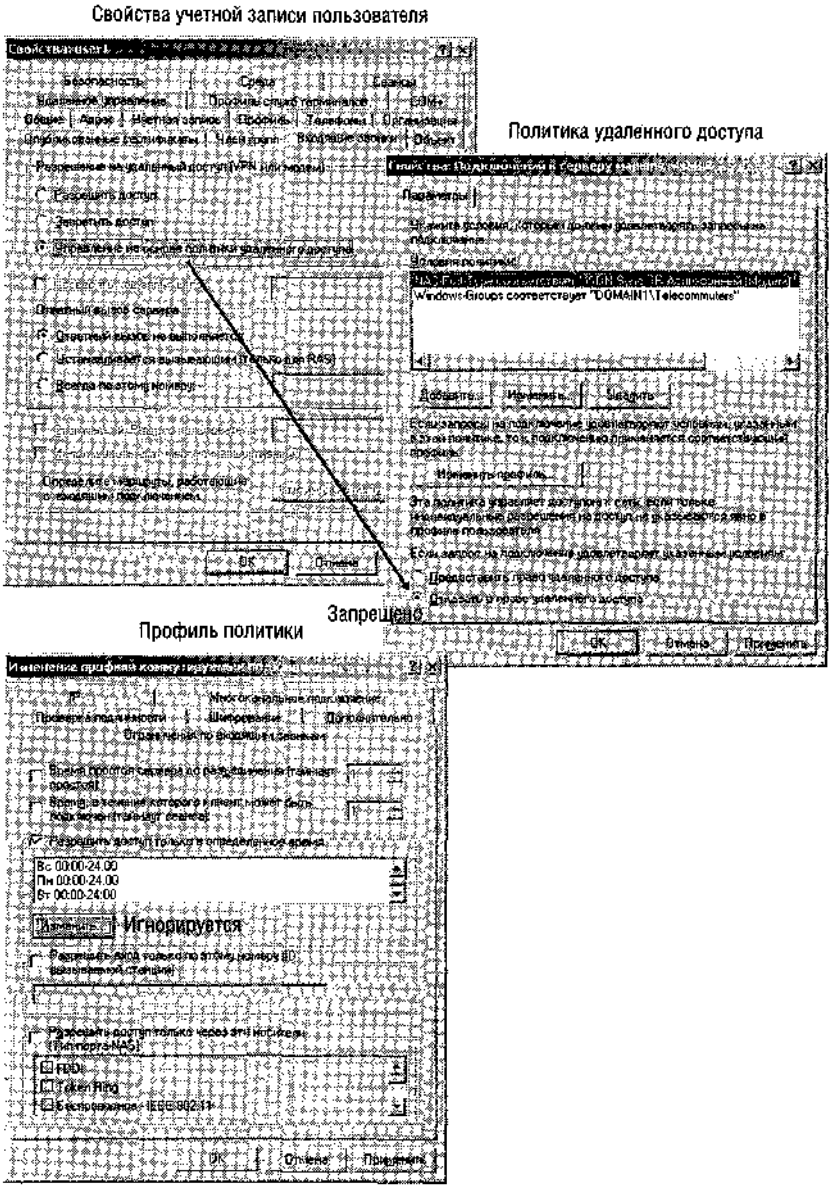


Рис. 10-22. Второй сценарий авторизации удаленного доступа

В третьем примере (рис. 10-23) в свойствах учетной записи Userl задан другой вариант разрешения — **Разрешить доступ (Allow Access). В** этом случае разрешение удаленного доступа, определяемое политикой Telecommuters, игнорируется. Однако профиль политики дает пользователю Userl разрешение на доступ в любое время кроме воскресенья.

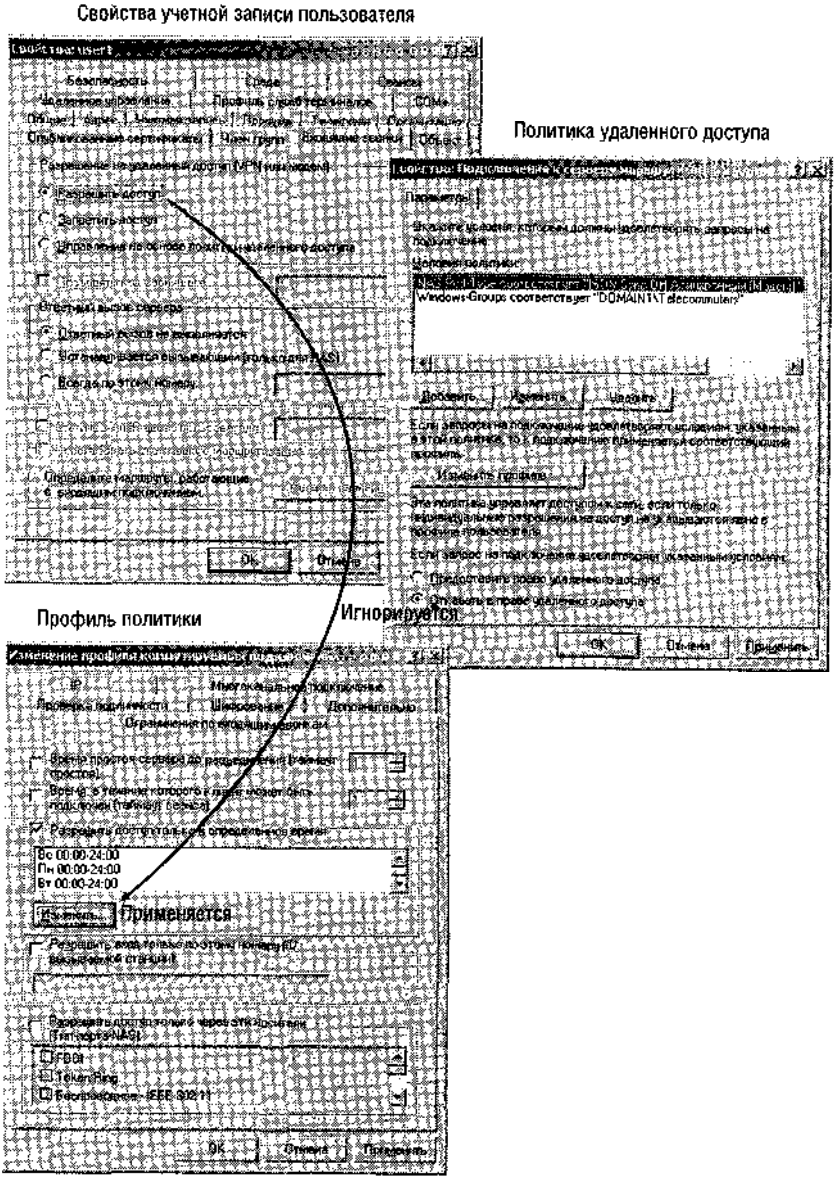


Рис. 10-23. Третий сценарий авторизации удаленного доступа

В четвертом примере (рис. 10-24) в свойствах учетной записи Userl задан третий вариант разрешения — **Запретить доступ (Deny Access).** Из-за этого удаленное подключение к серверу блокируется без рассмотрения политики удаленного доступа и соответствующего профиля.

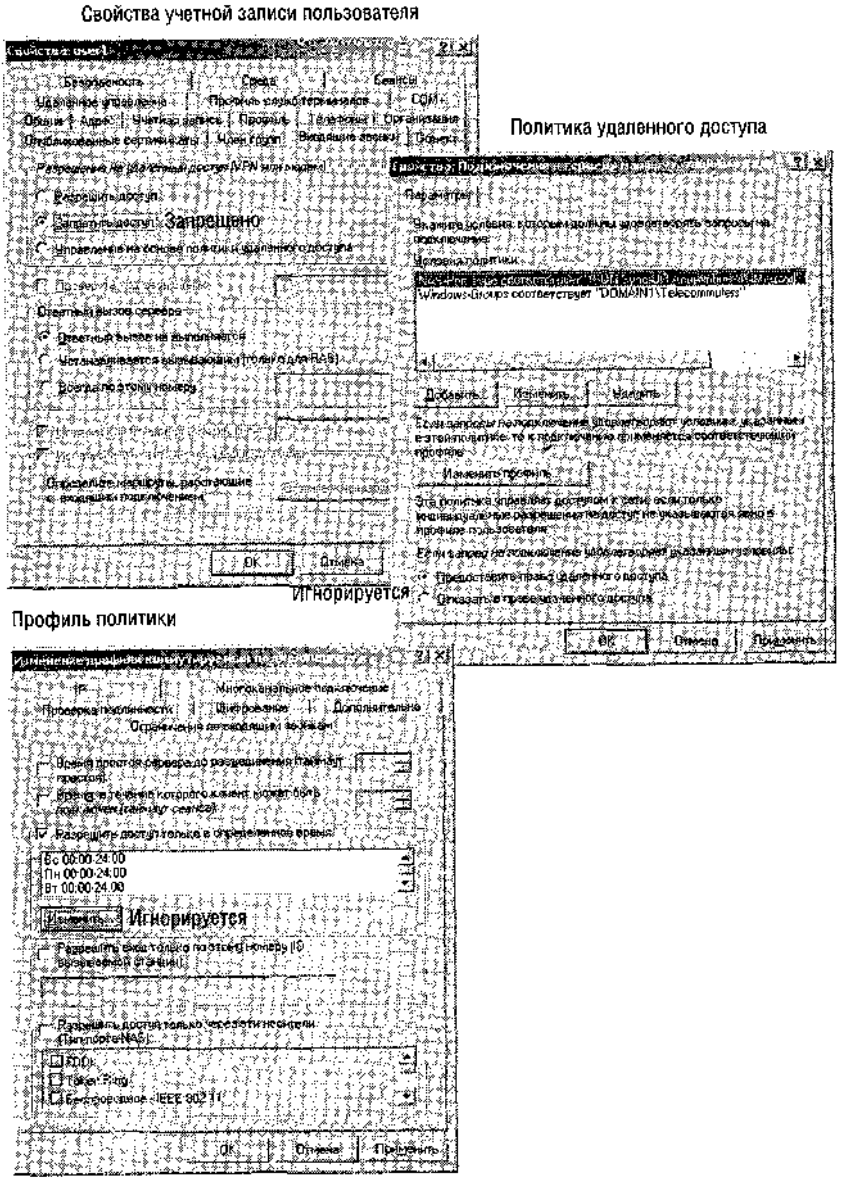


Рис. 10-24. Четвертый сценарий авторизации удаленного доступа

В пятом примере (рис. 10-25) на сервере удалены политики удаленного доступа, В результате входящее подключение не удается сопоставить никакой политике, и запрос подключения отклоняется независимо от параметра **Разрешить доступ,** заданного для учетной записи Userl.

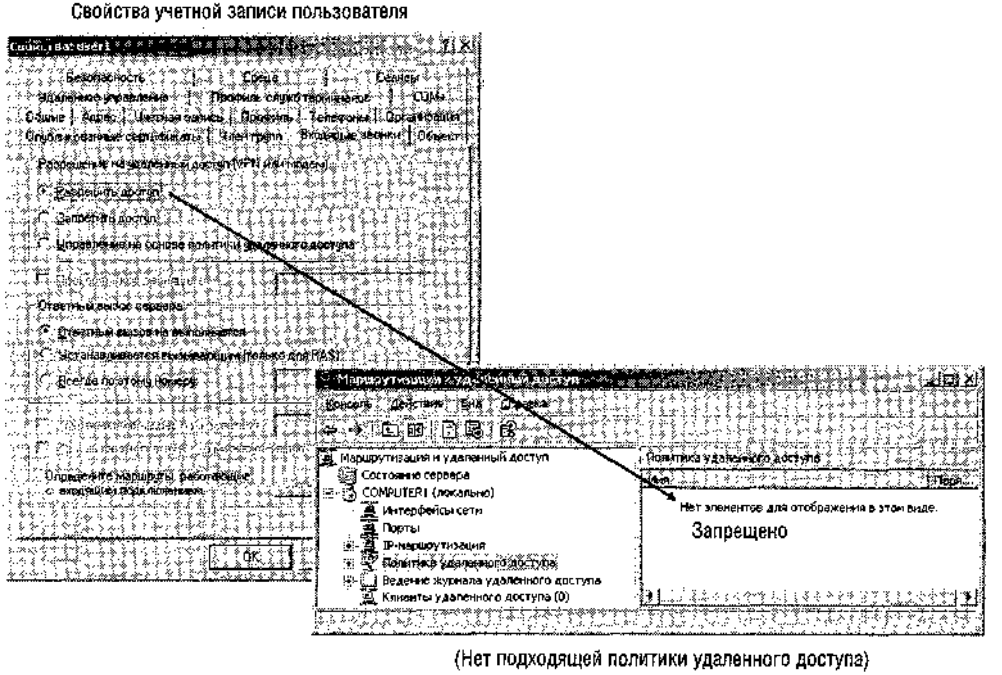


Рис. 10-25. Пятый сценарий авторизации удаленного доступа

Устранение неполадок при подключениях удаленного доступа по телефонным линиям

Устраняйте неполадки подключений по телефонным линиям в следующей последовательности.

- Убедитесь, что на вкладке **Общие (General)** свойств сервера в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) выбран вариант **Сервер удаленного доступа (Remote Access Server).**
- Если адреса берутся из статического пула, убедитесь, что его размер достаточен для одновременного подключения необходимого количества клиентов.
- Если сервер удаленного доступа настроен на присвоение адресов DHCP-сервером, убедитесь, что заданный на DHCP-сервере диапазон адресов достаточен для выделения блоков по 10 адресов, необходимых удаленному серверу.
- Убедитесь, что в узле **Порты (Ports)** достаточно устройств для одновременного подключения нужного количества клиентов.

в Убедитесь, что имеется хотя бы один протокол аутентификации, одновременно поддерживаемый клиентом, сервером и политикой удаленного доступа.

- Убедитесь, что имеется хотя бы один уровень шифрования, одновременно поддерживаемый клиентом, сервером и политикой удаленного доступа.
- Проверьте наличие надлежащих разрешений у подключения удаленного доступа по телефонной линии, установленных для учетной записи пользователя и в политиках удаленного доступа.

- Проверьте, входит ли компьютер, на котором установлен сервер удаленного доступа (или RADIUS-сервер), в группу безопасности *Серверы RAS и IAS* (RAS and IAS Servers) локального домена.
- Проверьте, не противоречат ли параметры профиля политики удаленного доступа свойствам сервера удаленного доступа.
- Если в качестве протокола аутентификации используется MS-CHAPv1, проверьте, не превышает ли длина пароля пользователя 14 символов.

Настройка доступа к ресурсам сети, обслуживаемой NAS-сервером

Чтобы превратить компьютер с Windows Server 2003 в сервер удаленного доступа, надо выполнить *Мастер настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard) и выбрать конфигурацию **Удаленный доступ (VPN или модем) [Remote Access (Dial-Up Or VPN)].** Однако даже в случае правильной настройки сервер удаленного доступа не позволит через телефонные подключения получить доступ к ресурсам внутренней сети.

Чтобы предоставить клиентам доступ к внутренним сетевым ресурсам, нужно сконфигурировать удаленный сервер как маршрутизатор. Для этого откройте в консоли *Маршрутизация и удаленный доступ* окно свойств сервера удаленного доступа и на вкладке **Общие (General)** установите флажок **Маршрутизатор (Router)** (рис. 10-26).

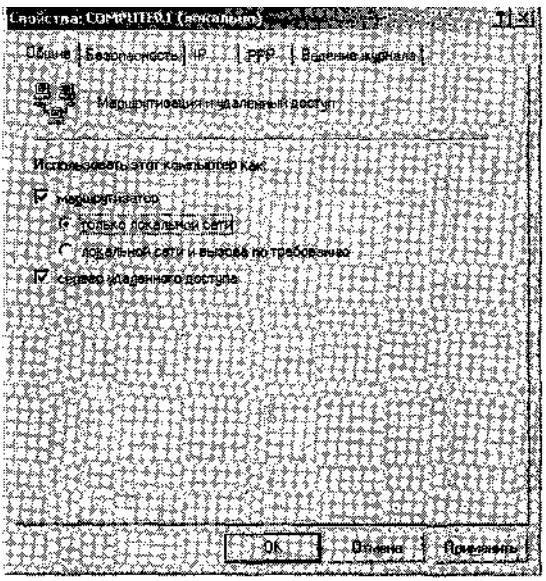


Рис. 10-26. Настройка доступа к ресурсам внутренней сети, обслуживаемой сервером удаленного доступа

Но и этого бывает недостаточно, так как доступ через сервер определяется конфигурацией других параметров сервера удаленного доступа. Во-первых, надо убедиться, что удаленный сервер назначает клиентам (через DHCP-сервер или из набора статических адресов) IP-адреса в логической подсети, в которой располагаются компьютеры, обслуживаемым сервером удаленного доступа. Если же удаленные клиенты получают адреса в другой подсети, настройте на сервере удаленного доступа протокол маршрутизации

или же задайте на сетевых маршрутизаторах конфигурацию статических маршрутов для доступа к подсети удаленного доступа.

Примечание После развертывания протокола маршрутизации на сервере удаленного доступа потребуется настроить соседние маршрутизаторы с учетом последних изменений на сервере.

Во-вторых, откройте в консоли *Маршрутизация и удаленный доступ* окно свойств удаленного сервера и убедитесь, что на вкладке IP установлен флажок по умолчанию **Разрешить IP-маршрутизацию (Enable IP routing).**

В-третьих, для обеспечения работы сетевых функций, которым требуется широковещательное разрешение NetBIOS-имен, например при поиске компьютеров в окне **Сетевое окружение (My Network Places),** а также для случаев, когда удаленные клиенты не располагаются в отдельной подсети, необходимо установить флажок **Разрешить широковещательное разрешение имен (Enable Broadcast Name Resolution)** на вкладке IP (он установлен по умолчанию). Если этот флажок сброшен, нужно сконфигурировать в сети WINS-сервер, который будет разрешать NetBIOS-имена, а в параметрах клиентов — указать адрес этого WINS-сервера.

Устранение неполадок при доступе к ресурсам внутренней сети через NAS-сервер

Неполадки получения доступа к ресурсам внутренней сети, обслуживаемой сервером удаленного доступа, устраняются в следующей последовательности.

- Убедитесь, что на вкладке **Общие (General)** диалогового окна свойств сервера установлен флажок **Маршрутизатор (Router).**
- Убедитесь, что на вкладке **Общие (General)** диалогового окна свойств сервера выбран вариант **локальной сети и вызова по требованию (LAN and demand-dial routing).**
- Убедитесь, что на вкладке **IP** диалогового окна свойств сервера установлен флажок **Разрешить IP-маршрутизацию (Enable IP Routing).**
- Если диапазон адресов, выделяемых удаленным клиентам, относится к подсети, отличающейся от подсети маршрутизатора, позаботьтесь, чтобы в параметрах маршрутизаторов были описаны маршруты к подсети удаленного доступа.
- Убедитесь, что на вкладке **IP** диалогового окна свойств сервера установлен флажок **Включить широковещание при разрешении имен (Enable Broadcast Name Resolution).** Он нужен только в том случае, если удаленная сеть применяет разрешение NetBIOS-имен, а удаленные клиенты размещаются в то же логической подсети, что и необходимые им службы NetBIOS.

Управление удаленными клиентами

Консоль *Маршрутизация и удаленный доступ* позволяет просматривать текущие подключения клиентов удаленного доступа. При выборе в дереве консоли узла **Клиенты удаленного доступа (Remote Access Clients)** в правой панели можно отслеживать состояние этих подключений, отключать клиентов или отправлять сообщения отдельным или всем клиентам.

Состояние подключений просматривают так.

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) выберите узел **Клиенты удаленного доступа (Remote Access Clients).**

2. В правой панели щелкните имя пользователя правой кнопкой и выберите **Состояние (Status).**

Отключают удаленного клиента так.

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) выберите узел **Клиенты удаленного доступа (Remote Access Clients).**
2. **В** правой панели щелкните имя нужного пользователя правой кнопкой и выберите **Отключить (Disconnect).**

Сообщение отдельному удаленному клиенту отправляют так.

1. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) выберите узел **Клиенты удаленного доступа (Remote Access Clients).**
2. **В** правой панели щелкните имя нужного пользователя правой кнопкой и выберите **Отправить сообщение (Send message).**
3. **В** окне **Отправить сообщение (Send message)** введите текст сообщения и щелкните **OK.**

Сообщение всем удаленным клиентам отправляют так.

1. В дереве консоли **Маршрутизация и удаленный доступ** (Routing and Remote Access) щелкните узел **Клиенты удаленного доступа (Remote Access Clients)** правой кнопкой и выберите **Отправить всем (Send To All.**
2. В окне **Отправить сообщение (Send message)** введите текст сообщения и щелкните OK.

Управление клиентами с помощью политик удаленного доступа

Помимо текущего управления подключившимися клиентами можно осуществлять общее управление клиентами удаленного доступа, описав определенные правила в политиках удаленного доступа. Таким образом можно ограничить время простоя клиентов и время подключения или разрешить доступ только к ограниченному кругу сетевых ресурсов. Такие ограничения задаются в профиле политики и применяются к определенному типу клиентов.

Лабораторная работа. Развертывание системы удаленного доступа

Вы создадите в домене учетную запись пользователя и соответствующую политику удаленного доступа. Затем вы проверите подключение по телефонной линии созданной учетной записи.

Упражнение 1. Создание группы Telecommuters и учетной записи

Вы создадите учетную запись пользователя Userl и введете ее в новую глобальную группу безопасности Telecommuters.

1. На Computer! войдите в систему как *Администратор* (Administrator) в домене *Domainl.*
2. В меню **Пуск (Start)\Администрирование (Administrative Tools)** щелкните **Active Directory — пользователи и компьютеры (Active Directory Users and Computers).** Откроется окно консоли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers).
3. В дереве консоли **Active Directory — пользователи и компьютеры** щелкните папку **Users** правой кнопкой и выберите **Создать (New)\Пользователь (User).**

4. В открывшемся окне Новый объект - Пользователь (New Object - User) в поле Полное имя (Full Name) введите user1.
5. В поле Имя входа пользователя (User Logon Name) введите use r1.
6. Щелкните Далее (Next). В окне Новый объект - Пользователь появится новый набор параметров.
7. В полях Пароль (Password) и Подтверждение (Confirm Password) введите пароль для учетной записи User1.
8. Снимите флажок Требовать смену пароля при следующем входе в систему (User must change password at next logon).
9. Щелкните Далее (Next), а затем — Готово (Finish).
10. На Computerl из командной строки исполните:

    net group telecommuters /add /domain

    Эта команда создаст в домене глобальную группу безопасности Telecommuters.

    Выполните команду net group telecommuters userl /add /domain.

    Она добавит в группу Telecommuters учетную запись Userl.
11. Когда в дереве консоли *Active Directory — пользователи и компьютеры* выбрана папка Users, щелкните правой кнопкой свободное место в правой панели и в контекстном меню выберите Обновить (Refresh). В правой панели появится значок новой группы безопасности Telecommuters.
12. В правой панели консоли *Active Directory — пользователи и компьютеры* двойным щелчком значка Userl откройте окно Userl - свойства (Userl Properties).
13. Перейдите на-вкладку Входящие звонки (Dial-In). В группе Разрешение на удаленный доступ (Remote Access Permissions) доступны только два параметра: Разрешить доступ (Allow Access) и Запретить доступ (Deny Access). Заметьте, что по умолчанию доступ запрещен. Щелкните OK.
14. В дереве консоли Active Directory — пользователи и компьютеры щелкните значок domain 1.local правой кнопкой и выберите Изменение режима работы домена (Raise Domain Functional Level). Откроется одноименное окно.
15. В списке Выберите режим работы домена (Select an available domain functional level) выберите Windows Server 2003.
16. Щелкните Изменить (Raise). Появится предупреждение о необратимости операции. Щелкните OK. Появится сообщение об успешном завершении операции.
17. Щелкните OK и перезапустите Computerl.
18. После перезапуска Computerl вновь войдите в *Domainl* как *Администратор* (Administrator).
19. Откройте консоль *Active Directory — пользователи и компьютеры*.
20. Откройте окно свойств Userl и перейдите на вкладку Входящие звонки (Dial-In). В группе Разрешение на удаленный доступ (Remote Access Permissions) теперь доступен и третий вариант Управление на основе политики удаленного доступа (Control Access Through Remote Access Policy), который и выбран по умолчанию.
21. Закройте консоль *Active Directory — пользователи и компьютеры*.

Упражнение 2. Создание политики удаленного доступа для учетной записи Telecommuter

Вы создадите политику удаленного доступа Telecommuters и изучите параметры этой политики.

1. На Computerl войдите в систему как *Администратор* (Administrator) в домене *Domain 1.*
2. В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **Политика удаленного доступа (Remote Access Policies)** правой кнопкой и выберите **Создать политику удаленного доступа (New Remote Access Policy).**
3. **В** окне **Мастер создания политики удаленного доступа (New Remote Access Policy Wizard)** щелкните **Далее** (Next).
4. На странице **Метод настройки политики (Policy Configuration Method)** в поле **Имя политики (Policy Name)** введите Telecommuters и щелкните **Далее.**
5. На странице **Метод доступа (Access Method)** выберите вариант **Удаленный доступ (через телефонную сеть) (Dial-Up)** и щелкните **Далее.**
6. На странице **Пользователь или группа доступа (User Or Group Access)** оставьте выбранный по умолчанию вариант **разрешения группы (Group)** и щелкните кнопку **Добавить (Add).**
7. **В** окне **Выбор: «Группы» (Select Groups)** в поле **Введите имена выбираемых объектов (Enter object names to select)** введите telecommuters и щелкните OK. В поле **Имя группы (Group Name)** появится запись **DOMAIN1\telecommuters.** Щелкните **Далее.**
8. На странице **Методы проверки подлинности (Authentication Methods)** оставьте выбранный по умолчанию протокол MS-CHAPv2 и щелкните **Далее.**
9. Параметры на странице **Уровень шифрования, указанный в политике (Policy Encryption Level)** позволяют шифровать только данные подключения, но не пароль. Уровни простого, сильного и стойкого шифрования выбраны по умолчанию. Поскольку MS-CHAP v2 поддерживает шифрование по протоколу MPPE, этими параметрами гарантируется шифрование данных, пересылаемых с Computer2 через подключение MyCompany. Щелкните **Далее,** оставив параметры по умолчанию.
10. На странице **Завершение мастера создания политики удаленного доступа (Completing The New Remote Access Policy Wizard)** щелкните **Готово (Finish).**

    В правой панели консоли *Маршрутизация и удаленный доступ* видно, что при выборе узла **Политики удаленного доступа (Remote Access Policies)** первой в списке отображается политика **Telecommuters.**
11. Дважды щелкните в правой панели значок политики **Telecommuters.** В открывшемся окне **Свойства: Telecommuters (Telecommuters Properties)** проверьте параметры, отображаемые в этом окне. Заметьте, что первое условие политики соответствует всем телефонным подключениям, а второе — глобальной группе безопасности *DOMAINl\telecommuters.* Обратите также внимание, что выбран переключатель **Предоставить право удаленного доступа (Grant Remote Access Permission).**
12. Щелкните кнопку **Изменить профиль (Edit Profile). В** открывшемся окне **Изменение профиля коммутируемых подключений (Edit Dial-In Profile)** изучите параметры, определенные на шести вкладках этого окна. Оставьте их без изменений.
13. Щелчком кнопки **Отмена (Cancel)** закройте окно **Изменение профиля коммутируемых подключений.**
14. Щелчком кнопки **Отмена** закройте окно **Свойства: Telecommuters.**
15. Выйдите из системы Computerl.

Упражнение 3 (дополнительное). Тестирование настройки удаленного доступа

Вы установите телефонное подключение под учетной записью Userl к Computer1 с компьютера Computer2. У каждого компьютера должна быть отдельная телефонная линия. Перед выполнением упражнения подключите компьютеры к соответствующим телефонным линиям.

Примечание На время выполнения упражнения отключите локальный кабель, соединяющий оба компьютера, чтобы убедиться, что подключение выполняется по телефонной линии.

1. На компьютере Computer2 нажмите Ctrl+Alt+Del, чтобы открыть окно **Вход в Windows (Log On To Windows).**
2. Установите флажок **С использованием удаленного доступа (Log On Using Dial-Up Connection).**
3. В поле **Пользователь (User Name)** введите user1.
4. В поле **Пароль (Password)** наберите пароль, установленный для пользователя Userl.
5. В списке **Вход в (Log On To)** выберите **DOMAIN!** и щелкните OK. Откроется окно **Сетевые подключения (Network Connections).**
6. В списке **Выберите сетевое подключение (Choose a Network Connection)** выберите **MyCompany,** а затем щелкните **Подключить (Connect).**

   Откроется окно **Подключение к MyCompany (Connect MyCompany).** Поле **Пользователь (User Name)** уже содержит имя user1, поле **Пароль (Password)—** скрытый пароль, а поле **Домен (Domain)** — имя домена DOMAIN 1.
7. Щелкните кнопку **Вызов (Dial).**

   В окне **Установка связи с MyCompany (Connecting MyCompany)** отображается состояние подключения. По завершении набора номера прозвучат два сигнала, и на вызов ответит служба *Маршрутизация и удаленный доступ* (Routing and Remote Access) компьютера Computerl. Проверяется имя пользователя и пароль, после чего компьютер регистрируется в сети. Затем окно **Установка связи с MyCompany (Connecting MyCompany)** закрывается и выполняется вход в домен с соответствующими реквизитами.
8. По завершении операции входа в домен откройте Microsoft Internet Explorer. Не обращайте внимания на получаемые сообщения и предупреждения.
9. В адресной строке введите \\computer1. domain 1. local и нажмите **Enter. В** окне браузера появится список общедоступных ресурсов Computerl, подтверждая, что Userl успешно подключился к Computerl по телефонной линии.
10. Закройте браузер и выйдите из системы Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В сети Windows Server 2003 новый домен создается по умолчанию в смешанном режиме Microsoft Windows 2000. Чем в данном случае отличается параметр **Разрешить доступ (Allow Access)** в окне свойств телефонного подключения учетной записи пользователя от такого же параметра в других серверных средах?

2. Предположим, что успешно выполнена аутентификация удаленного подключения, в свойствах удаленного подключения данной учетной записи установлено значение **Разрешить доступ (Allow Access),** а в первой подходящей политике удаленного доступа определено разрешение **Предоставить разрешение на удаленный доступ (Grant Remote Access Permission). В** чем может быть причина того, что удаленный клиент все равно не в состоянии подключиться к удаленному серверу?
3. Каким образом настроить на удаленном сервере 128-разрядное шифрование телефонных подключений?

Резюме

- При удаленном доступе сначала выполняется аутентификация подключения удаленного доступа, а затем авторизация. Последняя состоит из двух этапов: сначала проверяются свойства телефонного подключения, установленные для данной учетной записи пользователя, а затем к подключению применяется первая подходящая политика удаленного доступа.
- В свойствах телефонного подключения учетной записи пользователя задается одно из следующих разрешений удаленного доступа: **Разрешить доступ (Allow Access), Запретить доступ (Deny Access)** или **Управление на основе политики удаленного доступа (Control Access Through Remote Access Policy).**
- Политика удаленного доступа определяется тип подключения, к которому она применяется. Политики удаленного доступа просматриваются в определенной очередности, причем удаленному подключению применяется только первая политика, условиям которой оно удовлетворяет. При конфликте между разрешающей/запрещающей политикой удаленного доступа и параметрами учетной записи пользователя преимуществом обладают последние. В политику удаленного доступа также входит профиль политики, различные атрибуты которого, такие как требование аутентификации, шифрования и фильтры пакетов, накладывают дополнительные ограничения на подключение.
- Чтобы разрешить доступ клиентам к внутренним ресурсам, обслуживаемым сервером удаленного доступа, удаленный сервер должен выступать в качестве маршрутизатора, а в свойствах сервера маршрутизации и удаленного доступа нужно включить IP-маршрутизацию.
- Подключениями удаленных клиентов управляют через узел **Клиенты удаленного доступа (Remote Access Clients)** консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access).

Занятие 3. **Развертывание VPN**

Виртуальная частная сеть позволяет пользователям безопасно подключиться через Интернет к любой удаленной частной сети. В удаленном VPN-подключении с использованием средств Windows Server 2003 отдельный пользователь подключается через Интернет к компьютеру под управлением Windows Server 2003 со службой *Маршрутизация и удаленный доступ* (Routing and Remote Access). В экстрасети'частные ЛВС объединяются через Интернет с помощью двух компьютеров под управлением Windows Server 2003 со службой *Маршрутизация и удаленный доступ*.

Изучив материал этого занятия, вы сможете:

- V настроить удаленное VPN-подключение;
- V диагностировать и устранять неполадки удаленного доступа по VPN-подключениям;
- V обеспечить безопасную VPN-связь между частными сетями по схеме маршрутизатор — маршрутизатор;
- V устранять неполадки в VPN по схеме марштрутизатор — марштрутизатор;
- V управлять устройствами и портами;
- V управлять фильтрами пакетов;
- V устранять неполадки при доступе клиентов к службам удаленного доступа.

Продолжительность занятия — около 75 минут.

Основные сведения о виртуальных частных сетях

Виртуальные частные сети (virtual private network, VPN) — это логические сети, которые проходят через Интернет. В VPN пакеты с частной информацией сначала шифруются, а затем инкапсулируются в открытые пакеты, направляемые на удаленный VPN-сервер. Зашифрованные данные на пути следования к своей цели проходят через «туннель», проложенный внутри открытой сети. Получив из VPN-туннеля инкапсулированные данные, VPN -сервер удаляет открытый заголовок и дешифрует полезную информацию (рис. 10-27).

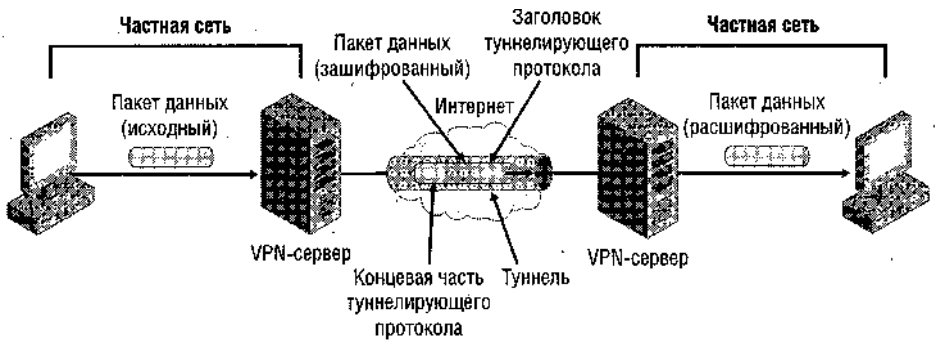


Рис. 10-27. VPN-туннелирование

Важная особенность VPN в том, что открытая физическая сеть, через которую пересылаются частные данные, становится «прозрачной» на обоих концах соединения. Два компьютера, Computerl и Computer2, физически оказываются связанными друг с другом только через Интернет (рис. 10-28). «Прозрачность» такой физической линии связи видна в результатах исполнения команды Tracert на каждом из компьютеров. Хотя оба компьютера разделяют многочисленные переходы, с точки зрения VPN-подключения между ними существует только один переход. Их частные IP-адреса находятся внутри подсети 192.168.10.0, как если бы оба находились в одном изолированном сегменте сети.

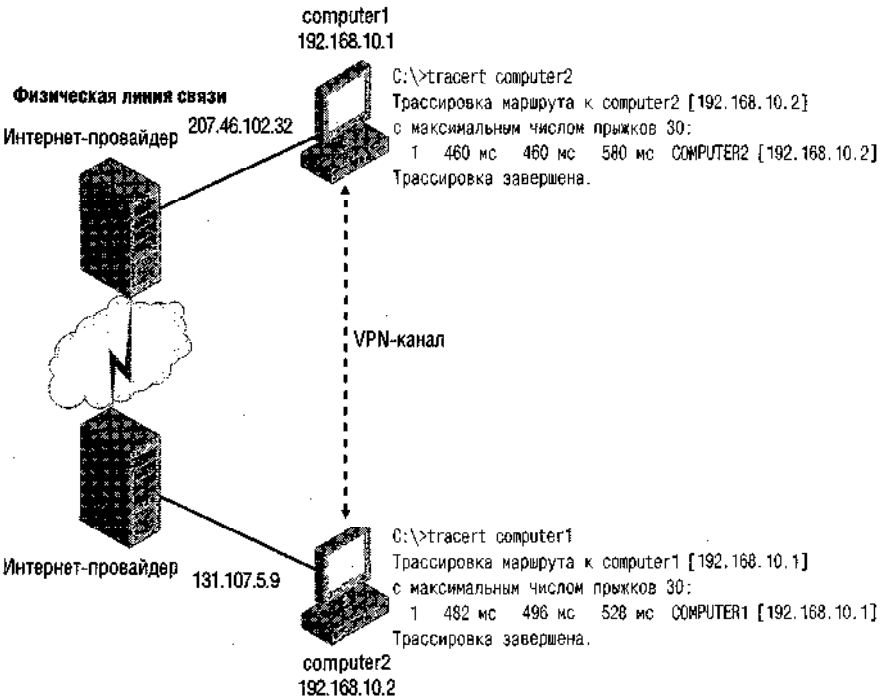


Рис. 10-28. Пример VPN-канала

Сценарии развертывания VPN

Обычно VPN применяется для предоставления пользователям удаленного доступа к некоторой сети и подключения друг к другу нескольких частных сетей. В данном разделе рассматриваются вопросы настройки уже упомянутых и еще одного варианта, когда VPN-сервер защищен брандмауэром. Поскольку для всех трех сценариев VPN требуется удаленный доступ к внешним ресурсам VPN-сервера, то в настройке VPN-сервера нужно включить поддержку локальной сети и маршрутизации с вызовом по требованию [на вкладке **Общие (General)** окна свойств консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access)]. Кроме того, во всех описанных ниже сценариях предполагается, что в свойствах входящих звонков для всех учетных записей пользователей оставлен без изменения вариант по умолчанию **Управление на основе политики удаленного доступа.**

Удаленный доступ через VPN

Согласно основному сценарию удаленного доступа, VPN позволяет удаленному пользователю подключиться через Интернет к сети своей компании. В этом случае администратор сети создает политику удаленного доступа, предоставляющую доступ подключениям при соблюдении следующих условий: атрибуту **NAS-Port-Type** присвоено значение **Virtual (VPN) [Виртуальная (VPN)],** а атрибуту **Windows-Groups** — имя группы, созданной специально для VPN. На стороне клиента удаленный пользователь создает VPN-подключение (с помощью *Мастера новых подключений),* указав свои реквизиты и IP-адрес VPN-сервера, дозванивается до своего интернет-провайдера и устанавливает связь с корпоративной интрасетью посредством упомянутого VPN-подключения. Если же

пользователь использует VPN для входа в домен, ему нужно в окне **Вход в Windows (Log On To Windows)** указать VPN-подключение и подключение к провайдеру (рис. 10-29).

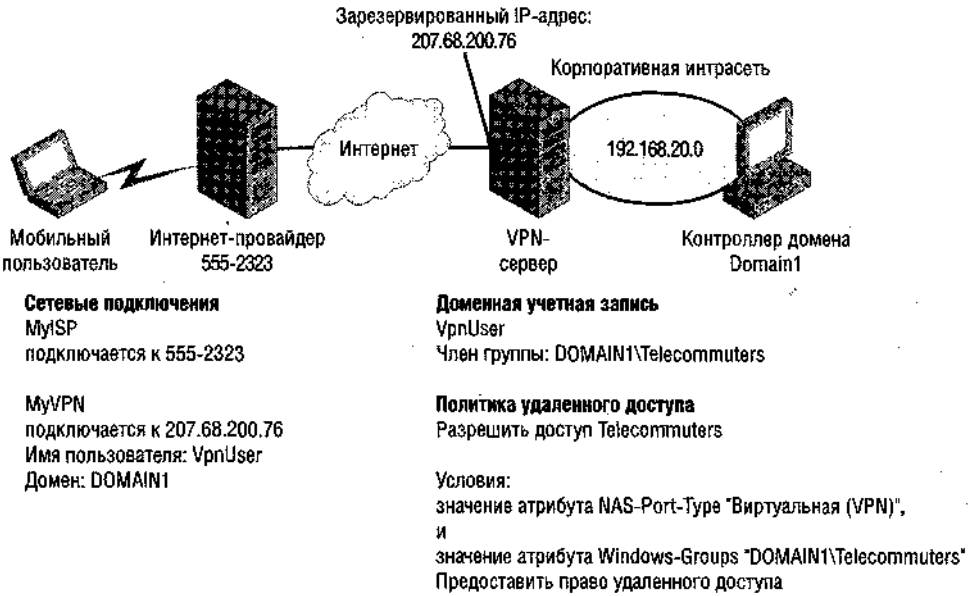


Рис. 10-29. Конфигурация VPN для удаленного доступа

VPN по схеме экстрасеть или маршрутизатор — маршрутизатор

Экстрасеть — это подключение друг к другу двух корпоративных сетей через VPN-серверы со службой *Маршрутизация и удаленный доступ*. На каждом сервере интерфейсы с вызовом по требованию инициируют и отвечают на запросы создания VPN-подключений. При подключении выполняется аутентификация интерфейсов, а не отдельных пользователей.

Примечание Для интерфейсов с вызовом по требованию не нужно описывать удаленные подключения. В службе маршрутизации и удаленного доступа VPN-интерфейсы рассматриваются как разновидность интерфейса с вызовом по требованию, даже если они запрашивают или отвечают на запрос подключения по линии T1.

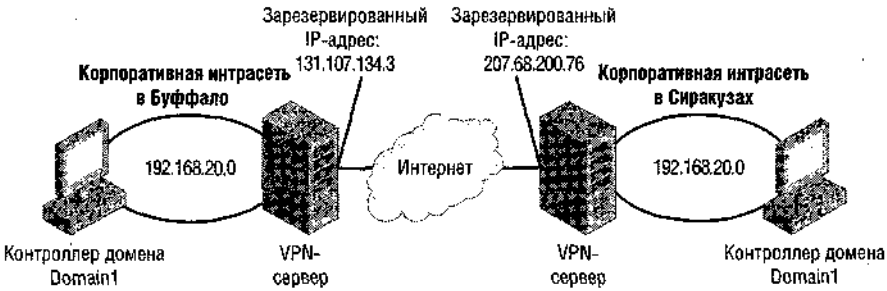
Для каждого VPN-интерфейса с вызовом по требованию необходимо создать набор «телефонных» реквизитов, включающих имя пользователя, пароль и домен. По умолчанию имя пользователя — это имя самого интерфейса. Однако имя пользователя должно совпадать с именем интерфейса и на ответном VPN-сервере. Настройка упростится, если взаимодействующим интерфейсам дать одинаковое имя.

На рис. 10-30 представлен сценарий, где обоим интерфейсам присвоено имя BufSyr. Оба сервера — члены одного домена Domain 1, и в обеих подсетях есть локальные контроллеры доменов. Для авторизации подключения в домене надо создать учетную запись Buf_Syr.

Подключение проходит авторизацию на предмет соответствия политикам удаленного доступа. В данном примере политика разрешает доступ VPN-подключениям, инициируемым учетными записями пользователей глобальной группы *VPN-Routers*. Посколь-

ку Buf_Syr — член группы, политика санкционирует VPN-подключения по схеме маршрутизатор — маршрутизатор с обеих сторон соединения.

Наконец, для полноценной реализации экстрасети нужно разместить на каждом VPN-сервере статические маршруты, предназначенные для трафика, направляемого в противоположную частную сеть через VPN-интерфейс с вызовом по требованию. Эти же статические маршруты служат и для ответного трафика, поэтому они конфигурируются на обоих серверах, даже если все удаленные запросы инициируются одной сетью.



Интерфейс с вызовом по требованию
Buf_Syr
подключается к 207.68.200.76

Доменная учетная запись
Buf_Syr
Член группы: DOMAIN1\VPN-Routers

Политика удаленного доступа
Разрешить экстрасетевые подключения

Условия:
значение атрибута NAS-Port-Type "Виртуальная (VPN)",
и
значение атрибута Windows-Groups
"DOMAIN1\VPN-Routers"

Предоставить право удаленного доступа

Статический маршрут
Назначение: 192.168.20.0
Маска сети: 255.255.255.0
Интерфейс: Buf_Syr

Интерфейс с вызовом по требованию
Buf_Syr
подключается к 131.107.134.3

Доменная учетная запись
Buf_Syr
Член группы: DOMAIN1\VPN-Routers

Политика удаленного доступа
Разрешить экстрасетевые подключения

Условия:
значение атрибута NAS-Port-Type "Виртуальная (VPN)",
и
значение атрибута Windows-Groups
"DOMAIN1\VPN-Routers"

Предоставить право удаленного доступа

Статический маршрут
Назначение: 192.168.10.0
Маска сети: 255.255.255.0
Интерфейс: Buf_Syr

Рис. 10-30. VPN-подключение по схеме маршрутизатор — маршрутизатор

Развертывание протоколов маршрутизации в VPN

В варианте с экстрасетью статические маршруты можно заменить на протокол маршрутизации типа RIP (Routing Information Protocol). Для этого сначала в консоли *Маршрутизация и удаленный доступ* надо добавить выбранный протокол во все VPN-серверы, а затем добавить и настроить для протокола VPN-интерфейс с вызовом по требованию. В частности, для RIP можно задать в качестве соседей другие VPN-серверы или включить одноранговое фильтрование на основании пароля или увеличить стандартный (30 секунд) интервал оповещения. При развертывании VPN с использованием телефонных линий надо предусмотреть автостатическое обновление на маршрутизаторах.

При установке протокола маршрутизации необходимо проверить его совместимость с остальными маршрутизаторами сети. И, наконец, убедиться в том, что сетевые маршрутизаторы способны обновляться по инициативе VPN-серверов.

Сочетание VPN с брандмауэром

В случае совмещения в сети средств удаленного доступа и экстрасети можно разместить брандмауэр (рис. 10-31). VPN-сервер с открытым адресом, размещается за брандмауэром в сети периметра.

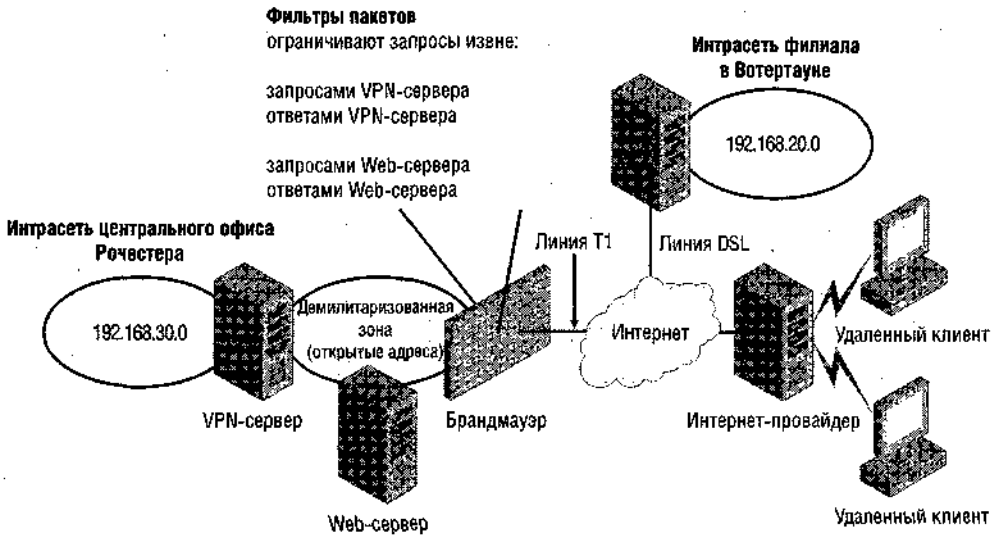


Рис. 10-31. Комбинированный вариант VPN

Обычно брандмауэры пропускают трафик, инициируемый во внутренней сети, и блокируют остальные пакеты. При необходимости фильтры пакетов настраивают на пропускание данных, приходящих в VPN-сервер из внешней сети.

Фильтры пакетов в примере на рис. 10-31 пропускают двусторонний трафик VPN-сервера. Поскольку Web-сервер тоже находится в сети периметра, фильтры пакетов пропускают входящий и исходящий трафик Web-сервера.

Фильтры пакетов не обязательны для доступа к службам, расположенным за VPN-сервером. Обычно брандмауэры не в состоянии фильтровать пакеты, инкапсулированные в VPN-туннеле. Попадая на VPN-сервер, пакеты освобождаются от VPN-заголовка и дешифруются. С этого момента они поступают в распоряжение служб внутренней сети.

Устранение неполадок удаленного доступа через VPN

Неполадки удаленного доступа через VPN-подключения устраняются в следующей последовательности.

- Проверьте на VPN-сервере: достаточно ли число портов, описанных в узле **Порты (Ports)** для требуемого типа VPN (no PPTP или L2TP) и сколько доступных портов в данный момент задействованы.
- Проверьте, включен ли на вкладке **Общие (General)** окна свойств сервера консоли *Маршрутизация и удаленный доступ* параметр **Сервер удаленного доступа (Remote Access Server).**

- Проверьте, есть ли у VPN-подключения надлежащие разрешения, заданные в свойствах учетной записи пользователя и политиках удаленного доступа.
- Выясните, есть ли в настройке VPN-клиента, удаленного сервера и политики удаленного хотя бы один общий протокол аутентификации.
- Проверьте, имеется ли в настройке VPN-клиента, удаленного сервера и политики удаленного доступа хотя бы с один общий метод шифрования.
- Проверьте, входит ли сервер удаленного доступа (или RADIUS-сервер) в группу безопасности *Серверы RAS и IAS* (RAS and IAS Servers) локального домена.
- Проверьте, не противоречат ли параметры профиля политики удаленного доступа свойствам сервера удаленного доступа.
- Проверьте, не превышает ли длина пароля пользователя 14 символов, когда в качестве протокола аутентификации используется MS-CHAP v1.

Устранение неполадок в VPN по схеме «маршрутизатор — маршрутизатор»

Неполадки удаленного доступа через VPN-подключения в схеме «маршрутизатор — маршрутизатор» устраняются в следующей последовательности.

- Проверьте, установлены ли на всех концах VPN-подключения параметры **Маршрутизатор (Router)** и **локальной сети и вызова по требованию (LAN and demand-dial routing)** на вкладке **Общие** окна свойств сервера консоли *Маршрутизация и удаленный доступ*.
- Проверьте установлен ли на вкладке IP окна свойств сервера консоли *Маршрутизация и удаленный доступ* параметр **Разрешить IP-адресацию (Enable IP Routing)** на всех серверах удаленного доступа.
- Проверьте, достаточно ли число портов, описанных в узле **Порты (Ports)** для требуемого типа VPN (no PPTP или L2TP) на всех серверах удаленного доступа.
- Убедитесь, что на всех для каждого интерфейса с вызовом по требованию для VPN-подключения в мастере интерфейса с вызовом по требованию был выбран параметр маршрутизации IP-трафика через данный интерфейс.
- Проверьте, определены ли на всех серверах удаленного доступа статические маршруты, предназначенные для сопоставления трафика, направляемого в противоположную сеть, с соответствующим VPN-интерфейсом.
- Убедитесь, что на всех серверах удаленного доступа локальные учетные данные запрашивающего интерфейса с вызовом по требованию совпадают с именем удаленного отвечающего интерфейса и с именем и паролем учетной записи пользователя в удаленном домене.
- Убедитесь, что все интерфейсы вызова по требованию принимающего сервера удаленного доступа и политика удаленного доступа на принимающей стороне имеют хотя бы один общий протокол аутентификации и уровень шифрования.
- Проверьте, у всех ли подключениях удаленного доступа есть надлежащие разрешения, определенные в свойствах телефонного подключения учетной записи пользователя (соответствующей имени интерфейса с вызовом по требованию) и в политиках удаленного' доступа.
- Проверьте, входит ли сервер удаленного доступа (или RADIUS-сервер) в группу безопасности *Серверы RAS и IAS* (RAS and IAS Servers) локального домена. Это нужно проверить на всех концах VPN.
- Убедитесь, что на всех серверах удаленного доступа их свойства не противоречат параметрам профиля политики удаленного доступа.

Настройка разных типов VPN-подключений

Windows Server 2003 поддерживает две разновидности VPN: по протоколу PPTP и L2TP поверх IPSec. Если в *Мастере настройки сервера маршрутизации и удаленного доступа* (Routing and Remote Access Server Setup Wizard) не была определена роль VPN-сервера удаленного доступа, каждому типу VPN назначается по пять портов. Поскольку один порт поддерживает лишь одно подключение, в стандартной службе маршрутизации и удаленного доступа разрешается не более 5 одновременных подключений каждого типа. Эти порты можно увидеть в консоли **Маршрутизация и удаленный доступ,** выбрав узел **Порты (Ports)** (рис. 10-32).

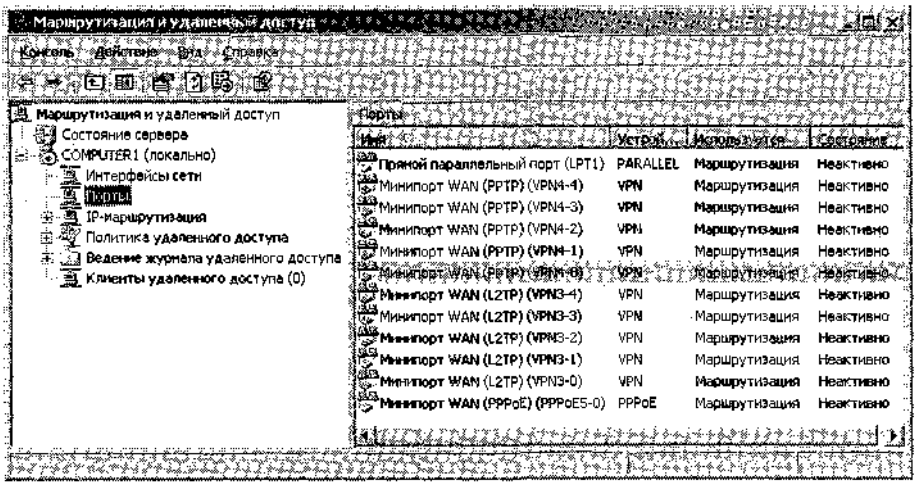


Рис. 10-32. VPN-порты сервера удаленного доступа

Однако число портов можно легко увеличить, изменив конфигурацию VPN-подключений. Откройте окно **Свойства: Порты (Ports Properties),** выберите тип портов и щелкните кнопку **Настроить (Configure).** В окне **Настройка устройства (Configure Device)** (рис. 10-33) укажите число одновременных подключений к VPN-серверу в поле **Максимальное число портов (Maximum Ports).**

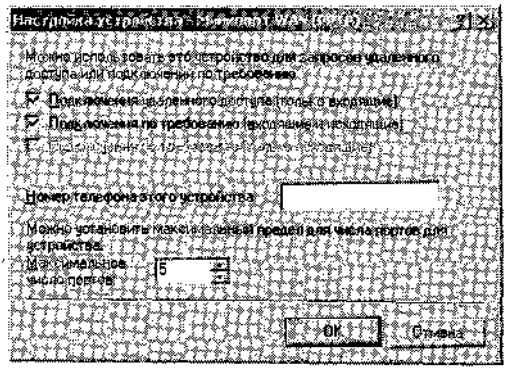


Рис. 10-33. Добавление портов VPN

Windows Server 2003 поддерживает одновременно до 1000 VPN-подключений, поэтому разрешается до 1000 портов для PPTP и столько же — для L2TP.

Примечание Если в *Мастере настройки сервера маршрутизации и удаленного доступа* вы указали роль VPN-сервера удаленного доступа, по умолчанию будет создано 128 VPN-портов каждого типа.

Подготовка к экзамену Будьте готовы к вопросам о причине блокировки доступа через VPN, связанной с недостаточным количеством портов, а также о максимальном разрешенном числе VPN-портов и числе одновременных подключений, поддерживаемых Windows Server 2003.

VPN на основе PPTP

Обычно VPN-туннели по протоколу PPTP проще в реализации, но менее безопасны, чем каналы на базе L2TP/IPSec (в последнем используются сертификаты). VPN-подключения на основе PPTP обеспечивают конфиденциальность передаваемых данных (нельзя узнать содержание перехваченных пакетов, не имея ключа), но не гарантируют целостность данных (возможно искажение при передаче) и аутентификацию источника (возможна передача данных посторонним пользователем).

При шифровании PPTP-подключений применяется стандарт MPPE, не требующий организации инфраструктуры PKI и получения сертификатов пользователей или компьютеров на обоих концах виртуального подключения. Однако PPTP можно использовать совместно с инфраструктурой сертификатов, если в качестве протокола аутентификации выбрать EAP-TLS.

Рис. 10-34 иллюстрирует инкапсуляцию с использованием PPTP. Связь между двумя конечными точками VPN рассматривается как PPP-подключение с шифрованием по MPPE. Затем к кадру добавляются заголовки GRE (Generic Routing Encapsulation) и IP.

Подготовка к экзамену Помните, что упоминание протокола GRE в вариантах ответов по сути представляет собой косвенную ссылку на PPTP.

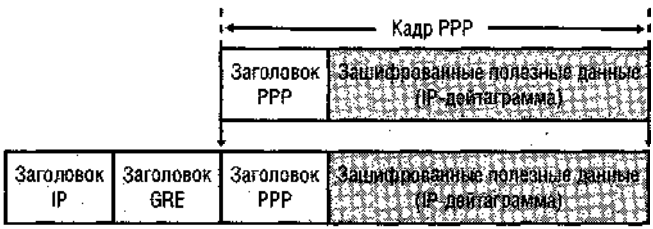


Рис. 10-34. Пример пакета PPTP

Настройка PPTP-подключений на VPN-сервере

Чтобы сконфигурировать политику удаленного доступа, разрешающую VPN-Нодключения, нужно добавить в атрибут **NAS-Port-Type** значение **Virtual (VPN) [Виртуальная (VPN)].** Доступ по VPN возможен, если определена подходящая разрешающая политика с такими условиями, как **Windows Group, NAS-Port-Type** или другими. Помимо описания политики удаленного доступа, для проверки подключения на соответствие задан-

аым условиям надо убедиться, что число PPTP-портов достаточно для одновременной эбработки всех подключений.

Чтобы запретить PPTP-подключения к VPN-серверу, в окне **Свойства: Порты (Ports Properties),** выберите **Минипорт WAN (PPTP) [WAN Miniport (PPTP)]** и щелкните кнопку **Настроить (Configure),** затем в окне **Настройка устройства - Минипорт *WAN* (PPTP) [Configure Device -WAN Miniport (PPTP)]** снимите флажки **Подключения удаленного доступа (только входящие) [Remote Access Connections (Inbound Only)]** и **Подключения по требованию (входящие и исходящие) [Demand-dial routing connections (inbound and outbound)].**

Примечание В политиках удаленного доступа VPN-подключения отличаются от остальных только значением Virtual (VPN) [Виртуальная (VPN)] атрибута NAS-Port-Type. Обратите внимание, что в политиках удаленного доступа PPTP- и Ь2TP/1P8ec-подключения никак не различаются.

Настройка PPTP-подключений на VPN-клиенте

Для настройки VPN-подключения по PPTP запустите *Мастер новых подключений* и выберите вариант **Подключение к виртуальной частной сети (VPN connection).** По умолчанию создается VPN-подключение автоматического режима, в котором сначала предпринимается попытка установить L2TP-связь с применением сертификатов IPSec, а в случае неудачи —по PPTP. Поэтому при отсутствии сертификатов для IPSec VPN-подключение по умолчанию переключается на PPTP. Кроме того, протокол PPTP для VPN-подключения устанавливается, если на вкладке **Сеть (Networking)** свойств подключения в списке **Тип VPN (Type of VPN)** выбрать значение **PPTP VPN** (рис. 10-35).

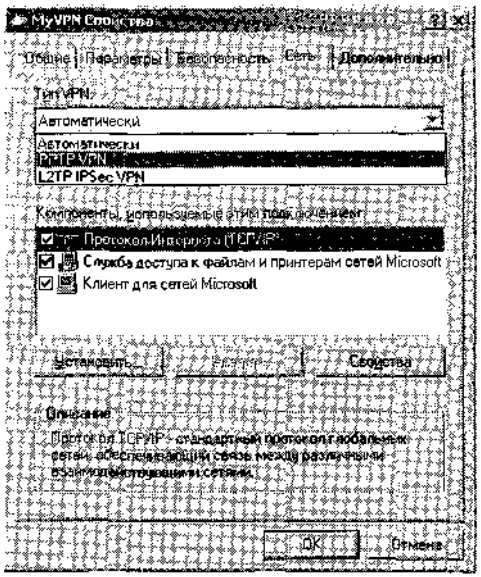


Рис. 10-35. Настройка типа VPN-подключения

На заметку VPN-подключения на базе PPTP пользуются незаслуженно плохой репутацией небезопасных подключений, а из-за простоты настройки их часто называют «VPN для чайников». В действительности, безопасность PPTP ниже, чем L2TP/IPSec, но не намного, а в некоторых случаях PPTP-подключения предпочтительнее L2TP/IPSec. В частности, когда требуется обеспечить подключение удаленных пользователей, использующих общедоступные компьютеры, например в библиотеке, применение сертификатов для компьютеров не реально и для VPN остается только вариант с PPTP.

VPN на основе L2TP/IPSec

В L2TP/IPSec-подключениях протокол L2TP служит для создания VPN-туннеля, а ESP (по сути одна из составляющих IPSec) — для шифрования данных. Структура пакета L2TP/IPSec показана на рис. 10-36.

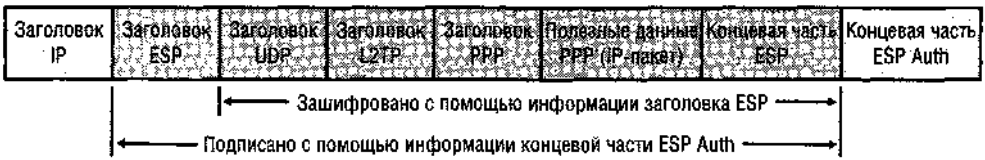


Рис. 10-36. Пример L2TP-пакета

В отличие от PPTP-подключений, в L2TP/IPSec-подключениям до аутентификации пользователя выполняется аутентификация компьютера. Причем эта процедура выполняется во всех попытках подключения между клиентами и серверами удаленного доступа. После аутентификации конечных пунктов туннеля и установки безопасного канала между клиентом и сервером выполняется аутентификация пользователя, в которой используются те же протоколы аутентификации, что и в PPTP и телефонных подключениях. По завершении аутентификации пользователь проходит авторизацию.

Сертификаты компьютеров и L2TP/IPSec

В большинстве VPN-подключений на базе L2TP/IPSec аутентификация компьютера выполняется с применением инфраструктуры сертификатов. Для успешной реализации этого типа VPN на всех VPN-клиентах и VPN-серверах надо установить сертификаты компьютеров, выпущенные одним центром сертификации (ЦС). При использовании в этом качестве ЦС предприятия Windows Server 2003 в домене Active Directory надо активизировать средствами групповой политики (Computer Configuration) *автоматическую подачу заявок* (autoenrollment) на сертификаты компьютеров. В этом случае каждый компьютер — член домена автоматически запрашивает сертификат компьютера при обновлении этой групповой политики.

Примечание Более подробное рассмотрение реализации L2TP/IPSec на основе сертификатов выходит за рамки экзамена 70-291. Подробнее — на Web-странице *http://www. microsoft, com/technet/treeview/'default, asp ?url=/technet/prodtechnol/windowsserver deploy/confeat/rmotevpn.asp.*

Каждый сертификат содержит расширения EKU (enhanced key usage), описывающие его назначение. Сертификат компьютера, назначаемый клиенту L2TP/IPSec должен содержать назначение сертификата — *Аутентификация клиента* (Client Authentication) или IPSec. Вместе с тем, у сертификата VPN-сервера должно быть назначение *Аутентифи-*

кация сервера, если он является сервером удаленного доступа, или оба назначения — если он установлен в VPN по схеме «маршрутизатор-маршрутизатор». Дополнительные назначения включаются в расширения этого же сертификата.

Примечание Если для аутентификации пользователя применяется EAP-TLS, пользовательский сертификат надо установить на всех VPN-клиентах, а если аутентифицирующим сервером является RADIUS, нужно установить на нем сертификат компьютера. Аутентификация пользователя в VPN no L2TP/IPSec не требует EAP-TLS.

Предварительные ключи и L2TP/IPSec

Единственный случай, когда для VPN-подключений на базе L2TP/IPSec не требуются сертификаты, — когда и на VPN-клиенте, и на VPN-сервере установлена ОС Windows Server 2003. В этом случае появляется возможность настроить аутентификацию компьютеров с применением *предварительного ключа* (preshared key) — текстовой строки, передаваемой открытым текстом и используемой для шифрования и расшифровки IPSec-информации. Это небезопасный метод аутентификации, и он рекомендуется только для тестирования.

Отключение поддержки подключений L2TP/IPSec

Чтобы закрыть доступ через VPN no L2TP/IPSec, достаточно установить в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) максимальное число L2TP-портов, равное нулю. (Заметьте, что для PPTP этот способ не годится.) Чтобы запретить L2TP/IPSec-подключения, откройте окно **Свойства: Порты (Ports Properties),** выберите **Минипорт WAN (L2TP) [WAN Miniport (L2TP)]** и щелкните кнопку **Настроить (Configure).** В окне **Настройка устройства - Минипорт WAN (L2TP) [Configure Device — WAN Miniport (L2TP)]** введите в поле **Максимальное число портов (Maximum Ports)** значение 0. Подтвердите изменение щелчком Да **(Yes).**

Лабораторная работа. **Настройка VPN**

На этой лабораторной работе вы настроите удаленный VPN-доступ по протоколам PPTP и L2TP/IPSec.

Упражнение 1. Организация VPN-доступа как условия политики удаленного доступа

Примечание Если за раз подключить к Интернету возможно только один компьютер, выполните только упражнения 1, 2 и 4.

Вы должны изменить политику удаленного доступа Telecommuters, чтобы она применялась не только к телефонным, но и к VPN-подключениям.

1. Создайте на Computed и Computer2 удаленное подключение к своему провайдеру, назвав его MyISP, как описано в упражнении 2 занятия 3 главы 4. Стандартные свойства удаленного подключения оставьте без изменений.

   Примечание При желании можно воспользоваться выделенным подключением к интернет-провайдеру, однако в описанную ниже инструкцию придется внести небольшие поправки.

2. Войдите из Computerl в Domainl как *Администратор* (Administrator) и откройте консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access).
3. **В** дереве консоли выберите узел **Политики удаленного доступа (Remote Access Policies)** и в правой панели дважды щелкните политику Telecommuters. Откроется окно **Свойства: Telecommuters (Telecommuters Properties).**
4. В области **Условия политики (Policy Conditions)** выберите условие **NAS-Port-Type** и щелкните кнопку **Изменить (Edit).**
5. **В** окне **NAS-Port-Type** в списке типов выберите **Virtual (VPN) [Виртуальная (VPN)].**
6. Щелкните кнопку **Добавить (Add).** В разделе **Выбранные типы (Selected Types)** появится **Виртуальная (VPN).** Щелкните **OK.**
7. **В** окне **Свойства: Telecommuters** щелкните OK.
8. Выйдите из домена Domainl.

Упражнение 2. Создание VPN-подключения типа PPTP

Вы должны создать на Computer2 VPN-подключение для связи с Computerl по его текущему IP-адресу. По умолчанию создается VPN-подключение по PPTP, так как протокол IPSec на основе сертификатов недоступен.

1. Войдите в систему Computerl как *Администратор* (Administrator) домена Domainl.
2. Откройте окно **Сетевые подключения (Network Connections).**
3. **В** меню **Файл (File)** щелкните **Новое подключение (New Connection).**
4. **В** окне **Мастер новых подключений (New Connection Wizard)** щелкните **Далее** (Next).
5. На странице **Тип сетевого подключения (Network Connection Type)** выберите **Подключить к сети на рабочем месте (Connect To The Network At My Workplace)** и щелкните **Далее.**
6. На странице **Сетевое подключение (Network Connection)** выберите **Подключение к виртуальной частной сети (Virtual Private Network Connection)** и щелкните **Далее.**
7. На странице **Имя подключения (Connection Name)** в поле **Организация (Company Name)** введите MyVPN и щелкните **Далее.**
8. На странице **Публичная сеть (Public Network)** в списке **Набрать номер для следующего предварительного подключения (Automatically Dial This Initial Connection)** выберите **MylSP** и щелкните **Далее.** Откроется страница **Выбор VPN-сервера (VPN Server Selection).**
9. С Computerl войдите в Domainl как *Администратор* и с использованием подключения MylSP установите связь с Интернетом. Затем исполните команду ipconf ig, определите текущий общедоступный IP-адрес, присвоенный Computerl и запишите его.
10. Вернитесь к Computer2. На странице **Выбор VPN-сервера** в поле **Имя компьютера или IP-адрес (Host name or IP address)** введите полученный IP-адрес Computerl и щелкните **Далее.**
11. На странице **Возможность подключения (Connection Availability)** выберите вариант **Для всех (Anyone's Use)** и щелкните **Далее.**
12. На странице **Завершение работы мастера новых подключений (Completing the New Connection Wizard)** щелкните **Готово (Finish).**
13. В открывшемся окне **Начальное подключение (Initial Connection)** щелкните Нет (No).
14. Откройте окно **Сетевые подключения (Network Connections)** с новым разделом **Виртуальная частная сеть (VPN) (Virtual Private Network). В** нем вы увидите значок нового подключения **MyVPN,** под которым отображается его текущее состояние — **Отключено (Disconnected)** и тип — **Минипорт WAN (PPTP) [WAN Miniport (PPTP)].**

15. Щелкните правой кнопкой **MyVPN** и в контекстном меню выберите **Свойства (Properties).**
16. На вкладке **Параметры (Options)** окна **MyVPN - Свойства (MyVPN Properties)** в разделе **Параметры набора номера (Dialing Options)** установите флажок **Включать домен входа в Windows (Include Windows Logon Domain).**
17. На вкладке **Сеть (Networking)** в списке **Тип VPN** (Type of **VPN)** обратите внимание на выбранное значение **Автоматически (Automatic). В** данном случае сначала выполняется попытка установить VPN-подключение на основе сертификатов L2TP/IPSec, и лишь затем — PPTP-подключение.
18. Щелкните OK.
19. На Computer2 выйдите из домена Domain 1.
20. До отключения Computer1 от Интернета выполните упражнение 3, чтобы проверить правильность адреса, введенного в п. 10.

Упражнение 3 (дополнительное). Подключение к домену по VPN-подключению

Вы подключитесь к Domainl по VPN-каналу. Перед выполнением упражнения убедитесь, что компьютеры подключены к разным телефонным линиям. На время выполнения упражнения можно также отключить сетевой кабель, соединяющий компьютеры, чтобы быть уверенным, что связь компьютеров поддерживается по телефонным линиям.

1. На Computer2 нажмите Ctrl+Alt+Del, чтобы открыть окно **Вход в Windows (Log On To Windows).**
2. Установите флажок **С использованием удаленного доступа (Log On Using Dial-Up Connection).**
3. В поле **Пользователь (User Name)** введите u s e d .
4. В поле **Пароль (User)** введите пароль учетной записи Userl.
5. В списке **Домен (Log On To)** выберите Domainl и щелкните OK. Откроется окно **Сетевые подключения (Network Connections).**
6. **В** списке **Выберите сетевое подключение (Choose a Network Connection)** выберите **MyVPN** и щелкните **Подключить (Connect).**
7. **В** открывшемся окне **Начальное подключение (Initial Connection)** и щелкните **Да (Yes).** Откроется окно **Подключение к MylSP (Connect MylSP).**
8. **В** полях **Пользователь** и **Пароль** введите реквизиты, полученные у интернет-провайдера, и щелкните кнопку **Вызов (Dial).**

   В окне **Установка связи с MylSP (Connecting MylSP)** отображается состояние подключения. Когда связь с провайдером установится, откроется окно **Подключить MyISP (Connect MyVPN).**
9. Введите:,
   - в поле **Пользователь—**userl;
   - в поле **Пароль** — пароль учетной записи Userl;
   - в поле **Домен (Domain)—** DOMAINl
10. Щелкните **Подключить (Connect). В** окне **Установка связи с MylSP** отображается состояние подключения. После завершения аутентификации, авторизации и установления подключения выполняется вход в домен.
11. После завершения входа в систему Computer2 откройте окно Microsoft Internet Explorer. Не обращайте внимания на появившиеся сообщения и предупреждения.

12. В адресной строке браузера введите:

    \\computer1.domainl.local

    и нажмите Enter. Спустя пару секунд установится подключение, и в окне браузера появятся общие ресурсы Computer 1.
13. Перейдите к Computerl и откройте консоль *Маршрутизация и удаленный доступ* (Routing and Remote Access).
14. В дереве консоли щелкните узел **Порты (Ports). В** правой панели видно, что в активном состоянии находится только один минипорт WAN, подключенный по PPTR
15. Выйдите из систем Computer2 и Computerl.

Упражнение 4. Создание VPN-подключения по L2TP/IPSec

Вы сконфигурируете VPN-подключение между Computerl и Computer2 по протоколу L2TP/IPSec. Но вначале создадите предварительный ключ на клиенте и сервере удаленного доступа.

1. Войдите с Computer2 в Domainl как *Администратор* (Administrator).
2. Откройте окно **Сетевые подключения (Network Connections).** Щелкните значок **MyVPN** правой кнопкой и выберите **Свойства (Properties).**
3. На вкладке **Безопасность (Security)** окна **MyVPN - Свойства (MyVPN Properties)** щелкните кнопку **Параметры IPSec (IPSec Settings)** — откроется одноименное окно.
4. Установите флажок **Для проверки подлинности использовать предварительный ключ (Use Pre-Shared Key For Authentication)** и в поле **Ключ (Key)** введите test.

   Примечание Предварительные ключи никак не защищены, поскольку передаются по сети открытым текстом. Однако они вполне годятся для проверки работоспособности IPSec-подключения. Предварительные ключи также позволяют получать компьютерные сертификаты в ходе развертывания инфраструктуры PKI. IPSec на базе сертификатов PKI считается более защищенным, чем VPN-подключения на базе PPTP.

5. Щелкните OK.
6. Оставьте открытым окно **MyVPN - Свойства** и перейдите к Computerl.
7. Войдите с Computerl в Domainl как *Администратор* (Administrator).
8. В дереве консоли *Маршрутизация и удаленный доступ* щелкните **COMPUTER1 (локально) [COMPUTER1 (Local)]** правой кнопкой и выберите **Свойства (Properties).** Откроется окно **Свойства: COMPUTER1 (локально) [COMPUTER1 (Local) Properties].**
9. На вкладке **Безопасность (Security)** установите флажок **Разрешать пользовательские IPSEC-политики для L2TP-подключения (Allow Custom IPSec Policy For L2TP Connection)** и в поле **Предварительный ключ (Pre-Shared Key)** введите test. Этот ключ должен совпадать с ключом клиента.
10. Щелкните OK.
11. Установите связь Computerl с Интернетом через подключение MylSP, после чего исполните команду Ipconfig и запишите текущий IP-адрес компьютера Computerl.
12. Вернитесь к Computer2 и в поле **Имя компьютера или IP-адрес назначения (Host name or IP address of destination)** на вкладке **Общие (General)** окна **MyVPN - Свойства** введите IP-адрес, присвоенный Computerl.

13. На вкладке Сеть **(Networking)** в списке **Тип VPN** *(Type* of **VPN)** выберите **L2TP IPSec VPN** и щелкните OK.
14. Выйдите на Computer2 из Domainl.
15. Оставив на Computerl активным подключение MylSP, перейдите к выполнению следующего упражнения.

Упражнение 5 (дополнительное). Проверка настройки L2TP/IPSec

Вы проверите работоспособность нового VPN-подключения.

1. Войдите с Computer2 в Domainl как Userl через подключение MyVPN. Выполните операции, описанные в упражнении 3.
2. После создания VPN-подключения перейдите к Computerl.
3. На Computerl' в дереве консоли *Маршрутизация и удаленный доступ* щелкните узел **Ports (Порты). В** правой панели видно, что активен только порт L2TP. Обратите внимание, сколько доступно портов по умолчанию: пять PPTP-портов, один порт PPTP over Ethernet (PPPoE) и пять Ь2ТР-портов — именно такое количество подключений разрешено на сервере в любой момент времени.
4. В дереве консоли щелкните узел **Порты** правой кнопкой и выберите **Свойства (Properties).** Откроется окно **Свойства: Порты (Ports Properties).**
5. В списке устройств выберите **Минипорт WAN (L2TP)** и щелкните кнопку **Настроить (Configure).** Откроется окно **Настройка устройства — Минипорт WAN (L2TP) [Configure Device - WAN Miniport (L2TP)].**

   Примечание По умолчанию флажок **Подключения по требованию (Demand-Dial Routing Connections)** сброшен. Его нужно установить, чтобы порт стал доступным для маршрутизации с вызовом по требованию по VPN.

6. В поле **Максимальное число портов (Maximum Ports)** введите 1500 и щелкните OK. Откроется окно с сообщением, что портов может быть от 0 до 1000. Другими словами, в конфигурации службы *Маршрутизация и удаленный доступ* допускается одновременно до 1000 L2TP-подключений. То же относится к PPTP-портам.
7. Щелкните OK.
8. В окне **Настройка устройства — Минипорт WAN (L2TP)** щелкните кнопку **Отмена.**
9. **В** окне **Свойства: Порты** щелкните кнопку **Отмена.**
10. Выйдите из системы Computerl и Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. В чем разница между сертификатами, применяемыми в протоколе аутентификации EAP-TLS и в VPN-протоколе L2TP/IPSec?
2. Пользователи иногда испытывают трудности с подключением к VPN-серверу, причем жалобы обычно поступают при высокой загруженности сети, то есть дело не в ошибочном адресе. Какова наиболее вероятная причина неполадки?
3. Почему считается, что предварительные ключи в IPSec не обеспечивают должную безопасность обмена данными?

Резюме

- Частные виртуальные сети — это сети, которые логически имитируют локальную сеть, но физически проходят через Интернет.
- В удаленном VPN-доступе в Windows Server 2003 одиночный пользователь устанавливает связь через Интернет с компьютером под управлением Windows Server 2003 и со службой *Маршрутизация и удаленный доступ* (Routing and Remote Access). При варианте реализации экстрасети частные локальные сети объединяются через Интернет посредством двух компьютеров под управлением Windows Server 2003 со службой *Маршрутизация и удаленный доступ*.
- VPN-туннели на базе протокола PPTP проще в использовании, но менее безопасны, чем туннели по протоколам L2TP/IPSec на основе сертификатов. В PPTP-подключениях применяются схема шифрования MPPE.
- В отличие от PPTP, при создании L2TP/IPSec-подключений помимо аутентификации пользователей требуется аутентификация компьютеров. Если аутентификация компьютера обеспечивается с помощью инфраструктуры сертификатов, VPN-подключения по протоколу L2TP считаются безопасными. Если аутентификация компьютера выполняется на основе предварительного ключа, безопасность подключений считается более низкой.

Занятие 4. Развертывание службы проверки подлинности в Интернете

Служба проверки подлинности в Интернете (Internet Authentication Service, IAS) — это ни что иное, как реализация корпорацией Microsoft RADIUS-сервера и RADIUS-прокси. В качестве RADIUS-сервера LAS выполняет централизованную аутентификацию, авторизацию и учет использования ресурсов подключений для сетевого доступа разных типов, например беспроводных сетей, коммутаторов с поддержкой аутентификации, VPN-сетей и доступа по телефонным линиям, а также подключения «маршрутизатор — маршрутизатор». В качестве RADIUS-прокси IAS переадресует данные аутентификации и учетные данные на другие RADIUS-серверы.

Изучив материал этого занятия, вы сможете:

S настроить службу LAS для выполнения аутентификации клиентов службы маршрутизации- и удаленного доступа.

Продолжительность занятия - около 45 минут.

Варианты использования RADIUS-серверов

Основным назначением сервера RADIUS является централизованная поддержка аутентификации, авторизации и учета удаленного доступа. RADIUS подходит, например, для крупных организаций, таких как интернет-провайдеры, которым нужно управлять множеством подключений удаленного доступа к разрозненным серверам удаленного доступа.

На рис. 10-37 представлен сценарий, в котором пользователи в четырех разных городах устанавливают связь по телефонной линии с одним провайдером. Серверы удаленного доступа.с установленной службой маршрутизации и удаленного доступа пересылают запросы удаленного доступа на RADIUS-сервер по протоколу RADIUS. Затем RADIUS-сервер соединяется с контроллером домена для выполнения аутентификации пользователей, после чего к подключению применяются политики удаленного доступа, описанные на RADIUS-сервере. Если подключение удаленного доступа обладает нужными разрешениями, RADIUS-сервер устанавливает соединение с сервером удаленного доступа и разрешает доступ к сети, в противном случае доступ к сети не предоставляется.

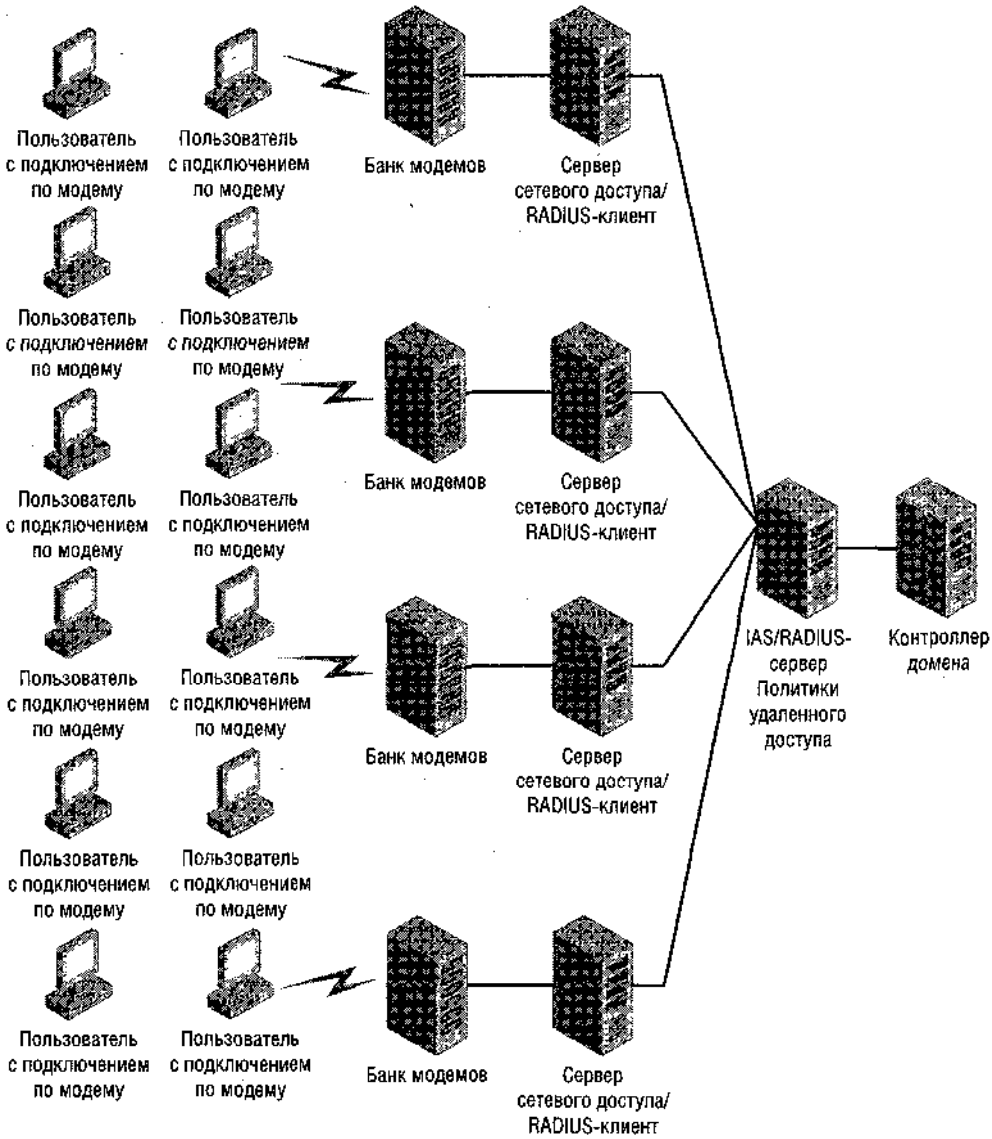


Рис. 10-37. IAS-сервер, развернутый у интернет-провайдера

RADIUS-серверы позволяют небольшим компаниям централизованно управлять удаленным доступом при использовании различных методов удаленного доступа, таких как VPN, беспроводные и телефонные подключения. Создание одной точки единой авторизации дает возможность проверять различные запросы на доступ на предмет соответствия единому набору политик удаленного доступа (рис. 10-38).

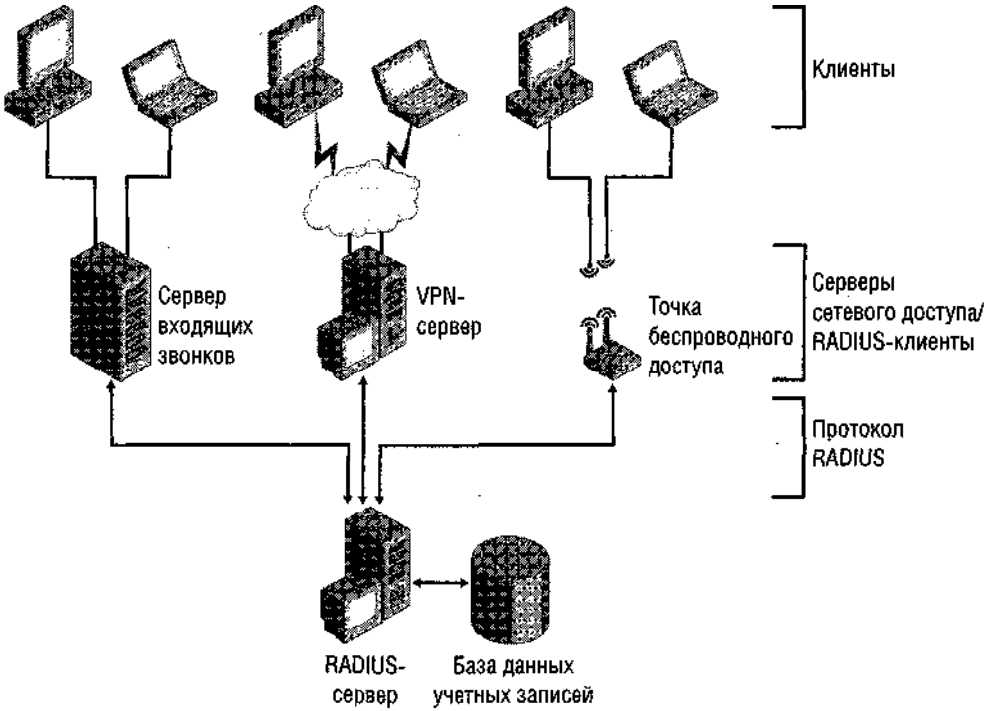


Рис. 10-38. Централизация авторизации на RADIUS-сервере при использовании различных методов доступа

И последнее: обычно RADIUS-сервер размещают на отдельном компьютере, но ничто не запрещает развернуть его на сервере удаленного доступа. Тогда запросы сетевого доступа, поступающие на внешний интерфейс сервера, обрабатываются службой маршрутизации и удаленного доступа, которая пересылает их в *Службу проверки подлинности в Интернете,* связанную с внутренним IP-адресом того же компьютера (рис. 10-39). Здесь IAS выступает в роли RADIUS-сервера не только для RADIUS-запросов, исходящих от локального компьютера, но и для RADIUS-запросов, исходящих от других серверов удаленного доступа локальной сети.

Варианты использования RADIUS-прокси

В Windows Server 2003 служба IAS может выполнять роль прокси-сервера RADIUS. В этом случае серверы удаленного доступа настраиваются на пересылку данных аутентификации и учетных данных на IAS-сервер, который выступает в роли RADIUS-прокси, пересылая эти данные группе серверов RADIUS.

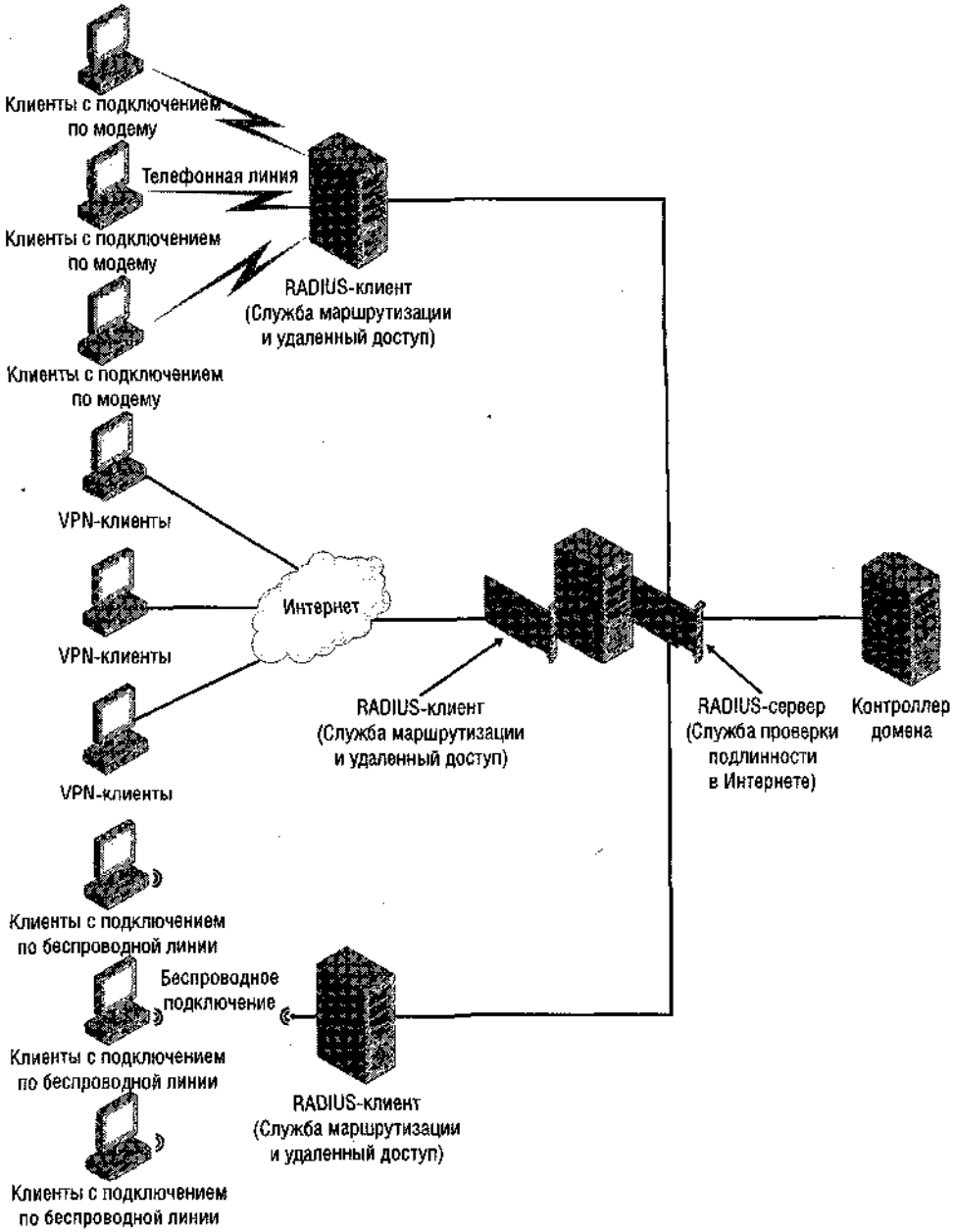


Рис. 10-39. Компьютер, выступающий в роли и сервера и клиента RADIUS

Группа RADIUS-серверов — это один или несколько RADIUS-серверов, между которыми RADIUS-прокси динамически распределяет запросы на удаленной доступ. Каждая такая группа представлена отдельным набором политик удаленного доступа для домена, леса или предприятия. Отдельные группы RADIUS-серверов могут описываться

для отдельных лесов, Kerberos-сфер или доменов, с которым не установлены отношения доверия. *Политики запросов на подключения* могут описываться в RADIUS-прокси для сортировки запросов на сетевой доступ в соответствии с их атрибутам (например имя пользователя или сферы) и ретрансляции этих запросов на соответствующую группу RADIUS-серверов.

На рис. 10-40 показан вариант использования IAS, в котором RADIUS-прокси размещен между RADIUS-клиентами (серверами удаленного доступа) и группой RADIUS-серверов.

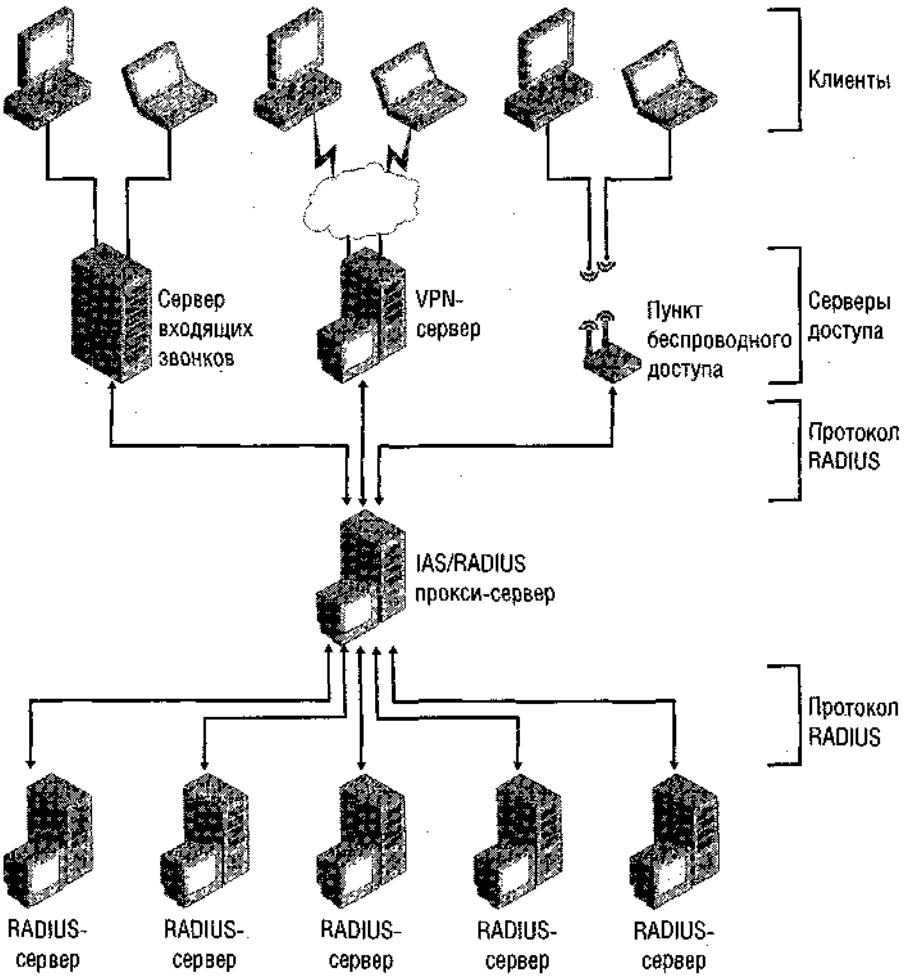


Рис. 10-40. RADIUS-прокси распределяет запросы среди членов группы RADIUS-серверов

Вот несколько сценариев реализации RADIUS-прокси.

- Провайдер услуг, предлагающий своим потребителям внешние службы сетевого доступа, может перенаправлять запросы на RADIUS-серверы клиентов в соответствии с политиками запросов на подключение, поступающими на RADIUS-прокси. Критерием политики может служить, к примеру, атрибут — название сферы.

- В ситуации, когда нужно обеспечить аутентификацию и авторизацию учетных записей, не являющихся членами домена, которому «доверяет» домен IAS-сервера, на основании политики запросов на соединения RADIUS-прокси может определять атрибут «название сферы» и перенаправлять запросы RADIUS-серверу соответствующего домена.
- Задачу эффективной обработки большого числа запросов на соединение можно решить за счет RADIUS-прокси, который обеспечит равномерное распределение запросов подключений и учета среди нескольких RADIUS-серверов.

Установка IAS в качестве RADIUS-сервера

При установке IAS в качестве RADIUS-сервера обычно требуется настройка и на стороне клиента со службой *Маршрутизация и удаленный доступ,* и на стороне сервера со службой IAS.

Настройка RADIUS-клиента

Чтобы настроить компьютер со службой *Маршрутизация и удаленный доступ* (Routing and Remote Access) как RADIUS-клиент, откройте окно свойств сервера в консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) и откройте вкладку **Безопасность (Security)** — она применяется для определения методов аутентификации и входа в систему. По умолчанию обе функции обрабатываются локальным компьютером. Чтобы передать обработку этих функций RADIUS-серверу, выберите в списке **Служба проверки подлинности (Authentication Provider)** значение **RADIUS — проверка подлинности (RADIUS Authentication),** а в списке **Служба учета (Accounting Provider)** выберите **RADIUS - учет (RADIUS Accounting)** (рис. 10-41).

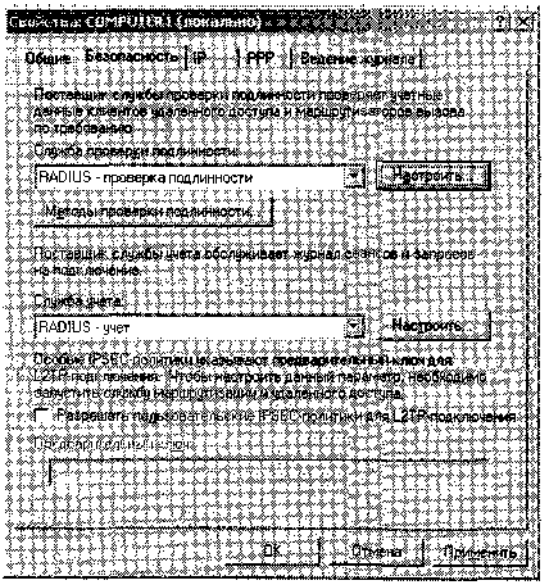


Рис. 10-41. Настройка службы *Маршрутизация и удаленный доступ* на пересылку запросов на доступ на RADIUS-сервер

Определение RADIUS-сервера

После выбора метода аутентификации и учета надо указать конкретный сервер (или серверы) RADIUS, причем для каждой функции серверы задаются одинаково, но по отдельности. Сначала щелкните кнопку **Настроить (Configure),** относящуюся к списку **Служба проверки подлинности (Authentication Provider)** или **Служба учета (Accounting Provider)** — откроется окно **RADIUS - проверка подлинности (RADIUS Authentication)** или **RADIUS - учет (RADIUS Accounting)** со списком RADIUS-серверов в порядке очередности обработки запросов (использование нескольких серверов позволяет повысить отказоустойчивость системы). Щелкните кнопку **Добавить (Add),** чтобы открыть окно **Добавление RADIUS-сервера (Add RADIUS Server)** (рис. **10-42).**

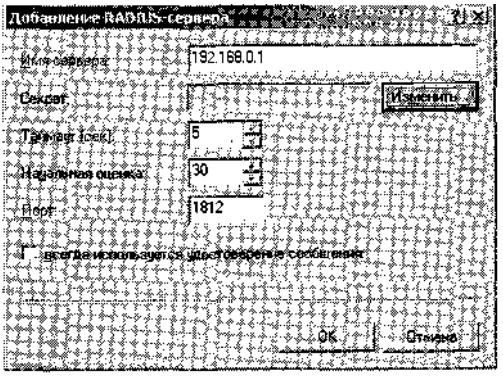


Рис. 10-42. Добавление сервера аутентификации RADIUS

В этом окне задаются имя или IP-адрес RADIUS-сервера, а также следующие параметры.

- **Секрет (Secret)** — это общий ключ в виде текстовой строки, являющийся паролем в виде открытого текста для клиента и сервера RADIUS. Такие ключи позволяют шифровать некоторые атрибуты сообщений, например пароль пользователя. Определяя ключ, помните, что на стороне клиента он должен быть в точности такой же, как на стороне сервера (вплоть до регистра букв), но в каждой паре «клиент — сервер» ключ должен быть свой. При выборе ключа рекомендуется использовать случайную последовательность букв, цифр и символов длиной не менее 22 знаков.
- **Таймаут (сек) [Time-Out (Seconds)]** — время, в течение которого RADIUS-клиент ожидает ответ от RADIUS-сервера до признания, что попытка подключения неудачна.
- **Начальная оценка (Initial Score)** — число, присваиваемое конкретному RADIUS-серверу и определяющее порядок выбора клиентом RADIUS-серверов из группы.
- **Порт (Port)** — UDP-порт, используемый для протокола RADIUS. Стандартными для RADIUS считаются UDP-порт 1812 — для аутентификации и UDP-порт 1813 — для учета. Однако по умолчанию многие серверы удаленного доступа используют для тех же целей порты 1645 и 1646 соответственно. Поэтому надо убедиться, что в параметрах IAS и сервера удаленного доступа указаны одинаковые номера портов.
- **Всегда используется удостоверение сообщения (Always Use Message Authenticator)** — параметр, действующий при добавлении сервера аутентификации RADIUS. Атрибут *проверки подлинности сообщения RADIUS* (RADIUS Message Authenticator) является]УШ5-хэшем всего сообщения RADIUS. В качестве ключа шифрования используется

общий секрет. Если *Атрибут проверки подлинности сообщения* (Message Authenticator) включен, хэш проверяется и в случае неудачи RADIUS-сообщение отклоняется. Если параметры клиента требуют применения этого атрибута, а он отсутствует, RADIUS-сообщение отклоняется.

- **Сообщения RADIUS о включении/отключении учета (Send RADIUS accounting On and accounting Off messages)** — параметр, заставляющий службу маршрутизации и удаленного доступа отправлять RADIUS-серверу сообщения о включении/отключении учета при запуске и остановке этой службы. Такие сообщения появляются только при добавлении сервера учета RADIUS.

Настройка RADIUS-сервера

Для настройки RADIUS-сервера сначала требуется установить элемент *Служба проверки подлинности в Интернете* (Internet Authentication Service Windows) компонента *Сетевые службы Windows* (Windows Networking Services). После установки IAS настраивают в консоли *Служба проверки подлинности в Интернете* (Internet Authentication Service) (рис. 10-43), доступной из меню **Администрирование (Administrative Tools).**

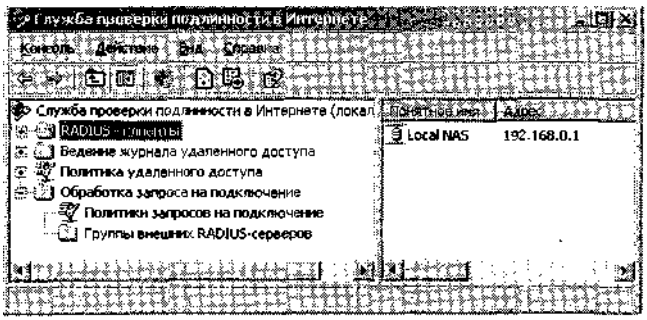


Рис. 10-43. Консоль IAS

Регистрация IAS-сервера

При развертывании IAS-сервера первым делом следует зарегистрировать его в Active Directory. При этом компьютер с IAS-сервером присоединяется к локальной группе безопасности *Серверы RAS и IAS* (RAS and IAS Servers) домена, в которую входит данный компьютер. Членам этой группы разрешается читать атрибуты удаленного доступа учетных записей пользователей.

Определение IAS-клиентов

В консоли IAS нужно перечислить всех RADIUS-клиентов, пересылающих запросы на доступ локальному IAS-серверу. Чтобы создать нового RADIUS-клиента, в дереве консоли *Служба проверки подлинности в Интернете* (Internet Authentication Service) щелкните папку **RADIUS-клиенты (RADIUS. Clients)** правой кнопкой и выберите **Новый RAS-клиент (New RADIUS Client). В** окне мастера нужно задать понятное имя Подключения (в виде отображаемого имени или IP-адреса), общий секрет, заданный для пары клиент — сервер и (при необходимости) атрибут проверки подлинности сообщения.

Подготовка к экзамену Конфигурацию RADIUS-сервера можно сохранять, восстанавливать и переносить с помощью утилиты командной строки Netsh в контексте AAAA. Сначала с помощью команды:

Netsh aaaa show config >*[имя файла]*.txt

выгрузите в файл сценария полную информацию о конфигурации IAS-сервера. Затем записанную в файле сценария конфигурацию можно установить на определенном IAS-сервере, исполнив на целевом компьютере команду:

Netsh exec *[путь]\[имя файла]*.txt.

Лабораторная работа. **Развертывание RADIUS-сервера**

Приведенные ниже упражнения помогут вам научиться настраивать IAS для поддержки аутентификации и авторизации удаленного доступа по запросам, поступающим в службу *Маршрутизация и удаленный доступ*.

Упражнение 1. Настройка RADIUS-клиента

Вы установите службу *Маршрутизация и удаленный доступ* на Computerl и сконфигурируете ее в качестве RADIUS-клиента.

1. Вставьте в дисковод Computerl установочный компакт-диск Windows Server 2003.
2. Войдите с Computerl в Domainl как *Администратор* (Administrator).
3. С помощью компонента *Установка и удаление программ* (Add Or Remove Programs) и *Мастера компонентов Windows* (Windows Components Wizard) установите компонент *Служба проверки подлинности в Интернете* (Internet Authentication Service), входящий в состав *Сетевых служб Windows* (Windows Networking Services).
4: В дереве консоли *Маршрутизация и удаленный доступ* (Routing and Remote Access) щелкните узел **COMPUTER1 (локально) [COMPUTER1 (Local)]** правой кнопкой и выберите **Свойства (Properties).**
5. На вкладке **Безопасность (Security)** окна **Свойства: COMPUTER1 (локально) [COMPUTER1 (Local) Properties]** в списке **Служба проверки подлинности (Authentication Provider)** выберите **RADIUS - проверка подлинности (RADIUS Authentication).**
6. Щелкните соответствующую выбору кнопку **Настроить (Configure).** Откроется окно **RADIUS — проверка подлинности (RADIUS Authentication).**
7. Щелкните кнопку **Добавить (Add).** Откроется окно **Добавление RADIUS-сервера (Add RADIUS Server).**
8. **В** поле **Имя сервера (Server Name)** введите 192.168.0.1.
9. Щелкните кнопку **Изменить (Change).** Откроется окно **Смена секрета (Change Secret).**

   Внимание! Этот ключ применяется для шифрования данных, которыми обмениваются RADIUS-клиент и RADIUS-сервер. Такой же ключ надо задать и на RADIUS-сервере. В реальной обстановке следует задавать ключ, состоящий из случайного набора букв, цифр и символов длиной не менее 22 знаков. В данном упражнении достаточно простого ключа.

10. В полях **Новый секрет (New Secret)** и **Подтвердить новый секрет (Confirm New Secret)** введите пароль.
11. В окне **Смена секрета (Change Secret)** щелкните **OK.**

12. В окне **Добавление RADIUS-сервера (Add RADIUS Server)** щелкните OK.
13. В окне **RADIUS - проверка подлинности (RADIUS Authentication)** щелкните OK.
14. В окне **Свойства: COMPUTER1 (локально)** выберите в списке **Служба учета (Accounting Provider)** значение **RADIUS - учет (RADIUS Accounting).** Этот параметр служит для переноса входа в удаленную систему на RADIUS-сервер. Повторите пп. 6—13, чтобы настроить сервер учета.
15. В окне **Свойства: COMPUTER1 (локально)** щелкните OK. Информационное окно известит, что для активизации нового провайдера аутентификации следует перезапустить службу *Маршрутизация и удаленный доступ*.
16. Щелкните OK. Информационное окно сообщит, что для активизации нового провайдера учета следует перезапустить службу *Маршрутизация и удаленный доступ*.
17. Щелкните OK.
18. Из командной строки исполните следующую команду:

    net stop RemoteAccess

19. После появления сообщения об остановке службы *Маршрутизация и удаленный доступ* исполните команду:

    net start RemoteAccess

Упражнение 2. Настройка RADIUS-сервера

Вы настроите IAS на Computerl для создания связи с настроенным в предыдущем упражнении RADIUS-клиентом.

1. Войдите с Computerl в Domainl *пак Администратор* (Administrator).
2. Выберите **Пуск ^ай)\Администрирование (Administrative Тоок)\Служба проверки подлинности в Интернете (Internet Authentication Service).** Откроется консоль *Служба проверки подлинности в Интернете* (Internet Authentication Service).
3. Выберите значок **Служба проверки подлинности в Интернете (локальная)** и щелкните меню **Действие (Action).** Обратите внимание на команду **Зарегистрировать сервер в Active Directory (Register Server in Active Directory).** Вообще-то RADIUS-серверы, выполняющие аутентификацию для домена, нужно регистрировать в Active Directory. Однако данный компьютер является также и контроллером домена, поэтому он уже автоматически зарегистрирован в Active Directory.
4. В дереве консоли выберите папку **Политика удаленного доступа (Remote Access Policies).** Обратите внимание, что на правой панели отображаются такие же политики, как в консоли *Маршрутизация и удаленный доступ* на локальном компьютере.
5. В дереве консоли щелкните узел **RADIUS-клиенты (RADIUS Clients)** правой кнопкой и выберите **Новый RAS-клиент (New RADIUS Client).**
6. На странице **Имя и адрес (Name and Address)** мастера *Новый клиент RADIUS* (New RADIUS Client) введите:
   - в поле **Понятное имя (Friendly Name)**— Local NAS;
   - в поле **Адрес клиента (Client Address)** — 192.168.0.1.
7. Щелкните **Далее** (Next).
8. На странице **Дополнительные сведения (Additional Information)** в полях **Общий секрет (Shared Secret)** и **Подтвердите общий секрет (Confirm Shared Secret)** введите пароль, определенный в п. 10 предыдущего упражнения.

9). Оставьте значение по умолчанию **RADIUS Standard** параметра **Клиент-вендор (Client-Vendor)** и щелкните **Готово (Finish).**

10. Закройте консоль *Служба проверки подлинности в Интернете* и выйдите из системы Computer 1.

Упражнение 3 (дополнительное). Проверка конфигурации RADIUS

Вам предстоит проверить созданную конфигурацию RADIUS путем подключения по телефонной линии к Domainl с Computer2. Это упражнение выполняется только при наличии отдельных телефонных линий для Computerl и Computer2.

1. На Computer2 нажмите сочетание клавиш Ctrl+Alt+Del, чтобы открыть окно **Вход в Windows (Log On To Windows).**
2. Установите флажок **С использованием удаленного доступа (Log On Using Dial-Up Connection).**
3. **В** поле **Пользователь (User Name)** введите user1.
4.. В поле **Пароль (Password)** введите пароль учетной записи Userl.
5. В списке **Домен (Log** On To) выберите **DOMAIN1** и щелкните OK. Откроется окно **Сетевые подключения, (Network Connections).**
6. **В** списке **Выберите сетевое подключение (Choose a Network Connection)** выберите **MyCompany.** Щелкните кнопку **Подключить (Connect).** Появится окно **Подключение к MyCompany (Connect MyCompany).**
7. Проверьте наличие в соответствующих полях учетных данных для Userl и щелкните **Вызов (Dial).**

   Пока идет подключение, отображается информационное окно **Установка связи с MyCompany (Connecting MyCompany).** После двух сигналов *Служба маршрутизации и удаленного доступа* отвечает на вызов Computer2. Сначала выполняется аутентификация и авторизация подключения удаленного доступа, а после этого — аутентификация и авторизация реквизитов для входа в домен. Процедура входа завершена. Вы успешно вошли в домен с помощью RADIUS-сервера.
8. Выйдите из системы Computer2.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Назовите два основных типа RADIUS-клиентов в составе Windows Server 2003.
2. В.чем состоит различие политик удаленного доступа и политик запроса на подключение на компьютере с IAS?
3. Как перенести конфигурацию IAS-сервера на другой компьютер?

Резюме

- *Служба проверки подлинности в Интернете* (Internet Authentication Service, IAS) — реализация корпорацией Microsoft RADIUS-сервера и RADIUS-прокси. Ее основное назначение — централизованное выполнение аутентификации, авторизации и входа в систему удаленных пользователей.
- В обычной реализации IAS/RADIUS-сервера несколько серверов удаленного доступа под управлением службы *Маршрутизация и удаленный доступ* пересылают запро-

сы доступа на RADIUS-сервер. Затем RADIUS-сервер запрашивает у контроллера домена аутентификацию и применяет к запросам на подключение политики удаленного доступа.

- *Службу проверки подлинности в Интернете* (Internet Authentication Service) можно развернуть как RADIUS-прокси. В таком варианте серверы удаленного доступа передают аутентификацию и учет LAS-серверу, который, будучи теперь сконфигурирован как RADIUS-прокси, пересылает эти сообщения группе RADIUS-серверов. Этот механизм позволяет более равномерно распределять запросы на доступ или дает возможность провайдеру внешних сетевых ресурсов ретранслировать запросы на доступ соответствующим организациям.

Пример из практики

Вас пригласили оказать помощь при развертывании службы удаленного доступа для сотрудников компании Lucerne Publishing. Объясните, как в каждом описанном ниже случае вы будете настраивать соответствующее средство удаленного доступа.

1. Нужно предоставить десяти сотрудникам Lucerne Publishing специальный доступ по телефонной линии. На деле, их аутентификация сводится к проверке телефонных (домашних) номеров, с которых поступает вызов. Ни имя пользователя, ни пароль указывать не требуется. Как реализовать такую конфигурацию?
2. В Lucerne Publishing уже установлена VPN на базе PPTP, но нужно избавить пользователей, входящих в домен компании, от повторного ввода имени и пароля. Что следует сделать, чтобы пользователи не вводили свои учетные данные и в окне **Вход в Windows (Log On To Windows),** и в окне подключения к VPN? Какие протоколы аутентификации можно задействовать в этом VPN-подключении?
3. Для отдельных сотрудников Lucerne Publishing надо предусмотреть возможность подключаться к сети компании по нескольким телефонным линиям, причем это правило не распространяется на остальной персонал. При этом упомянутые сотрудники могут подключаться не более чем по двум телефонным линиям, а когда загрузка подключения опускается ниже 40% пропускной способности канала более чем на 2 минуты, одна из телефонных линий отключается. Как реализовать такую конфигурацию?

Практикум по устранению неполадок

На этом практикуме вы восстановите неправильно установленную *Службу проверки подлинности в Интернете* (Internet Authentication Service).

1. Войдите с Computerl в Domainl как *Администратор* (Administrator).
2. В командной строке исполните команду `netsh aaaa dump >iasconf ig. txt`, которая создаст файл сценария iasconfig.txt с текущей конфигурацией LAS.
3. Откройте консоль *Служба проверки подлинности в Интернете* (Internet Authentication Service) и выберите узел **Политика удаленного доступа (Remote Access Policies).**
4. **В** правой панели щелкните политику **Telecommuters** правой кнопкой и выберите **Удалить (Delete).**
5. **В** информационном окне подтвердите удаление щелчком Да (Yes).

6. Закройте консоль **Служба проверки подлинности в Интернете.**
7. **В** окне командной строки исполните команду netsh exec iasconfig, txt — она выполнит сценарий, сохраненный в файле iasconfig.txt.
8. Откройте консоль IAS и выберите узел **Политика удаленного доступа.** Вы увидите, что политика *Telecommuters* восстановлена.
9. Выйдите из системы Computerl.

Резюме главы

- Серверы удаленного доступа со *Службой маршрутизации и удаленного доступа* (Routing and Remote Access) должны предоставлять IP-адреса клиентам удаленного доступа либо через DHCP-сервер, либо из статического пула адресов. Обычно клиенты получают адреса в той же логической подсети, что и компьютеры, обслуживаемые сервером удаленного доступа.
- Сначала выполняется аутентификация подключений удаленного доступа, а потом они проходят авторизацию. Аутентификация удаленного доступа осуществляется по протоколам аутентификации, в которых шифруются посылаемые по сети имя и пароль пользователя. Некоторые протоколы аутентификации (EAP-TLS, MS-CHAP v2 и MS-CHAPvl) шифруют также данные подключения.
- При подключении применяется наиболее безопасный метод аутентификации, поддерживаемый клиентом, сервером и политикой удаленного доступа, применяемой к подключению.
- Авторизация удаленного доступа происходит сначала путем поверки свойств телефонного подключения учетной записи пользователя, а затем применения к подключению первой подходящей политики.
- При удаленном подключении к домену вход в домен совершается отдельно и только после выполнения аутентификации и авторизации подключения удаленного доступа.
- Для получения доступа через сервер удаленного доступа его нужно сконфигурировать как маршрутизатор, а в свойствах сервера со службой *Маршрутизация и удаленный доступ* надо задать параметр **Разрешить IP-маршрутизацию (Enable IP routing).**
- Виртуальные частные сети (VPN) — это сети, имитирующие локальную сеть, но физически пролегающие через Интернет. При удаленном доступе по VPN выполняется аутентификация и авторизация учетной записи пользователя. В VPN по схеме «маршрутизатор — маршрутизатор» (экстрасеть) выполняется аутентификация и авторизация маршрутизаторов.
- Обычно VPN-туннели на основе PPTP проще в развертывании, но менее безопасны, чем аналогичные туннели на базе протоколов L2TP/IPSec с использованием сертификатов.
- *Служба проверки подлинности в Интернете* (Internet Authentication Service, IAS)— это RADIUS-сервер, реализованный компанией Microsoft. Основное назначение RADIUS-сервера — централизованно выполнять аутентификацию, авторизацию и вход в систему удаленных пользователей.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Будьте готовы рассказать о возможностях и ограничениях всех протоколов аутентификации, поддерживаемых Windows Server 2003.
- Будьте готовы описать различные этапы аутентификации авторизации удаленного доступа. Помните, при каких условиях разрешается подключение удаленного доступа.
- Вы должны уметь назвать параметры настройки в свойствах телефонного подключения учетной записи пользователя.
- Будьте готовы перечислить параметры настройки в профиле политики удаленного доступа.
- Вы должны понимать различие между типами VPN — PPTP и L2TP/IPSec.
- Будьте готовы описать функциональные различия между клиентами, серверами и RADIUS-прокси. Расскажите о ситуациях, в которых применяют RADIUS-серверы и RADIUS-прокси.

Основные термины

3DES (Triple Data Encryption Standard) — алгоритм самого безопасного шифрования данных, применяемый в Ь2ТР/1Р8ес-подключениях.

DES (Data Encryption Standard) — алгоритм 56-разрядного шифрования данных, применяемый в Ь2ТР/1Р8ес-подключениях.

MPPE (Microsoft Point-to-Point Encryption) — реализация семейства алгоритмов шифрования Rivest-Shamir Adleman (RSA) RC4, применяемая для шифрования данных совместно с протоколами аутентификации MS-CHAP (vl и v2) и EAP-TLS. Используется и для шифрования данных VPN-подключений совместно с PPTP.

RADIUS (Remote Authentication Dial-In User Service) — служба, обеспечивающая централизованную аутентификацию и авторизацию. RADIUS-сервер, реализованный Microsoft, называется *Служба проверки подлинности в Интернете* (Internet Authentication Service)

Вопросы и ответы

Занятие 1. Закрепление материала

1. Сервер удаленного доступа настроен на предоставление адресов клиентам удаленного доступа DHCP-сервером. Однако у некоторых клиентов удаленного доступа появляются APIPA-адреса. Назовите две возможные причины такого поведения.
   Правильный ответ: в сегменте сети нет DHCP-сервера, а DHCP-агент ретрансляции не сконфигурирован. При запуске сервера со службой Маршрутизация и удаленный доступ (Routing and Remote Access) в области DHCP-сервера отсутствовали 10 свободных адресов.

2. Какой протокол аутентификации необходим для поддержки смарт-карт?
   Правильный ответ: EAP-TLS.
3. Какие протоколы аутентификации обеспечивают шифрование данных?
   Правильный ответ: EAP-TLS, MS-CHAP V2 и MS-CHAPvl.

Занятие 2. Закрепление материала

1. В сети Windows Server 2003 новый домен создается по умолчанию в смешанном режиме Microsoft Windows 2000. Чем в данном случае отличается параметр **Разрешить доступ (Allow Access)** в окне свойств телефонного подключения учетной записи пользователя от такого же параметра в других серверных средах?

   Правильный ответ: в смешанном режиме Microsoft Windows 2000 параметр Разрешить доступ (Allow Access) не переопределяет набор разрешений доступа в политике удаленного доступа. В других серверных средах этот параметр берет верх над разрешениями, заданными в политике удаленного доступа.
2. Предположим, что успешно выполнена аутентификация удаленного подключения, в свойствах удаленного подключения данной учетной записи установлено значение **Разрешить доступ (Allow Access),** а в первой подходящей политике удаленного доступа определено разрешение **Предоставить разрешение на удаленный доступ (Grant Remote Access Permission).** В чем может быть причина того, что удаленный клиент все равно не в состоянии подключиться к удаленному серверу?

   Правильный ответ: установлению подключения препятствуют ограничения, заданные в профиле политики удаленного доступа, например разрешение телефонного подключения только в определенное время.
3. Каким образом настроить на удаленном сервере 128-разрядное шифрование телефонных подключений?

   Правильный ответ: в профиле применимых политик удаленного доступа отключите все параметры уровней шифрования, кроме параметра Стойкое шифрование (MPPE 128-бит) [Strongest Encryption (MPPE 128-Bit)].

Занятие 3. Закрепление материала

1. **В** чем разница между сертификатами, применяемыми в протоколе аутентификации EAP-TLS и в VPN-протоколе L2TP/IPSec?

   Правильный ответ: при аутентификации по протоколу EAP-TLS проверяются сертификаты пользователей. При аутентификации по протоколу L2TP/IPSec VPN проверяются сертификаты компьютеров.
2. Пользователи иногда испытывают трудности с подключением к VPN-серверу, причем жалобы обычно поступают при высокой загруженности сети, то есть дело не в ошибочном адресе. Какова наиболее вероятная причина неполадки?

   Правильный ответ: определено недостаточное число VPN-портов для одновременного обслуживания такого количества пользователей в период повышенной загрузки сети.
3. Почему считается, что предварительные ключи в IPSec не обеспечивают должную безопасность обмена данными?

   Правильный ответ: предварительные ключи передаются по сети в незашифрованном виде (открытым текстом).

Занятие 4. Закрепление материала

1. Назовите два основных типа RADIUS-клиентов в составе Windows Server 2003.
   Правильный ответ: первый тип — это сервер удаленного доступа под управлением службы Маршрутизация и удаленный доступ. Второй тип — это RADIUS-прокси под управлением Службы проверки подлинности в Интернете.
2. **В** чем различие политик удаленного доступа и политик запроса на подключение на компьютере с IAS?
   Правильный ответ: Политики удаленного доступа служба IAS применяет, когда выступает в роли RADIUS-сервера. В этом случае к подключениям применяются разрешения, ограничения или иные атрибуты. Политики запроса подключения служба применяет, когда он выступает в роли RADIUS-прокси. В такой ситуации политики запроса на подключение позволяют рассортировать подключения и перенаправления в соответствующую группу RADIUS-серверов.
3. Как перенести конфигурацию IAS-сервера на другой компьютер?
   Правильный ответ: сначала с помощью команды Netsh aaaa show config >*[имя файла], txt* полная конфигурация IAS-сервера записывается в файл сценария. Затем сохраненную конфигурацию можно развернуть на произвольном IAS-сервере командой Netsh **exec** *Iпуть]\[имя_файла]. txt.*

Пример из практики

Вас, в качестве консультанта, пригласили развернуть службы удаленного доступа для сотрудников компании Lucerne Publishing. Объясните, как в каждом конкретном случае, приведенном ниже, вы будете настраивать соответствующее средство удаленного доступа.

1. Нужно предоставить десяти сотрудникам Lucerne Publishing специальный доступ по телефонной линии. На деле, их аутентификация сводится к проверке телефонных (домашних) номеров, с которых поступает вызов. Ни имя пользователя, ни пароль указывать не требуется. Как реализовать такую конфигурацию?
   Правильный ответ: создайте политику удаленного доступа. При настройке условия политики выберите в качестве атрибута Calling-Station-ID. Введите номер домашнего телефона первого сотрудника. В эту же политику добавьте аналогичные условия для остальных 9 сотрудников. Настройте политику на предоставление доступа подключению, соответствующему условиям политики. Измените профиль политики, чтобы разрешить доступ без аутентификации. Завершив настройку политики, убедитесь, что в свойствах сервера разрешен доступ без аутентификации.
2. **В** Lucerne Publishing уже установлена VPN на базе PPTP, но нужно избавить пользователей, входящих в домен компании, от повторного ввода имени и пароля. Что следует сделать, чтобы пользователи не вводили свои учетные данные и в окне **Вход в Windows (Log On To Windows),** и в окне подключения к VPN? Какие протоколы аутентификации можно задействовать в этом VPN-подключении?
   Правильный ответ: проинструктируйте сотрудников, чтобы они в свойствах VPN-подключения на вкладке Безопасность (Security) установили флажок Использовать автоматически имя входа и пароль из Windows (и имя домена если существует) [Automatically Use My Windows Logon Name And Password (And Domain If Any)]. В этой ситуации возможно использовать только протоколы MS-CHAPvl и MS-CHAPv2.

3. Для отдельных сотрудников Lucerne Publishing надо предусмотреть возможность подключаться к сети компании по нескольким телефонным линиям, причем это правило не распространяется на остальной персонал. При этом упомянутые сотрудники могут подключаться не более чем по двум телефонным линиям, а когда загрузка подключения опускается ниже 40% пропускной способности канала более чем на 2 минуты, одна из телефонных линий отключается. Как реализовать такую конфигурацию? **Правильный ответ: создайте две группы безопасности Windows, соответствующие двум перечисленным группам сотрудников. Создайте две политики удаленного доступа, по одной на каждую группу безопасности Windows. В профиле первой политики отмените разрешение для многоканальных подключений, а в профиле второй, напротив, включите разрешение для многоканальных подключений, максимальное число портов установите равным 2, загруженность — 40% и время — 2 минуты.**

ГЛАВА 11

Управление безопасностью сети

Темы экзамена

- Развертывание процедур администрирования сетевой безопасности:
  - определение базовых параметров безопасности и аудита с применением шаблонов безопасности;
  - реализация принципа наименьших привилегий.
- Мониторинг безопасности сетевых протоколов. Используемые средства: конс'оль *Монитор IP-безопасности* (IP Security Monitor) и вспомогательные инструменты Kerberos.
- Устранение неполадок безопасности сетевого протокола. Используемые средства: консоли *Монитор IP-безопасности* (IP Security Monitor), *Просмотр событий* (Event Viewer) и *Сетевой монитор* (Network Monitor).

В этой главе

Отсутствие стратегии обеспечения безопасности сети сводит на нет все остальные усилия. Все тщательно продуманные и аккуратно реализованные системы можно погубить или лишить работоспособности атакой «отказ в обслуживании» или внедрением зловредного ПО. Данные воруются, подменяются, стираются или разрушаются по причине вирусов, неосторожности администратора или целенаправленных атак. Злоумышленник может удаленно управлять вашими компьютерами, изменять Web-сайт компании и т. д.

В этой главе описываются инструменты и методы повышения уровня защищенности сети, развертывания политик безопасности и мониторинга и устранения неполадок протоколов безопасности в сети. Вы научитесь обеспечивать безопасность отдельных систем, распространять защиту до масштаба целого предприятия и не терять контроля над данными в процессе их передачи между компьютерами. Кроме того, здесь описывается одна из важнейших парадигм безопасности — принцип наименьших привилегий.

Общие сведения о протоколах безопасности сети

Эти протоколы используются для управления и защиты аутентификации, авторизации, конфиденциальности, целостности данных и *невозможности отрицания авторства* (nonrepudiation). К основным протоколам безопасности в сетях Windows Server 2003 относятся: Kerberos, новый NTLM (New Technology Local Area Network Manager), IPSec (Internet Protocol Security) и их подвиды. Их поддерживают прочие протоколы сетевого взаимодействия, а их применение регулируется различными параметрами безопасности. В табл. 11-1 перечислены методы обеспечения безопасности и соответствующие им протоколы.

Табл. 1-1. Протоколы безопасности сети

Метод	Цель	Протоколы
Аутентификация (authentication)	Убедиться, что объект является тем, за кого себя выдает	Kerberos (NTLM по умолчанию недоступен, но его можно сконфигурировать для поддержки аутентификации)
Авторизация (authorization)	Определить операции в сети, разрешенные объекту, прошедшему аутентификацию	Kerberos и NTLM
Конфиденциальность (confidentiality)	Не допустить компрометации данных	Компоненты шифрования Kerberos, NTLM и IPSec (для защиты передачи данных, но не для целей аутентификации)
Целостность (integrity)	Убедиться, что получены именно те данные, которые были отправлены источником	Компоненты Kerberos, NTLM и IPSec
Невозможность отрицания авторства (nonrepudiation)	Точно определить, кто отправил и кто принял данные	Kerberos и IPSec

Основное внимание в этом разделе уделяется использованию двух оснасток: *Шаблоны безопасности* (Security Templates) *ж Анализ и настройка безопасности* (Security Configuration and Analysis), которые применяются для настройки параметров протоколов и подсистемы безопасности. Другие разделы этой главы посвящены использованию других инструментов администрирования, мониторинга и обеспечения безопасности протоколов безопасности сети— оснасток *Монитор IP-безопасности* (IP Security Monitor), *Сетевой монитор* (Network Monitor) и *Просмотр событий* (Event Viewer) и утилит Netcap, Netsh, Kerbtray и Klist. Прочие имеющиеся в Windows Server 2003 инструменты защиты в этой главе не рассматриваются.

Применение шаблонов безопасности для администрирования безопасности сети

Задача реализации защиты сервера в сетях Windows разбивается на три подзадачи. Во-первых, надо научиться понимать, какую защиту можно считать качественной. Во-вторых, надо уметь обеспечивать безопасности ИТ-инфраструктуры компании с помощью имеющегося оборудования. И наконец, надо позаботиться о наличии инструментов и методологий для быстрой настройки защиты и понимать, как их использовать и поддерживать.

Прежде всего

Для изучения материалов этой главы необходимо:

- домен Windows Server 2003 с контроллером (Computerl) и рядовым членом домена (Computer2);
- если в предыдущих упражнениях адрес рядового сервера определялся службой DHCP адрес, то сейчас ему нужно назначить статический IP-адрес;
- установить *Сетевой монитор* (Network Monitor);
- компьютер под управлением Microsoft Windows 2000 Professional, который не должен быть членом домена. Если такого компьютера нет, можно исключить рядовой сервер из домена и использовать его (то, что на нем установлена Windows Server 2003 на результат не повлияет).

Занятие 1. Реализация процедур безопасного администрирования сети

Управлять семейством ОС Windows Server 2003 довольно просто — большинство параметров безопасности сети определяется в двух интерфейсах: консолях *Локальная политика безопасности* (Local Security Policy) и *Управление политикой безопасности IP* (IP Security Policy Management). И совершенно не обязательно настраивать параметры безопасности поочередно на каждом компьютере — можно разработать базовую процедуру администрирования безопасности с использованием шаблонов безопасности и консоли *Анализ и настройка безопасности* (Security Configuration and Analysis). Можно применить несколько шаблонов безопасности — отдельно для каждой роли сервера, с использованием командных файлов, а в Windows Server 2003 — с помощью групповой политики. В этом случае все компьютеры домена будут периодически получать информацию о текущей политике безопасности.

Кроме того, администрировать, осуществлять мониторинг и устранять неполадки политик безопасности можно и с помощью встроенных инструментов. Здесь закладывается фундамент такого подхода к управлению безопасностью в масштабе всего предприятия и описываются соответствующие инструменты и процессы, а также формулируются основные аксиомы безопасности. Тем не менее, этот раздел не стоит считать справочником по управлению групповыми политиками и исчерпывающим описанием всех параметров, которые позволяют обеспечить надежную, всеобъемлющую защиту.

Изучив материал этого занятия, вы сможете:

- V реализовать базовую защиту различных ролей безопасности;
- V пользоваться оснасткой *Анализ и настройка безопасности* соответствия сервера политикам безопасности;
- V выбирать подходящие шаблоны для администрирования безопасности;
- V восстанавливать значения параметров безопасности по умолчанию;
- V разработать новый шаблон безопасности, удовлетворяющий особым требованиям;
- V перечислить встроенные инструменты обеспечения безопасности в Windows Server 2003 и описать порядок их применения;
- V реализовать принцип наименьших привилегий с помощью шаблона безопасности.

Продолжительность занятия — около 30 минут.

Общие сведения о протоколах безопасности сети

Эти протоколы используются для управления и защиты аутентификации, авторизации, конфиденциальности, целостности данных и *невозможности отрицания авторства* (nonrepudiation). К основным протоколам безопасности в сетях Windows Server 2003 относятся: Kerberos, новый NTLM (New Technology Local Area Network Manager), IPSec (Internet Protocol Security) и их подвиды. Их поддерживают прочие протоколы сетевого взаимодействия, а их применение регулируется различными параметрами безопасности. В табл. 11-1 перечислены методы обеспечения безопасности и соответствующие им протоколы.

Табл. 1-1. Протоколы безопасности сети

Метод	Цель	Протоколы
Аутентификация (authentication)	Убедиться, что объект является тем, за кого себя выдает	Kerberos (NTLM по умолчанию недоступен, но его можно сконфигурировать для поддержки аутентификации)
Авторизация (authorization)	Определить операции в сети, разрешенные объекту, прошедшему аутентификацию	Kerberos и NTLM
Конфиденциальность (confidentiality)	Не допустить компрометации данных	Компоненты шифрования Kerberos, NTLM и IPSec (для защиты передачи данных, но не для целей аутентификации)
Целостность (integrity)	Убедиться, что получены именно те данные, которые были отправлены источником	Компоненты Kerberos, NTLM и IPSec
Невозможность отрицания авторства (nonrepudiation)	Точно определить, кто отправил и кто принял данные	Kerberos и IPSec

Основное внимание в этом разделе уделяется использованию двух оснасток: *Шаблоны безопасности* (Security Templates) и *Анализ и настройка безопасности* (Security Configuration and Analysis), которые применяются для настройки параметров протоколов и подсистемы безопасности. Другие разделы этой главы посвящены использованию других инструментов администрирования, мониторинга и обеспечения безопасности протоколов безопасности сети — оснасток *Монитор IP-безопасности* (IP Security Monitor), *Сетевой монитор* (Network Monitor) и *Просмотр событий* (Event Viewer) и утилит Netcap, Netsh, Kerbtray и Klist. Прочие имеющиеся в Windows Server 2003 инструменты защиты в этой главе не рассматриваются.

Применение шаблонов безопасности для администрирования безопасности сети

Задача реализации защиты сервера в сетях Windows разбивается на три подзадачи. Во-первых, надо научиться понимать, какую защиту можно считать качественной. Во-вторых, надо уметь обеспечивать безопасности ИТ-инфраструктуры компании с помощью имеющегося оборудования. И наконец, надо позаботиться о наличии инструментов и методологий для быстрой настройки защиты и понимать, как их использовать и поддерживать.

Несомненно, самые важные политики безопасности определяются руководством, а материал позволит вам на основании этих политик определять конкретные параметры безопасности. В прошлом при определении политик безопасности приходилось применять множество инструментов и вносить низкоуровневые коррективы в реестр. Сегодня шаблоны безопасности и возможность их глобального применения с помощью групповой политики позволяют решить третью задачу: быстро развернуть политики безопасности в масштабе предприятия и обеспечить их поддержку. Итак, прежде всего разберемся, что позволяют делать шаблоны.

Оснастка *Шаблоны безопасности*

Оснастка *Шаблоны безопасности* (Security Templates) является одной из стандартных MMC-консолей. По умолчанию в оснастке присутствует определенный набор шаблонов, параметры которых можно определять, кроме того, можно добавлять другие шаблоны. К рекомендованным методам использования шаблонов относятся:

- определение базового уровня защиты для каждой из ролей компьютеров. Роли — это функции, выполняемые компьютерами, например контроллеры домена, файловые серверы и серверы печати, почтовые серверы, серверы баз данных серверы сетевых служб (DHCP, DNS, WINS и др.), Web-серверы, серверы удаленного доступа, «персоналки» и т. п.;
- определение принципов безопасности для основных серверных ролей. Общая для всех принципов конфигурация защиты обычно реализуется в виде *основного* (master) уровня защиты. Характерные для отдельных ролей детали реализуются в виде дополнительных уровней. В типовой сети Windows Server 2003 обычно определяются два основных уровня: для контроллера домена и всех остальных компьютеров;
- реализация основного и дополнительного уровней в шаблонах безопасности;
- применение основных шаблонов ко всем и дополнительных шаблонов — к конкретным компьютерам с помощью инструментов развертывания. Есть несколько способов развертывания шаблонов безопасности, в том числе командные файлы и групповая политика.

Определение основного и дополнительного уровней для шаблонов безопасности

Прежде всего при определении *базового уровня* (baseline) защиты надо понять требования организации к безопасности. Затем выясняют, какие параметры безопасности можно обеспечить с помощью шаблонов безопасности. В основной шаблон включают элементы, общие для всех ролей компьютеров, а в дополнительные — элементы, определяющие разницу между ролями.

Основная задача состоит в определении политики безопасности организации, но в этом разделе описываются параметры, которые можно реализовать' с помощью шаблонов. Дополнительные политики придется реализовывать с применением других инструментов. В табл. 11-2 перечислены все разделы и подразделы шаблона и описано, как они применяются при реализации политики безопасности. Полезно изучить стандартные шаблоны оснастки *Шаблоны безопасности* (Security Templates) — вы узнаете о сотнях доступных параметров настройки безопасности. Надо понимать, что добавлять в шаблон дополнительные элементы и как управлять ими, а также знать, что доступ к прочим параметрам безопасности получают через другие инструменты Windows Server 2003.

Примечание При просмотре шаблонов в оснастке *Шаблоны безопасности* и даже изменении их параметров политики компьютера не изменяются. Чтобы оказать влияние на конфигурацию безопасности, необходимо применить шаблон. В приведенных далее упражнениях вы научитесь загружать, просматривать, изменять, создавать и применять шаблоны безопасности.

Табл. 11-2. Разделы шаблона безопасности

Раздел	Подраздел	Описание
Политики учетных записей (Account Policies)	Политика паролей (Password Policy)	Конфигурация паролей, в том числе минимальная длина, история, сложность и частота использования
	Политика блокировки учетной записи (Account Lockout Policy)	Количество неудачных попыток, после которого учетная запись блокируется, порядок сброса и время между неудачными попытками входа в систему, при котором счетчик неудачных попыток сбрасывается в 0
	Политика Kerberos (Kerberos Policy)	Время жизни билета, период обновления билета, порядок применения ограничения на вход пользователя, погрешность синхронизации часов
Локальные политики (Local Policies)	Политика аудита (Audit Policy)	События безопасности, которые заносятся в журнал безопасности данного компьютера: успешные попытки, неудачные попытки или и те и другие, использование привилегий и изменения политики
	Назначение прав пользователя (User Rights)	Права пользователей и группы на выполнение действий в системе: права на вход в систему, архивирование и восстановление системы и др.
	Параметры безопасности (Security Options)	Включение или отключение параметров безопасности, таких как цифровая подпись данных, имена учетных записей администратора и гостя, доступ к дисководам гибких и компакт-дисков, установка драйверов и приглашения на вход в систему
Журнал событий (Event Log)		Атрибуты, относящиеся к приложениям, к безопасности, а также к журналам системы: максимальный размер журнала, права доступа ко всем журналам, параметры и способы их хранения

Табл. 11-2. *(окончание)*

Раздел	Подраздел	Описание
Группы с ограниченным доступом (Restricted Groups)		Права на управление членством в группах Windows. В управляемых этими политиками группах разрешается обычное добавление и удаление пользователей, но при повторном применении шаблона состав группы заменяется на указанный здесь
Системные службы (System Services)		Определение режима запуска всех системных служб (ручной, автоматический или отключение), а также разрешения на доступ к ним (запуск, остановка, приостановка)
Реестр (Registry)		Разрешения безопасности разделов и параметров реестра. При применении шаблона его параметры заменяют текущие разрешения. Использование этого раздела значительно облегчает управление безопасными ключами, так как разрешения одинаковы в пределах всего домена и их можно быстро вернуть в исходное состояние в случае изменений. Следует заметить, что в этом разделе нельзя создавать или менять существующие параметры и разделы реестра — можно лишь определить новую конфигурацию безопасности для существующих разделов и параметров
Файловая система (File System)		Разрешения безопасности файлов и папок

Шаблоны, доступные в оснастке *Шаблоны безопасности,* по умолчанию хранятся в папке *WINDOWS\Security\Templates.* «Резервный» набор стандартных шаблонов размещается в папке *WINDOWS\Inf,* откуда их при необходимости можно скопировать. Вы также вправе создать новую папку и добавить шаблоны из других источников.

Примечание «Белая книга» «Windows Server 2003 Security» *{http://go.microsoft.com/fwlink/?LinkId=14846)* — превосходный источник шаблонов безопасности, кроме того в ней описан пример применения шаблонов для реализации конкретной стратегии.

В табл. 11-3 описываются шаблоны, поставляемые с Windows Server 2003.

Табл. 11-3. Шаблоны безопасности

Шаблон	Местоположение	Описание
Compatws	*WINDOWS\Security\Templates*	Разрешения для файлов и реестра, обеспечивающие работу унаследованных приложений. Этот шаблон немного снижает планку безопасности
DC security	*WINDOWS\Security\Templates*	Параметры безопасности по умолчанию для контроллера домена (DC)
Hisecdc	*WINDOWS\Security \ Templates*	Обеспечивает более высокий уровень безопасности, чем Securedc, надежнее защищая контроллер домена, повышая уровень безопасности NTLM, отключая дополнительные службы, применяя дополнительную защиту к реестру и файлам. Удаляет всех членов из группы *Опытные пользователи* (Power Users)
Hisecws	*WINDOWS\Security\Templates*	Обеспечивает более высокий уровень безопасности, чем Securewc, надежнее защищая рабочую станцию, включая дополнительную защиту NTLM и удаляя всех членов из группы *Опытные пользователи* (Power Users). Оставляет членство в локальной группе *Администраторы* (Administrators) только группе *Администраторы домена* (Domain Admins) и учетной записи *Администратор* (Administrator)
lesacls	*WINDOWS\Security\Templates*	Применяет разрешения к разделам реестра, относящихся к Microsoft Internet Explorer. Этот шаблон устанавливает разрешения *Полный доступ* (Full Control) и *Чтение* (Read) для группы *Все* (Everyone)
Rootsec	*WJNDOWS\Security\Templates*	Применяет корневые разрешения к системному диску
Securedc	*WINDOWS\Security\Templates*	Укрепляет политики учетных записей. Применяет ограничения LAN Manager
Securews	*WINDOWS\Security\Templates*	Укрепляет локальные политики учетных записей. Применяет ограничения LAN Manager
Setup security	*WINDOWS\Security\Templates*	Представляет параметры безопасности текущей машины на момент установки
Defltsv	WINDOWS\Inf	Применяет шаблон сервера по умолчанию в состоянии на момент установки
Defltdc	WINDOWS\Inf	Применяет шаблон сервера по умолчанию в состоянии на момент установки Active Directory

Определение базовых шаблонов в оснастке *Шаблоны безопасности*

1. Отройте оснастку *Шаблоны безопасности* (Security Templates).
2. Добавьте папку для шаблонов организации.
3. Скопируйте шаблон, чтобы создать новый базовый уровень безопасности организации.
4. Измените шаблон.
5. Сохраните шаблон.
6. При необходимости измените шаблон, отредактировав соответствующий inf-файл.

Совет Старайтесь большинство параметров шаблона настраивать при помощи оснастки *Шаблоны безопасности*. Шаблон представляет собой обычный текстовый файл, однако его синтаксис может быть очень запутанным, а оснастка гарантирует корректность вносимых изменений. Из этого правила есть одно исключение: внесение параметров реестра, которые пока отсутствуют в разделе *Параметры безопасности* (Security Options) шаблона. Чтобы добавить их в шаблон безопасности, разместите информацию о них в разделе шаблона [Registry Values] (см. статью «How to Add Custom Registry Settings to Security Configuration Editor» по адресу *http://support.microsoft.com/?kbid=214752)*.

Использование оснастки *Анализ и настройка безопасности* для применения шаблонов и проверки их соответствия политике безопасности

Создание и изменение шаблонов само по себе никак не влияет на безопасность, пока вы их не примените. Для применения шаблона на локальной машине обычно используют оснастку *Анализ и настройка безопасности* (Security Configuration and Analysis). Она также позволяет сравнивать параметры любого шаблона с параметрами, действующими в настоящее время на компьютере. Польза от этого огромна. По завершении анализа различия между действующей реализацией безопасности и выбранным шаблоном отмечаются в интерфейсе пользователя красным крестом *(x)*. Такое сравнение наглядно показывает, что произойдет в случае применения шаблона.

Но еще полезнее возможность мониторинга безопасности компьютера путем периодического сравнения конфигурации безопасности с базовым шаблоном. Это позволяет выявить несоответствия текущих параметров безопасности базовому шаблону, а также изучить и вернуть систему в исходное состояние. (В упражнениях в конце раздела даются инструкции по использованию оснастки *Анализ и настройка безопасности* для применения шаблона и анализа на соответствие параметров безопасности базовому шаблону.)

Применяя дополнительные шаблоны, надо решить, следует ли очищать базу данных. При очистке базы данных применяются только параметры из нового шаблона. Но если до этого были применены параметры старого шаблона, его удаление из базы не влечет за собой отмену его параметров. Если база не очищается, добавление нового шаблона означает следующее:

- если параметр не определен в новом шаблоне, но определен в старом, его значение остается заданным в соответствии со старым шаблоном;
- если параметр определен в новом шаблоне и не определен в старом, его значение меняется в соответствии с новым шаблоном;
- если параметр определен как в новом, так и старом шаблонах, значение задается в соответствии с новым шаблоном.

Использование команды Secedit для применения шаблонов безопасности

Secedit — программа командной строки, аналог оснастки *Анализ и настройка безопасности,* при этом она обладает дополнительными возможностями. Ниже приводится ее синтаксис, а в табл. 11-4 — полное описание всех параметров.

```
Secedit [\configure /db filename.sdb / [/areas, area name, areaname]
[/cfg filename] [/log filename][/quiet][ | \analyze db filename.sdb /
[/cfg filename][/log filename] [/quiet] | \import /db filename.sdb /
mergedpolicy [/areas area name, areanname] [/cfg filename][/log filename]
[/quiet]| \export db filename.sdb /overwrite [/areas area name, areanname]
[/cfg filename][/log filename]|validate filename [/quiet]| | [\genereate
rollback [/cfg] [/RBK ][/logfile][/quiet]]
```

Табл. 11-4. Синтаксис команды Secedit

Параметр	Описание	Комментарии
Configure	Применяет параметры безопасности шаблона	Никогда не используйте этот параметр без создания информации отката, которая позволит вернуть большинство параметров в предыдущее состояние, если обнаружится, что применяемый шаблон некорректен или вызвал неполадки
Analyze	Сравнивает параметры в шаблоне базы данных с действующими на машине	Используется для аудита параметров безопасности на предмет соответствия политике
Import	Импортирует шаблон в базу данных	Служит для создания базы данных, которая в дальнейшем используется для конфигурирования или анализа. Можно импортировать и проводить конфигурирование и анализ одновременно
Export	Экспортирует шаблон из базы данных	Применяется для создания нового шаблона на основе двух или более существующих шаблонов. Шаблоны просто добавляются в нужном порядке в базу данных, а затем используется команда Export для создания Inf-файла скомбинированного шаблона
Validate	Проверяет синтаксис шаблона	Используется при добавлении параметра в Inf-файл вручную
Generate rollback	Создает шаблон «отката», т. е. такой, что отменяет большинство из параметров примененного шаблона	Всегда создавайте такой шаблон перед применением нового шаблона. Однако надо иметь в виду, что он не меняет списки управления доступом (ACL) файлов и реестра, которые назначены ранее примененным шаблоном

Табл. 11-4. *(окончание)*

Параметр	Описание	Комментарии
Db	Определяет имя создаваемого или используемого файла с базой данных	Желательно указывать полный путь
Cfg	Определяет имя используемого шаблона	Желательно указывать полный путь
Overwrite	Записывает новый шаблон в файле поверх существующего	Используется, если не нужно комбинирования при применении шаблонов. Если старый шаблон в файле уже применен, это не изменит параметры безопасности компьютера, которые не перекрываются новым шаблоном
Log	Указывает файл журнала для регистрации ошибок	Если файл журнала не задан, используется файл по умолчанию, т. е. *WINDOWS\Security\Logs\Scesrv.log*
Quiet	Подавляет вывод на экран любых данных, а также сообщений о ходе работы	Используется в сценариях, когда пользователю незачем знать о выполнении программы
Areas	Применяет только параметры указанных разделов шаблона. Остальные параметры игнорируются	Указываемые разделы: SECURITYPOLICY, GROUP_MGMT (ограниченные группы), USER_RIGHTS, REGKEYS, FILESTORE и SERVICES
Mergedpolicy	Объединяет и экспортирует локальную и доменную политики	Охватывает все параметры безопасности
RBK	Задает имя создаваемого параметра шаблона безопасности	Используется только совместно с параметром */generaterollback*

Далее приводятся примеры использования команды Secedit.

- Применение шаблона XYZ:

```
secedit /configure /db xyz.sdb /cfg xyz.inf / log xyz.log
```

- Создание шаблона отката (xyzrollback) в процессе применения шаблона XYZ:

```
secedit /generaterollback /cfg xyz.inf /rbk xyzrollback.inf /log
xyzrollback.log
```

Дополнительная информация о команде Secedit есть в справочной системе Windows Server 2003.

Параметры шаблона безопасности, влияющие на безопасность сети

Любой шаблон безопасности может иметь сотни параметров, затрагивающих все что угодно, начиная от политики паролей и заканчивая членством в группах и разрешениями на файлы. Параметры могут касаться как локальной, так и сетевой безопасности. Нет смысла перечислять все параметры и их значения, но вам обязательно надо знать о

параметрах, относящихся к безопасности доступа к сети и протоколам. В табл. 11-5 перечислены параметры и указаны разделы шаблона, в которых они находятся.

Табл. 11-5. Параметры, влияющие на сетевую безопасность

Параметр	Раздел шаблона	Описание
Доступ к компьютеру из сети (Access this computer from the network)	Назначение прав пользователя (User Rights)	Определяет, какие пользователи и компьютеры имеют доступ к данному компьютеру
Добавление рабочих станций к домену (Add workstations to a domain)	Назначение прав пользователя (User Rights)	По умолчанию все доменные пользователи имеют право добавить 10 компьютеров в домен
Различные права на вход в систему	Назначение прав пользователя (User Rights)	Это целая группа шаблонов, предусматривающая различные права на вход в систему, в том числе право на локальный вход или право запретить локальный вход
Несколько политик цифрового шифрования или подписания данных безопасного канала	Параметры безопасности (Security Options)	Определяет, как данные защищенного канала передаются по сети. Конечно, всегда хочется достичь наивысшего уровня зашиты, но иногда все же приходится ослаблять требования. Например, старые компьютеры не поддерживают высокую степень защиты, существующей в Windows Server 2003
Несколько политик управления анонимным доступом	Параметры безопасности (Security Options)	Определяют разрешенные варианты анонимного доступа
Не хранить хеш-значений LAN Manager при следующей смене пароля (Do not store LAN Manager hash value on next password change)	Параметры безопасности (Security Options)	Поскольку хэш нового пароля не сохранен, компьютер, использующий только LM не сможет аутентифицировать пользователя
Уровень проверки подлинности LAN Manager (LAN Manager authentication level)	Параметры безопасности (Security Options)	Допустимые версии протокола LM. Незащищенная версия по умолчанию запрещена, и требуется NTLM, NTLMv2 или Kerberos
Две политики, касающиеся безопасности сеансов	Параметры безопасности (Security Options)	Определяют необходимость контролировать целостность и конфиденциальность сообщения, а также шифровать его

Принцип наименьших привилегий

Одна из важнейших концепций разработки и реализации политики безопасности — *принцип наименьших привилегий,* который подразумевает, что ни один из сотрудников и пользователей информационной системы не должен иметь больше привилегий, чем тре-

буется ему для выполнения работы. Этот принцип подразумевает лишение пользователя привилегий и прав доступа при увольнении или смене работы внутри компании. То же справедливо и для всех гостей организации или любых ее ресурсов — общественности, контрактников, временных работников, представителей компаний-партнеров и т. п. Никто, включая системных администраторов и сотрудников службы ИТ, не должен иметь больше прав доступа, чем необходимо для работы.

Существует много способов реализации этого принципа, причем их условно разбивают на две категории: реализуемые с помощью шаблонов безопасности и требующие других механизмов. Это обширная тема, и приведенные далее списки не претендуют на исчерпывающую полноту — они помогут лучше понять сам принцип.

Реализация принципа наименьших привилегий на основе шаблонов безопасности

- Разработать строгую политику паролей с тем, чтобы лишить доступа к системе неавторизованных пользователей.
- Предоставлять пользователям «скупые» права доступа. Сократить их, насколько это возможно, особенно на доступ и вход в систему. Назначать различные права на компьютеры в зависимости от их ролей.
- Использовать параметры безопасности для запрещения доступа и ограничения круга возможных действий.
- Использовать *списки управления доступом* (Access Control List, ACL) файлов и параметров реестра.
- В разделе *Группы с ограниченным доступом* (Restricted Groups) ограничить членство в важных группах.

в В разделе *Системные службы* (System Services) запретить ненужные службы и ограничить круг лиц, которым разрешено управлять активными службами.

- Определить базовый уровень для каждой из ролей компьютера и реализовать его с помощью шаблонов, импортированных в объекты групповой политики в *основных подразделениях* (organizational units).
- Применить всестороннюю стратегию аудита.

Другие методы реализации принципа наименьших привилегий

- Сгруппировать пользователей по ролям, чтобы назначать привилегии и разрешения конкретным ролям.
- Настроить ACL-списки файлов, папок, параметров реестра, объектов каталога и принтеров так, чтобы к ним имели доступ только вполне определенные группы пользователей — те, кому это действительно необходимо.
- Обеспечить физическую защиту серверов. Разрешать доступ только авторизованному персоналу и обеспечить контроль доступа.

а Изучать журналы аудита (и прочие журналы) на предмет выявления необходимости более жесткого ограничения доступа.

- Использовать Web-прокси для ограничения доступа пользователей к внешним ресурсам.
- Использовать брандмауэры для ограничения доступа к внутренним сетям.

Лабораторная работа. **Создание и использование консоли *Анализ и настройка безопасности***

Шаблоны безопасности — мощный инструмент управления сетевой безопасностью. Проще всего использовать его и анализировать политики безопасности с помощью в консоли с оснастками *Шаблоны безопасности* (Security Templates) и *Анализ и настройка безопасности* (Security Configuration and Analysis).

Упражнение 1 .Создание консоли. Применение шаблонов по умолчанию

Вы создадите консоль, которая позволит просматривать, настраивать или копировать шаблоны безопасности, добавлять новые папки для хранения шаблонов, а также применять шаблоны к компьютеру. Работа с шаблонами в консоли никак не повлияет на безопасность компьютера.

- **Создание консоли *Анализ и настройка безопасности*.**

1. Выберите **Пуск (Start)\Выполнить (Run),** в открывшемся окне введите mm с и щелкните ОК.
2. В меню **Консоль (Console)** выберите **Добавить или удалить оснастку (Add/Remove Snap-In).**
3. В одноименном окне щелкните кнопку **Добавить (Add)** (рис. 11-1).

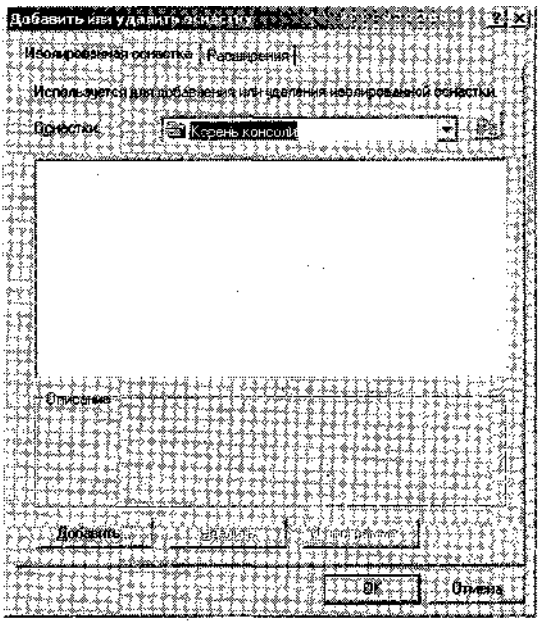


Рис. 11-1. Добавление оснастки

4. В окне **Добавить изолированную оснастку (Add Standalone Snap-In)** выберите **Шаблоны безопасности (Security Templates)** и щелкните кнопку **Добавить (Add)** (рис. 11-2).
5. Выберите оснастку **Анализ и настройка безопасности (Security Configuration and Analysis),** щелкните **Добавить,** а затем **Закрыть (Close).**
6. Щелкните ОК, чтобы добавить выбранные оснастки в консоль.

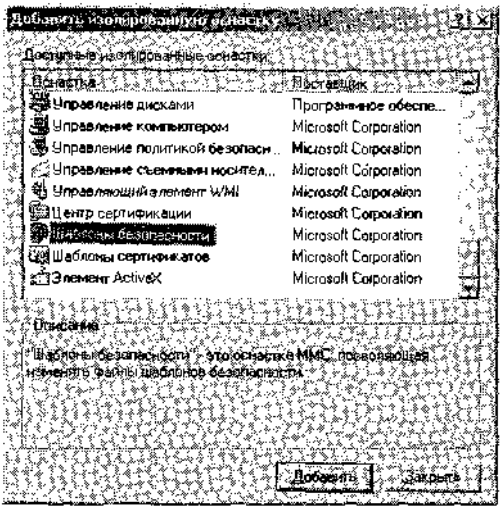


Рис. 11-2. Выбор оснастки *Шаблоны безопасности*

7. Сохраните консоль, выбрав в меню **Консоль** пункт **Сохранить как (Save As). В** поле имени файла введите Security Configuration Management и щелкните **Сохранить (Save).**

- **Подготовка места для нестандартных шаблонов безопасности и добавление их в консоль**

1. В окне *Проводника* создайте новую папку с именем **Custom Templates.**
2. Откройте консоль *Security Configuration Management.*
3. Щелкните **Шаблоны безопасности (Security Templates)** правой кнопкой и выберите **Новый путь для поиска шаблонов (New Template Search Path).**
4. Выберите папку **Custom Templates** и щелкните OK. В консоли *Security Configuration Management* появится новая папка (рис. 11-3).

Примечание Рекомендуется никогда не изменять шаблоны по умолчанию, а новые (или существующие, которые надо изменить) шаблоны размещать в отдельном месте. Таким образом шаблоны по умолчанию сохранятся, а пользовательские шаблоны, которые хранятся отдельно, не составит труда при необходимости сохранить в надежном месте.

Упражнение 2. Создание собственных шаблонов

Вы разработаете собственный шаблон: выберите стандартный шаблон, наиболее полно удовлетворяющий требованиям, скопируете его и внесете необходимые изменения. Параметры шаблона Securews.inf укрепляют безопасность сетевого взаимодействия.

- **Копирование существукнцего шаблона**

1. В консоли *Шаблоны безопасности* (Security Templates) щелкните файл **Securews.inf** правой кнопкой и выберите **Сохранить как (Save As).**
2. **В** качестве места хранения выберите созданную ранее папку **Custom Templates,** а в качестве имени файла — **Testl.** Щелкните **Сохранить (Save).**

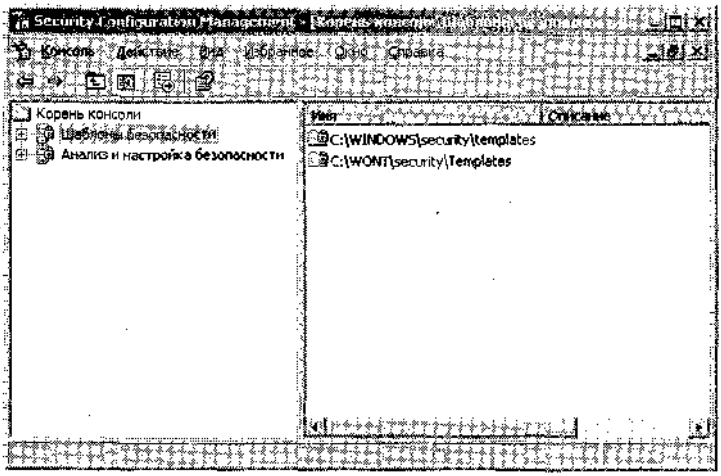


Рис. 11-3. Папка для пользовательских шаблонов

- **Изменение шаблона**

1. Раскройте папку **Custom Templates** в консоли *Security Configuration Management*. Чтобы увидеть шаблон Testl, возможно придется обновить консоль.
2. Раскройте разделы шаблона **Testl.**
3. Раскройте узел **Локальные политики (Local Policies)** и выберите **Параметры безопасности (Security Options)** (рис. 11-4).

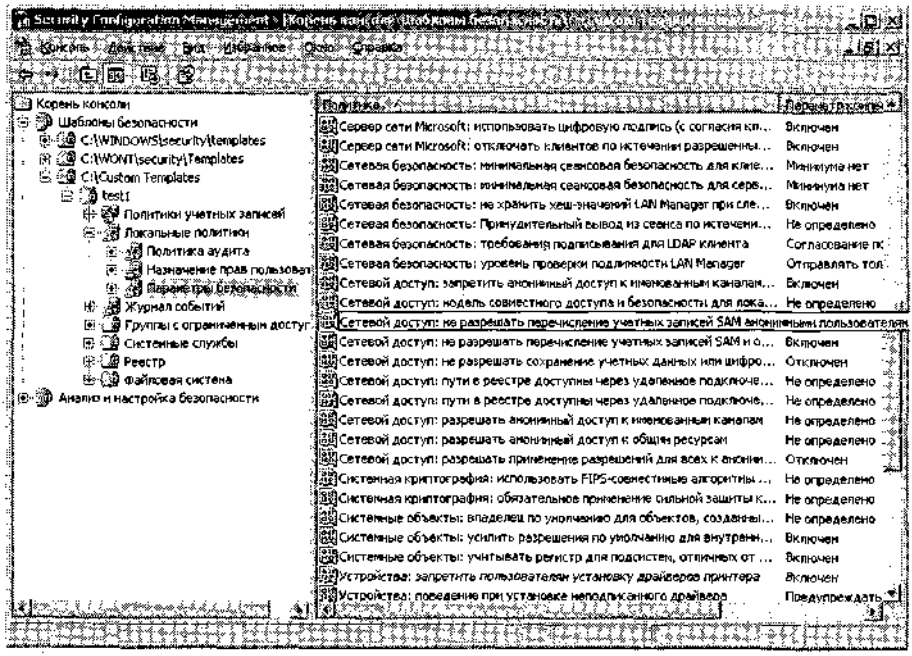


Рис. 11-4. Параметры безопасности

4. Найдите в правой панели разделы **Сетевой доступ (Network Access)** и **Сетевая безопасность (Network Security)** и изучите их значения. Обратите внимание, что значение политики — **Не определено (Not defined);**
5. Дважды щелкните политику **Завершение работы: разрешить завершение работы системы без выполнения входа в систему (Shutdown: Allow System to Be Shut Down Without Having to Log on).** Откроется окно свойств политики (рис. 11-5).
6. Установите флажок **Определить следующий параметр политики в шаблоне (Define This Policy Setting in The Template)** (если он еще не установлен) и отметьте переключатель **Отключен (Disabled).**

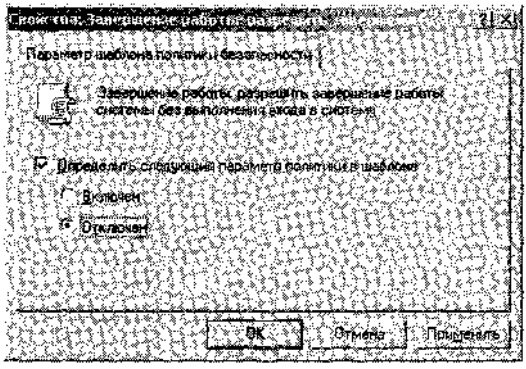


Рис. 11-5. Изменение параметров шаблона

7. Щелкните **OK.**

Примечание Параметры и методы определения зависят от параметра. Во многих политиках надо сначала установить флажок **Определить следующий параметр политики в шаблоне** — лишь после этого можно изменять отдельные параметры.

8. Сохраните внесенные изменения, щелкнув правой кнопкой имя шаблона и выбрав в контекстном меню **Сохранить (Save).**

- **Модификация шаблона путем редактирования М-файла**

1. В окне *Проводника* перейдите в папку **Custom Template.**
2. Дважды щелкните шаблон **Testl,** чтобы открыть его в окне **Блокнот (Notepad).**
3. Изучите раздел **[Registry Values]** (рис. 11-6). Здесь изменяют или добавляют разделы реестра, на которые подействует шаблон в случае его применения.

- **Применение шаблона**

1. Создайте шаблон отката командой:

```
secedit /generaterollback /cfg testl.inf /rbk testlrollback.inf
   /log test1rollback.log
```

Эта команда создает шаблон, который в случае неполадок вернет параметры к состоянию до применения шаблона Testl.inf. Сначала создается шаблон Testlrollback.inf, а затем применяется Testl.inf. Откат значений невозможен для параметров безопасности файлов и реестра, т. е. в случае применения «обратного» шаблона любые изменения, внесенные шаблоном в эти разрешения, не отменятся.

Рис. 11-6. Добавление в Inf-файл разделов реестра, которые будут затронуты при применении шаблона

2. В консоли *Security Configuration Management* щелкните узел **Анализ и настройка безопасности (Security Configuration And Analysis)** правой кнопкой и выберите **Открыть базу данных (Open Database).** База данных не образуется автоматически, поэтому сначала надо ее создать.
3. Введите имя базы данных в текстовое поле **Имя файла (File Name)** и щелкните кнопку **Открыть (Open).** Поскольку в п. 1 создан шаблон отката, то можно без опаски применять созданный нами шаблон.
4. В окне **Импорт шаблона (Import Template)** выберите шаблон **Testl.inf** и щелкните кнопку **Открыть (Open)** (рис. 11-7).
5. Щелкните узел **Анализ и настройка безопасности** правой кнопкой и выберите **Настроить компьютер (Configure Computer Now).**
6. На запрос подтверждения местоположения журнала ошибок щелкните OK. Журнал ошибок позволяет узнать, когда и какие шаблоны применялись к компьютеру.
7. Дождитесь окончания процесса конфигурирования и закройте консоль, не сохраняя ее.

Упражнение 4. Восстановление (откат) после применения шаблона

Может случиться так, что после изменения параметров безопасности обнаруживается, что компьютер стал недоступен из сети или наоборот степень его защиты стала ниже требуемой. Если перед применением шаблона был создан шаблон отката, систему можно вернуть в исходное состояние. Если также надо вернуть разрешения файловой системы и реестра в состояние, в котором они находились после установки, можно применить один из установочных шаблонов по умолчанию. Если этого не нужно, достаточно применить шаблон отката.

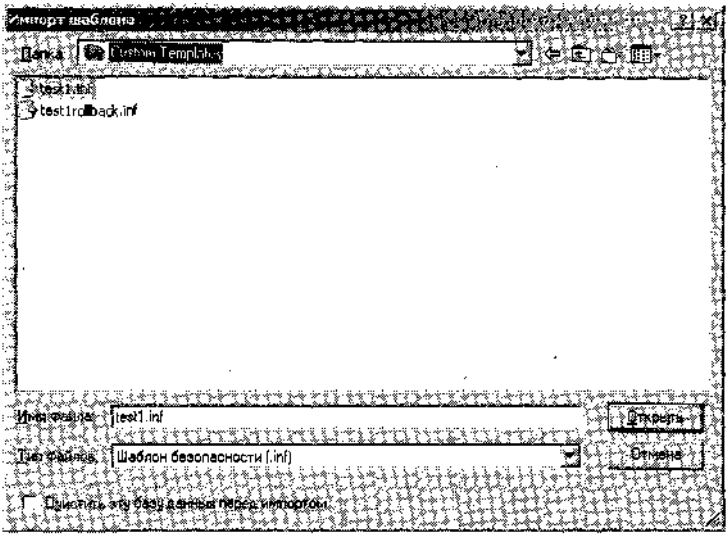


Рис. 11-7. Импорт шаблона

- **Восстановление конфигурации параметров безопасности путем применения шаблона отката**

1. В консоли *Security Configuration Management* (см. упражнение 1) щелкните узел **Анализ и настройка безопасности (Security Configuration And Analysis)** правой кнопкой и выберите **Импорт шаблона (Import Template).**
2. **В** одноименном окне выберите шаблон **TestIroIlback.inf** (рис. 11-8).
3. Установите флажок **Очистить эту базу данных перед импортом (Clear This Database Before Importing)** и щелкните кнопку **Открыть (Open).** Если флажок не установить, будет применена информация из обоих шаблонов.

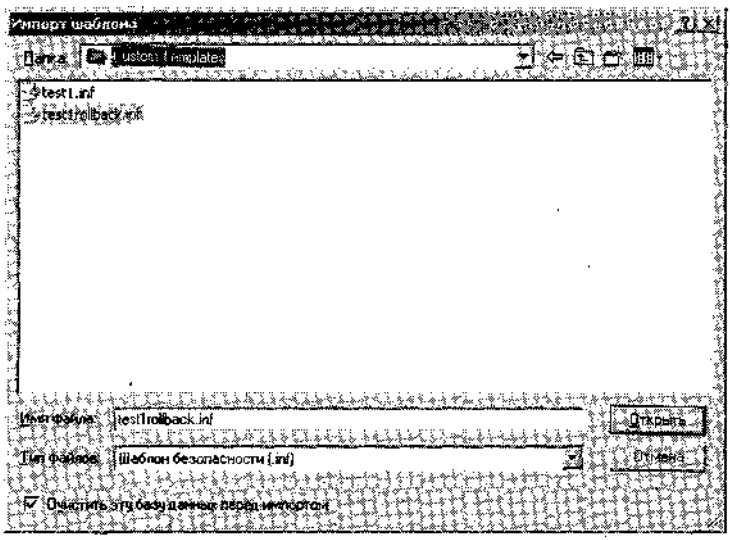


Рис. 11-8. Очистка базы данных

4. Щелкните узел **Анализ и настройка безопасности** правой кнопкой и выберите **Настроить компьютер (Configure Computer Now).**

5. Щелчком OK подтвердите местоположение файла журнала ошибок.
6. Закройте консоль **Security Configuration Management.**

Упражнение 5. Анализ соответствия политике безопасности

При конфигурировании систем часто используют политики безопасности, но затем с них благополучно забывают и при возникновении неполадок оказывается, что никто *ж* помнит, какие значения параметров задавались. С помощью оснастки *Анализ и настройка безопасности* (Security Configuration and Analysis) вы сравните текущие значения параметров с эталонным шаблоном.

1. В консоли *Security Configuration Management* щелкните узел **Анализ и настройка безопасности (Security Configuration And Analysis)** правой кнопкой и выберите **Импорт шаблона (Import Template).**
2. Выберите шаблон **Testl.inf** и щелкните кнопку **Открыть (Open).**
3. Щелкните узел **Анализ и настройка безопасности** правой кнопкой и выберите **Анализ компьютера (Analyze Computer Now).**
4. Щелчком OK подтвердите местоположение файла журнала ошибок. По завершении анализа вы сможете исследовать в консоли параметры базы данных и отличия от политики.
5. Поочередно раскройте каждый из узлов и внимательно ознакомьтесь с изменениями, которые представлены в правой панели (рис. 11-9). Изменения помечены красным крестом. Обратите внимание на столбцы **Параметр базы данных (Database Setting)** и **Параметр компьютера (Computer Setting)** — по ним вы сможете точно определить различия, а также обратите внимание на не проанализированные элементы — возможно, придется изучать их вручную.

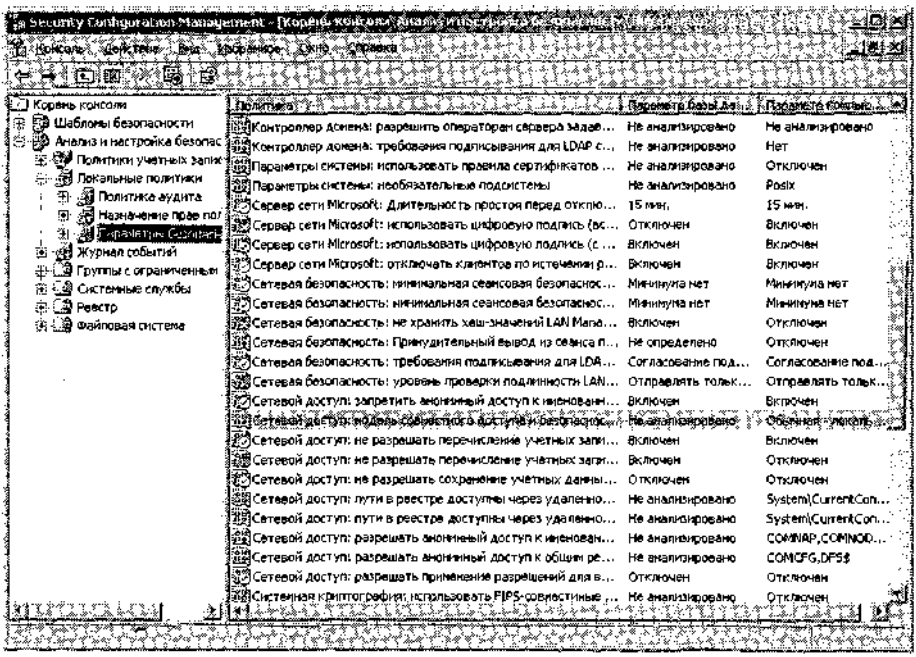


Рис. 11-9. Анализ изменений

6. Закройте консоль.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Надо применить новые параметры реестра на всех серверах сети. Как выполнить задачу с наименьшими усилиями?
2. Какие из приведенных далее параметров можно применить с помощью оснастки *Анализ и настройка безопасности* (Security Configuration and Analysis) и шаблона безопасности? (Выберите все подходящие варианты.)
   a. Пароль должен быть не менее 15 символов.
   b. Группе *Бухгалтеры* (Accountants) надо запретить доступ к этому компьютеру по сети.
   c. Любое сетевое взаимодействие компьютеров Computerl и Computer2 должно выполняться с использованием IPSec.
   d. Необходимо установить следующие корневые разрешения для файлов: уровень доступа *Полный доступ* (Full Control); группа — *Все* (Everyone).
3. Что необходимо предпринять для восстановления «статуса-кво» после применения шаблона безопасности, после которого файловый сервер стал недоступным по сети для всех пользователей? Выберите наиболее эффективный способ.
   a. Локально войти в систему файлового сервера как *Администратор* (Administrator) и применить корневой шаблон безопасности.
   b. Локально войти в систему файлового сервера как *Администратор* (Administrator) и применить шаблон отката, созданный перед применением «некорректного» шаблона безопасности.
   c. Выполнить удаленный вход в систему файлового сервера под учетной записью члена группы *Администраторы предприятия* (Enterprise Admin) и в консоли *Локальная политика безопасности* (Local Security Policy) изменить некорректные (на ваш взгляд) политики прав пользователей.
   d. Выполнить удаленный вход в систему файлового сервера как *Администратор* (Administrator) и применить шаблон отката, созданный на основе шаблона безопасности.

Резюме

- Шаблоны безопасности позволяют сконфигурировать большую часть базовой политики безопасности компьютера, как определено руководством компании.
- Существует возможность сконфигурировать дополнительные шаблоны базового уровня безопасности каждой из ролей компьютеров.
- Шаблоны безопасности можно использовать для анализа соответствия безопасности компьютера политикам. Применяют шаблоны безопасности средствами оснастки *Анализ и настройка безопасности* (Security Configuration And Analysis).
- Утилита командной строки Secedit служит для анализа и настройки параметров безопасности, а также экспорта шаблонов безопасности из базы данных.
- Secedit также позволяет создать шаблон отката, который отменяет все неприятные последствия, причиненные применением некорректного шаблона.

Занятие 2. Мониторинг безопасности протоколов сети

Казалось бы, что, добившись стабильной работы сети, можно расслабиться и почивать на лаврах, но отдыхать рано — самое время заняться мониторингом сетевых протоколов безопасности. Ведь если вы не знаете, как выглядит нормальный трафик, то как сможете выявить в нем аномалии? Как узнаете о грядущих проблемах или атаке злоумышленника? Даже если существующие проблемы никак себя не проявляют и сеть работает устойчиво, гораздо лучше узнать о них как можно раньше, а не когда они материализуются и вызовут крах системы.

Это наилучшее время для изучения утилит и инструментов, которые помогают, когда сеть перестает работать, или когда вице-президент или отдел маркетинга не может войти в домен, или вдруг пропала возможность подключения к бухгалтерской базе данных.

На этом занятии рассказывается об инструментах мониторинга протоколов безопасности сети, как их применять, а по ходу изложения приводятся сведения о самих протоколах.

Изучив материал этого занятия, вы сможете:

- использовать Netsh, чтобы разобраться в работе IPSec;
- использовать Netsh для управления IPSec;
- использовать оснастку *Монитор If-безопасности* для мониторинга трафика IPSec;
- использовать Netcap для записи сетевого трафика;
- понять основы Kerberos;
- использовать оснастку *Сетевой монитор,* чтобы разобраться в работе Kerberos;
- использовать инструменты Kerbtray и Klist для исследования кэша билетов Kerberos.

Продолжительность занятия — около 60 минут.

Основные сведения об IPSec

IPSec — это сложный протокол, который служит для:

- аутентификации и шифрования трафика между двумя компьютерами;
- блокирования определенного входящего и исходящего трафика;
- разрешения определенного входящего и исходящего трафика.

Специфическим особенностям протокола и его функционированию посвящено множество RFC-документов. В них детально описаны стандарты, которых должны придерживаться реализации этого протокола. А это сотни страниц печатного текста.

Примечание Чтобы получить исчерпывающее представление об IPSec вам придется ознакомиться с RFC-спецификациями с номерами 3457, 3456, 3281, 3193, 2857, 2709, 2451 и еще приблизительно 22 документами. Все они есть на сайте *http://www.ietf.org*.

Однако не обязательно слишком глубоко вникать в детали — достаточно базового представления о работе IPSec и умения реализовать политики IPSec в Windows Server 2003 и контролировать его работу по защите трафика. Для этого есть множество инструментов администратора, в том числе:

- оснастка *Монитор IP-безопасности* (IP Security Monitor);
- утилита с графическим пользовательским интерфейсом *Управление политикой безопасности IP* (IP Security Policy Management), существующая в виде оснастки и объекта групповой политики;
- утилита командной строки Netsh;
- утилита командной строки Netdiag;
- журналы событий.

Как работает IPSec

Политики IPSec (IPSec policies) можно рассматривать как набор фильтров пакетов, реализующих политику безопасности IP-трафика. Каждый *фильтр* (filter) описывает определенное действие сетевого протокола. Если входящий или исходящий трафик устройства (компьютера или иного оборудования IP-сети), на котором есть активная политика, удовлетворяет условиям одного из фильтров, соответствующие пакеты блокируются, пропускаются или перед дальнейшей пересылкой между источником и приемником устанавливается IPSec-подключение.

Фильтры могут реагировать на прием или инициализацию определенного протокола, на запрос подключения с (или к) определенного устройства, или на другое действие, определенное протоколом, портом, IP-адресом или диапазоном IP-адресов. Эти фильтры определяются в правилах политики IPSec. Примеры фильтров:

- весь трафик с IP-адреса 192.168.5.77;
- весь трафик по IP-адресу 192.168.5.101;
- весь трафик через порт 23 (порт по умолчанию для протокола telnet);
- трафик с IP-адреса 192.168.6.69, проходящий через порт 23.

Фильтры объединяются в *списки фильтров* (filter lists), которые в свою очередь являются частями правил. Каждое *правило* (rule) определяет *действие фильтра* и расширяемую информацию о конфигурации, определяющую особенности создания IPSec-подключения. Можно настроить следующие действия фильтра: *Разрешить* (Allow), *Блокировать* (Block) и *Согласовать безопасность* (Negotiate Security). Правилам соответствует только одно действие фильтра, но политика может состоять из нескольких правил.

Допустим, требуется принимать Telnet-сеансы, инициированные определенным компьютером и шифровать их. В этом случае надо написать два правила: одно — блокирующее весь telnet-трафик, а второе — пропускающее telnet-трафик с конкретного компьютера. При проверке политики IPSec более «узкое» правило обладает приоритетом. Если telnet-трафик пришел с указанного компьютера, взаимодействие будет разрешено (при условии выполнения остальных условий политики). Входящий трафик, пришедший с любого другого IP-адреса, блокируется общим правилом.

Новые возможности IPSec в Windows Server 2003

IPSec является компонентом ОС и применяется для защиты сетевого взаимодействия в Microsoft Windows 2000/XP Professional/Server 2003. Существует клиент для Microsoft Windows NT 4/98/Me, который доступен для загрузки с Web-страницы *http://www. microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient. asp*
Ниже перечислены новые возможности IPSec.

в Оснастка *Монитор IP-безопасности* (IP Security Monitor) предоставляет больше возможностей, чем утилита Ipsecmon.exe в Windows 2000 (она теперь также доступна в Windows XP Professional и Windows Server 2003).

- Используется более стойкий криптографический алгоритм Диффи-Хеллмана с 2048-битным ключом.

и Удобная утилита командной строки Netsh, которая к тому же предоставляет множество возможностей по конфигурированию, недоступных в оснастке *Управление политикой безопасности IP* (IP Security Policy Management).

- Если настроена безопасность при загрузке компьютера (или фильтр, хранящий состояние), она активизируется и управляет трафиком при запуске. При этом разрешается только исходящий трафик, инициируемый компьютером при запуске, входящий трафик в ответ на исходящие запросы и DHCP-трафик.
- Применяется политика сохранения состояния, если не удается применить локальную политику или IPSec-политики службы каталогов Active Directory.
- Освобожден от фильтрации только IKE-трафик (Internet Key Exchange) — он необходим для установления защищенных подключений.
- Специальные ограничения определяют возможность подключения компьютеров на основании их членства в домене, издателя сертификата или членства в группе компьютеров.
- Имя *центра сертификации* (Certification Authority, CA), или ЦС, можно исключать из запросов на сертификат, чтобы не допустить разглашения информации о доверительных связях с такими объектами, как домены, центры сертификации или компании.
- В локальной IP-конфигурации — DHCP-, DNS- и WINS-сервера — применяется локальная адресация для поддержки динамической адресации.
- Возможность работы IPSec через NAT позволяет ESP-пакетам (Encapsulation Security Payload) проходить через преобразование сетевых адресов, что в свою очередь разрешает UDP-трафик.

в Улучшена интеграция со службой балансировки сетевой нагрузки (Network Load Balancing), что положительно влияет на балансировку нагрузки основанных на IPSec службах виртуальных частных сетей (VPN).

в Обеспечена поддержка оснастки *Результирующая политика* (Resultant Set Of Policy, RSoP) для просмотра существующих параметров политики IPSec

Настройка процесса согласования

Согласование (negotiation) — это процесс определения используемого субпротокола IPSec, а также других особенностей: надежности ключа и используемых криптографических алгоритмов. Далее приводится список параметров, доступных при конфигуриро-

вании политики IPSec. Выбирают варианты с помощью мастеров IPSec или редактируя политику IPSec в оснастке *Управление политикой безопасности IP* (IP Security Policy Management), в групповой политике или с помощью утилиты командной строки Netsh. При использовании Netsh доступны дополнительные параметры. Выполняя задания в конце этого занятия, вы научитесь использовать мастер для создания политики, а также находить нужные элементы в графическом интерфейсе пользователя.

- **Аутентификация** — порядок подтверждения подлинности взаимодействующих компьютеров.
- **Тип подключения** — определение, к каким подключениям применяется политика.
- **Группа Диффи-Хеллмана** — размерность простых чисел, используемых при создании *основного ключа* (master key).
- **Фильтры** — каждый список может содержать несколько фильтров. Среди них фильтры по: протоколу, порту источника, IP-адресу источника, маске источника, имя DNS-сервера источника, порт приемника, имя DNS-сервера приемника, IP-адрес приемника и маска приемника.
- **Действия фильтра** — что произойдет при вызове фильтра.
- **Протокол шифрования IKE** — порядок шифрования 1KE-пакетов.
- **Протоколы целостности IKE** — порядок защиты IKE-пакетов от изменения в процессе передачи.
- Метод **безопасности IKE** — порядок согласования IKE.
- **Правила безопасности IP** — разрешенное число правил.
- **Списки фильтров IP** — разрешенное число списков фильтров.
- **Максимальная безопасности основного ключа** — при необходимости для каждой сессии создается новый основной ключ.
- **Параметр туннеля** — перенаправляется ли трафик по туннелю.

Примечание Многим людям тяжело дается понимание действий фильтров. Им бывает особенно трудно различать *Запрос безопасности* (Request Security) и *Требуется безопасность* (Require Security). При первом варианте система принимает незащищенный трафик, но отвечает всегда с использованием IPSec. Если клиент «не понимает» IPSec, обмен данными прекращается. Это аналогично ситуации, когда вы говорите только по-английски, а ваш собеседник — только по-испански. Вы задаете вопрос, собеседник что-то отвечает, но вы ни слова не понимаете. А когда безопасность требуется, поведение систем другое. Первый компьютер отвечает на не-IPSec запрос с использованием IPSec, но если второй компьютер не может ответить ему по IPSec, первый тоже прекращает использование этого протокола, но обмен данными не прерывает.

Процесс согласования

При наличии активизированной политики IPSec и действующей службы IPSec любой сетевой обмен — входящие и исходящие сообщения — проверяются на предмет соответствия политике IPSec. При обнаружении соответствия, например, когда исходящий трафик по протоколу SMTP отвечает условиям фильтра, фильтр активизируется и выполняется предусмотренное им действие. Если действие фильтра предусматривает *Разрешить* (Allow) или *Блокировать* (Block), трафик обслуживается соответствующим образом, однако в случае варианта *Согласовать безопасность* (Negotiate Security) требуется ряд дополнительных операций.

Обработка делится на два этапа: *основной* (main) и *быстрый* (quick) режимы согласования. В рассматриваемой модели согласования двух компьютеров им назначены имена Red и Blue, а сам процесс схематически показан на рис. 11-10.

1. Запрос активизирует фильтр IPSec.
2. Наступает основной режим согласования (определяются основной ключ и сопоставление безопасности IKE).
3. Завершается согласование пары сопоставлений безопасности (входящего и исходящего) для обмена прикладными пакетами.
4. Прикладные пакеты пересылаются с драйвера TCP/IP на драйвер IPSec.
5. Драйвер IPSec форматирует и криптографическим образом обрабатывает пакеты, а затем направляет их, используя исходящее сопоставление безопасности.
6. Защищенные пакеты пересылаются по сети.
7. Драйвер IPSec на компьютере-приемнике выполняет криптографическую обработку пакетов, прибывающих по входящему сопоставлению безопасности, форматирует их как обычные IP-пакеты и передает в драйвер TCP/IP.
8. Драйвер TCP/IP передает пакеты в приложение.

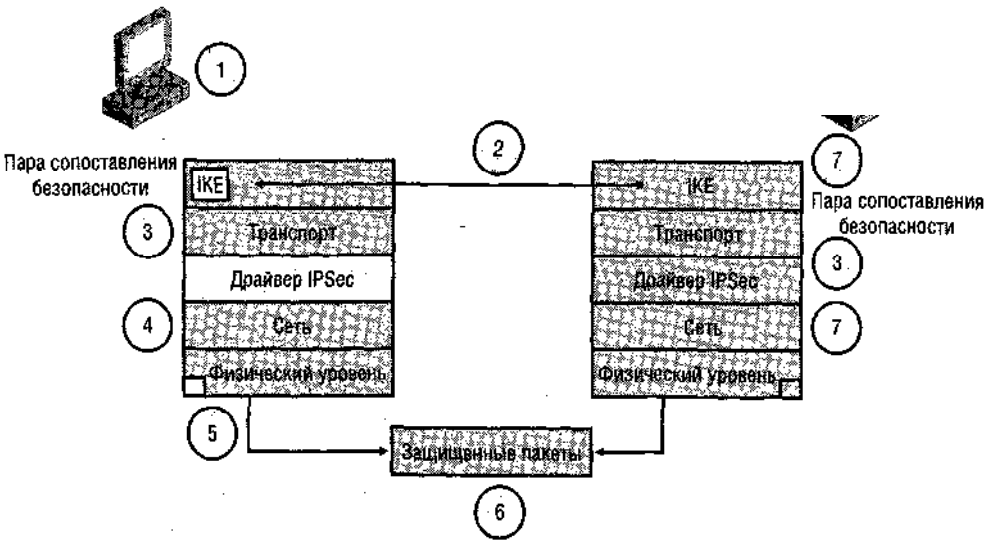


Рис. 11-10. Обработка IPSec

Примечание IKE — это алгоритм согласования первого безопасного *сопоставления безопасности* (Security Association, SA), которое включает аутентификацию, порядок вычисления *основного ключа* (master key) (ключа, на основании которого создаются все ключи сеанса) и сопоставления безопасности IKE. Наиболее примечательно в IKE то, что основной ключ рассчитывается независимо на каждом компьютере. Причем ключи совпадают и никогда не пересылаются по сети. При вычислении ключей используется сложный математический процесс, описанный в RFC 2409 *(http://www.ietf.org/rfc/rfc2409.txt)*.

Далее более подробно описывается основной режим согласования.

1. Информационный пакет пересылается с компьютера Red на компьютер Blue.
2. Драйвер IPSec на Red проверяет свой IP-фильтр исходящих сообщений и выясняет, что пакет удовлетворяет условиям фильтра, а также определяет действие фильтра — *Согласовать безопасность* (Negotiate Secutiry), то есть пакеты надо защитить (зашифровать).
3. Драйвер IPSec уведомляет IKE о необходимости начать согласование.
4. Red проверяет свою политику, регулирующую основной режим (аутентификация, группа Диффи-Хеллмана, шифрование, и целостность), чтобы предложить условия согласования компьютеру Blue.
5. Red направляет первое IKE сообщение с UDP-порта 500 источника на порт 500 приемника.
6. Blue принимает IKE-сообщение об основном режиме согласования с требованием обезопасить процесс согласования. Blue также проверяет IP-адреса источника и приемника на предмет соответствия условиям собственных фильтров IKE. Фильтр IKE обеспечивает требования по безопасности входящий связи от Red.
7. Если параметры защиты, предложенные Red, приемлемы для Blue, основной режим завершается.
8. Оба компьютера согласовывают параметры, обмениваются идентификационной информацией, аутентифицируют друг друга и генерируют основной ключ. Сопоставление IKE установлено.

Примечание Реализованная Microsoft версия IPSec поддерживает делегирование шифрования сетевым интерфейсным адаптерам. Шифрование поддерживает далеко не каждая карта, но есть специализированные устройства, которые обеспечивают эту функцию. Такие платы способны значительно повысить производительность серверов, поддерживающих много IPSec-подключен!ий (одна из таких плат описана в документе *http://www.3com.com/products/proddatasheet/datasheet/3c905b_fx.paj*).

Далее подробно описываются операции быстрого режима.

1. Red выполняет поиск режима IKE в политиках, чтобы определить полную политику. (При согласовании IKE не учитывается номер порта, IP-адрес и другие параметры, которые могли бы инициировать согласование.)
2. Red предлагает свои параметры (криптографический ключ, частоту его смены и др.) и направляет их на компьютер Blue.
3. Blue выполняет свой поиск режима IKE в политиках. Если он находит полное соответствие предложению Red, быстрый режим завершается и создается пара сопоставлений IPSec.
4. Одно сопоставление исходящее, а второе — входящее, каждое идентифицируется по *индексу параметров безопасности* (Security Parameters Index, SPI), который входит в заголовок каждого отправленного пакета. IPSec-драйвер компьютера Red использует выходное сопоставление и подписывает, а при необходимости и шифрует пакеты. Если на компьютере установлены криптоустройства поддержки IPSec, драйвер IPSec только форматирует пакеты. Если же таких средств нет, драйвер самостоятельно и форматирует, и шифрует пакеты.
5. Драйвер IPSec передает пакеты драйверу сетевого адаптера.
6. Драйвер сетевого адаптера направляет дейтаграммы в сеть.
7. Сетевой адаптер Blue принимает (зашифрованные) пакеты из сети.

8. SPI используется для нахождения нужного сопоставления. (Ему соответствует криптографический ключ, необходимый для расшифровки и обработки пакетов.)
9. Если сетевой адаптер поддерживает криптографические операции, он расшифровывает пакеты, которые затем передаются драйверу IPSec.
10. В случае необходимости драйвер IPSec компьютера Blue использует входное сопоставление для нахождения ключей и обработки пакетов.
11. Драйвер IPSec преобразовывает IP-пакеты в обычный формат и передает их драйверу TCP/IP, который в свою очередь пересылает их приложениею-приемнику.
12. IPSec продолжает использовать сопоставления для обработки пакетов. Сопоставления обновляются посредством быстрого режима IKE, пока идет обмен данными между приложениями. Когда сопоставления становятся неактивным, они уничтожаются.
13. Основной режим IKE не уничтожается при простое — его время жизни составляет 8 часов, хотя этот параметр поддается изменению (от 5 минут до 48 часов). Новый трафик инициирует новое согласование быстрого режима. Если истекает срок основного режима IKE, новый IKE-режим создается лишь при необходимости.

Примечание Коммутаторы и маршрутизаторы на пути между компьютерами Red и Blue просто пересылают зашифрованные пакеты их адресату, однако на брандмауэрах или фильтрующих пакеты маршрутизаторах надо разрешить пересылку IPSec-трафика.

Создание политики IPSec

Создать политику IPSec просто, намного сложнее создать такую, что будет делать в точности то, что требуется. Пока мы лишь узнали, *как* работает политика. Вы воспользуетесь полученными знаниями для создания простой политики, блокирующей доступ через порт 80, и еще одной, которая обеспечит шифрование данных при пересылке между двумя компьютерами. Есть два основных инструмента создания политики — это *Монитор IP-безопасности* (IP Security Monitor) и утилита командной строки Netsh. Далее рассказывается, как политика создается в командной строке. Упражнения в конце этого раздела научат вас совместно использовать инструменты с графическим пользовательским интерфейсом и Netsh.

Управление IPSec с помощью Netsh

Netsh — «родная» утилита командной строки в Windows Server 2003, служащая для отображения или изменения локальной или удаленной сетевой конфигурации компьютера под управлением Windows Server 2003. Netsh можно запускать из командного файла или командной строки. Команды Netsh, относящиеся к IPSec, не поддерживаются в других версиях Windows.

Примечание Исчерпывающий список относящиеся к IPSec команд Netsh вы найдете в *Центре справки и поддержки Windows Server 2003* (Windows Server 2003 Help And Support Center). Для этого щелкните **Служебные программы (Tools),** а затем — **Справочник по параметрам командной строки (Command Line Reference).** Многие из команд выглядят сложными, но можно не указывать все параметры. Значения, которые совпадают с определенными по умолчанию, указывать не обязательно. Например, совсем не обязательно использовать слово Kerberos, если именно эту форму аутентификации требуется использовать, так как в случае отсутствия этого значения программа по умолчанию задействует Kerberos-аутентификацию.

Чтобы в Netsh перейти в контекст IPSec, введите в контексте Netsh команду IPSec. При обсуждении утилиты мы ограничимся только командами, служащими для создания и управления IPSec-подключениями.

После перехода в контекст IPSec становятся доступными команды Netsh для создания политик или мониторинга IPSec. Поддерживаются два режима. Статический режим (команда static) позволяет создавать, изменять и назначать политику, не влияя на активную политику IPSec. Динамический режим (команда dynamic) служит для отображения активного состояния и немедленного изменения активной политики IPSec. Динамические команды Netsh влияют на службу только, если она активна. Если служба остановлена, динамические изменения политики игнорируются.

Внимание! Динамический режим оказывается весьма кстати, если, к примеру, надо внести немедленные изменения в процедуру обработки IPSec. Хотя некоторые команды IPSec требуют перезапуска служба IPSec, для многих этого не требуется. Вместе с тем динамический режим может оказаться опасным. Ошибка не видна, пока не внесены изменения, поэтому очень легко «поломать» конфигурацию, не получив при этом никаких предупреждений.

Использование Netsh для мониторинга IPSec. Процедура мониторинга состоит из отображения информации о политике, получения диагностической информации и ведения журнала IPSec. Любые сведения, получаемые в оснастке *Монитор IP-безопасности* (IP Security Monitor), доступны и через Netsh.

Отображение информации политики IPSec. Первым делом обычно выясняют, каковы текущие параметры политики IPSec. Для этого служит команда show. Особенно много сведений возвращает команда show all:

```
Netsh ipsec static show all
```

Иногда нужна лишь часть информации о конфигурации IPSec, для этого используются другие разновидности команды show, некоторые из которых описаны в табл. 11-6. Эти команды можно вводить в статическом или динамическом контексте Netsh или из командной строки.

Табл. 11-6. Команды show утилиты Netsh

Операция	Команда
Отображение заданного списка фильтров	Show Filterlist Name=<имя *списка фильтров*>
Отображение политики, назначенной указанному объекту групповой политики (GPO)	Show Gpoassignedpolicy *Name=<имя политики>*
Отображение указанной политики	Show Policy Name=<Имя *политики*>
Отображение указанного правила	Show Rule Name=<Имя *правила*>

Получение диагностической информации IPSec. Один из этапов диагностирования неполадок IPSec — или лишь определения, работает ли политика, как должна, — получение информации о текущей политике. Описанные в табл. 11-7 команды дают такую информацию. Сведения, предоставляемые каждой командой, определяют параметры политики. Например, Show Filterlist показывает информацию о списке фильтров политики (табл. 11-6).

Ниже перечислены некоторые примеры синтаксиса команды show. Знак «равно» (=) является частью команды, а угловые скобки и заключенный в них текст заменяется на соответствующий элемент.

- Show All Resolvedns=<Значение> — разрешает DNS-или NetBIOS-имя компьютера в IP-адрес. Эта команда позволяет выяснить, правильный ли компьютер выбран для применения политики.
- Show Mmsas — отображает информацию об основном режиме IPSec. Выводится информация об источнике и приемнике. При использовании параметра Resolvedns=yes дополнительно отображаются имена компьютеров.
- Show Qmsas — отображает информацию о быстром режиме IPSec.
- Show Stats — отображает статистическую информацию основного режима IKE, быстрого режима IPSec или и ту и другую одновременно. (Описание этих сведений см. в табл. 11-8.)

Помимо команд show можно использовать несколько диагностических команд динамического режима Netsh.

- Set Config Property=Ipsecdiagnostics value=<значение> — переменная может принимать значения из диапазона 0—7, указывая уровень регистрации диагностики IPSec. Значение по умолчанию — 0, то есть запись отключена. На уровне 7 регистрируется вся информация. Чтобы начать регистрацию, надо задать новый уровень и перезагрузить компьютер.
- Set Config Property=Ipseclogінterval value=<*значение*> —указывает, какчасто (в секундах) события IPSec отправляются в файл журнала. Диапазон значений: 60—86 400 сек., а значение по умолчанию — 3600 сек.
- Set Config Property=Ikelogging value=<*значение*> — параметру присваивается значение *0* или *1,* отключающее или включающее регистрацию IKE в журнале Oakley. В случае активизации регистрируется масса информации, для понимания которой надо владеть спецификациями RFC на уровне эксперта.
- Set Config Property=Strongcrlcheck value=<*значение*> — определяет, используется ли *список отзыва сертификатов* (certificate revocation list, CRL). При значении *0* проверка CRL отключена, а при / сертификат не проходит проверку, только если он отозван. При уровне проверки *2,* сертификат считается непригодным при любых ошибках проверки CRL, в том числе в случае невозможности найти CRL в сети.

Возможны и другие методы диагностики, например изменение текущей политики с ослаблением защиты. Например, задав вместо Kerberos аутентификацию на основе общего секрета или сертификатов, вы избавитесь от неполадки, если она связана с аутентификацией. *Netdiag.exe* — утилита командной строки, позволяющая отображать информацию IPSec, а также проверять и просматривать сетевую конфигурацию. Существуют версии Netdiag для Windows Server 2003, Windows 2000 и Windows XP. Однако в разных ОС она устанавливается по-разному. В Windows Server 2003 Netdiag устанавливается вместе с *Средствами поддержки Windows* (Windows Support Tools). В Windows 2000 она входит в *Комплект ресурсов Windows 2000* (Windows 2000 Resource Kit), который можно также загрузить из Интернета. В Windows XP утилита поставляется на установочном компакт-диске и устанавливается при выполнении команды *Setup.exe* из папки *Support\Tools.*

Получить общую информацию диагностики сети (не специально относящуюся к IPSec) можно утилитой *Netdiag.* Например, команда Netdiag /v /1 предоставляет сведения о конфигурации IP и маршрутизации на компьютере, проверяет разрешение WINS- и DSN-имен, сообщает версию ОС и установленные критические исправления

(hotfixes), проверяет действительность членства домена, проверяет связь членов домена с контроллерами, а также доверительные отношения. Вся эта информация часто оказывается полезной при устранении общесетевых неполадок до попытки диагностировать неполадки самого IPSec.

Утилита Netdiag.exe доступна в Windows Server 2003, но в этой версии нет параметра `/test:ipsec`, — вместо этого рекомендуется использовать команду Netsh. Команды контекста Netsh IPSec не работают в более старой ОС, поэтому на таких компьютерах рекомендуется использовать Netdiag. Иногда требуется дистанционно исследовать политику IPSec на компьютере под управлением Windows XP или Windows 2000, который подключен или пытается подключиться к компьютеру с Windows Server 2003. В этом случае применяется удаленный настольный сеанс и утилита Netdiag.

Использование оснастки *Монитор IP-безопасности* для наблюдения за трафиком IPSec

Монитор IP-безопасности (IP Security Monitor) — оснастка Windows XP и Windows Server 2003, служащая для мониторинга и устранения неполадок IPSec. Эта оснастка также позволяет изучать активную политику IPSec и ее действия. *Монитор IP-безопасности* можно использовать для наблюдения за компьютерами, где установлен монитор той же версии. Он позволяет получить следующую информацию:

- имя активной политики IPSec;
- подробные параметры активной политики IPSec;
- статистику быстрого режима;
- статистику основного режима,
- сведения об активных сопоставлениях.

Примечание Средства мониторинга IPSec есть и в Windows 2000: утилиты Netdiag и Ipsecmon.exe, по отдельности или совместно.

Статистика основного и быстрого режима в Мониторе IP-безопасности

Чтобы просмотреть статистику IPSec, достаточно просто развернуть узел **Основной режим** (Main Mode) или Быстрый режим **(Quick** Mode) и выбрать узел Статистика (Statistics). Намного сложнее понять, что означают отдельные строчки этой статистики. В табл. 11-7 описывается наиболее общая статистика основного, а в табл. 11-8 — быстрого режима. В табл. 11-7 некоторые данные относятся к быстрому режиму, но они инициализируются в процессе основного режима IKE, поэтому включены в статистику основного режима.

Табл. 11-7. Статистика основного режима IPSec

Параметр	Описание
Активных запросов (Active Acquire)	Количество запросов на запуск процесса согласования IKE для установления сопоставления безопасности между сторонами подключения IPSec. Статистика активных запросов включает число невыполненных запросов и запросов в очереди
Активных приемов (Active Receive)	Число принятых сообщений IKE, ожидающих обработки в очереди

Табл. 11-7. *(продолжение)*

Параметр	Описание
Ошибок запросов (Acquire Fanures)	Общее число полученных неудачных исходящих запросов, начиная с последнего запуска службы IPSec. Учитываются запросы на сопоставление безопасности между сторонами подключения IPSec
Ошибок приема (Receive Failures)	Общее количество ошибок, произошедших во время получения сообщений IKE, начиная с последнего запуска службы IPSec
Ошибок отправки (Send Failures)	Общее количество ошибок, произошедших во время посылки сообщений IKE, начиная с последнего запуска службы IPSec
Размер кучи запросов (Acquire Heap Size)	Число записей в куче запросов. Куча запросов хранит успешные запросы. Учитываются исходящие запросы на сопоставление безопасности между сторонами подключения IPSec
Размер кучи приема (Receive Heap Size)	Число записей в буферах приема IKE. Буферы приема хранят входящие сообщения IKE
Сбой проверки подлинности (Authentication Failures)	Общее число сбоев при проверке учетных данных (с использованием Kerberos, сертификата и общего ключа), произошедших при согласовании основного режима, начиная с последнего запуска службы IPSec. При наличии затруднений с безопасным обменом данными попробуйте установить соединение и посмотрите, увеличится ли число ошибок аутентификации. Если это значение увеличится, проверьте соответствие методов аутентификации или правильность настройки метода аутентификации (например соответствие используемых предварительных общих ключей)
Ошибки согласования (Negotiation Failures)	Общее количество ошибок согласования, произошедших во время согласования основного или быстрого режимов, начиная с последнего запуска службы IPSec. При наличии затруднений с осуществлением безопасного обмена данными попробуйте установить соединение и посмотрите, увеличится ли число ошибок согласования. Если это значение увеличится, проверьте соответствие методов аутентификации, правильность настройки метода аутентификации (например соответствие используемых . предварительных общих ключей) или соответствие методов или параметров безопасности
Получены недопустимые файлы «cookie» (Invalid Cookies Received)	Общее количество файлов «cookie», которые не удается согласовать с сопоставлением безопасности активного основного режима, полученных с последнего запуска службы IPSec
Всего запросов (Total Acquire)	Общее количество запросов, отправленных в IKE для установления сопоставления безопасности, начиная с последнего запуска службы IPSec

Табл. 11-7. *(окончание)*

Параметр	Описание
Всего получено SPI (Total Get SPI)	Общее число запросов, отправленных IKE в драйвер IPSec для получения уникального индекса параметров безопасности (Security Parameters Index, SPI), начиная с последнего запуска службы IPSec
Дополнения по ключам (Key Additions)	Общее количество исходящих сопоставлений безопасности быстрого режима, добавленных IKE к драйверу IPSec, начиная с последнего запуска службы IPS
Обновлений ключей (Key Updates)	Общее количество входящих сопоставлений безопасности быстрого режима, добавленных IKE к драйверу IPSec, начиная с последнего запуска службы IPSec
Ошибок получения SPI (Get SPI Failures)	Общее число невыполненных запросов, отправленных IKE в драйвер IPSec для получения уникального SPI
Дополнительные сбои ключей (Key Addition Failures)	Общее количество невыполненных дополнительных исходящих запросов на сопоставление безопасности быстрого режима, отправленных IKE драйверу IPSec
Ошибок обновлений ключей (Key Update Failures)	Общее количество невыполненных дополнительных входящих запросов на сопоставление безопасности быстрого режима, отправленных IKE драйверу IPSec
Размер списка ISADB (ISADB List Size)	Число записей состояния основного режима. Учитываются успешно согласованные основные режимы, текущие основные режимы, а также несогласованные или просроченные основные режимы, которые не были удалены
Размер списка подключений (Connection List Size)	Количество согласующихся в данный момент быстрых режимов
Главный IKE-режим (IKE Main Mode)	Общее число успешных сопоставлений безопасности, созданных во время согласований основного режима
Быстрый IKE-режим (IKE Quick Mode)	Общее число успешных сопоставлений безопасности, созданных во время согласований быстрого режима
«Мягкие» сопоставления (Soft Associations)	Общее число сопоставлений безопасности с компьютерами, не ответившими на попытки согласования основного режима, начиная с последнего запуска службы IPSec. Хотя данные компьютеры не ответили на попытки согласования основного режима, политика IPSec разрешила связь с ними. IPSec не используется для обеспечения безопасности мягких сопоставлений безопасности
Получено неправильных пакетов (Invalid Packets Received)	Общее число неправильных сообщений IKE, полученных с последнего запуска службы IPSec. Учитываются сообщения IKE с недопустимыми полями заголовка, неправильным размером полезных данных и неправильными значениями cookie отвечающей стороны. Неправильные сообщения IKE в основном вызываются повторно переданными сообщениями IKE или несоответствующим общим ключом между подключениями IPSec

Табл. 11-8. Статистика быстрого режима IPSec

Параметр	Описание
Активных сопоставлений безопасности (Active Security Association)	Число активных сопоставлений безопасности быстрого режима
Разгруженные сопоставления безопасности (Offloaded Security Associations)	Число активных сопоставлений безопасности быстрого режима, разгруженных на аппаратное обеспечение
Незаконченные операции с ключами (Pending Key Operations)	Число текущих незавершенных операций обмена ключами IPSec
Дополнения по ключам (Key Additions)	Общее число ключей для сопоставления безопасности быстрого режима, добавленных с последнего запуска компьютера
Удаления ключей (Key Deletions)	Общее число ключей для сопоставления безопасности быстрого режима, удаленных с последнего запуска компьютера
Повторное создание ключей (Rekeys)	Общее число успешных операций по повторному созданию ключей для сопоставления безопасности быстрого режима, прошедших с последнего запуска компьютера
Активных туннелей (Active Tunnels)	Число активных туннелей IPSec
Сбойных пакетов SPI (Bad SPI Packets)	Число пакетов с неправильными идентификаторами SPI, пришедших с последнего запуска компьютера. Неправильный индекс параметров безопасности может означать, что срок действия входящего сопоставления безопасности истек и недавно был получен пакет, использующий старое сопоставление безопасности. Это значение может быть большим при коротких интервалах смены ключей и большом числе сопоставлений безопасности. Большое количество пакетов с неправильными SPI, пришедших за небольшой промежуток времени, может указывать на атаку с *подменой пакетов* (spoofing)
Незашифрованных пакетов (Packets Not Decrypted)	Общее число пакетов, пришедших с последнего запуска компьютера, которые не удалось расшифровать. Пакет может быть не расшифрован, если он не прошел проверку
Непроверенных пакетов (Packets Not Authenticated)	Общее число пакетов, данные которых не удалось проверить (которые не прошли проверку на целостности с использованием алгоритма хеширования), пришедших с последнего запуска компьютера. Рост этого числа может указывать на атаку с использованием подмены или изменения пакетов, или на порчу пакетов сетевыми устройствами
Пакеты с определением ответа (Packets With Replay Detection)	Общее число пакетов, содержащих неправильный порядковый номер, пришедших с последнего запуска компьютера. Рост этого числа может указывать на проблемы с сетью или на атаку, основанную на повторном воспроизведении трафика (Replay)

Табл. 11-8. *(окончание)*

Параметр	Описание
Послано байт (секретных) (Confidential Bytes Sent)	Общее число байт, отправленных по протоколу ESP (в том числе и через ESP без шифрования), начиная с последнего запуска компьютера
Получено байт (секретных) (Confidential Bytes Received)	Общее число байт, полученных по протоколу ESP (в том числе и через ESP без шифрования), начиная с последнего запуска компьютера
Послано байт (проверенных) (Authenticated Bytes Sent)	Общее число проверенных байт, отправленных по протоколу AH (Authentication Header) или протокол ESP, начиная с последнего запуска компьютера
Получено байт (проверенных) (Authenticated Bytes Received)	Общее число проверенных байт, полученных по протоколу AH или протокол ESP, начиная с последнего запуска компьютера
Транспортных байтов отправлено (Transport Bytes Sent)	Общее число байт, посланных через режим транспорта IPSec, начиная с последнего запуска компьютера
Получено транспортных байтов (Transport Bytes Received)	Общее число байт, полученных через режим транспорта IPSec
Отправлено в туннель, байтов (Bytes Sent In Tunnels)	Общее число байт, посланных через туннельный режим IPSec
Получено из туннеля, байтов (Bytes Received In Tunnels)	Общее число байт, полученных через туннельный режим IPSec
Отправлено разгруженных байтов (Offloaded Bytes Sent)	Общее число байт, посланных через аппаратную разгрузку IPSec
Получено разгруженных байтов (Offloaded Bytes Received)	Общее число байт, полученных через аппаратную разгрузку IPSec

Использование Netcap для записи сетевого трафика

Утилиту Netcap.exe можно применять для записи сетевого трафика в файл, который позже можно просматривать и анализировать в консоли *Сетевой монитор* (Network Monitor). Причем чтобы использовать Netcap, не обязательно устанавливать сетевой монитор на компьютере с Windows Server 2003. Netcap также мсожно использовать на компьютерах *под управлением Windows XP.* Утилита устанавливается в составе Средств *поддержки Windows,* при первом ее запуске автоматически устанавливается драйвер сетевого монитора.

В табл. 11-9 описан синтаксис записи данных.

Табл. 11-9. **Синтаксис Netcap**

Параметр	Описание
/b:Number	Задает объем буфера: допустимые значения 1—1000 Мб, а значение по умолчанию — 1 Мб
/t Type Buffer HexOffset HexPattern	Сообщает триггеру, когда остановить запись данных: при заполнении буфера или получении шаблонного значения. Если триггер не определен, запись прекращается при заполнении буфера. Чтобы продолжить запись при.заполнении буфера, используют параметр /t N. В этом случае новые кадры записываются поверх старых. Разрешенные значения параметра *Type:* B — буфер; P — шаблон; BP — буфер, а затем шаблон; PB — шаблон, а затем буфер; N — триггер не определен. Разрешенные значения параметра *Buffer* — процентная доля буфера — 25%, 50%, 75% и 100%. Этот параметр используется со всеми значениями *Type* кроме *P.* Разрешенные значения параметра *HexOffset* — шестнадцатеричное смещение от начала кадра; используется с типами *P, BP, PB,* но не *B.* Разрешенные значения параметра HexPattern — шестнадцатеричный шаблон, с которым сравнивается кадр; используется с *P, BP, PB,* но не *B.* Образец должен состоять из четного числа цифр
/C:CaptureFile	Определяет место хранения временных файлов записи Netcap. Путь к любой действительной локальной или удаленной папке. Если /C не определен, временные файлы размещаются во временной папке по умолчанию
/F:FilterFile.cf	Определяет фильтр, применяемый в процессе записи. Расширение файла фильтра — .cf
/L:HH:MM:SS	Запись на протяжении определенного времени
/TCF:FolderName	Изменяет временную папку записи данных. Это должна быть папка на локальном жестком диске
/Remove	Удаляет установленную Netcap копию драйвера сетевого монитора
/N:Number	Указывает на интерфейс данного компьютера. Обычно *0* соответствует интерфейсу PPP/SLIP, а *1* — подключению по локальной сети. Определить номер интерфейса можно командной Netcap /?

Вот примеры команд.

Запись пакетов, поступающих с сетевой платы 2 с использованием буфера размером 20 Мб:

```
Netcap  /n:2  /b:20
```

Запись данных на протяжении одного часа:

```
Netcap  /1:01:00:00
```

Основные сведения о Kerberos

Kerberos— сложный протокол аутентификации, описанный в RFC 1510. Это предпочтительный протокол аутентификации в доменах Windows Server 2003 и Windows 2000. Компьютеры — члены домена под управлением Windows XP Professional, Windows 2000 и Windows Server 2003 также по возможности используют аутентификацию Kerberos. Понимание процесса аутентификации позволяет выяснить:

- используется ли в сети Kerberos. Он намного безопаснее своего предшественника, NTLM;
- являются ли ошибки Kerberos некритичными, нуждаются в исправлении или информируют об атаке;
- связаны ли ошибки Kerberos с неполадками репликации, работой Active Directory, DNS или других критически важных сетевых служб.

Ознакомление с RFC или даже с сокращенной версией алгоритма полезно, но намного эффективнее исследовать Kerberos-вход в систему с помощью *Сетевого монитора* (Network Monitor), журнала событий безопасности и утилит из комплекта ресурсов — Kerbtray.exe и Klist.exe. Именно об этом мы поговорим в следующих разделах. Обязательно выполните все упражнения, чтобы уметь самостоятельно выполнять мониторинг Kerberos.

Примечание Спецификация Kerberos, RFC 1510, есть на Web-странице *http://www.ietf.org/rfc/rfc1510.txt?number=1510*. Подробно о реализации Kerberos в Windows можно почитать в «белой книге» *http://www.micmsoft.com/TechNet/prodtechnol/windows2000serv/deploy/kerber*

Практическое руководство по мониторингу Kerberos

Для отслеживания входа в систему прежде всего надо подготовить и запустить необходимые утилиты и инструментальные средства.

- Позаботьтесь об активизации аудита и записи событий входа в систему на контроллерах и членах домена. Это выполняется в консоли *Политика Default Domain Policy* (Default Domain Policy). Убедитесь, что политика обновлена.
- Загрузите и установите утилиты Kerbtray.exe и Klist.exe. Позаботьтесь об установке копии утилиты на клиенте, который будет входить в систему.
- Запустите *Сетевой монитор* (Network Monitor) и до выполнения входа в систему запустите запись данных.
- При необходимости создайте папку на контроллере домена для размещения файлов с записями сетевых данных и копии журнала записи событий безопасности. Эту папку можно временно сделать общей, чтобы загрузить файлы на сервер для анализа. Таким образом вы сможете изучать их в консоли журнала событий безопасности и просматривать билеты в кэше Kerberos. Это намного удобнее, чем постоянно перемещаться между двумя компьютерами или создавать сеанс терминала.

В приведенном здесь примере мы назвали папку Captures. Кроме того, мы использовали маленький текстовый файл со словами «Hello World». После начала записи данных на контроллере домена клиентский сервер, член домена, был перезагружен. В домен вошли с рядового сервера под учетной записью *Администратор* (Administrator). После успешного входа в систему запись данных была остановлена, а результаты сохранены в папке. В папку также скопировали журнал событий безопасности.

Kerberos при загрузке компьютера

При загрузке сервера — члена домена под управлением Windows Server 2003 он проходит аутентификацию на контроллере домена. Первый этап — запрос поиска контроллера домена. На рис. 11-11 показан DNS-запрос поиска LDAP-службы (Lightweight Directory Access Protocol).

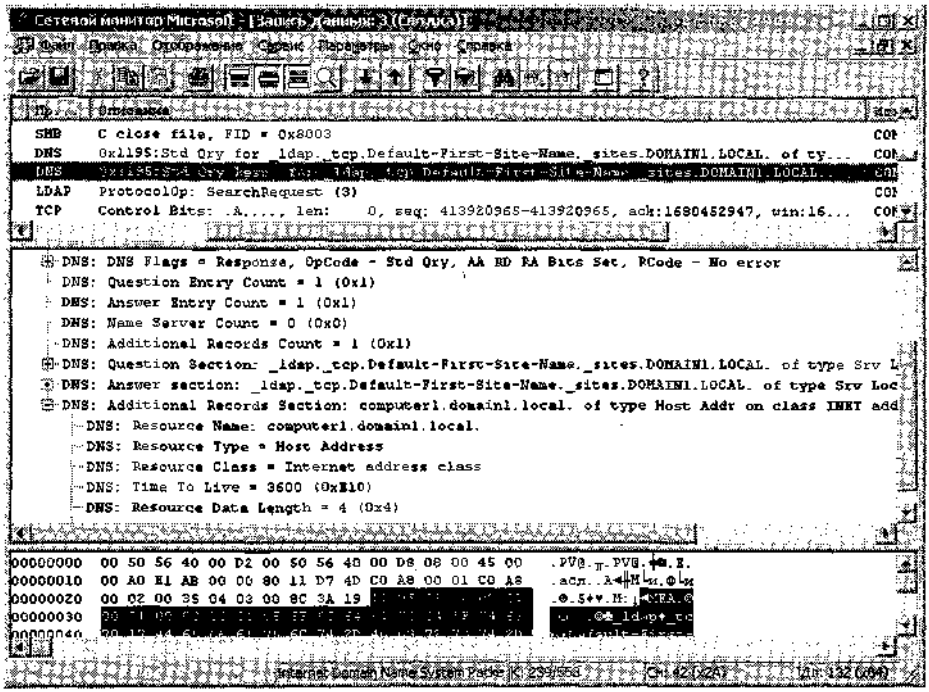


Рис. 11-11. Клиент, запрашивающий у DNS сведения о LDAP-службах

На рис. 11-12 показан LDAP-запрос службы *Сетевой вход в систему* (Netlogon) и прием ответа.

Затем сервер направляет UDP-запрос на Kerberos-порт 88 на контроллере домена и получает от контроллера ответ. Это запрос билета TGT (Ticket Granting Ticket). На рис. 11-13 показана часть этого пакета. Билет TGT необходим для предъявления до получения доступа к каким бы то ни было ресурсам. Пароль учетной записи сервера используется как ключ при создании криптографического хеша *метки времени* (timestamp). С хешем отправляется копия метки времени открытым текстом.

На контроллере домена время незашифрованной метки времени сравнивается с временем контроллера. По умолчанию если разница больше 5 минут, вход в систему не разрешается. [Если не удается организовать Kerberos-аутентификацию, используется NTLM, например при *подключении* (mapping) дисков.] Если проверка метки времени проходит успешно, *центр распространения ключей* (Key Distribution Center, KDC) на основании своей копии пароля сервера вычисляет хеш незашифрованной метки. Два хеша сравниваются и при совпадении сервер считается прошедшим аутентификацию.

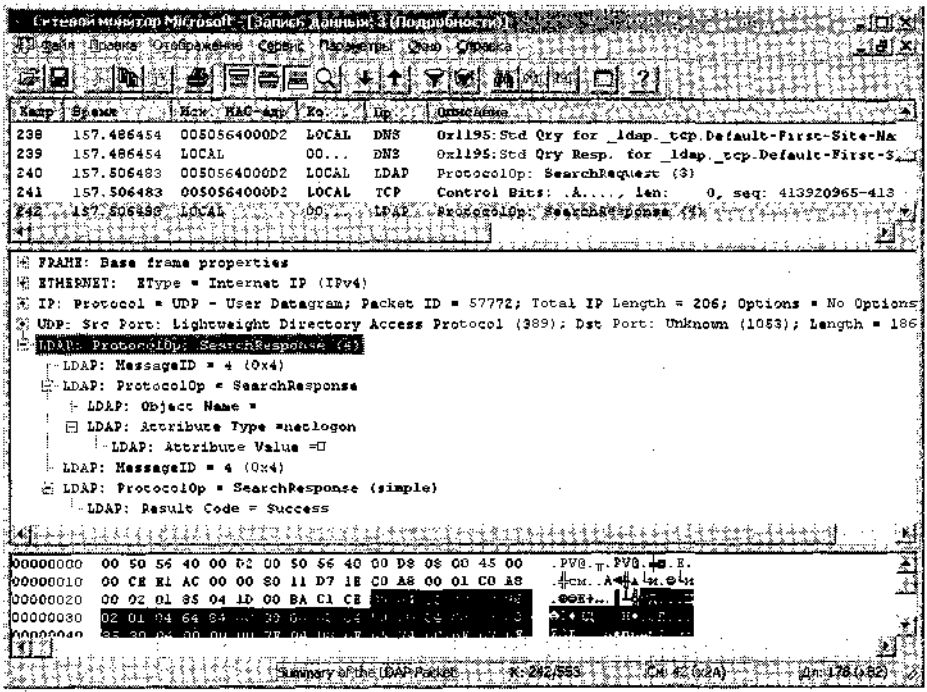


Рис. 11-12. Клиент, выполняющий LDAP-запрос

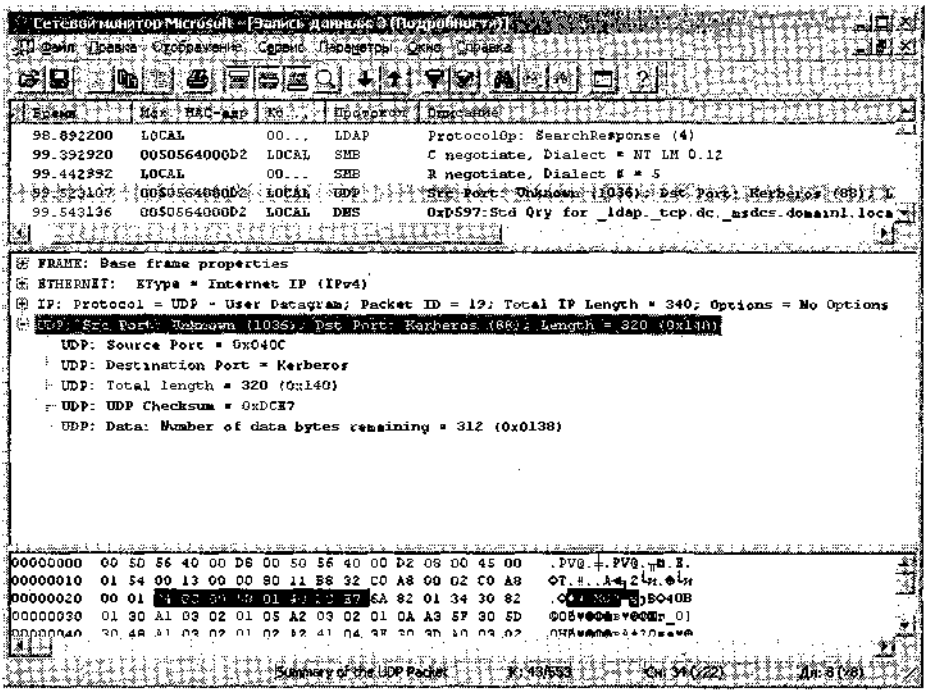


Рис. 11-13. Запрос TGT в KDC через порт 88 Kerberos

KDC направляет билет TGT на сервер в другом UDP-пакете. И снова пакет нечитабелен в сетевом мониторе. Это нормально, но как узнать, что запрос билета и пакет с билетом выполняют свои задачи? В этом нам поможет журнал *Безопасность* (Security). На рис. 11-14 показано сообщение о событии успешного входа в систему с контроллера домена. Обратите внимание на время события и сравните его со временем Kerberos-сообщения на рис. 11-13.

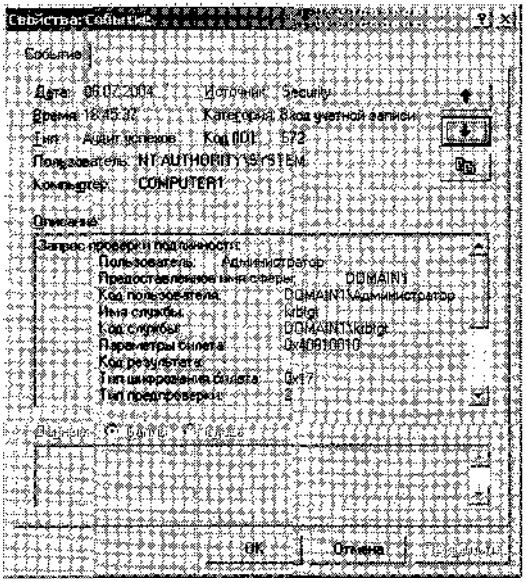


Рис. 11-14. Сообщение о событии запроса TGT и успешного результата

Рядовой сервер домена кэширует TGT и использует его для запроса доступа к службам, то есть запроса билетов служб у KDC. Внимательное изучение дополнительных записей в журнале событий безопасности рядом с запросом TGT позволяет выяснить, что запрос билета службы также успешно удовлетворен.

На этом этапе сервер использует TGT для получения билета службы для доступа к собственным ресурсам. Из Kerberos-пакетов не удается почерпнуть полезной информации — они зашифрованы.

Kerberos при входе пользователя в систему

Далее, когда пользователь домена — в данном случае *Администратор* (Administrator) — входит в систему, процесс повторяется: представляются реквизиты и запрашивается TGT. После успешной проверки реквизитов выдается TGT. В журнале сетевого монитора много UDP-кадров, направленных в порт 88 контроллера домена, и полученных ответов. Заметьте время этих кадров (рис. 11-15) и найдите соответствующие события в журнале событий безопасности.

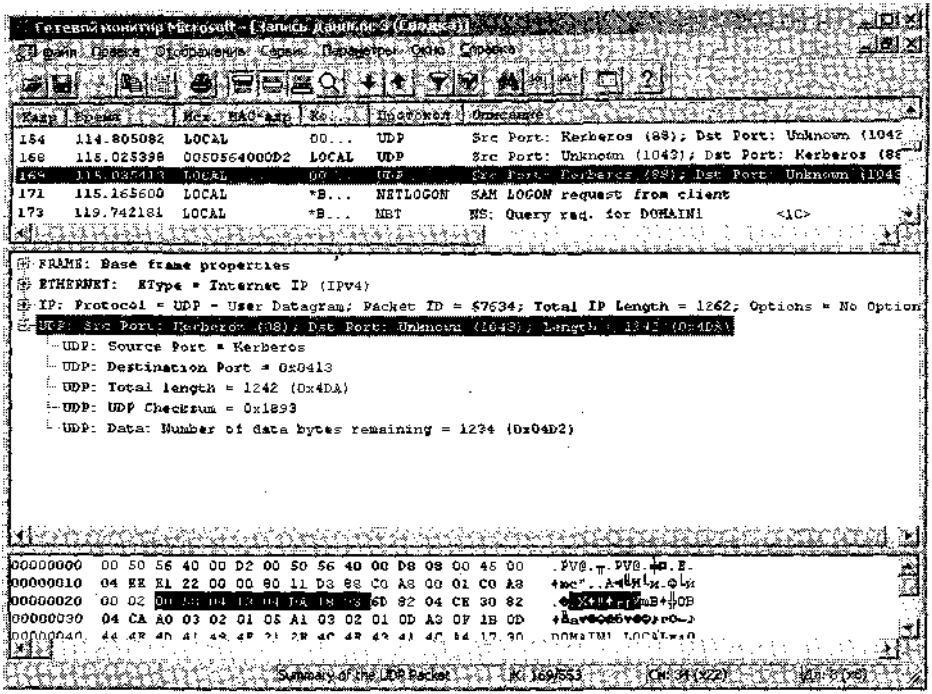


Рис. 11-15. Журнал *Безопасность* с запросом TGT

На рис. 11-16 показан успешный запрос TGT для учетной записи *Администратор*.

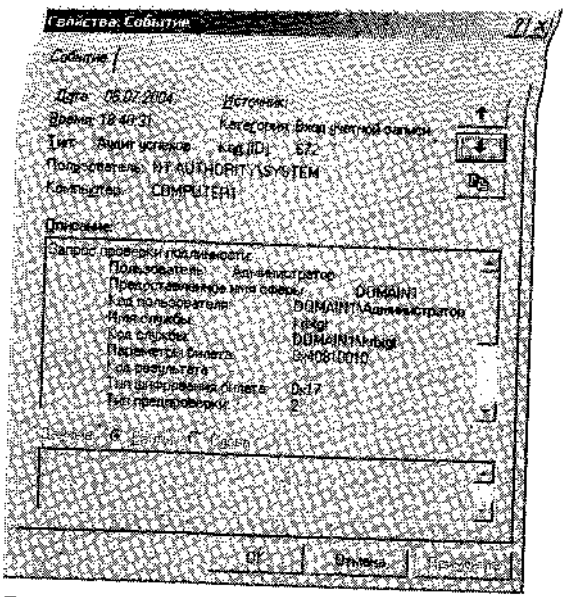


Рис. 11-16. Журнал *Безопасность* с успешным запросом

Теперь начинается самое интересное. Билет TGT учетной записи *Администратор,* как и TGT для доступа к системе, сохраняется в кэше билетов Kerberos — этот билет нужен для доступа к службам. Увидеть содержимое кэша билетов позволяет утилита Kerbtray.exe. После ее запуска в панели задач размещается значок, щелчок которого открывает окно с информацией о билетах в кэше (рис. 11-17).

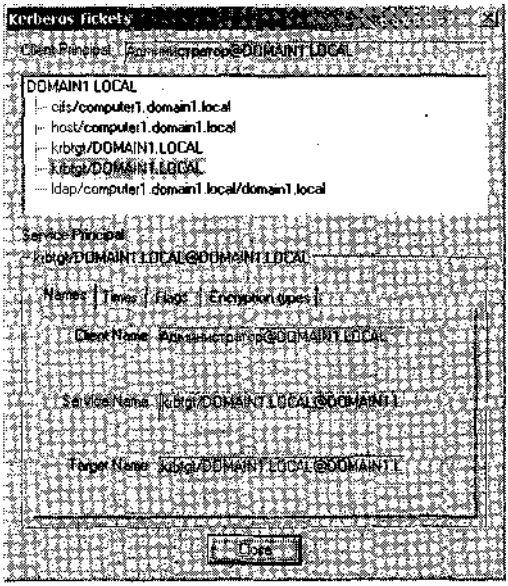


Рис. 11-17. Использование утилиты Kerbtray.exe для просмотра билетов Kerberos в кэше локальной машины

Один из первых запросов — запрос служб локального компьютера (рис. 11-17): узла (host), IAMS, CIFS (Common Internet File System) и LDAP. Все эти службы требуются для входа в систему и необходимы учетной записи *Администратор* для доступа к локальному компьютеру (узел и IAMS) и общему ресурсу контроллера домена (CIFS), а также для выполнения LDAP-запросов в службе каталогов (LDAP).

Запросы билетов службы содержат TGT и другой *аутентификатор* (authenticator). Поскольку TGT размещен в кэше, возникает подозрение, что его можно перехватить и воспользоваться для атаки *повторного воспроизведения трафика* (replay). Новый аутентиФИШОр защищает KDC. Поскольку время на сервере изменилось сообщение-аутентификатор, или метка времени, будет всегда свежим, а KDC всегда проверяет соответствует ли разница во времени, определенной в политике домена. *[Разница во времени* (time skew) - это различие между временем KDC и клиента; если эта величина больше разрешенной политикой, Kerberos-запрос отклоняется.]

Роль Kerberos в авторизации

Kerberos — протокол аутентификации, но он участвует и в авторизации. При подключении диска к общему файловому ресурсу Kerberos TGT запрашивает билет сеанса у службы сервера CIFS. Системный монитор позволяет прослеживать эти операции.

Однако билет службы не дает пользователям доступа к общему ресурсу. Билет аутентифицирует пользователей только на доступ к серверу. В сущности такой билет говорит, что пользователь — тот, за кого себя выдает, и серверу не надо обращаться к контролле-

ру для проверки. Часть билета службы шифруется с использованием хеша пароля сервера — это дает серверу возможность расшифровывать содержимое билета. Следует помнить, что контроллер домена хранит хеши паролей всех компьютеров и пользователей. Расшифровав билет, сервер признает его действительным, так как тот создан контроллером, ведь только последний знает пароль сервера.

Откуда берется информация для авторизации? Билет службы содержит нужные сведения, хотя является лишь инструментом аутентификации пользователя. Это та же информация, которую получает KDC, когда предоставляет при первом обращении пользователем предоставляет свои доменные реквизиты — *идентификатор безопасности пользователя* (security identifier, SID) и SID-идентификаторы групп, членом которых является пользователь. Файловый сервер использует эту информацию для создания маркера доступа, на основании которого определяет разрешения пользователя на доступ к общим папкам и файлам.

Определить, разрешен или запрещен доступ, позволяет журнал событий безопасности, а Kerbtray.exe показывает билет службы CIFS в кэше. Обратите внимание, что билет службы CIFS в кэше выпущен для определенного сервера (рис. 11-17). При следующей попытке доступа к общему ресурсу сервера (или при восстановлении подключения в случае его нарушения) можно повторно использовать этот билет службы. Для получения доступа к другому серверу пользователю надо получить другой, новый билет службы. Повторимся: содержимое запросов билетов службы нельзя увидеть в системном мониторе, однако Kerbtray.exe позволяет проверить, предоставлен ли соответствующий билет службы.

Изучите свойства билетов в кэше. Билеты службы и **TGT** возобновляемы. По истечении срока службы билет службы обновляется (путем получения нового) незаметно, «прозрачно» для пользователя — если, конечно, в кэше есть действительный билет TGT. Если это не так, придется повторно получить новый TGT, то есть повторно войти в систему. Время жизни билетов можно узнать на вкладке **Times,** где указаны параметры политик Kerberos для домена. Процедура управления билетами полностью идентична на членах домена под управлением Windows 2000 и Windows XP Professional.

Для получения списка билетов в кэше можно использовать другую утилиту из комплекта ресурсов — Klist.exe. Она выполняется из командной строки или командного файла. Результаты работы утилиты можно вывести в текстовый файл командой `Klist. exe > Textf ile. txt`. Klist.exe не предоставляет столько же информации, как и Kerbtray.exe, но у нее есть замечательное преимущество — она позволяет удалять билеты (командой Ри где) — все за раз ИЛИ выборочно по одному.

Другие варианты использования инструментов Kerberos

Kerbtray.exe и Klist.exe предоставляют массу информации, но дополнительные сведения о работе Kerberos получают с помощью Netdiag. Все эти инструменты сравнительно просты в использовании.

Основные сведения о Kerbtray

Одни вопросительные знаки в значке Kerbtray означают, что в кэше нет никаких билетов Kerberos. Эта ситуация наблюдается, когда компьютер не подключен к сети или нет доступных контроллеров домена.

Дважды щелкните значок Kerbtray, чтобы увидеть список билетов, полученных, начиная с момента входа в систему. По щелчку правой кнопкой открывается меню с двумя полезными командами: **List Tickets** и **Purge Tickets.** Выбор первой команды эквива-

лентен двойному щелчку значка Kerbtray. Если выбрать вторую команду, билеты будут удалены и придется вновь войти в систему, чтобы получить нужные билеты Kerberos.

В окне Kerbtray отображается имя участника безопасности (пользователя), получившего билеты, и список билетов служб. При выборе билета отображается его назначение: для доступа к какому ресурсу он нужен. Внизу экрана представлена информацию о выбранном билете, в том числе название, время, флаги и тип шифрования. На рис. 11-17 показана вкладка **Names,** а на рис. 11-18, 11-19 и 11-20 — другие вкладки.

Вкладка **Names** содержит следующую информацию:

- **Client Name** — имя клиента, затребовавшего билет;
- **Service Name** — название учетной записи для запрошенной службы. Имя службы начального билета TGT — krbtgt;
- **Target Name** — название службы, для которой затребован билет, например CIFS.

Вкладка **Times** содержит:

- **Start Time** — время начала действия билета;
- **End Time** — время окончания действия билета. Билет с истекшим сроком непригоден для аутентификации при доступе к службе;
- **Renew Until** — для возобновляемых билетов здесь указывается максимальное время жизни билета. Билеты могут возобновляться до наступления времени окончания действия билета и до достижения максимального времени жизни. Возобновление выполняется незаметно для пользователя.

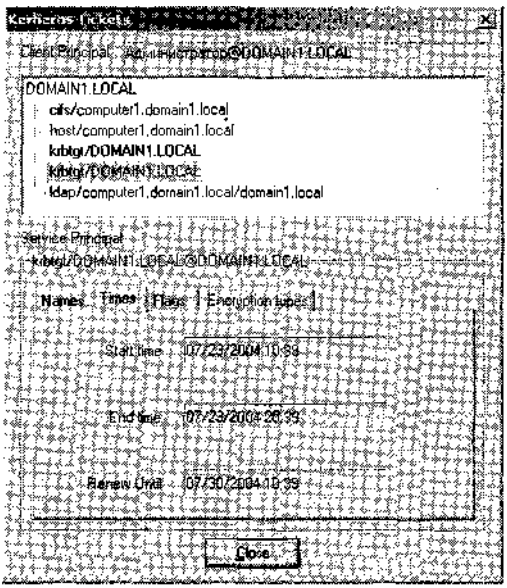


Рис. 11-18. Вкладка Times с информацией о сроках действия

Флаги Kerberos указывают на состояние билета, а также определяют область применимости билета. Вкладка **Flags** содержит следующую информацию.

- **Forwardable** — аутентификационная информация может пересылаться и при использовании билета пользователю не надо вводить пароль.
- **Forwarded** — служба TGS (Ticket Granting Service) центра распространения ключей (KDC) устанавливает этот флаг, если пользователь представляет билет с установленным флагом FORWARDABLE и запрашивает установку флага FORWARDED.

- **Proxiable** — информация в билете с таким флагом может пересылаться для предоставления удаленному серверу разрешения на выполнение удаленного запроса от имени пользователя. TGS выпускает новый билет службы с другим сетевым адресом (билет службы для другого компьютера от имени клиента).
- **Proxy** — если билет выпущен для другого компьютера от имени пользователя (по получении билета с флагом PROXIABLE), новый билет отмечается как прокси-билет (proxy ticket). Сервер приложений можно настроить на выполнение аудита по признаку этого флага, при этом можно установить флаги, которые потребуют дополнительной аутентификации от любого клиента, представляющего прокси-билет.
- May **Postdate** — этот флаг нужен в билете TGT, если на основании представленного билета надо выпустить билет с отложенной датой. Билет службы обычно требуется для немедленного доступа к службе, а билет с отложенной датой предназначен для использования через некоторое время, в будущем.
- **Postdated** — билет с отложенной датой, то есть датой более поздней, чем дата выпуска.
- **Invalid** — признак недействительности билета. Билет с отложенной датой выпускается с этим флагом. Перед началом использования его нужно представить центру KDC для визирования и подтверждения действительности. KDC проверяет правильность билета только по истечении начальной даты.
- **Initial** — билет выпущенный не по представлению TGT. Пример — первый билет для доступа к службе krbtgt. Это и есть билет TGT, но для его выпуска другого TGT не требуется.
- **Renewable** — возобновляемый билет используется на протяжении более длинного периода. Повторная аутентификация при этом не выполняется.
- **HW Authenticated** — дополнительная информация о начальной аутентификации.
- **Preauthenticated** — информация запроса на начальную аутентификацию.
- OK **As Delegate** — указанный в билете сервер (не клиент) годится для делегирования. Реквизиты пользователя переправляются только в службы, которые отмечены этим признаком.

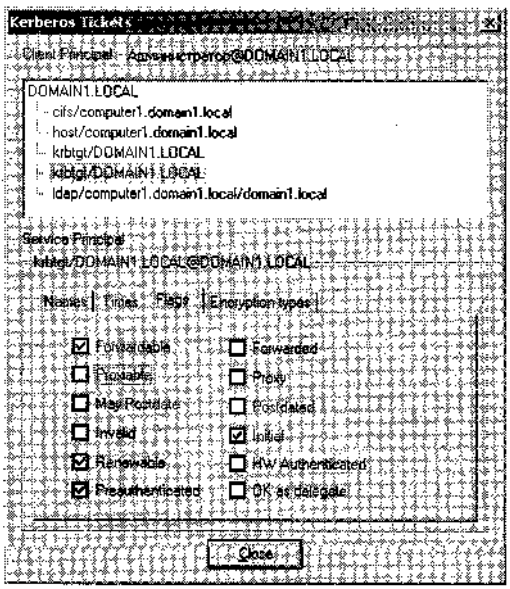


Рис. 11-19. Вкладка Flags с информацией об области применимости билета

Вкладка **Encryption Types** предоставляет следующую информацию.

- **Ticket Encryption Type** — метод, примененный для шифрования билета Kerberos.
- **Key Encryption Type** — метод, примененный для шифрования содержащегося в *билете ключа сеанса* (session key).

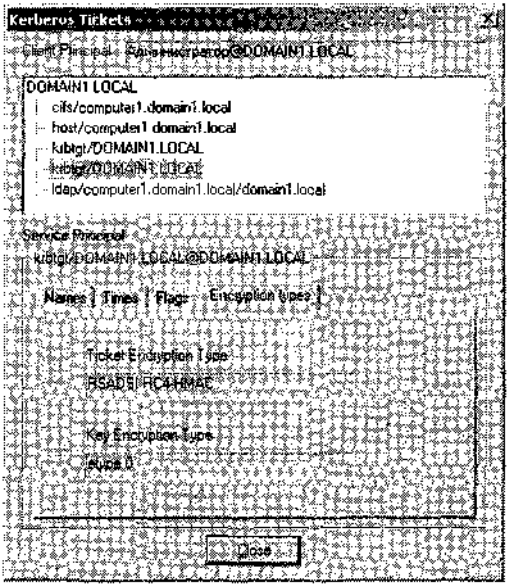


Рис. 11-20. Вкладка Encryption Types с информацией о примененном способе шифрования билета

Общие сведения о Klist

Klist используется в командной строке для отображения информации о билетах или для их удаления. Есть несколько вариантов:

- Klist Tgt — отображение билетов TGT;
- Klist Tickets — отображение всех билетов;
- Klist Purge — удаление всех билетов из кэша.

Команда Klist Tickets отображает следующую информацию:

- *Server*— сервер и домен для билета *[основное имя службы* (service principal name, SPN)];
- *Kerbticket encryption type* — метод, примененный для шифрования билета Kerberos;
- *End Time* — время окончания срока действия билета;
- *Renew Time* — в возобновляемых билетах показывает полный срок действия билета;

Подробную информацию о билетах TGT предоставляет команда Klist Tgt.

- *ServiceName* — название службы, для доступа к которой предназначен билет. Так как это TGT, единственная отображаемая служба — *krbtgt.*
- *TargetName* — запрашиваемая служба.
- *FullServiceName* — каноническое основное имя службы.
- *DomainName* — имя домена службы.
- *TargetDornainName* — если билет предназначен для другой сферы (realm) (например TGT для другого домена).

- *AltTargetDomainNdme* — основное имя службы (SPN) службы, то есть контекст службы, в котором создается билет.
- *TicketFlags* — список флагов билета в шестнадцатеричном формате. (КегЬTray позволяет увидеть флаги на английском.)
- *Key Expiration Time* — срок действия билета,
- *StartTime* — время начала действия билета.
- *EndTime* — время окончания действия билета.
- *RenewUntil* — максимальный срок действия билета.
- *TimeSkew* — сообщенная разница во времени между клиентом и сервером.

Klist.exe и Kerbtray.exe предоставляют массу информации для устранения неполадок. Например, можно выяснить действительность билета, использовался ли Kerberos для аутентификации и если да, то выполнялась ли аутентификация в домене по методу Kerberos.

Использование Netdiag для проверки работы Kerberos

После изучения схемы работы Kerberos и освоения *Сетевого монитора* (Network Monitor), журнала *Безопасность* (Security), Kerbtray.exe и Klist.exe, возникает законный вопрос: как же лучше всего выполнять мониторинг Kerberos? Не проводить же по несколько часов ежедневно за изучением всех данных, чтобы убедиться в нормальной работе этого протокола. Суть, конечно же, не в ежедневном исследовании тысяч или даже миллионов записей, а в поиске тревожных знаков в журналах и записях трафика, говорящих о «нездоровье» Kerberos. Netdiag — именно та утилита, что позволяет быстро получить информацию о состоянии Kerberos.

Netdiag выполняет много проверок, в числе которых тест Kerberos. При выполнении Netdiag из командной строки достаточно предоставить совсем немного информации, чтобы проверить Kerberos. При выполнении такого теста с параметром /v (verbose — подробная информация) или /debug (еще больше информации) выдается список билетов, результаты теста аутентификации, информация о домене и т. п. Результаты тестов можно выгрузить в файл:

```
Netdiag /test:Kerberos /debug > ktest.txt
```

На рис. 11-21 показаны результаты удачного, а на рис. 11-22 — неудачного теста Kerberos.

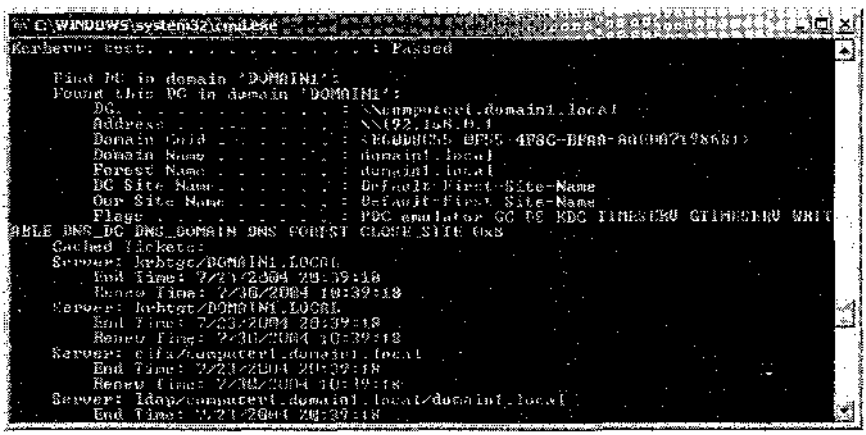


Рис. 11-21. Удачный тест Kerberos

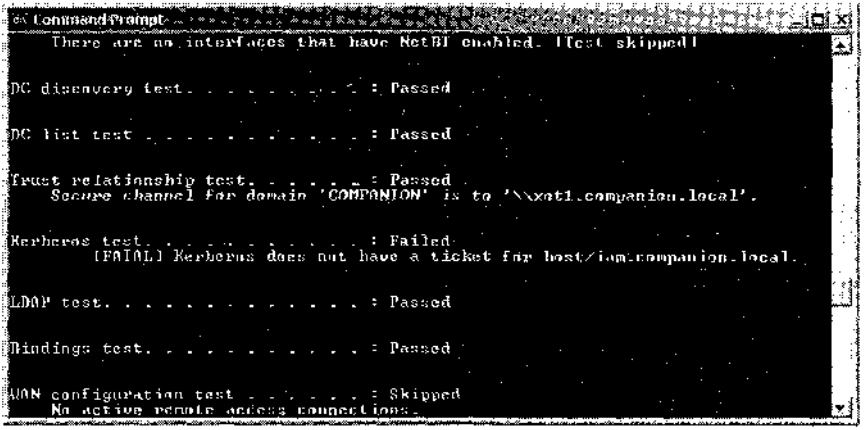


Рис. 11-22. Неудачный тест Kerberos

Лабораторная работа. Использование протоколов сетевой безопасности

Вы примените оснастку *Управление политикой безопасности IP* (IP Security Policy Management) и утилиту Netsh для управления политикой IPSec.

Упражнение 1. Создание запрещающей политики в оснастке *Управление политикой безопасности IP*

В Windows Server 2003, Windows 2000 и Windows XP Professional доступ к IP-безопасности можно получить через объект групповой политики (GPO) или в оснастке **Управление политикой безопасности IP (IP Security Policy Management).** Для упрощения задачи вы загрузите оснастку в консоль, чтобы обратиться к ней позже. Прежде всего вы создадите запрещающую политику, которая блокирует прием нежелательного трафика.

- **Создание пустой консоли**

1. **Выберите Пуск(Start)\Выполнить (Run),** в открывшемся окне введите mmc и щелкните OK.
2. В меню **Консоль (Console)** выберите **Добавить или удалить оснастку (Add/Remove Snap-In).**
3. В одноименном окне щелкните кнопку **Добавить (Add).**
4. В окне **Добавить изолированную оснастку (Add Standalone Snap-In)** выберите **Управление политикой безопасности IP (IP Security Policy Management)** и щелкните кнопку **Добавить (Add)** (рис. 11-23).
5. В окне **Выбор компьютера или домена (Select Computer or Domain)** щелкните **Готово (Finish),** оставив вариант по умолчанию **Локальный компьютер (Local Computer).** Щелкните **Готово (Close). В** окне **Добавить или удалить оснастку** (рис. 11-24) указана выбранная оснастка **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer).** Этот инструмент используется для управления политиками, а его название отличается от указанного на рис. 11-23.

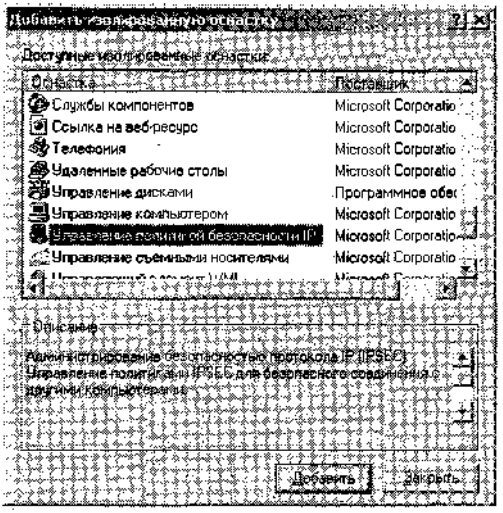


Рис. 11-23. Выбор оснастки *Управление политикой безопасности IP*

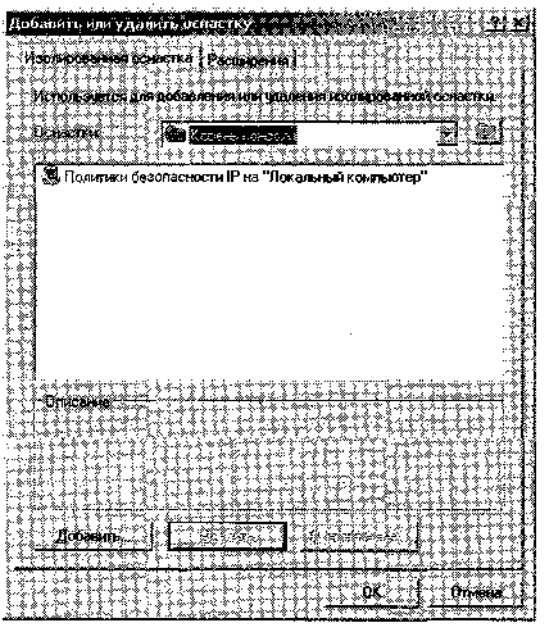


Рис. 11-24. Подтверждение добавления оснастки *Политики безопасности IP*

6. Щелкните OK.
7. Сохраните консоль, выбрав в меню **Консоль** пункт **Сохранить как (Save** As), введите имя файла IP Security Policy Management и щелкните **Сохранить (Save).**

- **Создание запрещающей политики**

1. **В** консоли *Политики безопасности* щелкните узел **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** правой кнопкой и выберите **Создать политику безопасности IP (Create IP Security Policy).**

2. **В** окне **Мастер политики IP-безопасности (IP Security Policy Wizard)** щелкните **Далее** (Next).
3. В поле **Имя** (Name) введите block web server access. В поле **Описание (Description)** введите описательный текст и щелкните **Далее.**
4. Сбросьте флажок **Использовать правило по умолчанию (Activate the default response rule)** и щелкните **Далее.** Это правило разрешает небезопасную связь. В большинстве случаев это надо предотвратить, и правило удаляется. Впрочем, его всегда можно при необходимости восстановить.
5. Щелкните **Готово (Finish).**
6. **В** окне свойств новой политики (рис. 11-25) сбросьте флажок **Использовать мастер (Use Add Wizard).** Мастер позволяет создавать сложные политики, а при создании простых лишь усложняет дело. Нам достаточно окна свойств политики. Щелкните кнопку **Добавить (Add).**

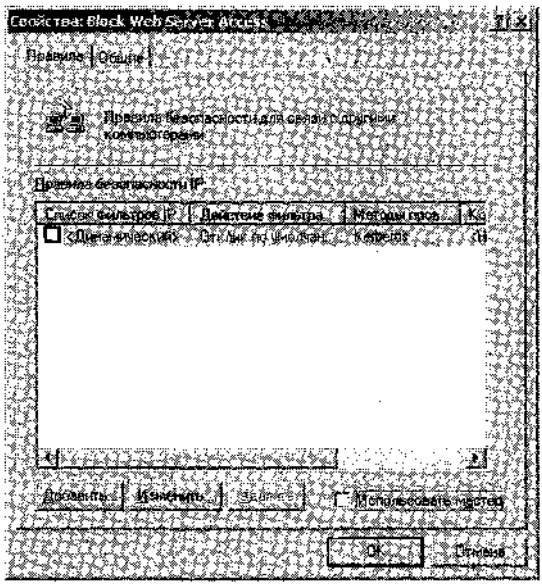


Рис. 11-25. Сбросьте флажок *Использовать мастер*

7. На вкладке **Список фильтров IP (IP Filter List)** (рис. 11-26) щелкните **Добавить (Add).**
8. **В** поле **Имя (Name)** введите blocking, а в поле **Описание (Description)—** blocking protocols.
9. Сбросьте флажок **Использовать мастер (Use Add Wizard)** и щелкните кнопку **Добавить (Add),** чтобы добавить фильтр.
10. В списке **Адрес назначения пакетов (Source Address)** выберите **Любой IP-адрес (Any IP Address),** а в списке **Адрес источника пакетов (Source Address)** выберите **Мой IP-адрес (My IP Address)** (рис. 11 -27).
11. На вкладке **Протокол (Protocol)** в поле со списком **Выберите тип протокола (Select a protocol type)** выберите TCP.

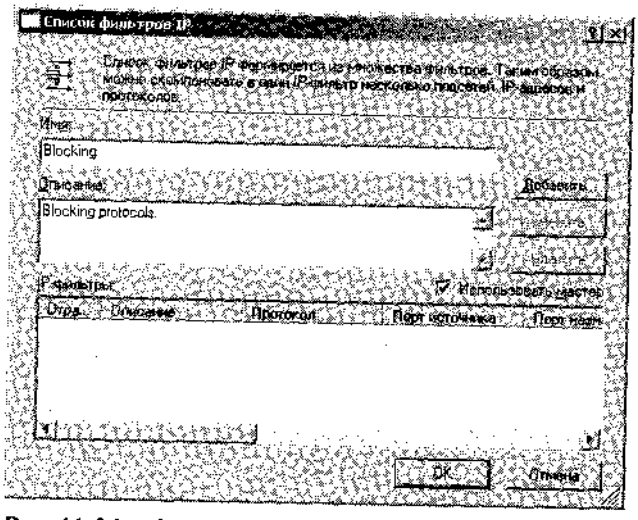


Рис. 11-26. Создание списка фильтров

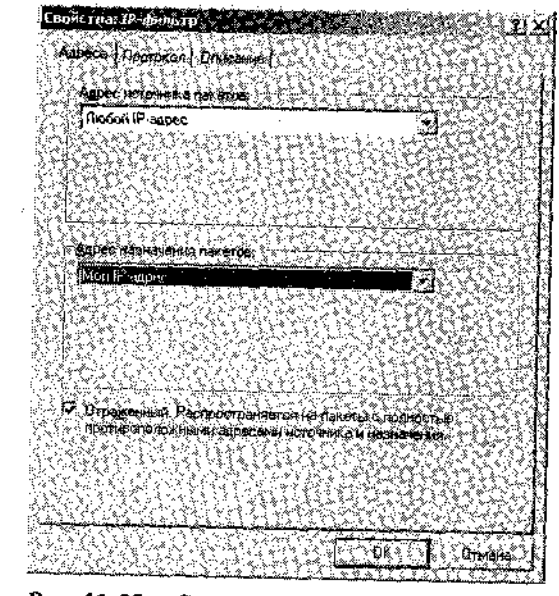


Рис. 11-27. Создание фильтра

12. В области **Установка порта для протокола IP (Set The IP Protocol Port)** выберите **Пакеты на этот порт (to this port),** введите 80 и щелкните OK (рис. 11-28).
13. Выберите запись **Blocking** в списке IP-фильтры и перейдите на вкладку **Действие фильтра (Filter Action).**
14. Сбросьте флажок **Использовать мастер (Use Add Wizard)** и щелкните кнопку Добавить **(Add),** чтобы определить действие фильтра, то есть то, что происходит, когда фильтр активизируется. В данном случае фильтр блокирует любой входящий трафик чеоез порт 80.

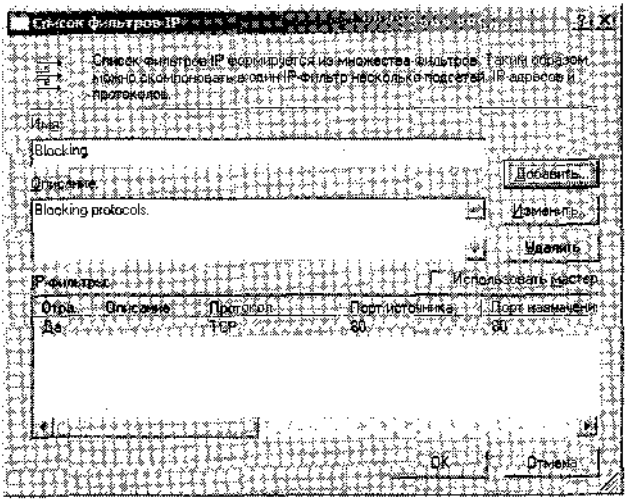


Рис. 11-28. Определение портов фильтра

15. На вкладке **Методы безопасности (Security Methods)** (рис. 11-29) выберите вариант **Блокировать (Block).**

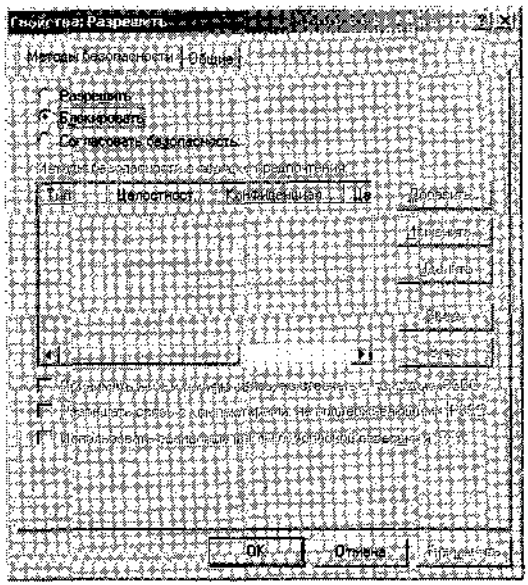


Рис. 11-29. Создание блокирующего действия фильтра

16. На вкладке **Общие (General)** и в поле **Имя (Name)** введите block и щелкните OK.
17. На вкладке **Действие фильтра (Filter Action)** выберите действие **Блокировать (Block),** щелкните **Закрыть (Close),** а затем — OK.

Создание политики не изменяет поведение компьютера — для этого надо применить политику: щелкнуть значок политики правой кнопкой и выбрать **Назначить (Assign).** На машине разрешается только одна активная политика. В упражнениях 2–5 вы назначите политику и проследите за действием политики IPSec.

Упражнение 2. Создание политики согласования

При создании запрещающей политики достаточно определить правило только на одном компьютере. Она блокирует поступление данных на компьютер. Однако обеспечить защищенную связь между двумя компьютерами намного сложнее. В этом упражнении вы сначала создаете более сложную политику и назначите ее на обоих компьютерах.

- **Создание политики шифрования связи между двумя компьютерами**

Политики согласования должны практически совпадать на обоих компьютерах. Политику, которую вы определите, надо экспортировать, а затем импортировать на Computerl. Далее политики надо назначить на обоих компьютерах — только после этого станет возможным обмен шифрованными данными. Если в домене Windows многие компьютеры используют одну политику, ее можно создать как часть объекта групповой политики (GPO).

1. В консоли *Security Configuration Management* (см. упражнение 1) щелкните правой кнопкой **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** и выберите **Создать политику безопасности IP (Create IP Security Policy).**
2. В окне **Мастер политики IP-безопасности (IP Security Policy Wizard)** щелкните **Далее (Next).**
3. **В** поле **Имя (Name)** введите encrypt telnet t raf f ic. В поле **Описание (Description)** введите описательный текст и щелкните **Далее.**
4. Сбросьте флажок **Использовать правило по умолчанию (Activate the default response rule)** и щелкните **Далее,** а затем — **Готово (Finish)..**
5. В окне свойств политики перейдите на вкладку **Общие (General)** (рис. 11-30) и щелкните кнопку **Параметры (Settings),** чтобы просмотреть и скорректировать параметры обмена ключами.

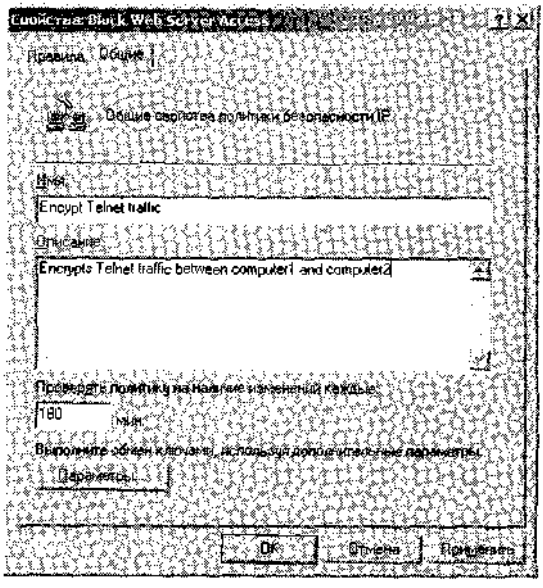


Рис. 11-30. Корректировка параметров обмена ключами

6. В окне **Параметры обмена ключами (Key Exchange Settings)** (рис. 11-31) щелкните кнопку **Методы (Methods). В** окне **Методы безопасности при обмене ключами (Key Exchange Settings)** определяют особенности создания основного ключа. Параметры описаны в табл. 11-6. Хотя частое обновление ключей обеспечивает повышенную безопасности связи, оно часто отрицательно сказывается на производительности.

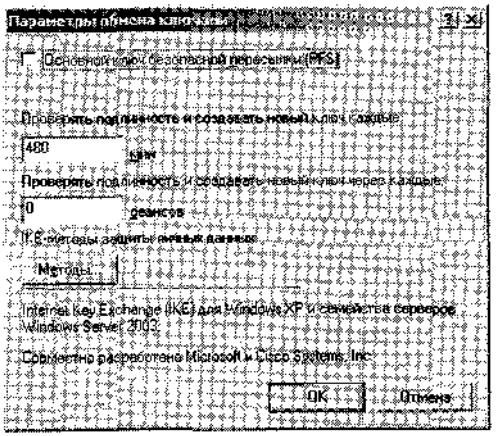


Рис. 11-31. Методы защиты

7. В окне **Методы безопасности при обмене ключами** выберите четвертый (последний) заданный по умолчанию метод защиты и щелкните кнопку **Удалить (Remove).** Затем удалите третий метод защиты. Должны остаться два первых метода (рис. 11-32).

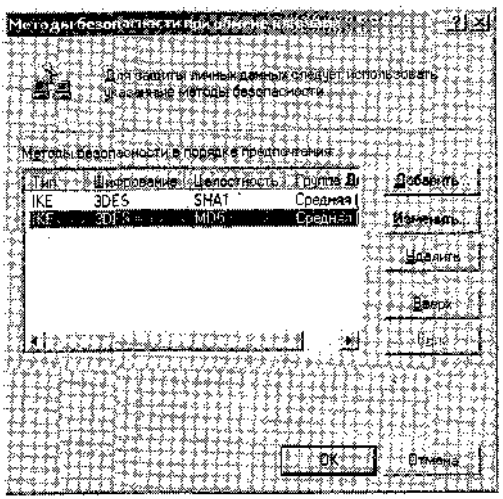


Рис. 11-32. Сокращенный список методов защиты

Удаление двух методов и изменение группы Диффи-Хеллмана оставшихся методов защиты укрепляет безопасность основного ключа, но может отрицательно сказаться на производительности. Компьютер, пытающийся создать подключение, должен поддерживать по крайней мере один из двух оставшихся методов, иначе подключение создать не удастся.

8. Выберите один из оставшихся методов защиты и щелкните **Изменить (Edit).**

9. В окне **Алгоритмы безопасности IKE (IKE Security Algorithms)** в поле со списком **Группа Диффи-Хелмана (Diffie-Hellman Group)** выберите **Высокая (2048) [High (2048)],** как показано на рис. 11-33. Щелкните OK. Повторите аналогичную операцию со вторым методом защиты.

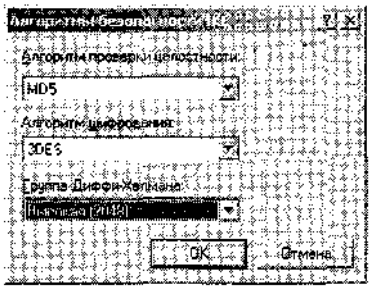


Рис. 11-33. Изменение группы Диффи-Хелмана

Изменение группы Диффи-Хелмана способствует укреплению безопасности по двум причинам. Во-первых, для вычисления основного ключа используются большие простые числа; во-вторых, связь возможна только с другими компьютерами под управлением Windows Server 2003, потому что только они поддерживают этот параметр. Выбор самой надежной группы Диффи-Хелмана часто вызывает проблемы, так как пользователи с «устаревшими» ОС утрачивают способность создавать подключения. Это также может отрицательно сказаться на производительности, ведь ключ длиннее и ресурсов на шифрование затрачивается больше.

10. Два раза щелкните **OK,** чтобы возвратиться к вкладке **Общие.** Затем перейдите на вкладку **Правила (Rules).**
11. Установите флажок **Использовать мастер (Use Add Wizard)** и щелкните **Добавить (Add),** чтобы добавить правило.
12. В окне **Мастер создания новых правил IP-безопасности (Create IP Security Rule Wizard)** щелкните **Далее.**
13. На странице **Конечная точка туннеля (Tunnel Endpoint)** щелкните **Далее. В** этой политике туннель не нужен.
14. На странице **Тип сети (Network Type)** щелкните **Далее,** приняв значение по умолчанию — **Все сетевые подключения (All network connections).** Эта политика действует независимо от того, где инициируется подключение.
15. На странице **Список фильтров IP (IP Filter List)** щелкните **Добавить (Add),** чтобы создать список фильтров.
16. В поле **Имя (Name)** введите `negotiate`, а в поле **Описание (Description)** — описательный текст.
17. Установите флажок **Использовать мастер (Use Add Wizard)** и щелкните кнопку **Добавить (Add),** чтобы добавить фильтр.
18. В окне **Мастер IP-фильтра (IP Filter Wizard)** щелкните **Далее (Next).**
19. **В** поле **Описание (Description)** введите описание фильтра и щелкните **Далее.**
20. **В** поле со списком **Адрес источника пакетов (IP traffic source)** (рис. 11-34) выберите **Определенный IP-адрес (A Specific IP Address).**
21. **В** поле **IP-адрес (IP Address)** введите IP-адрес компьютера Computerl и щелкните Далее.

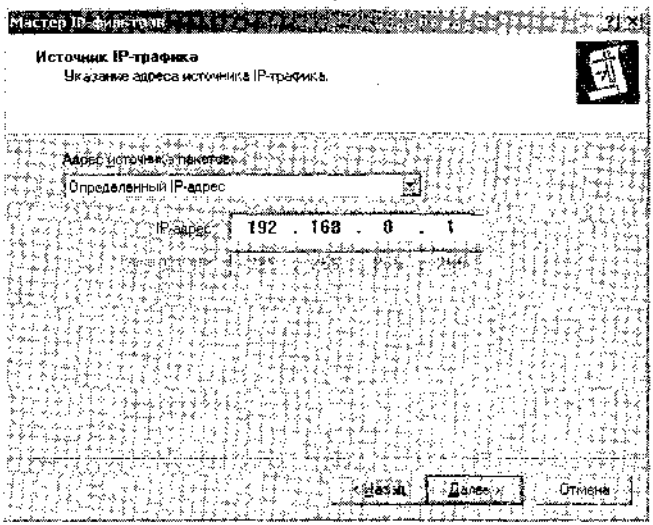


Рис. 11-34. Ввод конкретного источника трафика

22. На странице Назначение IP-трафика (IP Traffic **Destination)** в поле со списком Адрес назначения (Destination Address) выберите Определенный IP-адрес (A Specific IP Address) и введите IP-адрес Computer2. Щелкните Далее.
23. На странице Тип IP-протокола (IP Protocol Type) выберите TCP и щелкните Далее.
24. В пбле Пакеты на этот порт (to this port), введите 23, щелкните Далее, а затем — Готово (Finish).
25. Щелкните OK, чтобы возвратиться в окно Мастер правил безопасности.
26. Выберите фильтр Negotiate и щелкните Далее.
27. Выберите Требуется безопасность (Require Security) и щелкните Далее.
28. В качестве метода аутентификации выберите Kerberos и щелкните Далее, а затем — Готово (Finish).
29. Щелкните OK, чтобы завершить создание правила. Щелкните OK еще раз, чтобы закончить процедуру.

Импорт и последующий экспорт политики на другой компьютер

До назначения политики согласования надо позаботиться, чтобы на другом компьютере(ах) конфигурация политики совпадала. Один способ решения этой задачи — создать политику на другом компьютере вручную, но можно экспортировать политику с одного компьютера и импортировать на другой компьютер. Это вы и сделаете в этому упражнении.

1. В консоли *Управление политикой безопасности IP* (IP Security Policy Management) на Computer2 щелкните **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** правой кнопкой и выберите **Все задачи (All Tasks)\Экспортировать политики (Export Policies).**

Примечание Загвоздка в том, что при экспорте в файл выгружаются все политики локального компьютера, однако это не всегда нужно.

2. Перейдите к общей папке на Computerl, введите имя файла и щелкните **Сохранить (Save).**
3. На Computerl создайте консоль **Управление политикой безопасности IP (IP Security Policy Management).**
4. Щелкните правой кнопкой **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** и выберите **Все задачи (All Tasks)\Импортировать политики (Import Policies).**
5. Выберите файл политики и щелкните **Открыть (Open).** Политика безопасности успешно скопирована на компьютер. Закройте все консоли и выйдите из системы обоих компьютеров.

Упражнение 3. Управление IPSec с помощью Netsh

Любую задачу, доступную в оснастке *Управление политикой безопасности IP* (IP Security Policy Management), можно выполнить с помощью команды Netsh. Более того, эта утилита позволяет делать то, что невозможно в оснастке, например: применение безопасности компьютера при запуске, определение ограничения трафика при загрузке, определение уровня диагностика, соблюдение ограничений трафика по умолчанию, выполнение строгой проверки CRL, журналирование IKE (Oakley), изменение интервалов записи в журналы и создание постоянной политики.

Вы создадите политику путем настройки параметров IKE и добавления правил, состоящих из списков фильтров, действий фильтров и других параметров. В этом упражнении команды позволят создать политику IPSec, которая обезопасит telnet-трафик между Computerl и Computer2 и запретит telnet-доступ с любых других компьютеров помимо Computer2. Создать политику надо как на Computerl, так и на Computer2. В упражнении предлагается выполнять эту задачу по команде за раз. Хотя, вы вправе создать командный файл и применить политику «одним махом». В реальности последний метод намного популярнее, но наша задача — научиться использовать утилиту. Каждая команда вводится нажатием клавиши Enter. На рис. 11-35 показан результат выполнения команд по созданию политики на Computer2 (пп. 2—5). Столкнувшись с сообщением об ошибке, внимательно проверьте синтаксис команды. Если надо начать все сначала, удалите политику командой Delete Policy Name=Telnet.

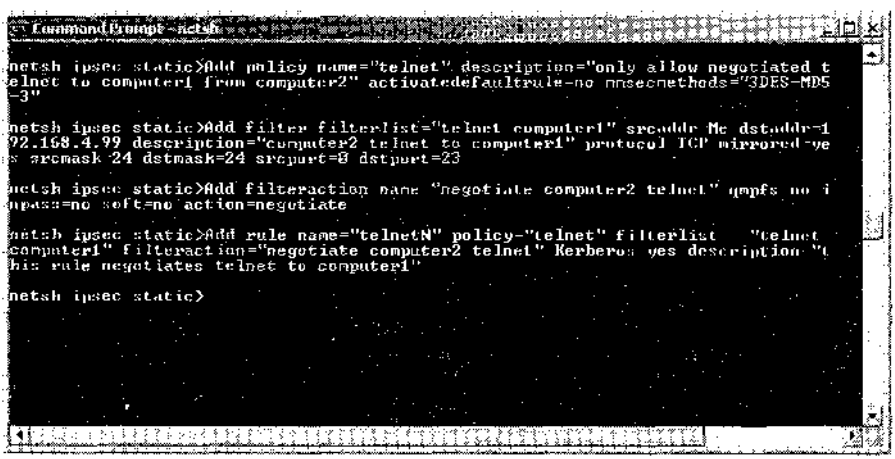


Рис. 11-35. Создание политики средствами Netsh

1. Выполните команду входа в Netsh, а затем переведите утилиту в статический контекст:

   ```
   Netsh
   NetshMpsec static
   ```

2. Создайте политику на Computerl командой:

   ```
   Add policy name="telnet"
   description="only allow negotiated telnet from computer2 to computerl"
   activatedefaultrule=no mmsecroethods="3D ES-MD5-3"
   ```

   В этой политике надо задать два правила. Одно блокирует весь telnet-трафик, а второе организует согласование telnet между Computer2 и Computerl. Перед созданием правил надо задать список фильтров, сами фильтры и действие фильтра. Если создать фильтр для несуществующего списка фильтра, список фильтров создается автоматически.

3. Создайте список с одним фильтром, который реагирует на telnet, а в качестве IP-адреса источника задайте 192.168.0.2 (Computer2):

   ```
   Add filter filterlist="telnet computer2"
   srcaddr=192.168.0.2 dstaddr=Me description="computer2 telnet to computerl"
   protocol=TCP mirrored=yes srcmask=32 dstmask=32 srcport=0 dstport=23
   ```

4. Следующая команда определяет действие фильтра, согласующего telnet между Computer2 и Computerl:

   ```
   Add filteraction name="negotiate computer2 telnet"
   qmpfs=no inpass=no soft=no action=negotiate qmsecmethods="ESP[3DES,MD5]"
   ```

5. Добавьте правило, управляющее согласованием telnet:

   ```
   Add rule name="telnetN" policy="telnet"filterlist="telnet computer2"
   filteraction="negotiate computer2 telnet"
   Kerberos=yes description="this rule negotiates telnet if the source computer is
   computer2"
   ```

   Обратите внимание, что правило связывает список фильтров, действие фильтра и метод аутентификации. Если метод аутентификации не задан, по умолчанию используется Kerberos.

6. Подготовьте список фильтров и действие фильтра для второго правила: создайте список с одним фильтром, который реагирует на telnet и запрещает telnet-трафик с любых компьютеров:

   ```
   Add filter filterlist="blocktelnet"
   srcaddr=Any dstaddr=Me description="all telnet to computerl"
   protocol=TCP mirrored=yes srcmask=24 dstmask=24 srcport=0 dstport=23
   ```

7. Добавьте действие фильтра — блокировка telnet-трафика:

   ```
   Add filteraction name="block all telnet" inpass=yes action=block
   ```

8. Создайте правило, управляющее согласованием telnet:

   ```
   Add rule name="telnetN" policy="telnet"filterlist="blocktelnet"
   filteraction="block all telnet"
   ```

Kerberos=yes description="this rule negotiates telnet if the source computer is computer2"

9. Назначьте политику:

   set policy name=telnet assign=yes

10. Войдите в систему Computer2 как *Администратор* (Administrator) и откройте окно командной строки.
11. Откройте контекст Netsh. На Computer2 надо задать один список фильтров, с одним фильтром и действием. Это позволит согласовать telnet-подключение с Computed. Сначала создадим политику командой:

    Add policy name="telnet"
    description="only allow negotiated telnet to computeri from computer2"
    activatedefaultrule=no mmsecrnethods="3D ES-MD5-3"

12. Затем создайте список фильтров:

    Add filter filterlist="telnet computeri"
    srcaddr=Me dstaddr=192.168.0.2 description="computer2 telnet to computeri"
    protocol=TCP mirrored=yes srcmask=32 dstmask=32 srcport=0 dstport=23

13. Далее создайте действие фильтра:

    Add filteraction name="negotiate computer2 telnet"
    qmpfs=no inpass=no soft=no action=negotiate

14. Теперь добавьте правило, управляющее согласованием telnet:

    Add rule name="telnetN" policy="telnet"filterlist = "telnet computeri"
    filteraction="negotiate computer2 telnet"
    Kerberos=yes description="this rule negotiates telnet to computeri"

15. Наконец, назначите политику. Помните, что в каждый момент времени активна только одна политика. Эту команду надо выполнить на обоих компьютерах.

    set policy name=telnet assign=yes

16. Закройте Netsh.

Упражнение 4. Применение Netsh для мониторинга IPSec

После создания и назначения политики IPSec средствами Netsh, вы примените эту же утилиту для мониторинга сеанса.

1. На любом из компьютеров запустите Netsh:

   Netsh
   Netsh>ipsec static

2. Командой Show проверьте активную политику, чтобы убедиться в успешности применения политики:

   show policy name=telnet level=verbose

3. Перейдите в динамический режим:

   dynamic

4. Включите диагностику и запись всех событий (по умолчанию определено значение *0,* то есть запись отключена):

```
set config property=ipsecdiagnostics value=7
```

5. Установите интервал IPSec в 60 сек.:

```
set config property=ipseclogginterval value=60
```

6. Отобразите информацию об основном и быстром режиме сопоставления командами Show Mmsas All (рис. 11-36) и Show Qmsas All (рис..11-37) соответственно.

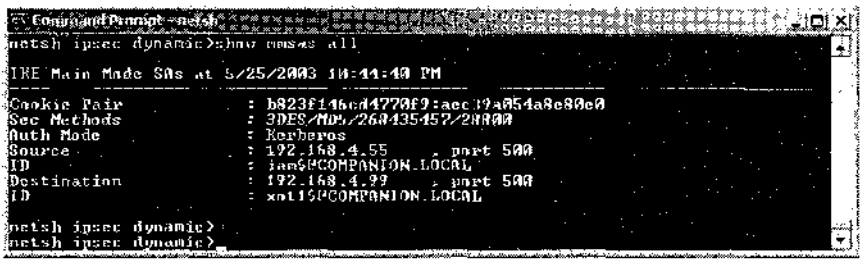


Рис. 11-36. Просмотр статистики основного режима IKE

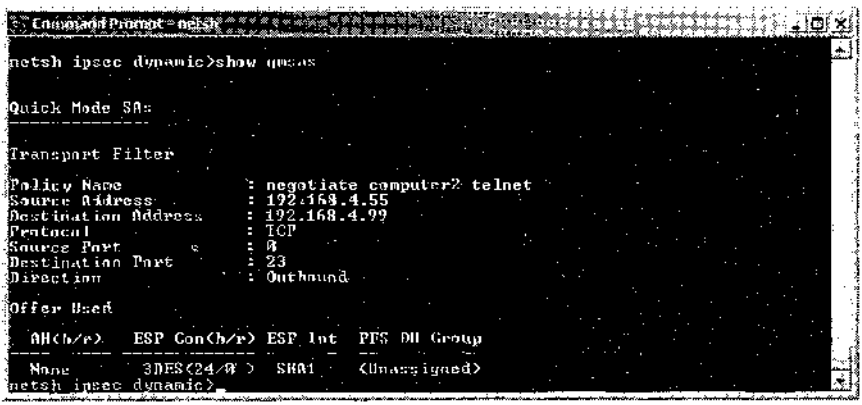


Рис. 11-37. Просмотр статистики быстрого режима IKE

7. Введите quit, чтобы выйти из Netsh.

Упражнение 5. Применение *Монитора IP-безопасности* для мониторинга IPSec-подключения

Вы проследите за работой IPSec с помощью оснастки *Монитор IP-безопасности* (IP Security Monitor).

1. Откройте оснастку **Монитор IP-безопасности** на обоих компьютерах.
2. Убедитесь, что активна назначенная вами политика **IPSec.** Ознакомьтесь с параметрами активной политики. Совпадают ли они с теми, что вы задали?

3. Последовательно дважды щелкните подузлы **Сопоставления безопасности (Security Associations)** узлов **Основной режим (Main Mode)** (рис. 11-38) и **Быстрый режим (Quick Mode)** (рис. 11-39). Этот позволит узнать, какой метод шифрования используется.

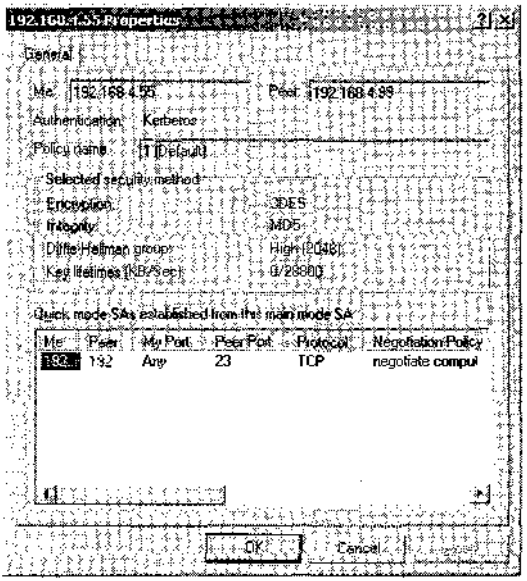


Рис. 11-38. Свойства основного режима с информацией о методе шифрования

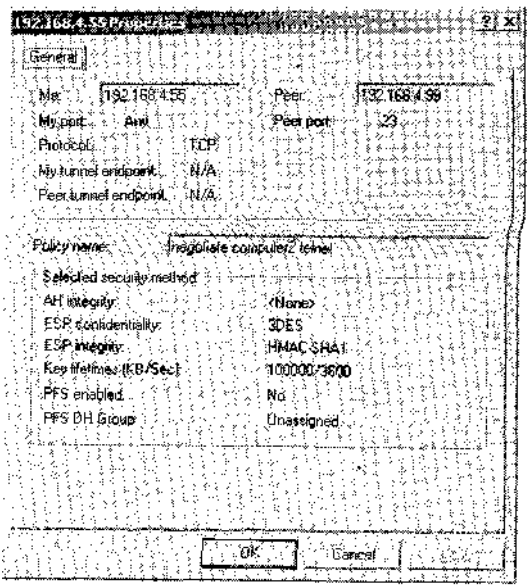


Рис. 11-39. Свойства быстрого режима с информацией о методе шифрования

4. Закройте окна.

Упражнение 6. Использование Netcap для записи сетевой информации протокола IPSec

1. На Computerl создайте файл Testl.txt, щелкнув правой кнопкой общую папку **Shared Captures** в *Проводнике* (Windows Explorer), выбрав **Создать (New)** и **Текстовый документ (Text Document).** Затем укажите имя файла — Testl.txt — и щелкните OK.
2. На Computer2 откройте окно командной строки и выполните Netcap с буфером 1 Мб и сохраните записанные данные в файл *C:\Authentication.cap* (рис. 11-40):

   ```
   netcap /c:c:\authentication.cap /n:0
   ```

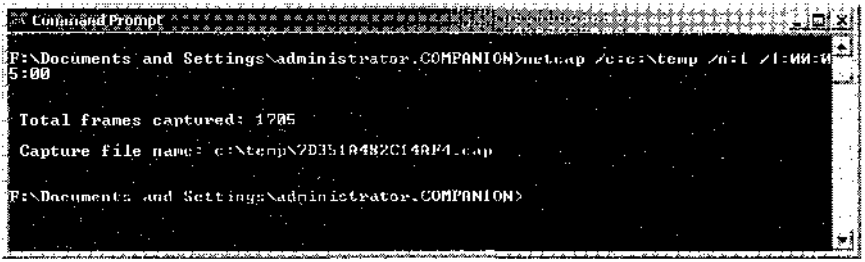


Рис. 11-40. Использование Netcap для запуска и остановки записи данных без загрузки *Сетевого монитора* (Network Monitor)

3. При включенной записи данных подключитесь к общей папке *\\Computerl\Captures* на контроллере домена и дважды щелкните файл Testl.txt, чтобы открыть его в *Блокноте* (Notepad).
4. Измените содержимое файла и попытайтесь сохранить его. Появится сообщение о запрещении доступа, так как по умолчанию группе *Все* (All) предоставлено разрешение только на чтение.
5. В другом окне командной строки подключитесь по telnet к контроллеру домена командой:

   ```
   telnet computerl
   ```

6. Вернитесь в окно командной строки для Netcap и нажмите клавишу «пробел», чтобы остановить сбор данных. В окне отобразится информация о названии файла с записанными данными.
7. Откройте файл с записями в Network Monitor и найдите информацию, подтверждающую чтение файла. Текст в файле должен отображаться открытым текстом.
8. Найдите согласование ISAKMP и кадры ESP. Ответьте на вопрос.
   О чем говорит информация кадров?
9. Закройте файл записи данных и окно сетевого монитора.

Упражнение 7. Просмотр кэша билетов Kerberos с помощью утилиты Kerbtray

При устранении неполадок Kerberos часто полезной оказывается проверка содержимого кэша билетов. Следует узнать, как это делается. В этом упражнении вы увидите, как при подключении к общему файловому ресурсу клиентский компьютер получает билет службы CIFS, который нужен для аутентификации на удаленном компьютере. Билет остается в кэше и может использоваться повторно.

1. На Computer2, загрузите и установите комплект ресурсов Windows Server 2003 со страницы *http://www.microsoft.com/downlaods/details.aspx?=9d467a69-57ff-4ae7-96ee-bl8c4790cffd&*
2. Выйдите и снова войдите в систему компьютера.
3. Создайте новое подключение к общей папке *Мои записи {My Captures)* на Computerl.
4. Запустите программу Kerbtray.exe из папки *the C:\Program Files\Windows Resource Kits\Tools.*
5. В строке состояния рабочего стола дважды щелкните значок Kerbtray.
6. Выберите билет, используемый для аутентификации при доступе к общему файловому ресурсу и ответьте на вопрос.
   Какая служба используется для доступа к общему файловому ресурсу?
7. Исследуйте вкладки свойств всех билетов в кэше, чтобы узнать, какие сведения на них отображаются.
8. Отключитесь от общего ресурса.
9. В строке состояния щелкните правой кнопкой значок **Kerbtray** и выберите **Exit Kerb Tray.**

Упражнение 8. Использование Klist для очистки и просмотра кэша билетов Kerberos

Вы воспользуетесь командой Klist для управления кэшем билетов Kerberos.

1. Выберите **Пуск (Start)\Все программы(A11 Programs)\Windows Resource Kit Tools\Command Shell.**
2. В командной строке выполните команды:
   - `klist tgt` — чтобы получить информацию о билетах на компьютере;
   - `klist tickets` — чтобы увидеть информацию о всех билетах на компьютере;
   - `klist purge` — чтобы удалить все билеты.

   Ответьте на вопросы: Удается ли подключиться к общему файловому ресурсу? Почему?
3. Выйдите и снова войдите в систему.
4. Командой `Klist Tickets` просмотрите билеты в кэше билетов.
5. Закройте командную строку и выйдите из системы компьютера.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

1. Протокол IPSec обычно применяется для защиты связи между двумя компьютерами. Какие еще функции он поддерживает? (Выберите все подходящие варианты.)
   a. Анализ билетов Kerberos.
   b. Поблочную пересылку отдельных пакетов протокола.
   c. Передачу пакетов с TCP-порта назначения 23 с любого компьютера на локальный компьютер.
   d. Подключение одного пользователя по telnet к компьютеру с одновременной блокировкой доступа другим пользователям.

2. Какой самый весомый аргумент в пользу назначения политики средствами Netsh, когда групповая политика используется для назначения политики IPSec на многих компьютерах?
   a. Netsh — единственный способ применить политику, которая может использоваться для предоставления пользователю доступа по telnet одновременно с запрещением такого доступа с других компьютеров.
   b. Netsh решает задачу намного быстрее, если речь идет об единовременном конфигурировании многих машин.
   c. Применять Netsh можно, даже если компьютеры не относятся к домену, а групповая политика поддерживается только в домене.
   d. Netsh позволяет создать постоянную политику, которая будет работать в условиях, где групповая политика не поддерживается.
3. Netsh применяется для создания и назначения политики IPSec на автономном сервере с Windows Server 2003. Одна из команд выполнена в статическом контексте (Netsh IPSec Static):

   ```
   Add rule name="SMTPBlock" policy="smtp"filterlist="smtp computerlist"
   filteraction="negotiate smtp" description="this rule negotiates smtp"
   ```

   Почему политика не работает?
   a. В политике определены неправильные IP-адреса.
   b. Политики определяют разные алгоритмы шифрования.
   c. Шифрование отсутствует, а есть только «мягкие» согласования.
   d. Политика предусматривает Kerberos в качестве метода аутентификации, но компьютер не является членом домена.

Резюме

- Статический режим (команда Netsh IPSec Static) утилиты Netsh применяют для создания и назначения политики IPSec.
- Динамический режим (команда Netsh IPSec Static) утилиты Netsh применяют для активизации диагностики, добавления постоянной политики и изменения других параметров конфигурации.
- Постоянная политика — та, что применяется в условиях, когда невозможна доменная политика или политика, созданная в оснастке *Управление политикой безопасности IP (IF* Security Policy Management).
- Kerbtray.exe применяется для просмотра информации о билетах пользователей, вошедших в систему с применением Kerberos.
- Klist.exe применяется для просмотра и очистки кэша билетов путем выполнения команд в командной строке.
- Netcap применяется для записи данных в системе, где нет или нельзя установить *Сетевой монитор* (Network Monitor). Записанные данные изучаются на компьютере с сетевым монитором.

Занятие 3. Устранение неполадок протоколов сетевой безопасности

Структура этого раздела такова: сначала формулируется суть неполадки, а затем подробно описывается, как ее устранять, применяя те или иные инструментальные средства.

Внимание! Применяя указанные здесь рекомендации, делайте поправку на реалии действительности. Надо тщательно следить, чтобы в процессе устранения неполадки случайно не уничтожить данные или не нарушить критически важные транзакции. Рекомендации часто слишком категоричны.

Например такая рекомендация: *Очистите файлы журналов — это позволит значительно сократит обьем данных, которые надо проанализировать.* В реальном мире перед этим обязательно сохранить копию файла журнала, чтобы не потерять данные. Более того — сохраненные файлы рекомендуется позже проанализировать на другом компьютере.
Нельзя перегружать систему, если вы не уверены, что это не скажется отрицательно на производственной системе или на работе сотрудников, которые ее используют.

Внимание! При устранении неполадок помните, что единственная задача сети — поддержка бизнеса компании. Таким образом к каждому случаю устранения неполадки надо подходить как к уникальному событию и тщательно взвешивать, в какой последовательности и как решать задачу. Например, решение проблемы на отключенной от сети критически важной системе кардинальных образом отличается от устранения незначительной неполадки в работающей на полной мощности сети.

Чтобы получить максимум от примеров устранения неполадок, а также для облегчения работы над упражнениями, которые вы будете выполнять самостоятельно, выполните перечисленные далее операции — это сократит объем данных, которые придется анализировать.

- Очистите журналы *Безопасность* (Security), *Система* (System) и *Приложение* (Application)
- Отмените назначение политики IPSec, которая возможно была назначена. Даже в упражнениях по устранению неполадок IPSec надо убедиться, что нет никаких политик, и лишь затем назначать нужную, неполадки которой будете устранять. А лучше всего отменить назначение политики и затем перегрузить сервер. Чтобы отменить назначение политики, просто щелкните правой кнопкой назначенную политику и выберите Снять (Unassign). Сделав это, вы будете уверены, что устраняете неполадки известной вам политики.
- Если вы решили не перезагружать компьютер, очистите кэш билетов и повторно войдите в систему. Приступая к устранению неполадок Kerberos, выключите сервер. Запустите запись сетевых данных на контроллере домена и затем перезагрузите сервер.

Изучив материал этого занятия, вы сможете:

- использовать такие инструментальные средства, как оснастки *Сетевой монитор* (Network Monitor), *Просмотр событий* (Event Viewer) и *Монитор IP-безопасности* (IP Security Monitor);
- использовать инструментальные средства Kerberos — Klist и Kerbtray — для устранения неполадок протоколов сетевой безопасности.

Продолжительность занятия — около 60 минут.

Задача 1. Не удается заставить работать созданную политику IPSec

Вы создадите и назначите политику IPSec, но обнаружите, что два компьютера вообще не в состоянии «общаться». Вы выполните ряд операций и примените несколько инструментов, чтобы устранить неполадки политики IPSec. Последовательность процедур оформлена в виде списка рекомендаций.

Примечание Аудит IKE включен по умолчанию. При включенном аудите событий входа в систему, события согласования IKE регистрируются в журнале *Безопасность* (Security). После назначения и начала успешной работы политики аудит можно выключить, добавив в раздел реестра *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Audit* параметр *DisableIKEAudits* со значением *1.* После этого надо перезапустить службу IPSec.

Есть также возможность увеличить объем информации, регистрируемый в журнале событий безопасности, определив запись события для каждого пакета. Для этого уровень аудита повышают до 7. Это делается с помощью Netsh или путем присвоения значения 7 параметру реестра *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec\EnableDiagnostic* вне зависимо от используемого метода изменения вступают в силу только после перезагрузки компьютера.

- Политика назначена? С помощью *Монитора IP-безопасности* или команды Netsh Ipsec Static Show Gpoassignedpoli убедитесь, что активна именно она.
- Если политика не та, что нужно, выясните какой объект групповой политики ответственный за это? Для этого воспользуйтесь командой Netsh Ipsec Static Show Gpoassignedpolicy или оснасткой *Результирующая политика* (Resultant Set of Policy).
- Каковы параметры политики? Выполните команду Netsh Ipsec Static Show All — надо убедиться, что политика назначена и что ее параметры корректны. Эту же информацию можно получить, просмотрев политику локальной машины средствами оснастки *Управление политикой безопасности IP* (IP Security Policy Management).
- Успешно ли проходит IKE-согласование? Проверьте журнал событий безопасности. Если аудит не включен, активизируйте его средствами оснастки *Редактор объектов групповой политики* (Group Policy Object Editor). События IKE-согласования (успех или неудача) отображаются в категории *Вход в систему* (Logon Events). Если IKE-согласование терпит сбой, проверьте параметры IKE. Одинаковы ли методы аутентификации, шифрования и смены ключа, настроенные на обоих компьютерах?

- Если IKE выполняется успешно, удачно ли выполняется быстрый режим? Проверьте журнал событий безопасности. Если быстрый режим сбоит, выясните, совпадают ли параметры шифрования быстрого режима, целостности', длины ключа, смены ключа, и др. Согласованы ли фильтры? Например, если вход и выход осуществляется по IP-адресам, то соответствуют ли они друг другу? Если на одном компьютере настроены порты для ввода и вывода, то наблюдается ли такая же ситуация на втором компьютере?
- Доходят ли пакеты до нужного компьютера? Для записи пакетов IPSec можно применить *Сетевой монитор*. Зашифрованный текст увидеть не удастся, но главное — убедиться, что пакеты доходят до компьютера. (Адреса источника будет достаточно.) Также, это позволит узнать, задействован ли протокол IPSec. Вы также вправе отменить шифрование в политике — это позволит анализировать содержимое записанных пакетов.
- Блокируются ли пакеты? Счетчика производительности для протокола IPSec не существует, но отброшенные IPSec-пакеты учитываются счетчиками *Отброшено полученных датаграмм* (Datagrams Received Discarded) и *Исходящих датаграмм отброшено* (Datagrams Outbound Discarded) объекта производительности IPv4. Однако оптимальный способ выяснить, блокируются ли пакеты заключается в использовании оснастки *Монитор IP-безопасности*.

Задача 2. Выяснение корректности работы запрещающих правил IPSec

Запрещающие (блокирующие) правила применяются для предотвращения прохождения входящих/исходящих пакетов на основании определенных условий: пакеты с/на определенные IP-адреса или диапазоны IP-адресов, определенного протокола или на конкретный порт. Проверить просто: достаточно взять другой компьютер и попытаться подключиться к закрытым входным портами, IP-адресам или по запрещенному протоколу. Намного сложнее убедиться, что такая ситуация наблюдается постоянно, то есть что доступ закрыт не случайно, а именно политикой, и что политика будет вести себя так же и далее. Для такой проверки используют два средства:

- Netsh — для настройки журналирования каждого события блокировки пакета;
- оснастки — для определения уровня диагностики и просмотра событий.

Задача 3. Выяснение, используется ли Kerberos при аутентификации

Windows Server 2003, Windows 2000 и Windows XP Professional — все эти ОС поддерживают аутентификацию на основе Kerberos при работе в доменах Windows Server 2003 или Windows 2000. Однако при невозможности использования Kerberos для аутентификации применяется NTLM, а в случае недоступности контроллера домена вход в систему выполняется на основе кэшированных реквизитов. Также, если при *подключении дисков* (mapping) по IP-адресу, а не имени сервера, для аутентификации применяется NTLM. Вполне возможно, что в достаточно большом домене Kerberos не используется постоянно, — это нормально.

Нельзя просто «выключить» NTLM и заставить использовать в домене только Kerberos. Однако можно облегчить процедуру применения Kerberos и наблюдать и выяснять, в каких случаях и когда для аутентификации используется Kerberos. Сначала проанализируйте журналы событий на предмет ошибок Kerberos.

Одна из самых популярных ошибок связана с расхождением времени компьютера и контроллера домена более, чем на 5 минут — Kerberos сбоит и соответствующие сообщения появляются в журналах. Служба времени на клиентах пытается синхронизироваться с контроллером, но если разница во времени превышает 30 минут, синхронизация невозможна. Другие ошибки обычно указывают на неполадки сети.

Записи событий входа в систему в журнале *Безопасность* (Security) содержат указание на используемый протокол. Они позволяют выяснить, какой протокол аутентификации использовался. Узнать, какой протокол используется также позволяет запись данных в сетевом мониторе.

Лабораторная работа 1. **Устранение неполадок IPSec с помощью оснастки *Монитор IP-безопасности***

IPSec — один из самых «крепких орешков», когда речь заходит об устранении неполадок этого протокола, но наилучший инструмент устранения неполадок — знание механизма работы IPSec и особенностей политики, а также оснастка *Монитор IP-безопасности* (IP Security Monitor).

Упражнение 1. Подготовка подсистемы аудита для записи событий IPSec

1. Убедитесь, что включен аудит событий: входа в систему, входа в систему под учетной записью и изменения политики.
2. На Computerl создайте новую MMC-консоль с двумя копиями *Редактора объектов групповой политики* (Group Policy Object Editor): первую — для политики домена по умолчанию и вторую — для политики контроллеров домена по умолчанию.
3. Сохраните консоль под именем *Domain GPOs.*
4. Разверните узлы: **Политика Default Domain Controllers Policy (Default Domain Controllers Policy), Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings)** и **Локальные политики (Local Policies).** Выберите узел **Политика аудита (Audit Policy).** Обратите внимание, что включен аудит событий входа в систему под учетной записью, управления учетными записями и доступа к объектам.
5. Ознакомьтесь с политикой аудита в политике домена по умолчанию и ответьте на вопрос.

   Определена ли эта политика?
6. Активизируйте политики *Аудит входа в систему* (Audit Logon Events), *Аудит управления учетными записями* (Audit Account Management) и *Аудит доступа к объектам* (Audit Object Access) для регистрации успехов и отказов. При настройке доменной политики по умолчанию она определяется для всех компьютеров домена. Это в нормально в данном случае, но в производственной среде это не очень хорошо. К настройке параметров аудита надо подходить очень осторожно, чтобы они не противоречили целям политики безопасности.
7. Откройте консоль *Управление политикой безопасности IP* (IP Security Policy Management), созданную в упражнении 1 занятия 3.
8. Добавьте еще одну оснастку *Управление политикой безопасности IP,* но для локального компьютера.
9. Посмотрите в правую панель консоли обоих оснасток, чтобы убедиться, что нет назначенных политик IPSec. Если такие политики есть, отмените их, щелкнув правой кнопкой и выбрав Снять (Unassign).

10. Включите дополнительный аудит утилитой Netsh:

```
netsh Ipsec Dynamic Set Config Property=Ipsecdiagnostics value=7
```

Упражнение 2. Изменение политики IPSec на Computer 1

1. В дереве консоли *Управление политикой безопасности IP* (IP Security Policy Management) выберите узел **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer).**
2. В правой панели дважды щелкните политику, созданную в упражнении 1 занятия 3.
3. Выберите активный (отмеченный) список IP-фильтров.
4. На вкладке **Действие фильтра (Filter Action)** выберите активное действие и щелкните кнопку **Изменить (Edit).**
5. На вкладке **Методы безопасности (Security Methods)** выберите метод защиты и щелкните **Изменить (Edit).**
6. Выберите **Настраиваемая безопасность (Custom)** и щелкните **Параметры (Settings).**
7. Измените алгоритм шифрования с **3DES** на **DES.**
8. Два раза щелкните OK и укажите оставшиеся методы защиты (рис. 11-41), не забыв изменить алгоритмы шифрования с 3DES на DES. Два раза щелкните OK.

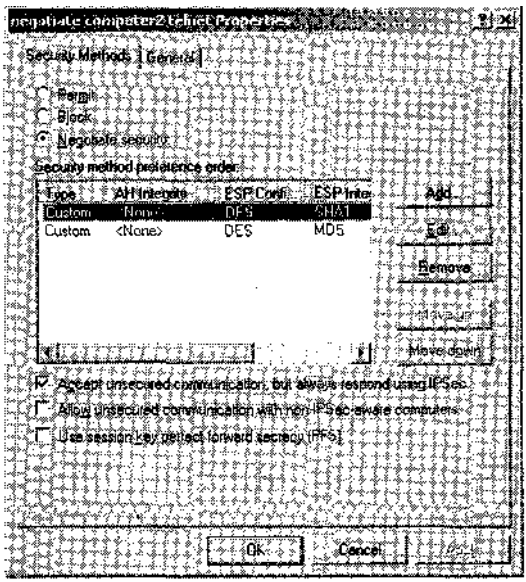


Рис. 11-41. Настройка смены ключа сеанса быстрого режима

9. Два раза щелкните OK. Затем щелкните **Закрыть (Close)** и **OK,** чтобы сохранить изменения политики.
10. Назначьте политику *telnet* на обоих компьютерах. Эта политика работала ранее, но она изменилась.
11. Попытайтесь подключиться по telnet с Computer2 к Computer 1. Удается ли это сделать?
12. В консоли *Управление политикой безопасности IP* откройте оснастку *Монитор IP-безопасности* (IP Security Monitor) для Computerl и выберите узел **Активная политика (Active Policy).** Какова активная политика и что в ней изменилось?

13. Активной должна быть политика *telnet.* Если это не так, скорее всего это и есть причина неполадки. Вернитесь и проанализируйте предыдущую часть упражнения. Запишите время — в производственной среде обязательно документировать любые изменения политики IPSec. Сравнивая время с временем создания интерфейса, можно обнаружить неправомочное изменение. Это объясняет причину проблемы, но не устраняет ее.
14. Перейдите в оснастку *Монитор IP-безопасности* на Computer2 и выберите узел **Активная политика.** Какова активная политика и когда она в последний раз менялась?
15. Откройте на обоих мониторах подузел **Статистика** (Statistics) узла **Основной режим (Main Mode)** и ознакомьтесь с содержанием правой панели. Есть ли сообщения о сбоях?
16. Откройте на обоих мониторах подузел **Статистика (Statistics)** узла **Быстрый режим (Quick Mode)** и ознакомьтесь с содержанием правой панели. Что обнаружилось?
17. Отмените назначение измененной политики и исправьте ее (верните «старый» тип шифрования— 3DES.)
18. Назначьте политику и перезапустите службу IPSec.
    Что теперь показывает монитор IPSec?
19. Отмените назначение политики на обоих компьютерах.

Лабораторная работа 2. **Устранение неполадок входа в систему с помощью *Сетевого монитора***

Часто приходится узнавать, какой протокол аутентификации используется, чтобы выяснить, почему некоторые пользователи испытывают трудности с доступом к ресурсам. Это также важно при определении, к каким ресурсам получают доступ посетители при подключении к сети, а также для планирования защиты протокола. Эти задачи вы будете решать в этом упражнении.

1. На Computer2 удалите все подключенные диски и другие подключения к Computerl.
2. Выйдите из системы Computer2.
3. Отключите сетевой кабель. Если компьютер не подключен к сеть, он не в состоянии получать билеты Kerberos, однако у пользователей, ранее прошедших аутентификацию в домене, сохранится способность входа в систему. Но они все равно не смогут использовать Kerberos.
4. С Computerl войдите в домен.
5. Запустите Kerbtray и убедитесь, что в кэше нет никаких билетов Kerberos.
6. Подключите обратно сетевой кабель.
7. Запустите запись данных в оснастке **Сетевой монитор (Network Monitor)** на Computerl.
8. Подключитесь к общей папке с записями на Computerl. В пути надо указать имя компьютера, то есть *\\Computerl\Captures*.
9. В меню **Запись (Capture)** сетевого монитора выберите **Остановить и просмотреть (Stop And View)** и ответьте на следующие вопросы.
   Удалось ли это сделать? Почему?
10. Для подтверждения проверьте запись сетевого трафика. Вы должны найти кадр согласования SMB (рис. 11-42), который указывает на использование NTLM. Запишите время регистрации кадра.

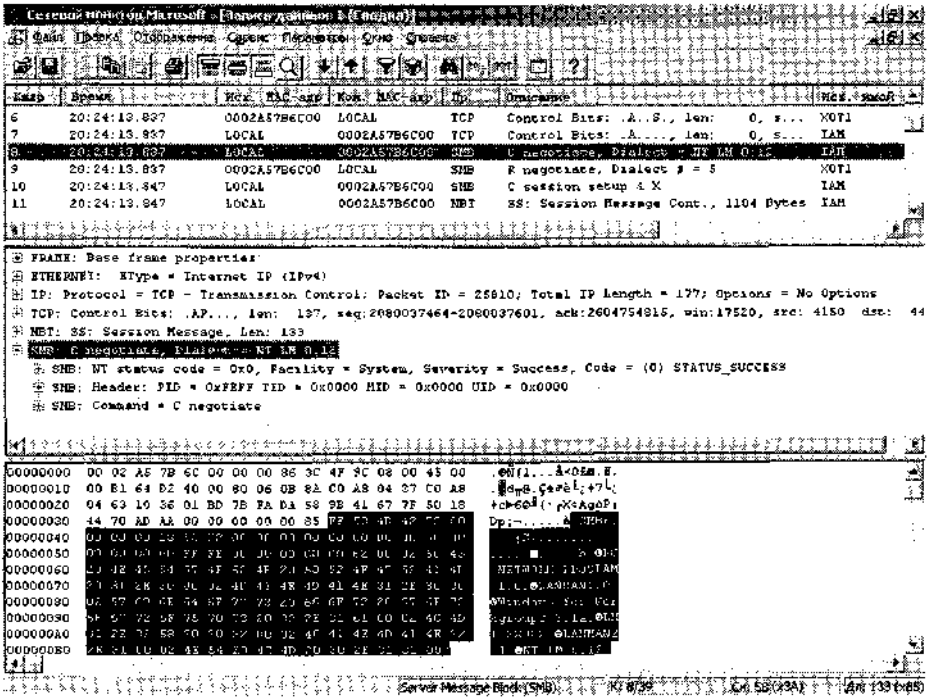


Рис. 11-42. Кадр NTLM-согласования в сетевом мониторе

Лабораторная работа 3. **Использование журналов событий для устранения неполадок**

В предыдущих двух упражнениях вы изменили политику IPSec и исследовали ее поведение в оснастке *Монитор IP-безопасности* (IP Security Monitor). Вы также использовали *Сетевой монитор* (Network Monitor) для исследования пакетов, которые показали, что для аутентификации Kerberos не применялся. В этом упражнении вы исследуете журналы, чтобы найти события, которые соответствуют тем, что обнаружены *Мониторе IP-безопасности* и *Сетевом мониторе*.

1. Воспользуйтесь временем, записанными в лабораторной работе 1, и найдите в журнале событий безопасности компьютера Computerl события IPSec. Вы должны найти запись об IKE-согласовании и ESP-пакеты, а также несколько сообщений об ошибках, связанных с потерей пакетов.
2. Воспользуйтесь временем входа в систему, записанными в лабораторной работе 2, и найдите в журнале событии безопасности компьютера Computerl события входа в систему под вашей учетной записью во время, записанное в процессе выполнения упражнения 2. Исследуйте эти события и ответьте на вопрос.

   Какое событие говорит об успешном входе в систему с применением NTLM?

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в разделе «Вопросы и ответы» в конце главы.

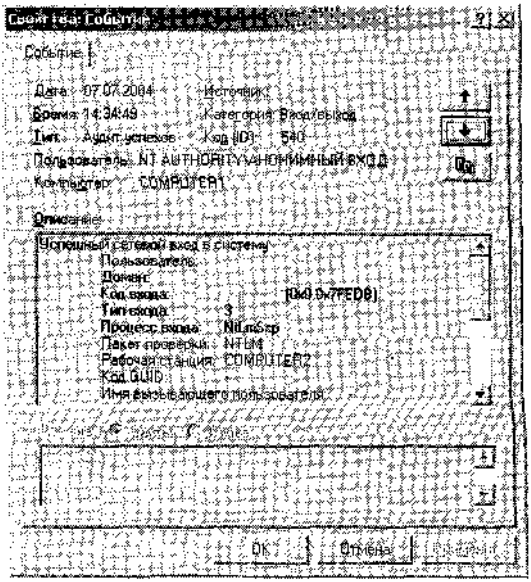


Рис. 11-43. NTLM-согласование в событиях успешного входа в систему

1. Политика IPSec назначена, но не удается обеспечить связь между двумя компьютерами. В *Мониторе IP-безопасности* обнаружено событие (рис. 11-44), метка времени которого указывает, что оно произошло в момент неудачного подключения. Какова наиболее вероятная причина сбоя?
   a. Ошибка аутентификации.
   b. Сбой согласования основного режима.
   c. Сбой согласования быстрого режима.
   d. Запрещена пересылка пакетов конкретного типа, которые должна блокировать политика.
2. В сеансе связи между двумя компьютерами в оснастке *Монитор IP-безопасности* наблюдается состояние, показанное на рис. 11-45. Что оно означает?
   a. Сеанс не шифруется, как ожидалось.
   b. Сеанс шифруется, как ожидалось.
   c. Сеанс отсутствует.
   d. На данном компьютере сеанс не принимается.
3. Вы вошли в домен, подключили диск к общей папке *\\192.168.5.55\share* и скопировали несколько файлов. Затем вы загрузили Kerbtray.exe, чтобы исследовать билеты Kerberos. В кэше обнаружились билет, вашей, учетной записи и службы krgbt, но нет билета CIFS для сервера. Какова наиболее вероятная причина неполадки?
   a. Для данного типа подключения предназначен билет krgbt.
   b. Использован IP-адрес, а не имя сервера, поэтому система задействовала NTLM.
   c. Утилита Kerbtray.exe показывает только TGT билеты, а в качестве билета для общего ресурса используется билет сеанса или пользователя.
   d. Утилита Kerbtray.exe показывает только билеты сеансов, а билет для общего ресурса — это TGT.

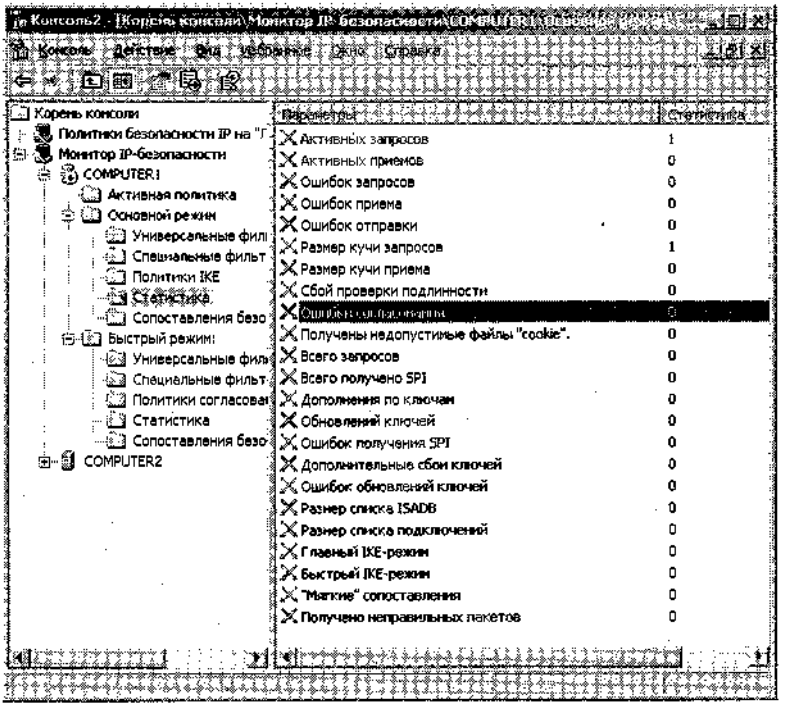


Рис. 11-44. Просмотр статистики

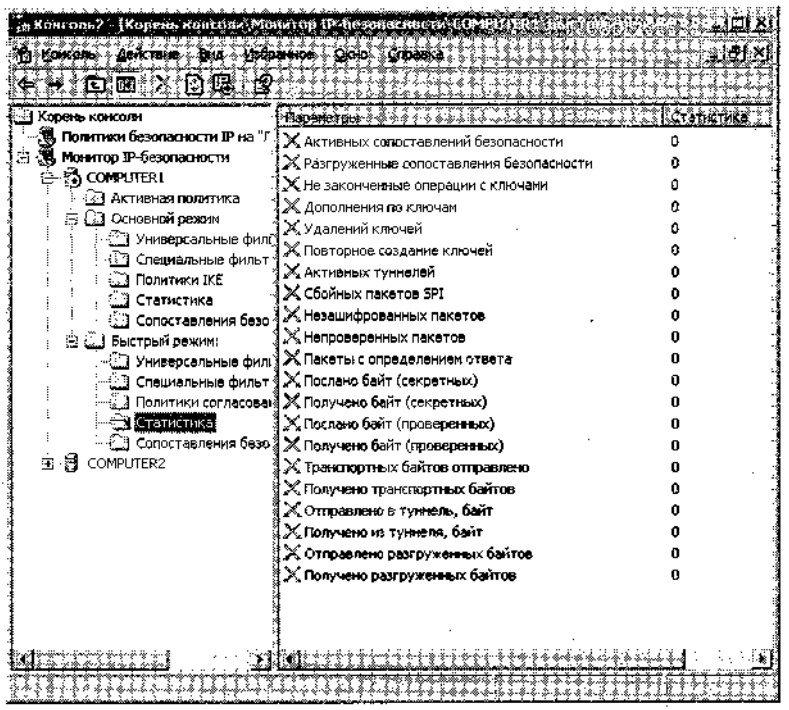


Рис. 11-45. Устранение неполадок путем анализа статистики

Резюме

- Есть несколько утилит, применяемых для устранения неполадок IPSec, в том числе оснастка *Монитор IP-безопасности* (IP Security Monitor), утилита Netsh, журнал событий *Безопасность* (Security) и *Сетевой монитор* (Network Monitor).
- Уровень записи в журнал можно изменять в соответствии потребностью в информации для устранения неполадок. Если записываемая информации переполняет журналы событий, а проблем выявить не удается, уровень записи снижают, изменяя соответствующий параметр реестра.
- Самые популярные ошибки реализации IPSec можно избежать, если предварительно проверить политику на предмет полноты и соответствия на разных компьютерах.
- Kerberos не всегда используется в домене для аутентификации.

Практикум по устранению неполадок

Вы воспользуетесь полученными в этой главе знаниями для устранения неполадок связи. Задача состоит в обеспечении защищенной telnet-связи по протоколу IPSec с Computerl.

Установка

1. Войдите в систему как член группы *Администраторы домена* (Domain Admins).
2. Откройте консоль *Управление политикой безопасности IP* (IP Security Policy Management), созданную в этой главе для проверки политики IPSec на Computerl и Computer2. Если политика IPSec назначена, щелкните ее значок правой кнопкой и выберите Снять (Unassign).
3. Запустите службу telnet на Computerl.
4. На Computer2 в окне командной строки откройте telnet-сеанс с Computerl.
5. После подключения выйдите из сеанса telnet.
6. На Computer2 скопируйте файл Ipsec2.bat из папки *\70-291\Labs\Chapterll* на прилагаемом компакт-диске на диск С.
7. В окне командной строки перейдите в корень диска С и запустите командный файл Ipsec2.bat на исполнение.
8. На Computerl скопируйте файл Ipsecl.bat из той же папки файл на диск С.
9. В окне командной строки перейдите в корень диска С и запустите командный файл Ipsecl.bat на исполнение.
10. Попытайтесь подключиться к Computerl с Computer2 по протоколу telnet. Удается ли открыть telnet-сеанс с Computerl?

Выяснение причины неполадки

Вчера стандартная операция проходила без сучка и задоринки, а сегодня ее просто невозможно выполнить. Что произошло? Ясно, что-то изменилось. Иногда вполне понятные сообщения об ошибках позволяют выяснить, в чем причина, но бывает и так, что компонент просто отказывается работать. Именно на вас, на администратора возлагается задача найти и устранить неполадку. Первым делом надо выяснить причины неполадки.

1. Назовите несколько причин, из-за которых telnet может отказываться работать?
2. Соберитесь с мыслями. Это иногда позволяет отмести часть причин и определить список задач.

   Какие задачи надо выполнить и каком порядке? Имеются ли любые задачи, которые Вы не должны делать?
3. Выполняйте задачи согласно списка. На Computer2 выполните команду ping compute r1.

   Удается ли получить эхо-ответ с Computerl?
4. Откройте оснастку *Службы* (Services) и в меню **Действие (Action)** выберите **Подключиться к другому компьютеру (Connect To Another Computer).**
5. На Computerl найдите службу Telnet.

   Работает ли служба telnet?
6. Запустите службу.
7. Откройте консоль *Управление политикой безопасности IP* (IP Security Policy Management) и исследуйте узлы **Политики безопасности IP «Локальный компьютер» (IP Security Policies On Local Computer)** и **Политики безопасности IP на \\Computerl (IP Security Policies On \\Computerl).**

   Назначена ли новая политика, которую вы никогда прежде не видели, на обоих узлах?
8. Отмените назначение политики на Computerl и Computer2.
9. В командной строке на Computer2 попытайтесь подключиться по telnet к Computerl.

   Удалось ли подключиться?
10. Итак, неполадка в одной или обеих политиках. Перейдите к следующему упражнению, чтобы устранить неполадки политик.

Устранение неполадок IPSec

Устранение неполадок IPSec ничем не отличается от аналогичной процедуры в других компонентах — надо применить свои знания о том, какие параметры необходимы, и устранить неполадку, применяя имеющиеся инструменты.

1. Мысленно проследите порядок, в котором выполняются действия в политике.

   Каков порядок этих действий?
2. В консоли *Управление политикой безопасности IP* (IP Security Policy Management) выберите узел **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** и дважды щелкните назначенную политику.
3. Щелкните **Изменить (Edit),** чтобы отредактировать список 1Р-фильтров.
4. На вкладке **Список фильтров IP (IP Filter List)** щелкните фильтр с выбранным вариантом и затем дважды щелкните 1Р-фильтр.

   Назначено ли в поле **Адрес источника пакетов (Source Address)** значение **Мой IP-адрес (My IP Address)?**

   Назначен ли в поле **Адрес назначения пакетов (Source Address)** определенный IP-адрес и является ли он адресом компьютера Computerl?
5. Замените IP-адрес на адрес компьютера Computerl. Поле маски подсети должно быть недоступным.
6. Щелкните OK четыре раза, чтобы закрыть политику.
7. Щелкните узел **Политики безопасности IP на «Computerl» (IP Security Policies On Computerl)** и дважды щелкните активную политику. Здесь два правила, которые надо проанализировать.

8. Выберите первое правило и проверьте его действие фильтра, перейдя на вкладку **Действие фильтра (Filter Action)** и дважды щелкнув выбранное действие.

   Каково действие фильтра?

9. Щелкните OK, а затем перейдите на вкладку **Список фильтров IP (IP Filter List).**
10. Дважды щелкните выбранное действие фильтра, а затем — сам фильтр.

    Назначен ли в поле **Адрес назначения пакетов (Source Address)** определенный IP-адрес и является ли он адресом компьютера Computer2?

    Назначено ли в поле **Адрес источника пакетов (Source Address)** значение **Мой IP-адрес (My IP Address)?**

11. Замените IP-адрес на адрес компьютера Computerl. Щелкните OK. четыре раза, чтобы закрыть политику.

    Теперь, когда IP-адреса гарантировано правильные, лучший способ увидеть, есть ли другие неполадки и если да, то где они встречаются, — запустить правило и исследовать информацию, представленную в оснастке *Монитор IP-безопасности* (IP Security Monitor).

12. Возвратитесь в консоль *Управление политикой безопасности IP* (IP Security Policy Management) на Computer2. Назначите все политики.
13. Из командной строки Computer2 попытайтесь подключиться по telnet к Computerl.
14. Вернитесь в консоль *Монитор IP-безопасности* на Computerl и выберите подузел **Статистика (Statistics)** узла **Основной режим (Main Mode).**

    Наблюдаются ли сбои аутентификации?

15. В консоли *Монитор IP-безопасности* выберите подузел **Универсальные фильтры (Generic Filters)** узла **Основной режим (Main Mode)** и дважды щелкните нужный фильтр в правой панели.
16. Перейдите на вкладку **Методы проверки подлинности (Authentication Methods).**

    Какой метод аутентификации используется?

17. Выберите подузел **Универсальные фильтры** узла **Основной режим** на Computer2.

    Какой метод аутентификации используется?

    Теперь понятна причина неполадки: методы аутентификации не совпадают. Поскольку оба компьютера относятся к домену и Kerberos — более безопасный метод аутентификации, надо заменить на Kerberos метод в политике на Computer2.

18. Выберите узел **Политики безопасности IP на «Локальный компьютер» (IP Security Policies On Local Computer)** и дважды щелкните назначенную политику.
19. Щелкните **Изменить (Edit),** чтобы открыть окно свойств правила.
20. На вкладке **Методы проверки подлинности** щелкните кнопку **Добавить (Add)** и выберите значение по умолчанию **Стандарт службы каталогов (Active Directory default).** Щелкните OK.
21. Выберите метод **Предварительный ключ (Preshared Key)** и щелкните кнопку **Удалить (Remove).** Подтвердите удаление щелчком Да (Yes).
22. Щелкните два раза OK, чтобы закрыть окно свойств политики.
23. В командной строке попытайтесь подключиться по telnet к Computerl.

    Успешна ли попытка?

Резюме главы

- Для проверки корректности работы политики IPSec применяют средства мониторинга: Netsh, *Монитор IP-безопасности* (IP Security Monitor), *Сетевой монитор* (Network Monitor) и журнал событий *Безопасность* (Security).
- Чтобы убедиться в использовании надежного протокола аутентификации Kerberos, применяют *Сетевой монитор* (Network Monitor) и журнал событий *Безопасность* (Security).
- Устраняя неполадки протоколов безопасности, следует помнить, что их отказ — это не просто мелкое неудобство. Если политика IPSec сбоит и связь становится невозможной, это — очень важная проблема. Однако если при «неисправной» политике IPSec подключение выполняется, этого допускать нельзя, точнее нельзя оставлять трафик не защищенным шифрованием, иначе компания сильно рискует своей безопасностью.
- Проблемы с Kerberos часто указывают на неполадки Active Directory, особенно сбои репликации.
- Неполадки Kerberos могут указывать как на нормальную работу этого протокола, так и на сбой или сигнал об атаке на сеть. Только знания позволят отличить нормальное поведение от патологии.
- Шаблоны безопасности используются для определения параметров защиты. На автономных компьютерах готовые шаблоны применяются средствами оснастки *Анализ и настройка безопасности* (Security Configuration and Analysis), а в доменах — путем импорта шаблона в доменную групповую политику.
- Оснастка *Анализ и настройка безопасности* (Security Configuration and Analysis) позволяет выяснить, соответствует ли конфигурация компьютера той или иной политике.
- Необходимо следовать, принципу наименьших привилегий, то есть предоставлять пользователям только те привилегии и доступ, которые нужны им для выполнения пяботы.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Разберитесь, какое поведение протоколов безопасности следует считать нормальным, — это облегчит устранение неполадок.
- Запомните, что билет TGT предоставляется пользователю после успешного входа в систему с использованием протокола Kerberos. Билет службы Kerberos или билет службы *предоставляются для доступа к определенной службе, например к общему файловому* ресурсу или службе LDAP. *TGT* нужен для получения *билета* службы.
- Запомните, что билеты Kerberos каптируются и могут использоваться повторно, а также обновляться. Когда билет становится невозобновляемым, надо получить новый билет, повторно войдя в систему.

- Научитесь использовать средства мониторинга IPSec — Netsh, журнал *Безопасность* (Security) и *Монитор IP-безопасности* (IP Security Monitor).

Основные термины

Netsh — утилита, служащая для управления и устранения неполадок IPSec в Windows Server 2003. Работает в одном из двух режимов — статическом или динамическом.

Основной режим ~ Main Mode — первая стадия подключения IPSec, в процессе которой компьютеры взаимно аутентифицируют друг друга, а затем с помощью IKE вычисляется основной ключ, на основе которого создаются остальные ключи. Также создаются согласования безопасности IKE, необходимые для организации быстрого режима.

Быстрый режим ~ Quick Mode — вторая стадия IPSec, в течении которой согласуются методы шифрования, алгоритмы контроля целостности и другие параметры политики. Создаются два согласования безопасности — входящее и исходящее.

Ticket Granting Ticket (TGT) ~ билет TGT — билет, выданный центром распространения билетов (KDC) Kerberos для получения билета от службы TGS. Билет TGT также называется билетом пользователя. Чтобы получить TGT, пользователь должен пройти аутентификацию в центре распространения билетов Kerberos.

Билет сеанса ~ session ticket — билет на доступ к ресурсам. Для запроса билета сеанса нужен билет TGT.

Щ Вопросы и ответы

Занятие 1. Закрепление материала

1. Надо применить новые параметры реестра на всех серверах сети. Как выполнить задачу с наименьшими усилиями?

   Правильный ответ: любой параметр реестра можно указать в Inf-файле шаблона безопасности (в разделе [Registry Wues]), используя *Блокнот* (Notepad). При применении шаблона, параметры реестра изменятся. Чтобы применить шаблон на многих машинах, можно воспользоваться сценарием или импортировать шаблон в групповую политику.

2. Какие из приведенных далее параметров можно применить с помощью оснастки *Анализ и настройка безопасности* (Security Configuration and Analysis) и шаблона безопасности? (Выберите все подходящие варианты.)

   a. Пароль должен быть не менее 15 символов.

   b. Группе *Бухгалтеры* (Accountants) надо запретить доступ к этому компьютеру по сети.

   c. Любое сетевое взаимодействие компьютеров Computerl и Computer2 должно выполняться с использованием IPSec.

   d. Необходимо установить следующие корневые разрешения для файлов: уровень доступа *Полный доступ* (Full Control); группа — *Все* (Everyone).

   Правильные ответы: a, b, d.

3. Что необходимо предпринять для восстановления «статуса-кво» после применения шаблона безопасности, после которого файловый сервер стал недоступным по сети для всех пользователей? Выберите наиболее эффективный способ.

a. Локально войти в систему файлового сервера как *Администратор* (Administrator) и применить корневой шаблон безопасности.

b. Локально войти в систему файлового сервера *как Администратор* (Administrator) и применить шаблон отката, созданный перед применением «некорректного» шаблона безопасности.

c. Выполнить удаленный вход в систему файлового сервера под учетной записью члена группы *Администраторы предприятия* (Enterprise Admin) и в консоли *Локальная политика безопасности* (Local Security Policy) изменить некорректные (на ваш взгляд) политики прав пользователей.

d. Выполнить удаленный вход в систему файлового сервера как *Администратор* (Administrator) и применить шаблон отката, созданный на основе шаблона безопасности.

Правильный ответ: b.

Занятие 2. Упражнение б

8. Найдите согласование ISAKMP и кадры ESP. Ответьте на вопрос.

   О чем говорит информация кадров?

   Правильный ответ: согласование прошло успешно и данные зашифрованы.

Занятие 2. Упражнение 7

6. Выберите билет, используемый для аутентификации при доступе к общему файловому ресурсу и ответьте на вопрос.

   Какая служба используется для доступа к общему файловому ресурсу?

   Правильный ответ: служба CIFS.

Занятие 2. Упражнение 8

7. В командной строке выполните команду klist purge, чтобы удалить все билеты.

   Ответьте на вопросы: Удается ли подключиться к общему файловому ресурсу? Почему?

   Правильный ответ: да, потому что применяется протокол NTLM.

Занятие 2. Закрепление материала

1. Протокол IPSec обычно применяется для защиты связи между двумя компьютерами. Какие еще функции он поддерживает? (Выберите все подходящие варианты.)

   a. Анализ билетов Kerberos.

   b. Поблочную пересылку отдельных пакетов протокола.

   c. Передачу пакетов с TCP-порта назначения 23 с любого компьютера на локальный компьютер.

   d. Подключение одного пользователя по telnet к компьютеру с одновременной блокировкой доступа другим пользователям.

   Правильные ответы: b, c.

2. Какой самый весомый аргумент в пользу назначения политики средствами Netsh, когда групповая политика используется для назначения политики IPSec на многих компьютерах?

a. Netsh — единственный способ применить политику, которая может использоваться для предоставления пользователю доступа по telnet одновременно с запрещением такого доступа с других компьютеров.
b. Netsh решает задачу намного быстрее, если речь идет об единовременном конфигурировании многих машин.
c. Применять Netsh можно, даже если компьютеры не относятся к домену, а групповая политика поддерживается только в домене.
d. Netsh позволяет создать постоянную политику, которая будет работать в условиях, где групповая политика не поддерживается.

Правильный ответ: d.

3. Netsh применяется для создания и назначения политики IPSec на автономном сервере с Windows Server 2003. Одна из команд выполнена в статическом контексте (Netsh IPSec Static):

```
Add rule name="SMTPBlock" policy="smtp" filterlist="smtp computerlist" filteraction=
"negotiate smtp" description="this rule negotiates smtp"
```

Почему политика не работает?

a. В политике определены неправильные IP-адреса.
b. Политики определяют разные алгоритмы шифрования.
c. Шифрование отсутствует, а есть только «мягкие» согласования.
d. Политика предусматривает Kerberos в качестве метода аутентификации, но компьютер не является членом домена.

Правильный ответ: d.

Занятие 3. Упражнение 1

5. Ознакомьтесь с политикой аудита в политике домена по умолчанию и ответьте на вопрос.

Определена ли эта политика?

Правильный ответ: нет.

Занятие 3. Упражнение 2

11. Попытайтесь подключиться по telnet с Computer2 к Computer 1. Удается ли это сделать?

Правильный ответ: Нет.

12. В консоли *Управление политикой безопасности IP* откройте оснастку *Монитор IP-безопасности* **(IP** Security Monitor) для Computerl и выберите узел **Активная политика (Active Policy).** Какова активная политика и что в ней изменилось?

Правильный ответ: активной должна быть ваша политика *telnet*. Время ее изменения позволяет узнать, какая политика изменилась. Однако если вы проверили обе политики, это не пригодится.

15. Откройте на обоих мониторах подузел **Статистика (Statistics)** узла **Основной режим (Main Mode)** и ознакомьтесь с содержанием правой панели. Есть ли сообщения о сбоях?

Правильный ответ: да, сообщение о сбое согласования.

16. Откройте на обоих мониторах подузел **Статистика (Statistics)** узла **Быстрый режим (Quick Mode)** и ознакомьтесь с содержанием правой панели. Что обнаружилось?

Правильный ответ: ничего не обнаруживается.

18. Назначьте политику и перезапустите службу IPSec.
Что теперь показывает монитор IPSec?
Правильный ответ: вы должны увидеть, что политика нормально функционирует.

Занятие 3. Лабораторная работа 2

9. В меню **Запись (Capture)** сетевого монитора выберите **Остановить и просмотреть (Stop And View)** и ответьте на следующие вопросы.
Удалось ли это сделать? Почему?
Правильный ответ: да. Поскольку применялся протокол NTLM.

Занятие 3. Лабораторная работа 3

2. Воспользуйтесь временем входа в систему, записанными в лабораторной работе 2, и найдите в журнале событий безопасности компьютера Computerl события входа в систему под вашей учетной записью во время, записанное в процессе выполнения упражнения 2. Исследуйте эти события и ответьте на вопрос.
Какое событие говорит об успешном входе в систему с применением NTLM?
Правильный ответ: событие на рис. 11-43 говорит об успешном входе в систему и используемом методе аутентификации — NTLM.

Занятие 3. Закреплейие материала

1. Политика IPSec назначена, но не удается обеспечить связь между двумя компьютерами. В *Мониторе IP-безопасности* обнаружено событие (рис. 11-44), метка времени которого указывает, что оно произошло в момент неудачного подключения. Какова *наиболее вероятная причина сбоя?*
   a. Ошибка аутентификации.
   b. Сбой согласования основного режима.
   c. Сбой согласования быстрого режима.
   d. Запрещена пересылка пакетов конкретного типа, которые должна блокировать политика.

   Правильный ответ: c.
2. В сеансе связи между двумя компьютерами в оснастке *Монитор IP-безопасности* наблюдается состояние, показанное на рис. 11-45. Что оно означает?
   a. Сеанс не шифруется, как ожидалось.
   b. Сеанс шифруется, как ожидалось.
   c. Сеанс отсутствует.
   d. На данном компьютере сеанс не принимается.

   Правильный ответ: b.
3. Вы вошли в домен, подключили диск к общей папке *\\192.168.5.55\share* и скопировав в - *несколько файлов. Затем вы загрузили Kerbtray.exe, чтобы исследовать билеты* Kerberos. В кэше обнаружились билет вашей учетной записи и службы krgbt, но нет билета CIFS для сервера, Какова наиболее вероятная причина неполадки?
   a. Для данного типа подключения предназначен билет krgbt.
   b. Использован IP-адрес, а не имя сервера, поэтому система задействовала NTLM.

c. Утилита Kerbtray.exe показывает только TGT билеты, а в качестве билета для общего ресурса используется билет сеанса или пользователя.

d. Утилита Kerbtray.exe показывает только билеты сеансов, а билет для общего ресурса — это TGT.

Правильный ответ: Ь.

Практикум по устранению неполадок. Установка

10. Попытайтесь подключиться к Computerl с Computer2 по протоколу telnet.

Удается ли открыть telnet-сеанс с Computerl?

Правильный ответ: нет.

Практикум по устранению неполадок. Выяснение причины неполадки

1. Назовите несколько причин, из-за которых telnet может отказываться работать?

Правильные ответы:

а **В одной из систем изменились разрешения.**

- **Отменены ваши административные привилегии.**
- **Computerl отключен от сети.**
- **На Computerl не работает служба telnet.**
- **На Computerl есть активная политика IPSec, и с ней что-то не в порядке.**

2. Соберитесь с мыслями. Это иногда позволяет отмести часть причин и определить, список задач.

Какие задачи надо выполнить и каком порядке? Имеются ли любые задачи, которые Вы не должны делать?

Правильный ответ: наиболее очевидное решение — проверить доступность Computerl в сети. Если он недоступен, любые другие методы устранения неполадок бесполезны.

Затем надо удаленно проверить, работает ли служба telnet на Computerl. Это решает несколько задач. Ясно, что для доступа к Computerl по этому протоколу служба telnet должна работать. Но если вы в состоянии удаленно открыть консоль *Службы* (Services) на Computerl, это значит, что административные привилегии остались прежними, кроме того вы можете удаленно запустить службу telnet.

Наконец, поищите доказательства активности политики IPSec. Если она назначена, ее можно отменить и проверить работу telnet. Если теперь telnet заработает, понятно, что источник неполадок — политика IPSec.

3. Выполняйте задачи согласно списка. На Computer2 выполните команду ping compute r1.

Удается ли получить эхо-ответ с Computerl?

Правильный ответ: да.

5. На Computerl найдите службу Telnet.

Работает ли служба telnet?

Правильный ответ: нет.

7. Откройте консоль **Управление политикой Политики безопасности IP на безопасности IP (IP Security Policy Management)** и исследуйте узлы **«Локальный компьютер» (IP Security Policies On Local Computer)** и **Политики безопасности IP на \\Computerl (IP Security Policies On \\Computerl).**

Назначена ли новая политика, которую вы никогда прежде не видели, на обоих узлах?

Правильный ответ: да.

9. В командной строке на Computer2 попытайтесь подключиться по telnet к Computer!.. Удалось ли подключиться?

   Правильный ответ: да.

Практикум по устранению неполадок. Устранение неполадок IPSec

Устранение неполадок IPSec ничем не отличается от аналогичной процедуры в других компонентах — надо применить свои знания о том, какие параметры необходимы, и устранить неполадку, применяя имеющиеся инструменты.

1. Мысленно проследите порядок, в котором выполняются действия в политике. Каков порядок этих действий?

   Правильный ответ: инициируется политика.

   Проверяется действие фильтра. Блокировка? Разрешение? Согласование? Блокирующее правило просто запрещает связь, а разрешающее — пропускает трафик.

   В последнем случае выполняется согласование, состоящее из нескольких операций: аутентификации, генерации основного ключа, создания согласований (основной режим), генерации ключа сеанса, согласований протоколов, шифрования и связи.

   Следующий шаг по устранению неполадок IPSec — посмотреть, можно ли «отсечь» некоторые из этих операций. Надо выяснить, где источник проблем. Если аутентификация проходит успешно, то ясно, что проблема не в ней. Или если есть ограничительные адреса IP и они неправильны, политика работать не будет. Поскольку проще всего сначала отсечь очевидные неполадки, в первую очередь рекомендуется проверить IP-адреса.

4. На вкладке **Список фильтров IP (IP Filter List)** щелкните фильтр с выбранным вариантом и затем дважды щелкните 1P-фильтр.

   Назначено ли в поле **Адрес источника пакетов (Source Address)** значение **Мой IP-адрес (My IP Address)?**

   Правильный ответ: да.

   Назначен ли в поле **Адрес назначения пакетов (Source Address)** определенный IP-адрес и является ли он адресом компьютера Computerl?

   Правильный ответ: нет.

8. Выберите первое правило и проверьте его действие фильтра, перейдя на вкладку **Действие фильтра (Filter Action)** и дважды щелкнув выбранное действие.

   Каково действие фильтра?

   Правильный ответ: согласование безопасности.

10. Дважды щелкните выбранное действие фильтра, а затем — сам фильтр.

    Назначен ли в поле **Адрес назначения пакетов (Source Address)** определенный IP-адрес и является ли он адресом компьютера Computer2?

    Правильный ответ: нет.

    Назначено ли в поле **Адрес источника пакетов (Source Address)** значение **Мой IP-адрес (My IP Address)?**

    Правильный ответ: да.

14. Вернитесь в консоль *Монитор IP-безопасности* на Computerl и выберите подузел **Статистика (Statistics)** узла **Основной режим (Main Mode).**

    Наблюдаются ли сбои аутентификации?

    Правильный ответ: да.

16. Перейдите на вкладку **Методы проверки подлинности (Authentication Methods).** Какой метод аутентификации используется?
Правильный ответ: Kerberos.
17. Выберите подузел **Универсальные фильтры** узла **Основной режим** на Computer2. Какой метод аутентификации используется?
Правильный ответ: общедоступный секрет.
23. **В** командной строке попытайтесь подключиться по telnet к Computerl. Успешна ли попытка?
Правильный ответ: да.

ГЛАВА 12

Поддержка сетевой инфраструктуры

Темы экзамена

- Мониторинг сетевого трафика.
- Устранение неполадок связи с Интернетом.
- Диагностика и устранение неполадок служб сервера:
  - зависимости служб;
  - параметры восстановления служб.

В этой главе

Настройкой сети дело не ограничивается — оставлять ее без присмотра просто опасно. При этом особое внимание нужно уделять трем моментам.

Во-первых, нужно контролировать, чтобы серверы сети имели доступ к. ресурсам, необходимым для обслуживания пользователей. Оптимальность работы серверов проверяется некоторыми встроенными средствами семейства Windows Server 2003. Надо также организовать оповещение о любых значимых событиях сети.

Во-вторых, важно следить за наличием подключения к Интернету. Наряду с электронной почтой, доступ в Интернет очень важен пользователям. В этой главе описано, что нужно проверять в первую очередь, когда пользователи жалуются на отсутствие доступа в Интернет.

Наконец, надо уметь настраивать и поддерживать работу служб сервера. Если пользователи сообщают об отказе, а сервер при этом нормально работает, то дело скорее всего в сбое нужной пользователям службы. Для устранения неполадок такого рода нужно уметь фиксировать их и устранять в самых различных обстоятельствах.

Прежде всего

Для изучения материала данной главы вам потребуется:

- два объединенных в сеть компьютера Computed и Computer2, оба под управлением ОС Windows Server 2003. Компьютеру Computed надо назначить статический адрес 192.168.0.1/24, а Computer2 нужно настроить на автоматическое присвоение адреса, а также определить на нем альтернативную конфигурацию с адресом 192.168.0.2/24;
- отдельные телефонные линии для каждого компьютера (рекомендуется);
- две учетных записи у интернет-провайдера или одна учетная запись, которая годится для одновременного подключения к Интернету двух компьютеров (рекомендуется) (можно использовать и выделенную линию, но тогда придется внести коррективы в упражнения).
- на Computed установить DNS-сервер с основной зоной, интегрированной в Active Directory, *domain 1. local;*

m Computerl назначить контроллером домена *domainl.local,* а Computer2 присоединить к этому домену в качестве рядового члена. Домен должен работать в смешанном режиме Windows 2000;

- на Computerl установить DHCP-сервер. DHCP-сервер надо авторизовать в домене и разместить на нем область Test Scope с диапазоном IP-адресов 192.168.0.11/24—192.168.0.254/24 с исключениями 192.168.0.100 и 192.168.0.200-192.168.0.205. Область надо активизировать.

Занятие 1. **Наблюдение за работой сети**

По завершении развертывания сети нужно убедиться, что узлам сети предоставлено достаточно пропускной способности для выполнения задач. *Пропускная способность* (bandwidth) для приложений, что воздух для человека — если его не хватает наступает удушье. Windows Server 2003 поддерживает несколько возможностей наблюдения за производительностью сети.

Наблюдение сети помогает локализовать неполадку и отбросить несущественные причины, поэтому важно знать, как выполняется мониторинг сети в Windows Server 2003.

В этом занятии описаны три способа, которыми применяются для устранения неполадок сети. Во-первых, это вкладка **Сеть (Network)** утилиты *Диспетчер задач* (Task Manager). Более подробное исследование проводят с помощью консоли *Производительность* (Perfomance). Наконец, вы узнаете о некоторых дополнительных возможностях записи данных утилитой *Сетевой монитор* (Network Monitor).

Изучив материал этого занятия, вы сможете:

- *S* открывать и использовать вкладку **Сеть (Networking)** утилиты *Диспетчер задач* (Task Manager);
- *S* открывать и настраивать оповещения в консоли *Производительность* (Perfomance);

S записывать нужные данные с помощью утилиты *Сетевой монитор* (Network Monitor) из состава Windows Server 2003.

Продолжительность занятия — около 60 минут.

Вкладка *Сеть* утилиты *Диспетчер задач*

Иногда нужно просто оперативно узнать, что происходит. Если вам нужен телефонный номер местной пиццерии, вы можете заглянуть в телефонную книгу, войти в Интернет и найти пиццерию в радиусе 5 миль либо спросить приятеля. Есть еще способ: позвонить в справочную службу и получить информацию немедленно. В такой ситуации важна именно скорость получения желаемого.

Если пользователи жалуются на недоступность определенного сервера, медлить нельзя — нужно срочно выявить причины неполадки. Она может иметь *преходящий характер* (transient), то есть спонтанно появляться и так же неожиданно исчезать. Например, «перекачка» файла объемом 20 Гб на/с сервера может блокировать все остальные запросы. Другие неполадки сети появляются регулярно (intermittent), появляясь и исчезая без всякой видимой закономерности. Такая ситуация может возникнуть, когда кто-то настроил задание на взаимодействие с сервером по какому-то графику или изменил обычную процедуру на непредусмотренную.

Но какой бы ни была проблема, избавляться от нее надо как можно скорее. *Диспетчер задач* (Task Manager) в Windows Server 2003 как раз и дает такую возможность.

Диспетчер задач — великолепное средство для одновременной проверки многих сторон деятельности сервера, одна из которых — производительность сети. *Диспетчер задач,* возможно, и не самое мощное средство (о других утилитах рассказывается далее), но оно легко доступно и предоставляет массу сведений о работе сети.

Чтобы вызвать диспетчер задач, нажмите Ctrl+Alt+Del, в открывшемся окне щелкните кнопку **Диспетчер задач (Task Manager)** и перейдите на вкладку **Сеть (Networking)** (рис. **12-1).**

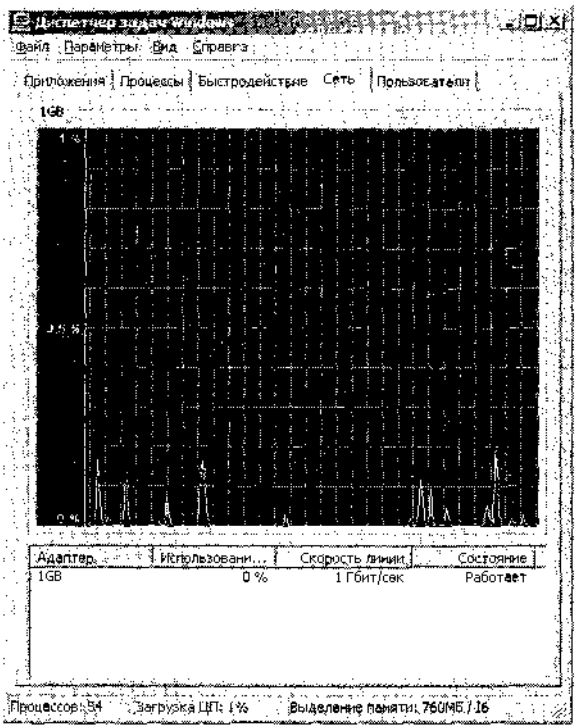


Рис. 12-1. Вкладка *Сеть* утилиты *Диспетчер задач*

Вкладка **Сеть** предоставляет информацию об использовании сетевой карты. Шкала слева — это процентная доля загруженности и масштаб ее автоматически меняется в зависимости от интенсивности использования линии. Здесь есть и другая информация, в частности в столбце **Состояние (State)** отражено состояние линия — работает или отключена, а в столбце **Скорость линии (Link Speed)** отображаются данные о скорости обмена данными.

Выбор просматриваемых данных

Если сервер недостаточно быстро выполняет чтение или запись, может понадобиться просматривать не весь сетевой трафик, а часть его. Вы вправе выбрать просмотр всего трафика сети или только отправляемых или только получаемых байт (рис. 12-2).

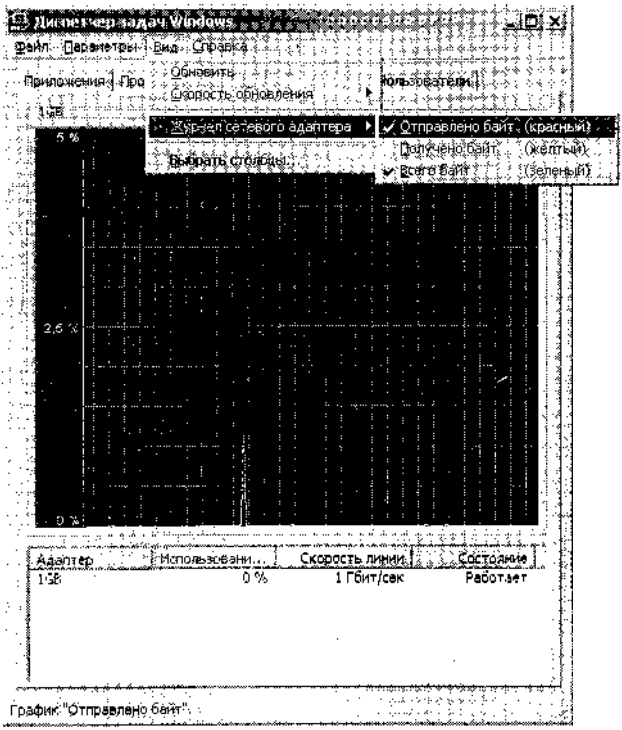


Рис. 12-2. Установка фильтра просмотра: *Всего байт, Отправлено байт* и *Получено байт*

Установка фильтра позволяет игнорировать другие направления потоков в сети. Так, устраняя неполадки записи сервера, можно игнорировать отправляемые байты, или при решении проблем с чтением временно игнорировать получаемые байты.

Выбор столбцов

Диспетчер задач (Task Monitor) дает важную информацию о состоянии линии, например ее скорость (рис. 12-1). Однако это еще мощное средство определения типа трафика, проходящего через интерфейс. Возможности по получению информации значительно увеличиваются при использовании сетевого *счетчика* (counter) — отображаемого элемента данных, иногда также называемого информационной точкой, который помогает оценить текущее состояние сети. При определении значения информационной точки в течение периода времени вы получаете *выборку* (sampling) данных.

Можно включить в рассмотрение больше счетчиков. Для этого в меню **Вид (View)** выберите команду **Выбрать столбцы (Select Columns),** чтобы открыть окно со списком всех возможных счетчиков (рис. 12-3).

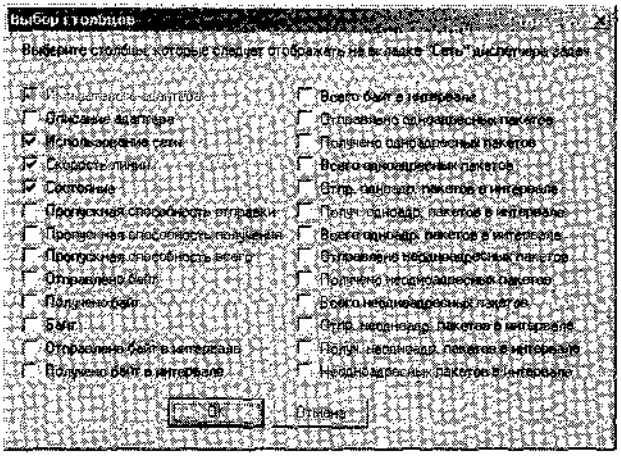


Рис. 12-3. Выбор отображаемых счетчиков

Всего счетчиков 26, однако не все одинаково полезны для устранения неполадок. В табл. 12-1 показаны лишь наиболее важные для устранения неполадоюсети.

Табл. 12-1. Популярные счетчики

Счетчик	Описание
Имя сетевого адаптера (Network Adapter Name)	Имя сетевого адаптера. Этот флажок всегда установлен. Если в системе несколько сетевых адаптеров, будет отображаться информация для всех
Скорость линии (Link Speed)	Скорость подключения интерфейса. Если возникает подозрение, что узкое место здесь, нужно проверить, действительно ли это максимальная скорость в сети. Иногда сетевая карта по сигналу с маршрутизатора переходит на более низкую скорость (например 10 Мбит/сек вместо 100 Мбит/сек)
Всего байт в интервале (Bytes/Interval)	Общее число байт, полученное и отправленное за наблюдаемый промежуток времени через сетевой адаптер. Лучше оценить этот параметр позволяет его сравнение с базисным значением, полученным при нормальной работе сети
Получ. одноадр. пакетов в интервале (Unicasts/Interval)	Число одноадресных пакетов, полученных за рассматриваемый промежуток времени. Если этот счетчик содержит данные, то это скорее всего реальные данные, а не трафик широковещания, информацию о котором предоставляет следующий счетчик
Получ. неодноадр. Пакетов в интервале (Nonunicasts/Interval)	Число многоадресных и широковещательных дейтаграмм, полученных в течение наблюдаемого промежутка времени. Если в этом счетчике есть данные, то это скорее всего фоновый или широковещательный трафик. Если показания этого счетчика высоки, скорее всего проблемы в сети не обусловлены данным сервером

Использование консоли *Производительность*

Консоль *Производительность* (Perfomance) имеет смысл использовать для обработки больших объемов данных.

Примечание В более ранних версиях Windows консоль *Производительность* называлась *Системный монитор* (Perfomance Monitor).

Диспетчер задач удобен для мгновенной оценки сетевой производительности локального сервера, однако консоль *Производительность* дает подробную информацию для углубленного анализа и предоставляет механизм оповещений, удобный для обнаружения проблем еще до проявления очевидных симптомов. Вы сами увидите это на примере триггеров ниже в разделе «Триггеры *Сетевого монитора*».

Запуск консоли *Производительность*

Открыть консоль *Производительность* (Perfomance) можно разными способами. Самый простой: выбрать меню **Пуск (Start)\BbmofIHHTb (Run),** в открывшемся окне ввести ре rf шоп. exe и щелкнуть OK. При этом откроется окно **Системный монитор (Perfomance monitor)** и автоматически отобразятся три наиболее используемых счетчика (рис. 12-4).

* **Обмен страниц в сек (Pages/Sec)** показывает, насколько часто происходит перекачка страниц из оперативной памяти на диск. Стабильно высокое показание свидетельствует о недостаточном объеме оперативной памяти.
* **Средняя длина очереди диска (Avg Disk Queve Length)** информирует, сколько событий находится в очереди на обработку дисковой подсистемой. Стабильно высокое показание этого счетчика говорит о недостаточной пропускной способности дисковой подсистемы.

- *%* **загруженности процессора (%Processor Time)** — уровень загруженности процессора. Постоянное высокое значение этого показателя указывает на недостаточную мощность процессора.

Добавление сетевых счетчиков

Консоль *Производительность* позволяет наблюдать за большим количеством счетчиков производительности — их число гораздо больше, чем *Диспетчер задач.* В действительности, эта консоль позволяет вести наблюдение за многими сетевыми и несетевыми компонентами, которые делятся на несколько категорий (рис. 12-5).

Примечание Перечень доступных категорий зависит от установленного на сервере программного обеспечения.

Тем не менее, нас интересует наблюдение за сетью. Вот ключевые объекты производительности сети.

- **Сетевой интерфейс (Network Interface)** — содержит некоторые из счетчиков, которые использовались в *Диспетчере задач,* но есть здесь еще счетчики для наблюдения за некоторыми особыми характеристиками сетевых пакетов.
- **TCPv4** — содержит счетчики, относящиеся к подключениям протокола TCP версии 4.
- **TCPv6** — содержит счетчики, относящиеся к подключениям TCPv6.

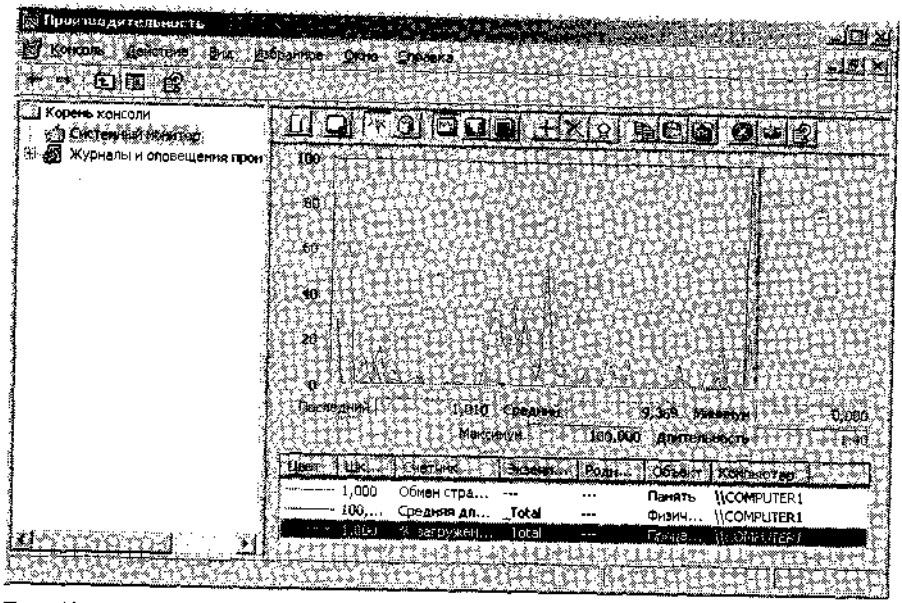


Рис. 12-4. Консоль *Производительность* с загруженными по умолчанию счетчиками

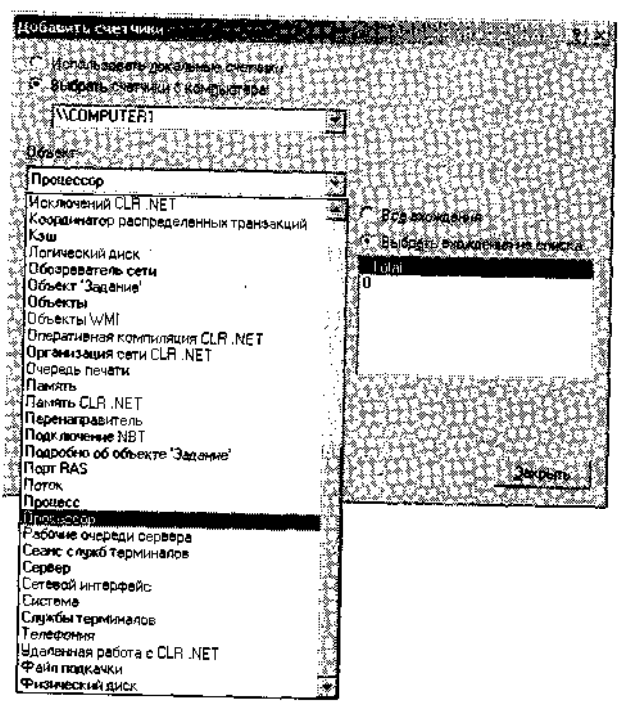


Рис. 12-5. Категории счетчиков производительности

- **Подключение NBT (NBT Connection)** — содержит счетчики, позволяющие определить число подключений по протоколу SMB, обычно это открытые подключения совместного доступа.

- **Порт RAS (RAS Port)** — полезен при наличии виртуальной частной сети (VPN) или других подключений службы удаленного доступа (RAS). В этом случае можно выбрать устранение неполадок вашего подключения на основе конкретных портов. Можно проверить ошибки порта или значения других счетчиков, например **Процент сжатия на выходе (Percent Compression Out).**
- **Всего RAS (RAS Total)** — счетчики этого объекта показывают совокупную производительность RAS-подключений, в отличие от объекта **Порт RAS (RAS Port),** который относится к конкретному порту.

Создание оповещений в консоли *Производительность*

Мы узнали, что *Диспетчер задач* — простое в использовании средство, но консоль *Производительность* намного мощнее. Как узнать, когда лучше использовать ту или иную утилиту? Выбор в пользу последней делают, когда надо:

- получить доступ к большему количеству счетчиков производительности;
- иметь возможность создавать триггеры оповещений на основе конкретных условий.

Вы уже узнали об огромном числе счетчиков в консоли *Производительность,* а теперь пора познакомиться с другим мощным инструментом этой консоли — *триггерам оповещений* (triggered alerts).

Когда нет времени на регулярное изучение показаний консоли *Производительность* можно настроить в ней триггеры, которые своевременно проинформируют о ненормальном поведении системы. Например, настроить инициирование оповещения в ситуации, когда определенная система особенно интенсивно занята обработкой сетевого трафика или выдает в сеть ошибки.

Сначала оповещения создаются в оснастке *Журналы и оповещения производительности* (Perfomance Logs And Alerts) консоли *Производительность* (Perfomance). Правой кнопкой щелкните **Оповещения (Alerts)** и выберите **Новые параметры оповещений (New Alert Settings) (рис. 12-6).**

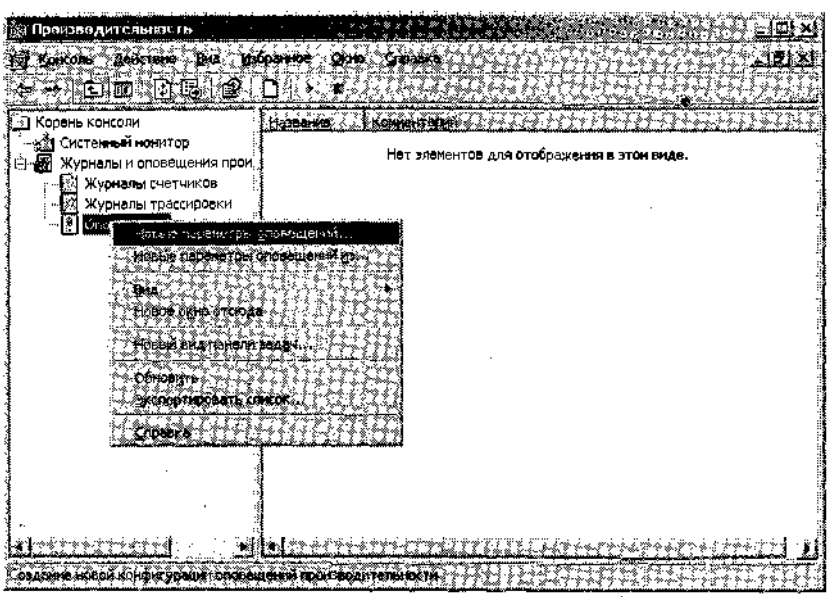


Рис.12-6. Настройка новых оповещений

Обычно названия оповещениям присваивают, используя тип наблюдаемого счетчика (счетчиков), а затем выбирают счетчик(и). После щелчка кнопки **Добавить (Add)** (рис. 12-7) сначала выбирают категории счетчиков, а затем — конкретные счетчики.

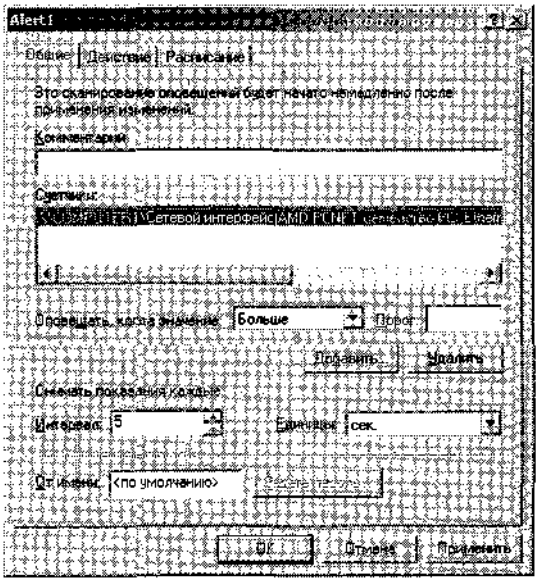


Рис. 12-7. Настройка наблюдаемых счетчиков до определения способа обработки оповещений

Совет Иногда для вызова оповещения нужны показания более одного счетчика. Например, оповещение о ситуации, когда пропускная способность сети недостаточна *и одновременно* генерируется много ошибок.

Перед выбором способа оповещения на вкладке **Общие (General)** нужно подробнее описать, как должен происходить съем показаний счетчиков. Ниже перечислены некоторые параметры вкладки **Общие.**

- **Комментарий (Comment)** — если имя оповещения недостаточно информативно, можно снабдить его комментарием, чтобы пользователю было легче понять, в чем цель и назначение оповещения.
- **Оповещать, когда значение (Alert when the value is).**— определение, когда происходит оповещения: когда счетчик выше или ниже заданного значения. " ———-"
- **Порог (Limit)** — задается пороговое значение наблюдаемого счетчика. При пересечении этой черты [сверху вниз или наоборот — в зависимости от выбора параметра **Оповещать, когда значение (Alert when the value is)]** инициируется оповещение.
- **Интервал (Interval)** — интервал, в течение которого консоль *Производительность* запрашивает у системы значения наблюдаемых счетчиков. Наблюдение за показаниями выполняется не непрерывно, а путем выборки с определенной периодичностью. Чем больше интервал, тем меньше точность выборки. И наоборот: короткий интервал дает более репрезентативную выборку, но существенно нагружает процессор.

м **Единицы (Units)** — единицы времени периода выборки. Например, 5 секунд или полминуты. Опять-таки: при снижении частоты выборки процессор загружен меньше, но точность падает.

* **От имени (Run As)** — выборка счетчиков может производиться с учетной записью *Система* (System) или с любой другой. Изредка, при необходимости, счетчики могут работать под пользовательской учетной записью, но в подавляющем большинстве случаев вполне достаточно учетной записи *Система* (System).

Совет При наблюдении за несколькими счетчиками они выбираются по одному и для каждого заполняются поля **Оповещать, когда значение (Alert when the value is), Порог (Limit), Интервал (Interval)** и **Единицы (Units).** Поля **Комментарий (Comment)** и **От имени (Run As)** являются общими для всех счетчиков оповещения.

После настройки указанных параметров переходят на вкладку **Действие (Action)** (рис. 12-8).

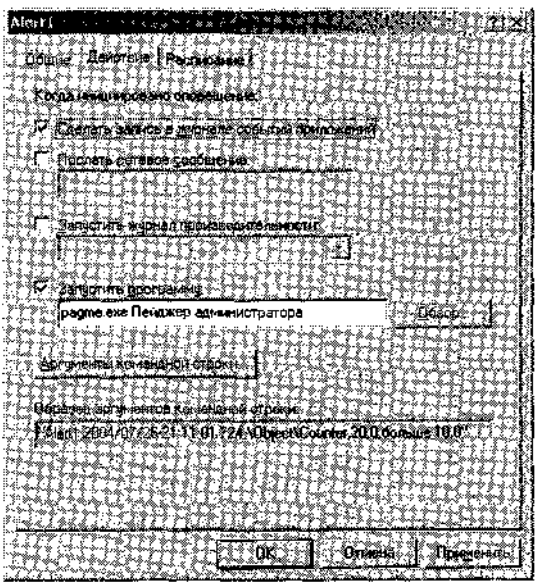


Рис. 12-8. Вкладка *Действие*

Здесь определяют, что происходит при инициировании оповещения, причем можно задать несколько действий в ответ на оповещение.

- **Сделать запись в журнале событий приложений (Log an entry in the aplication event log)** — запись события в журнал событий, содержание которого позднее доступно для просмотра в окне **Просмотр событий (Event Viewer).** Помимо прочей информации записи журнала обязательно содержать показания счетчика и порогового значения (рис. 12-9).
- **Послать сетевое сообщение (Send A Network Message)** — активизация этого параметра эквивалентна команде net send с сообщением оповещения. Здесь нужно определить имя компьютера, а не пользователя. Для отправления сообщений с компьютера, на котором производится наблюдение, на нем должна работать служба *Оповещатель* (Alerter). Для получения сообщений на принимающем компьютере необходима *Служба сообщений* (Messenger). На вновь установленной копии ОС Windows Server 2003 ни одна из этих служб не активизирована и их нужно запустить вручную, изменив их состояние с **Отключено (Disabled)** на **Авто (Automatic).**

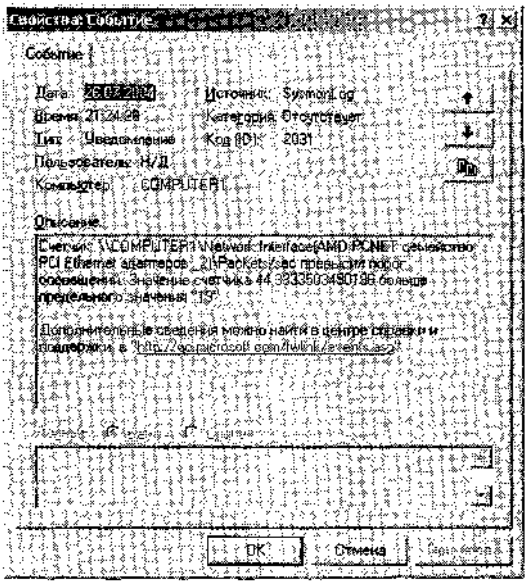


Рис. 12-9. Пример события, инициированного триггером

- **Запустить журнал производительности (Start Perfomance Data Log)** — оповещение можно настроить на запись дополнительных счетчиков в файл журнала для последующего анализа. Нужно предварительно настроить файл журнала в подузле **Журналы счетчиков (Counter Logs)** узла **Журналы и оповещения производительности (Perfomance Logs And Alerts)** (рис. 12-6).
- **Запустить программу (Run This Program)** — при срабатывании триггера выполняется внешняя программа. Можно настроить оповещение на внешнюю пейджинговую сеть или другой способ информирования о срабатывании триггеров. В особо опасных случаях можно предусмотреть останов системы встроенной командой Windows Server2003Shutdown.exe.

Далее настраиваются параметры на вкладке **Расписание (Schedule),** где определяется время инициирования оповещения. Например, в периоды спада сетевой активности или в выходные.

Если график запуска оповещений на вкладке **Расписание (Schedule)** не определен, нужно запустить оповещение вручную. Для этого правой кнопкой щелкните созданное оповещение и выберите в контекстном меню **Запуск (Start)** (рис. 12-10). *

Мониторинг сетевого трафика с помощью утилиты *Netstat*

Утилита командной строки Netstat дает информацию о существующих сетевых подключениях и статистике активности в сети. Например, если надо определить, на каких портах система прослушивает подключения, нужно выполнить команду Netstat-a. Это поможет, к примеру, убедиться, что порты, которые нужно закрыть, действительно заблокированы.

Однако знать открытые порты подчас недостаточно, чтобы заткнуть все «лазейки» — нужна информация о том, кто (какое приложение) и зачем использует порт, чтобы при необходимости предотвратить опасную деятельность, закрыв порт. Данные о взаимосвязи открытых портов и приложений можно получить командой Netstat -o. Она

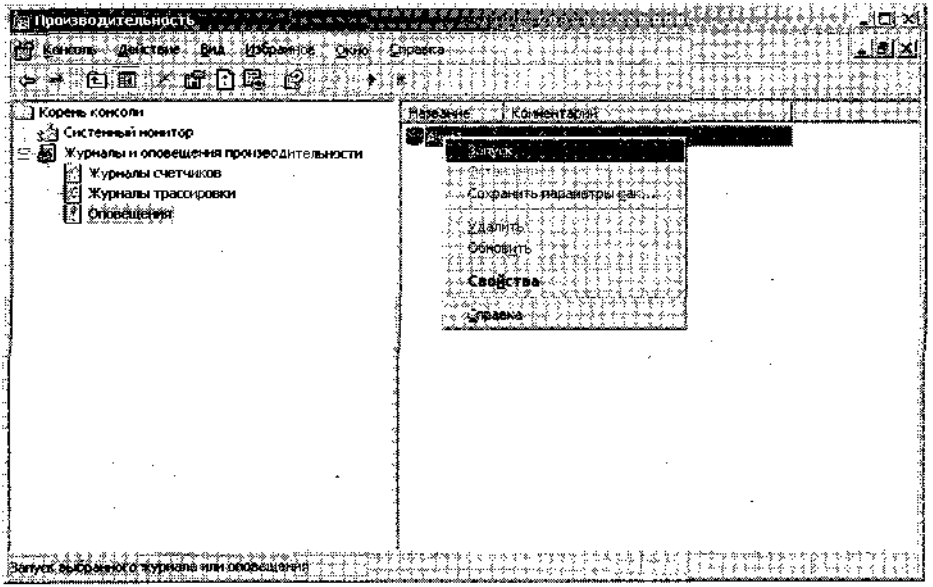


Рис. 12-10. Запуск оповещения вручную

позволяет увидеть протокол, открытый локальный входящий порт, подключение с другого компьютера и порт, который оно использует (рис. 12-11).

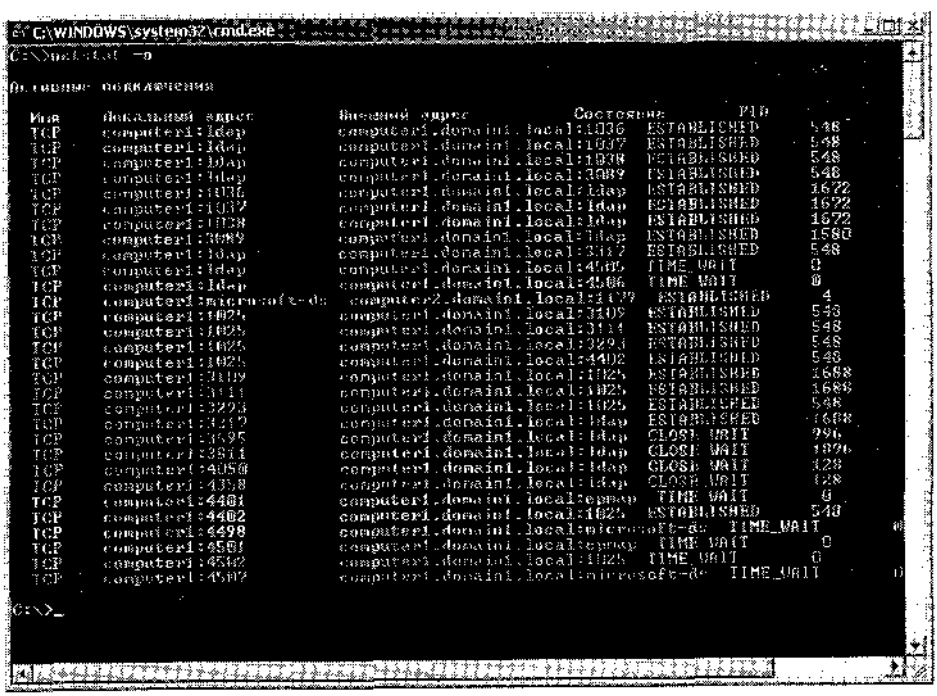


Рис. 12-11. Команда `Netstat -o` показывает все используемые процессы и порты сервера

В данном примере Computerl и Computer2 взаимодействуют через порт 3389, а идентификатор процесса (PID) — 736. Если далее потребуется соотнести этот PID конкретному процессу, использующему порт, нужно перейти на вкладку **Процессы (Processes)** окна **Диспетчер задач (Task Manager).** По умолчанию на этой вкладке не отображаются PID процессов, поэтому в меню **Вид (View)** надо выбрать команду **Выбрать столбцы (Columns)** и отметить флажок **Идентиф. процесса (PID) [PID (Process Identifier)]** (рис. 12-12).

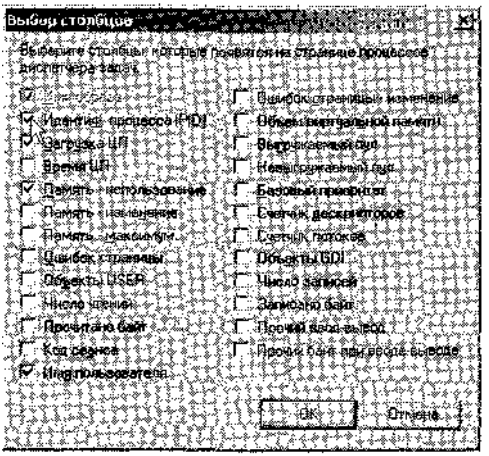


Рис. 12-12. Отображение идентификаторов процессов в *Диспетчере задач*

После этого в списке процессов отображаются PID-идентификаторы (рис. 12-13).

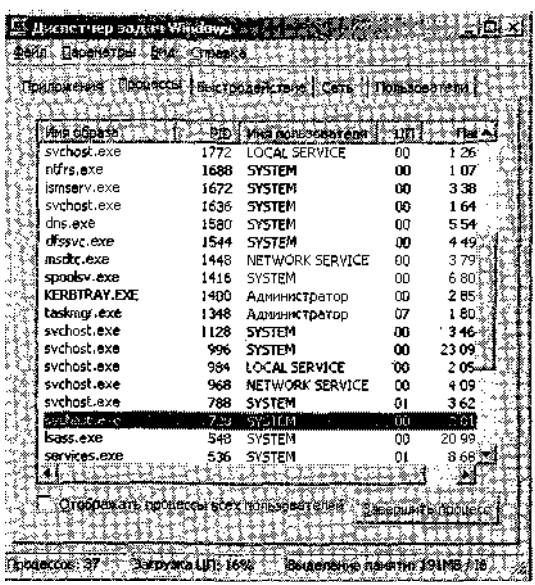


Рис. 12-13. Идентификаторы процессов PID в *Диспетчере задач*

Так, сопоставив PID и процесс, можно узнать, какой процесс или приложение открыло порт. Если PID указывает на svchost, то, скорее всего, несколько служб работают как единый процесс. Чтобы узнать, какие это службы выполните команду Tasklist /svc.

В нашем примере при выполнении этой команды окажется, что svchost с PID 736 относится к *Службе терминалов* (Terminal Services). *Службы терминалов* используют для взаимодействий порт 3389.

Именно так выясняют, какие приложения и службы открывают порты, и при необходимости закрывают их.

Облегченная и полная версии *Сетевого монитора* в Windows Server *2003*

В главе 3 устанавливалась облегченная версия *Сетевого монитора* (Network Monitor), входящая в комплект поставки Windows Server 2003 и для бесплатной программы весьма эффективна. Однако у Microsoft существует более мощная, полная версия *Сетевого монитора,* но она поставляется только вместе с Microsoft Systems Management Server и позволяет решать две задачи, недоступные для облегченной версии.

- Возможность работы в *сквозном* (promiscuous) режиме, т. е. способность записывать 100 % сетевого трафика.
- Возможность увидеть, где еще работает *Сетевой монитор. Эта.* информация полезна, когда в сети настроено несколько станций наблюдения и полученные ими данные затем собираются в центральной точке. Эту возможность также используют для наблюдения и предупреждения хакерских атак изнутри (рис. 12-14).

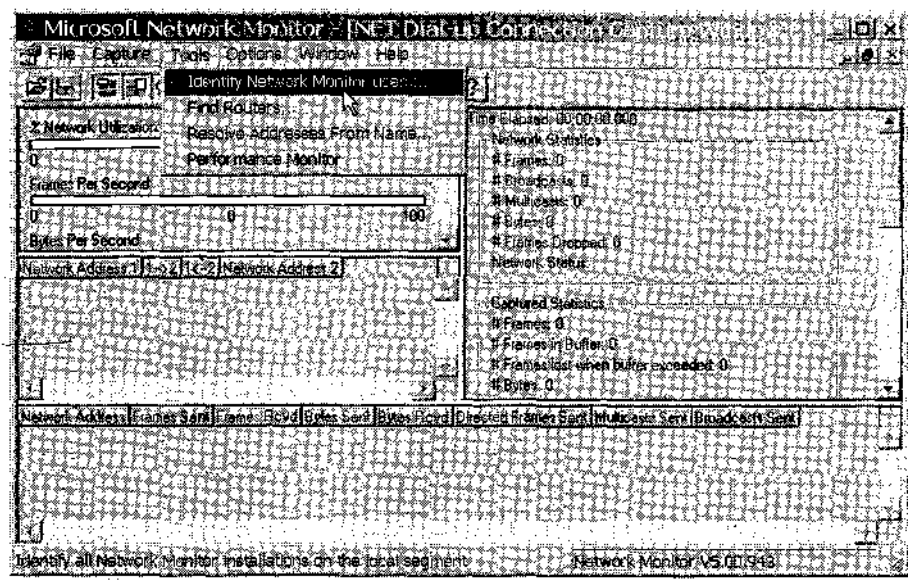


Рис. 12-14. Отслеживание других запущенных копий *Сетевого монитора*

Триггеры *Сетевого монитора*

Основная задача *Сетевого монитора* (Network Monitor) — запись пакетов проходящих в сети. Но в сети происходит так много событий одновременно, что получить нужную информацию часто почти невозможно. Поэтому одно из важнейших умений в работе с *Сетевым монитором* (Network Monitor) — способность быстро найти нужную информацию, когда что-то происходит в сети.

Настройка триггеров

Сетевой монитор оповещает при выполнении определенных условий. Это полезно в тех случаях, когда после настройки *Сетевого монитора,* переходят к другим задачам. Именно эту функцию реализуют с помощью триггеров. Для настройки триггеров в окне **Сетевой монитор** в меню **Запись (Caption)** выберите **Триггер (Trigger).** Откроется диалоговое окно **Триггер записи (Capture Trigger) (рис. 12-15).**

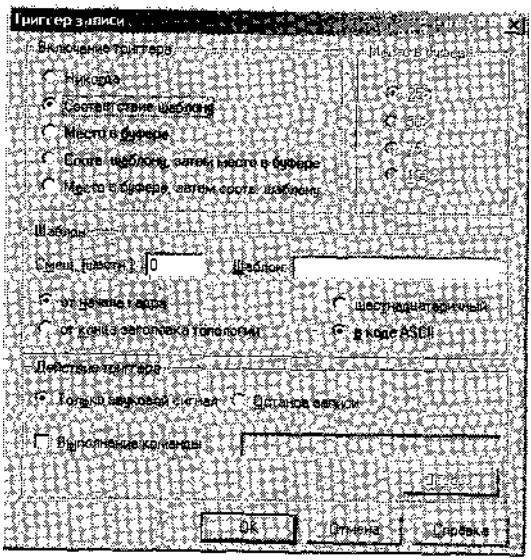


Рис. 12-15. Настройка триггера на оповещение при определенных условиях

Параметры триггера

По умолчанию параметр **Включение триггера (Trigger On)** имеет значение Никогда (Nothing), то есть триггер отключен. Можно настроить триггер на оповещение при выполнении определенных ключевых условий. Например, можно получить уведомление о том, что буфер заполнен на 25%, 50%, 75% или 100%. Это станет сигналом просмотреть его *и* очистить, иначе некоторые пакеты будут потеряны из-за переполнения буфера.

Иногда очень полезной оказывается параметр **Соответствие шаблону (Pattern Match)** (задаваемый в числовом формате): позволяющий найти вполне определенную строку в шестнадцатиричном формате или в виде ASCII.

Лабораторная работа. **Измерение производительности**

Вы изучите дополнительные возможности *Диспетчера задач* (Task Manager) и консоли *Производительность* (Perfomance).

Упражнение 1. Мониторинг сетевого трафика с помощью *Диспетчера задач*

Вы скопируете большой файл (75 Мб) *Dtiver.cab* с Computerl на Computed и проследите за трафиком с помощью *Диспетчера задач* (Task Manager),

1. На Computed создайте папку *C:\Temp* и сделайте ее общей для группы *Администраторы* (Administrators) с правами полного доступа.

2. Перейдите к Computed и, находясь в сеансе *Администратор* (Administrator), откройте окно **Диспетчер задач (Task Manager),** нажав клавиши Ctl+Alt+Del.
3. Перейдите на вкладку **Сеть-(Networking)** и в меню **Вид (View)** выберите команду **Выбрать столбцы (Select Columns).**
4. Выберите наблюдение следующих счетчиков:
   - а , **Использование сети (Network Utilization);**
   - а **Скорость линии (Link Speed);**
   - а **Состояние (State);**
   - а **Всего одноадр. пакетов в интервале (Unieasts/Interval);**
   - • **Неодноадресных пакетов в интервале (Nonunicasts/Interval).**
5. Щелкните OK.
6. В командной строке выполните команды:

   net use T:\\compuLer2\temp

   copy "c:\windows\driver cache\i386\driver.cab" T: /y

   net use T:/delete

   Вы увидите на графике пик, соответствующий использованию сети. Заметьте также, что показания счетчика **Всего одноадр. пакетов в интервале** возросло, а счетчика **Неодноадресных пакетов в интервале (Nonunicasts/Interval)** — не изменилось. Такие значения счетчиков указывают на передачу корректных данных.

Упражнение 2. Создание сетевого оповещения в консоли *Производительность*

Средствами консоли *Производительность* (Perfomance) вы создадите сетевое оповещение в журнале событий компьютера Computer 1, инициируемое, когда счетчик **Отправлено пакетов/сек (Packets Sent/Sec)** «зашкаливает» за 5.

_1^_-В-консоли *Производительность* (Perfomance) раскройте узел **Журналы и оповещения производительности (Perfomance Logs And Alerts),** щелкните **Оповещения (Alerts)** правой кнопкой и выберите **Новые параметры оповещений (New Alert Settings).**

2. **В** поле **Имя** (Name) введите Packets Sent Alert и щелкните OK.
3. На вкладке **Общие (General)** открывшегося окна **Packets Sent Alert** щелкните **Добавить (Add).**
4. **В** списке **Объект (Perfomance Object)** выберите объект **Сетевой интерфейс (Network Interface),** а в списке счетчиков — **Отправлено пакетов/сек (Packets Sent/Sec).**
5. Выберите используемую сетевую карту и щелкните **Добавить (Add),** а затем **Закрыть (Close).**
6. **В** окне **Packets Sent Alert** на вкладке **Общие (General)** в поле **Порог (Limit)** введите 5.
7. Выберите вкладку **Действие (Action)** и убедитесь, что установлен флажок **Сделать запись в журнале событий приложений (Log An Entry In The Application Event Log).**
8. На вкладке **Расписание (Schedule)** выберите запуск мониторинга в текущее время (по умолчанию) и щелкните OK.
9. В окне командной строки выполните команды:

   net use T:\\computer2\temp

   copy "c:\windows\driver cache\i386\driver.cab" T: /y

10. На Computerl просмотрите *Журнал приложений* (Application event log) и найдите вызванное событие.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вам сообщили, что Computerl медленно отвечает на запросы пользователей. Вы решили быстро просмотреть сетевой трафик с помощью окна *Сетевой монитор* (Network Monitor) и выяснить, есть ли на Computerl трафик широковещания. Какой счетчик нужно активизировать?
   a. *Неодноадресных пакетов в интервале* (Nonunicasts/Interval).
   b. *Всего одноадр. пакетов в интервале* (Unicasts/Interval).
   c. *Отправлено байт в интервале* (Bytes Sent/Interval).
   d. *Получено байт в интервале* (Bytes Received/Interval).
2. Вы настроили в оснастке *Журналы и оповещения производительности* (Perfomance Logs And Alerts) оповещение с отправкой сообщения оператору на Computer2 о слишком высокой загруженности сети на Computerl. Однако Computer2 не удается принимать' сообщения от Computerl. Как активизировать передачу сообщений от Computerl и прием их на Computer2. (Выберите все подходящие ответы).
   a. На Computerl запустить *Службу сообщений* (Messenger).
   b. На Computerl запустить службу *Оповещатель* (Alerter).
   c. На Computer2 запустить *Службу сообщений* (Messenger).
   d. На Computer2 запустить службу *Оповещатель* (Alerter).
3. Вы подозреваете, что компьютер под управлением Windows Server 2003 заражен вирусом и вирус передает данные по сети с сервера через определенный порт. Нужно выяснить, какой процесс использует этот порт. Какая команда позволит это выяснить?
   a. `Nbtstat -RR`.
   b. `Nbtstat -г`.
   c. `Netstat -a`.
   d. `Netstat -o`.

Резюме

- *Диспетчер задач* (Task Manager) предоставляет оперативные сведения о производительности системы.
- Консоль *Производительность* (Perfomance) позволяет более глубоко анализировать поведение системы за счет использования счетчиков, помогающих найти проблемные точки. Оповещения консоли *Производительность* (Perfomance) дают возможность отправлять уведомления при срабатывании триггера.
- *Сетевой монитор* (Network Monitor) записывает определенные сетевые пакеты и позволяет анализировать работы сети, а триггеры сетевого монитора дают возможность отправлять сообщение при определенных условиях — при переполнении буфера записи или при обнаружении в сети определенных данных.

Занятие 2. Устранение неполадок связи с Интернетом

Конечные пользователи часто обращаются в службу поддержки за помощью в наладке интернет-подключения. На самом деле, обычно не работает конкретное подключение конкретного пользователя к Интернету, то есть не хватает какого-то одного звена в цепи, соединяющей рабочее место пользователя и Интернет.

Существует два метода устранения неполадок связи с Интернетом: сверху вниз или снизу вверх. То есть можно начинать от сервера и двигаться к клиенту, или наоборот — от клиента к серверу. Оба, строго говоря, равноценны. С одной стороны, начав с клиентского компьютера, проблему, возможно, удастся решить лучше и быстрее, но здесь препятствием и потерей времени может обернуться само перемещение к рабочему месту пользователя. А устранение неполадки со стороны сервера может и оперативнее, если проблема обнаруживается сразу, в противном случае все-таки придется отправиться к клиенту.

Поэтому лучше всего при устранении подобных неполадок начинать снизу вверх и перемещаться от клиента к выходу в сеть и Интернет.

Локализация неполадок сети

Первым делом при устранении неполадок связи с Интернетом определяют, связана ли проблема с неполадками сети или разрешения имен. Ниже разобраны возможные варианты.

Неполадки связи в сети

Начинают выяснение неполадок связи с команды Ping (рис. 12-16).

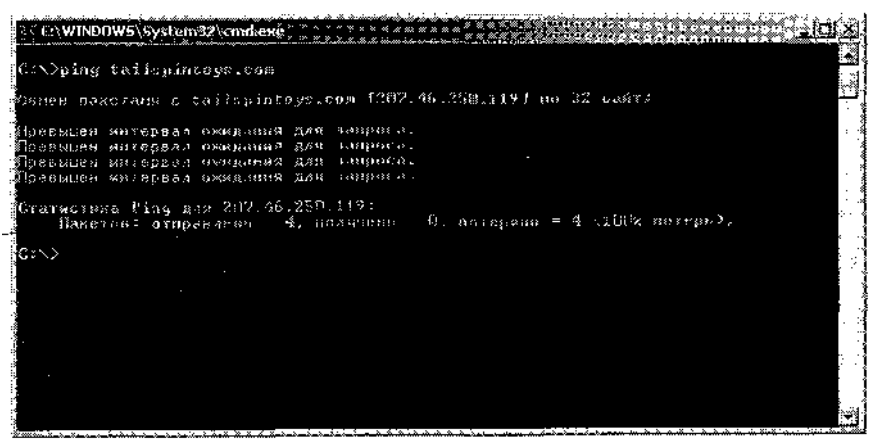


Рис. 12-16. DNS реагирует на эхо-запрос, но пакеты не находят адресата

Если внимательно посмотреть, можно сразу понять, что мешает пользователю подключиться к Интернету: Ping возвращает правильное имя адресата (tailspintoys.com), но сами эхо-запросы команды не доходят до адресата. Получается, что разрешение имен на DNS-сервере работает нормально, но пакеты не доходят до адресата.

Дальше по логике следует обратиться к команде PathPing, которая покажет полный маршрут от клиента к адресату и поможет найти «слабое звено».

Неполадки разрешения имен

На рис. 12-17 показан другой пример. Здесь очевидны неполадки разрешения имен. В такой ситуации нужно проверить параметры DNS пользователя и сервера, чтобы убедиться, что оба возвращают ожидаемые значения при выполнении команды Ping.

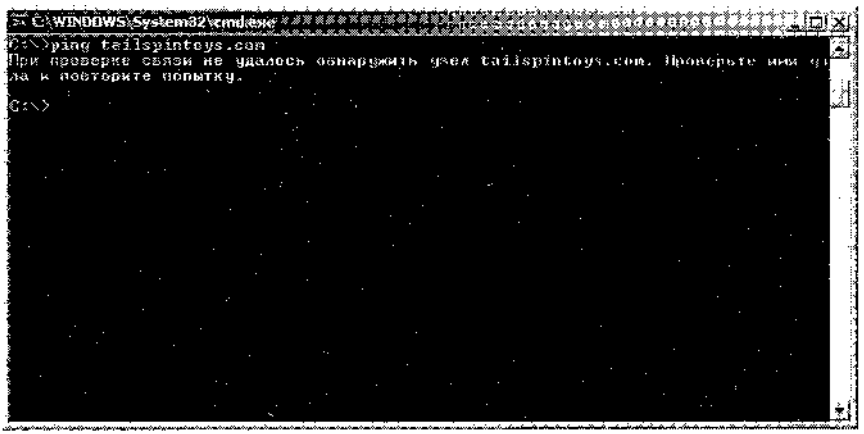


Рис. 12-17. DNS не разрешает запрашиваемое имя узла

Надо проверить, определен ли на сетевом адаптере клиента DNS-сервер локальной сети. (См. следующий раздел «Проверка сетевых параметров компьютера»).

Внимание! Как правило, компьютер клиента настроен на один из внутренних DNS-серверов, а не на DNS-сервер интернет-провайдера.

При подозрении на проблемы разрешения DNS-имен на внутренних серверах рекомендуется с клиентского компьютера выполнить команду Nslookup, которая поможет выяснить, получает ли клиент от DNS-сервера информацию о нужных ему записях ресурсов.

Примечание Статья 200525 из Базы знаний Microsoft прекрасно подходит для начального ознакомления cNslookup.

Если есть основания подозревать, что причины неполадки при разрешении имен находятся за пределами области конкретного сервера или относятся к внешним именам, нужно проверить сам DNS-сервер. Сначала проверьте, осуществляет ли DNS-сервер пересылку на следующее логическое звено архитектуры сети, воспользовавшись вкладкой **Пересылка** (Forwarders) (рис. 12-18).

Обычно DNS-сервер пересылает запрос серверу, который обладает большей информацией о данном уровне сети, либо непосредственно интернет-провайдеру. Если это не так, следует скорректировать параметры на вкладке **Пересылка (Forwarders).**

Кроме того, убедитесь, что сам сервер отвечает на запросы и получает ответы от серверов, которым пересылает информацию. В примере (рис. 12-19) сам сервер отвечает на запросы разрешения имен, но не может получить отклик от серверов, которым он пересылает запросы.

В такой ситуации не работает разрешение имен не на локальных серверах, а на тех, которым они пересылают запросы.

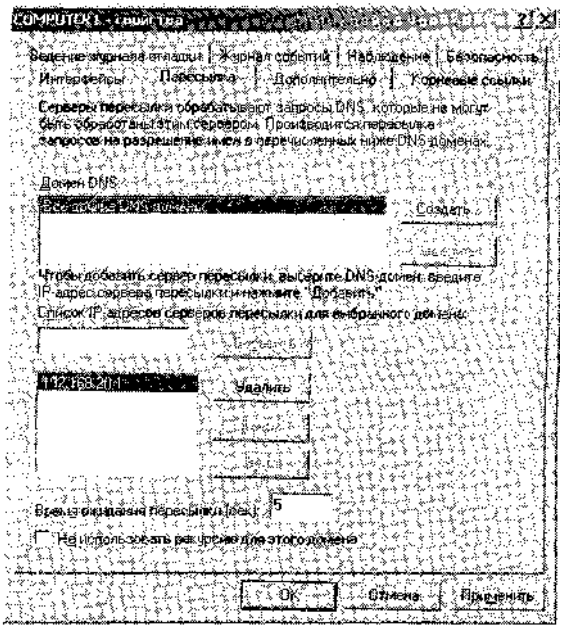


Рис. 12-18. Проверка корректности настройки серверов пересылки

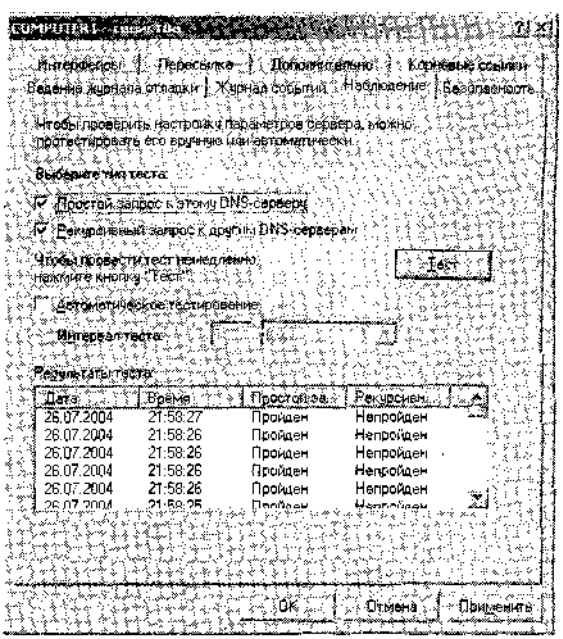


Рис. 12-19. Не работает рекурсия запросов, что указывает на проблемы пересылки

Проверка сетевых параметров компьютера

Если при проверке клиентского компьютера обнаруживается неожиданная настройка сетевого адаптера, этому может быть несколько причин. Если клиент использует протокол DHCP, нужно убедиться, что сетевой адаптер правильно получает данные **DHCP.**

Если окажется, что IP-адрес клиентского компьютера относится к **APIPA-**диапазону (169.254.0.0—169.254.255.255), значит компьютер не получает данные от DHCP-сервера.

Использование кнопки *Исправить*

Одна из новых возможностей графического интерфейса пользователя в Windows Server 2003 — кнопка **Исправить (Repair)** — позволяет сразу решить массу задач. Эта кнопка доступна в окне состояния сетевого адаптера (рис. 12-20).

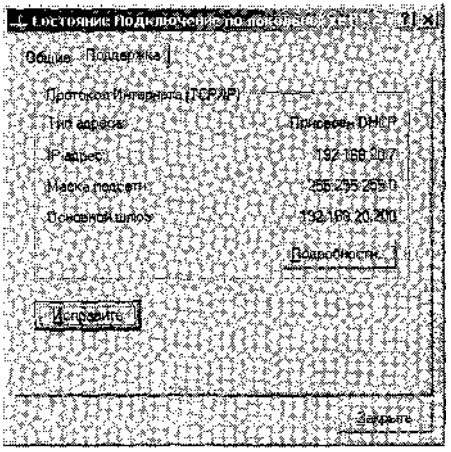


Рис. 12-20. Кнопка *Исправить* используется для перенастройки множества параметров

Щелчок кнопки **Исправить** инициирует несколько действий, соответствующих нескольким командам, выполняемым в командной строке в том порядке, в каком они перечислены в табл. 12-2.

Совет Функция **Исправить** работает как в Windows Server 2003, так и в Windows XP Professional.

Табл. 12-2. Операции, инициируемые кнопкой: *Исправить*

Эквивалентная команда командной строки	Операция
Ipconfig /renew	Попытка обновления DHCP-аренды
Arp -d *	Очистка кэша протокола ARP
Nbtstat -R	Перезагрузка кэша NetBIOS
Nbtstat -RR	Отправка NetBIOS-имени компьютера службе WINS для обновления
Ipconfig /flushdns	Очистка кэша DNS
Ipconfig /registerdns	Регистрация имени на DNS-сервере

Совет Кнопка **Исправить** также инициирует аутентификацию беспроводного соединения ШЕЕ 802. Их.

Примечание Подробнее о кнопке **Исправить** — в статье 289256 Базы знаний Microsoft.

Проверка DHCP-сервера

Если клиентский компьютер не получает IP-адрес или адрес хотя бы основного DNS-сервера, то ясно, что к Интернету ему не подключиться. Вот несколько причин, по которым клиент не получает данные DHCP;

- маршрутизатор блокирует протокол **BOOTP** (Boot Protocol);
- не определены агенты пересылки DHCP для сегментов без поддержки пересылки BOOTP;

в все адреса в области DHCP уже задействованы.

Далее проверяют корректность диапазона адресов, выделяемых DHCP-сервером, шлюза, а также корректность указания узлов на DNS-серверах.

Тем не менее, иногда приходится сталкиваться с ситуацией, когда одни клиенты подключаются к Интернету, а другие нет. Допустим, проверка сетевых характеристик клиентов обнаруживает, что компьютеры настроены по-разному, тем не менее все клиентские компьютеры настроены на использование DHCP. Возможно, дело здесь в наличии *неавторизованного* DHCP-сервера, то есть DHCP-сервера, который установлен для особых целей, например для тестирования. В этом случае сервер снабжает клиентов неверной информацией о шлюзе и/или адресе DNS-сервера.

Чтобы нормально работать, DHCP-серверы в Microsoft Windows 2000 и Windows Server 2003 должны быть авторизованы в службе каталогов Active Directory. В противном случае они автоматически останавливаются. Можно воспользоваться утилитой Dhploc. exe [из состава *Средств поддержки Windows* (Windows Support Tools)] для обнаружения DHCP-серверов, которые не должны авторизоваться или DHCP-серверы, которые можно не авторизовать, например DHCP-серверы из состава ОС Microsoft более ранних весий и DHCP-серверы, не разработанные Microsoft.

Организация сетевых мостов

Все чаще приходится устранять неполадки подключения к Интернету беспроводных компьютеров. Часто используется совместный доступ по одному WAP-подключению для множества разнообразных топологий (рис. 12-21).

В данном примере связь с Интернетом обеспечивается через единственное WAP-подключением, а затем через беспроводную сетевую карту (NIC) сервера. Кроме того, к другим сетям сервер связывается через Ethernet-подключение и подключение Token Ring.

Если установить для этого подключения *сетевой мост* (network bridge), все точки входа на сервер (беспроводная сеть, Token Ring и Ethernet) попадут в одну сеть и все смогут совместно использовать беспроводное подключение для выхода в Интернет.

Для установки сетевого моста нужно, нажав клавишу Ctrl, щелкнуть все подключения сервера. Затем щелкнуть правой кнопкой и в контекстном меню выбрать **Настройка моста (Bridge Connections)** (рис. 12-22).

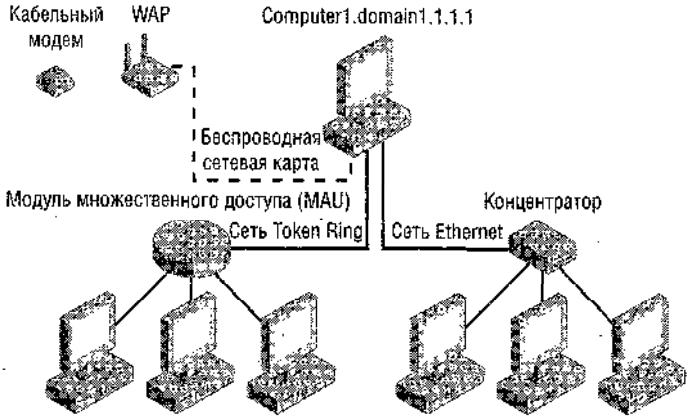


Рис. 12-21. Пример сети, в которой имеет смысл использовать сетевой мост

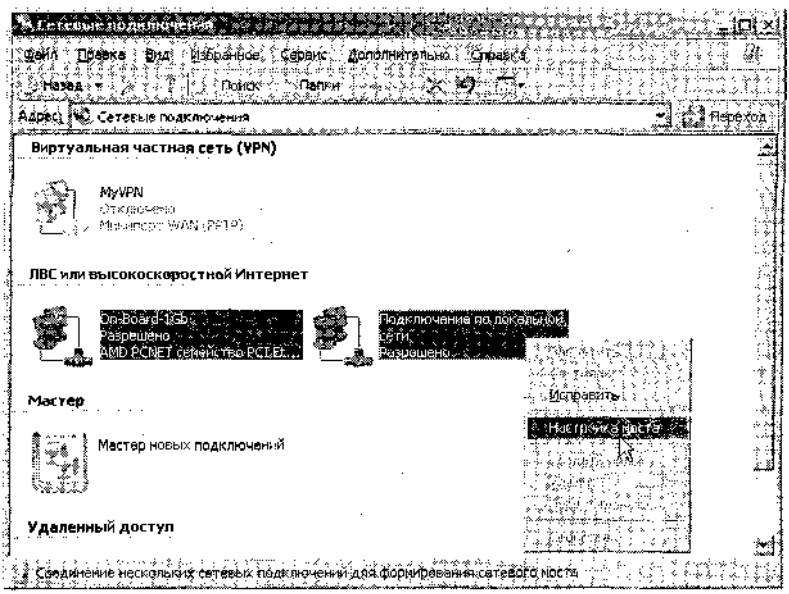


Рис. 12-22. Выбор нескольких сетей и создание моста

При установке сетевого моста трафик разных сетевых карт (беспроводной сети, Ethernet и Token Ring) совместно использовать единое сетевое пространство. Таким образом одна беспроводная сетевая карта становится шлюзом для разнородных сетей.

Возникающие в такой ситуации неполадки доступа в Интернет устраняют в такой последовательности.

и На вкладке **Общие (General)** свойств подключения с установленным мостом нужно убедиться, что мост действительно соединяет все сети.

- У самого моста должен быть собственный IP-адрес, что проверяют командой Ipconf ig /a11. Если это не так, IP-адрес моста нужно удалить и создать снова.
- Надо проверить физическое соединение между всеми сегментами моста.

Лабораторная работа. Проверка **настройки DNS-пересылки**

Вам предстоит с помощью консоли *DNS* определить, правильно ли настроена DNS-пересылка.

Упражнение 1. Проверка параметров **DNS-пересылкн**

Вы воспользуетесь вкладкой Наблюдение (Monitoring) консоли DNS, чтобы проверить работу пересылки.

1. Войдите в систему Computer! как *Администратор* (Administrator).
2. В консоли DAW щелкните Computerl правой кнопкой и выберите Свойства (Properties).
3. На вкладке Наблюдение (Monitoring) окна свойств выберите Рекурсивный запрос к другим DNS-серверам (Recursive Query To Other DNS Servers) и щелкните кнопку Тест (Test Now).

Об успешности теста свидетельствуют результаты, отображаемые в столбце Рекурсивный запрос (Recursive Query).

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите материал занятия. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

Три следующих вопроса относятся к схеме сети компании Taiispin Toys (рис. 12-23). Предполагается, что вы сетевой администратор этой компании.

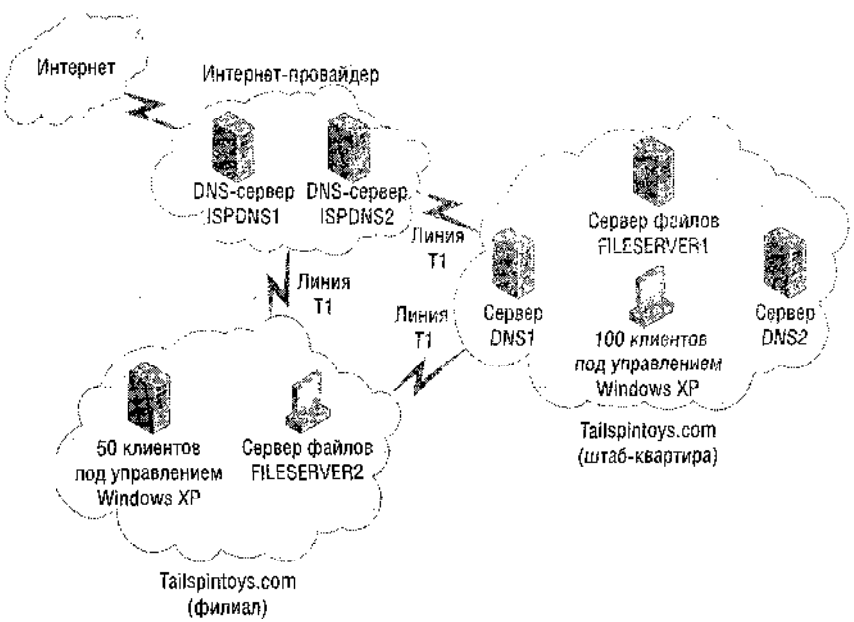


Рис. 12-23. Сеть компании Tailspin Toys

1. Пользователь из филиала сообщает, что ему не удается с помощью Internet Explorer открыть часто используемый Web-сайт. Эхо-запрос ping указанного адреса с клиентского компьютера в штаб-квартире проходит без проблем, а с клиентского компьютера пользователя — нет. Что предпринять для устранения неполадки? (Выберите все подходящие ответы).

a. С клиентского компьютера пользователя проверить командой ping адрес назначения.
b. На клиентском компьютере пользователя воспользоваться кнопкой **Исправить (Repair)** для сетевого подключения.
c. На DNS-сервере выполнить тест простым запросом.
d. На DNS-сервере выполнить тест рекурсивным запросом.

2. Вы настраиваете 50 новых клиентских машин в филиале, где другой администратор уже настроил службу DHCP. При выходе первого клиентского компьютера в сеть обнаружилось, что **DHCP** не предоставляет ни IP-адреса, ни адресов основного и „дополнительного DNS-серверов.

   Надо устранить неполадки службы DHCP и настроить ее так, чтобы клиентские компьютеры получили доступ к внутренним ресурсам и к Интернету. Как настроить DHCP-сервер? (Выберите все подходящие варианты.)

   a. Настроить DHCP-сервер на предоставление клиентам адреса DNS1.
   b. Настроить DHCP-сервер на предоставление клиентам адреса ISPDNS1.
   c. Настроить DHCP-сервер на предоставление клиентам адреса DNS2.
   d. Настроить DHCP-сервер на предоставление клиентам адреса ISPDNS2.

3. Пользователь из филиала сообщает, что ему не удается с помощью Internet Explorer открыть часто используемый Web-сайт. При запуске Nslookup с клиентского компьютера в штаб-квартире возвращается правильный адрес, а при выполнении той же команды с клиентского компьютера пользователя возвращается некорректный адрес. Что предпринять, чтобы устранить неполадку? (Выберите все подходящие варианты.)

   a. Проверить правильность определения DNS-серверов на клиенте.
   b. Выполнить команду I peon fig /flushdns.
   c. Выбрать значок **Сетевые подключения (Network Connections).**
   d. Выполнить команду Ipconfig /renew.

Резюме

- При устранении неполадок связи нужно сначала классифицировать проблему: неполадки сети или разрешения имен.
- Если проблемы связи связаны с маршрутизацией TCP/IP, рекомендуется команда PathPing для выяснения, в какой точке маршрута не проходят пакеты.
- Если причина неполадки в DNS, то прежде всего проверяют корректность данных DNS-сервера на клиенте. Если с этим все в порядке, командой Nslookup проверяют, правильные ли результаты возвращает сервер. И лишь в конце проверяют DNS-серверы пересылки.

Занятие 3. Устранение неполадок служб сервера

Итак, сервер работает и вроде бы можно расслабиться, но на всегда все так гладко и следует сохранять бдительность. Здесь описывается, как устранять неполадки служб и обеспечивать бесперебойную работу сервера.

Изучив материал этого занятия, вы сможете:

- *S* диагностировать и устранять неполадки, обусловленные зависимостями служб;
- *S* использовать функцию восстановления служб для диагностики и устранения неполадок, связанных со службами.

Продолжительность занятия — около 30 минут.

Диагностика и устранение неполадок из-за зависимостей служб

На сервере под управлением Windows Server 2003 (или любой другой ОС Microsoft) постоянно работают десятки и сотни процессов, выполняющих самые разные задачи. Многие из них функционируют как *службы* (services) — одни из них работают на первом плане, требуя взаимодействия с пользователем, а другие — в фоновом режиме, не требуя к себе внимания со стороны пользователя. В зависимости от выбранной при установке конфигурации Windows Server 2003 может поддерживать более 100 служб! Многие другие продукты Microsoft или сторонних поставщиков также часто загружают дополнительные службы.

Чтобы увидеть, какие службы в текущий момент установлены на сервере, в меню **Пуск (Start)** правой кнопкой щелкните **Мой компьютер (My Computer),** в контекстном меню выберите **Управление (Manage)** и в появившейся консоли *Управление компьютером* (Computer Management) выберите узел Службы (Services) (рис. 12-24).

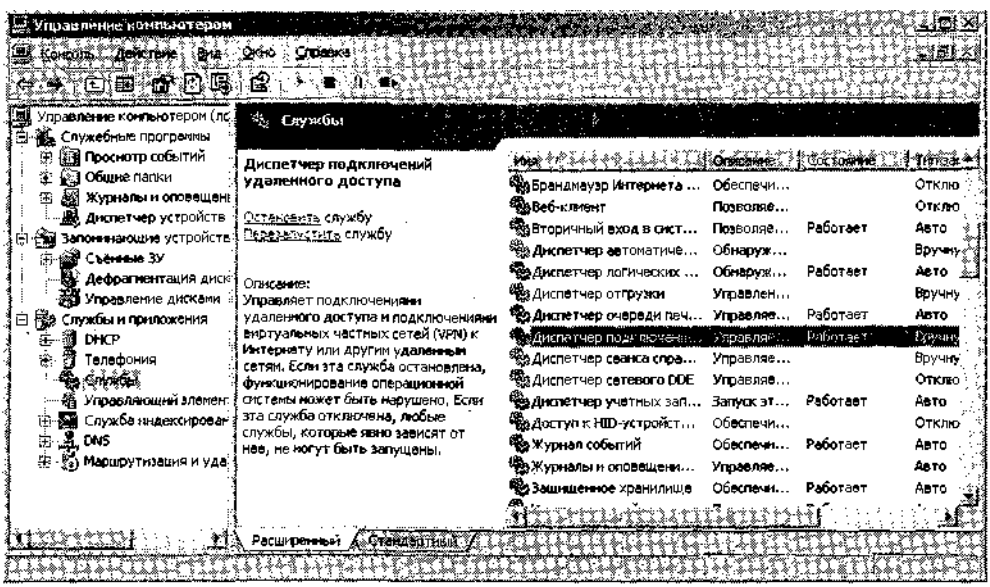


Рис. 12-24. Узел *Службы* показывает состояние всех служб

Служба находится в одном из трех возможных состояний: рабочее, останов и пауза. В соответствии с этим есть три возможных способа настройки запуска службы.

- **Авто (Automatic)** — служба запускается автоматически при перезапуске системы.

- **Вручную (Manual)** — служба не запускается автоматически при перезапуске системы, но если другой процесс обратится к этой службе, она активизируется.
- **Отключено (Disabled)** — служба не запускается ни автоматически при перезапуске системы, ни при обращении к ней другого процесса.

Работа некоторых служб зависит от других служб. Это как в автомобиле: двигатель не заведется, если топливный насос не работает, поставляя бензин. Так и службы: некоторые из них являются многоуровневыми, и не запускаются, пока не начнут правильно работать «нижележащие» службы. Такая связь называется *зависимостью служб* (service dependency). Например, если в списке дважды щелкнуть службу **Диспетчер подключений удаленного доступа (Remote Access Connection Manager),** то на вкладке **Зависимости (Dependencies)** вы увидите как службы, от запуска которых зависит данная служба, так и те, запуск которых зависит от данной (рис. 12-25).

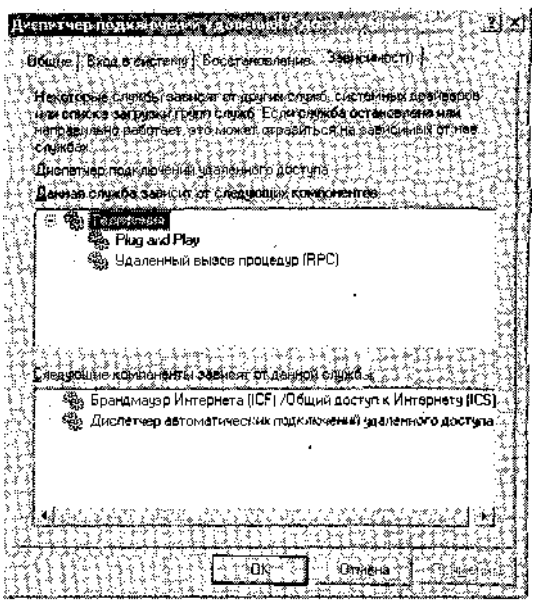


Рис. 12-25. Вкладка *Зависимости* показывает зависимости служб

Взаимосвязи одной этой службы весьма сложны: она зависит от службы *Телефония* (Telephony), которая в свою очередь зависит от *Plug And Play* и *Удаленный вызов процедур* [Remote Procedure Call (RPC)]. С другой стороны, если отключен *Диспетчер подключений удаленного доступа* (Remote Access Connection Manager), то не запустятся ни *Брандмауэр Интернета (\C¥)/Общий доступ к Интернету* (ICS) [Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)], ни *Диспетчер автоматических подключений удаленного доступа* (Remote Access Auto Connection Manager).

Использование функции восстановления служб для их диагностики и устранения неполадок

Большая часть служб Windows Server 2003 работает в контексте локальной системы (Local System), то есть под специальной учетной записью. Дополнительно загружаемые службы (фирмы Microsoft или сторонних поставщиков) могут запускаться в других контекстах. Обычно администратор должен определять реквизиты, с которым загружается

служба. Таким образом «поле деятельности» службы ограничивается заданной учетной записью — никакого неограниченного доступа к системе. Часто это учетная запись локального пользователя компьютера (скажем, учетная запись локального администратора), а иногда права учетной записи службы могут еще более ограничиваться. Уровень доступа определяется требованиями загружаемых приложений и служб.

Наилучший подход состоит в предоставлении учетной записи минимально необходимые полномочия. Например, если учетная запись службы может работать с правами локального пользователя, то нет необходимости предоставлять ей права локального администратора только потому, что эта учетная запись будет использоваться для управления службой. При планировании загрузки каждого приложения выясняйте вопрос о необходимых ему полномочиях.

Иногда после установки нового приложения и идущих с ним «в связке» служб, оказывается, что новые службы не работают. Проконтролировать запуск служб можно с помощью утилиты *Управление компьютером* (Computer Management), однако журнал *Система* (System) дает намного больше информации, (рис. 12-26 и рис. 12-27).

Внимание! В реальности вам не придется менять свойства учетной записи службы Telnet. В данном примере служба Telnet использована лишь для демонстрации, как выглядит результат изменения свойств учетной записи, скажем, для службы стороннего поставщика.

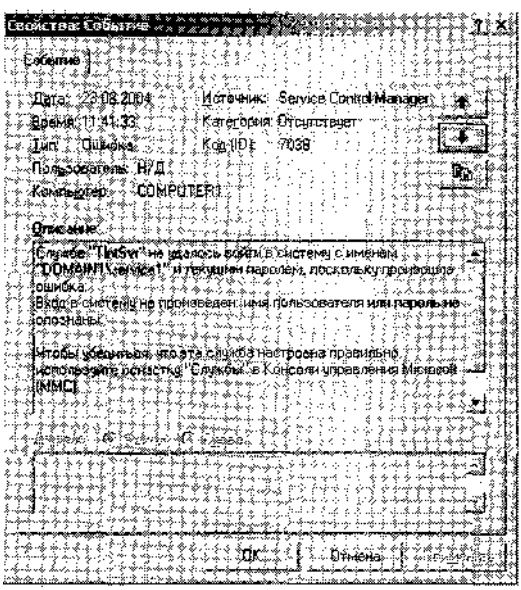


Рис. 12-26. Возможная ошибка из-за неверных реквизитов учетной записи

Однако даже информация из журнала событий требует дополнительной расшифровки. Недостаточно просто знать, что произошел сбой при входе в систему, ведь возможных причин такого события масса:

- имя пользователя в учетной записи изменено, удалено, запрещено или стало неверным по какой-либо другой причине;
- пароль учетной записи истек и требует сброса;

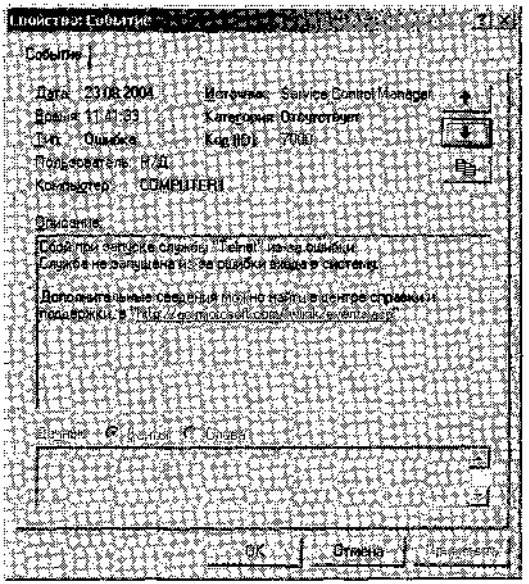


Рис. 12-27. Другая возможная ошибка по причине ошибочных данных учетной записи

- учетной записи, определенной для запуска службы, не предоставлено право *Вход в качестве службы* (Log on as a service).

Чтобы разобраться в этих проблемах, нужно вначале в самой службе проверить вкладку **Вход в систему (Logon)** (рис. 12-28), чтобы убедиться, что данные учетной записи со-

ОТКР.ТгТпУТОТ ТТЯПЯДуГР.ТПЯМ ТТПiТТТО"ЖР,НИЯ_

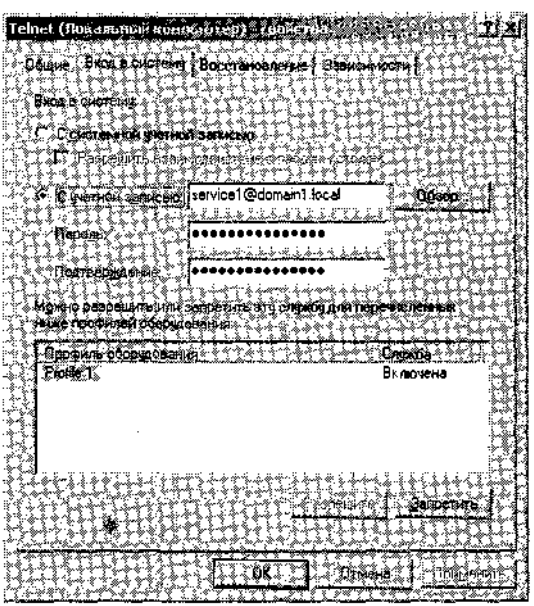


Рис. 12-28. Вкладка *Вход в систему* позволяет проверить правильность данных учетной записи службы

После проверки имени и пароля учетной записи нужно убедиться, что учетной записи предоставлено право *Вход в качестве службы.* Если для запуска службы используется учетная запись доменного уровня, то нужно проверить политику контроллера домена по умолчанию. Для этого выберите **Пуск (81ar1)\Администрирование (Administrative Too18)\Политика безопасности контроллера домена (Domain Controller Security Policy).** В левой панели отрывшегося окна раскройте узел **Локальные политики (Local Policies),** дважды щелкните **Назначение прав пользователя (User Rights Assignment)** и в правой панели выберите политику **Вход в качестве службы (Log on as a Service)** (рис. 12-29).

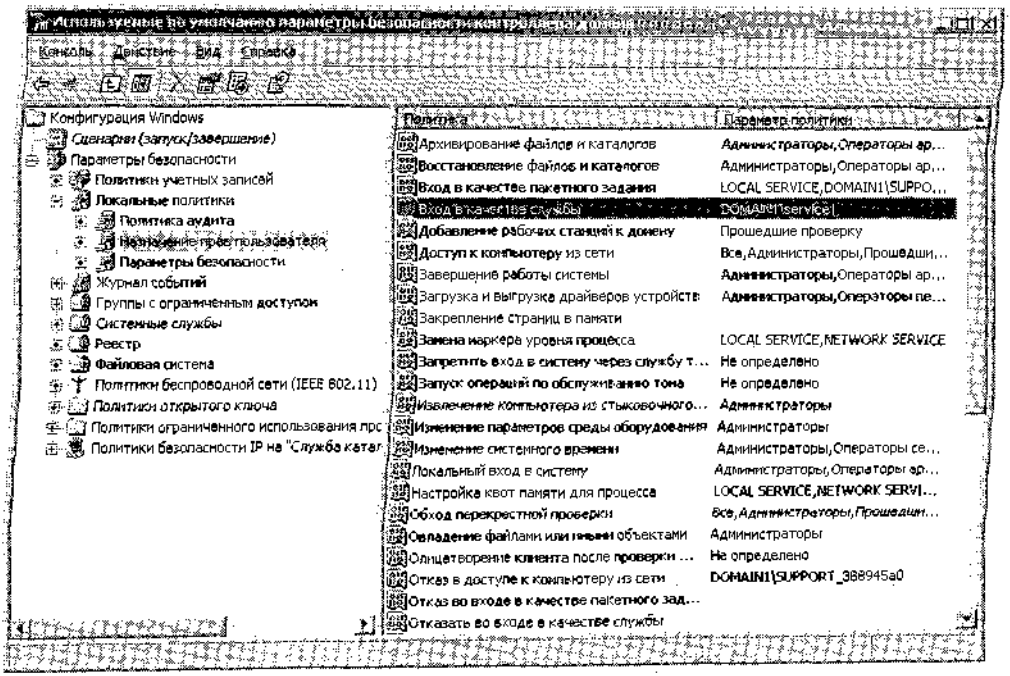


Рис. 12-29. Проверка, предоставлено ли службе право *Вход в качестве службы*

Убедитесь, что используемая учетная запись доменного уровня определена в списке параметров политики безопасности и перезапустите службу.

Если надо использовать учетную запись на изолированном компьютере под управлением Windows Server 2003, следует воспользоваться командой Gpedit. msc. Затем в консоли последовательно раскройте узлы: **Политика «Локальный компьютер» (Local Computer Policy), Конфигурация компьютера (Computer Configuration), Конфигурация Windows (Windows Settings), Параметры безопасности (Security Settings), Локальные политики (Local Policies)** и, наконец, выберите **Назначение прав пользователя (User Rights Assignment).** Выберите политику **Вход в качестве службы (Log On As A Service)** и убедитесь, что в списке есть учетная запись, которую предполагается использовать.

В Windows Server 2003 есть несколько возможностей разрешения ситуации, когда служба не запускается по одной из описанных выше причин. События сбоя запуска службы записываются в журналы сервера, на котором она загружалась. Однако можно более активно подойти к управлению службой.

Вкладка **Восстановление (Recovery)** окна свойств службы предоставляет возможность выбора действий при сбое службы (рис. 12-30).

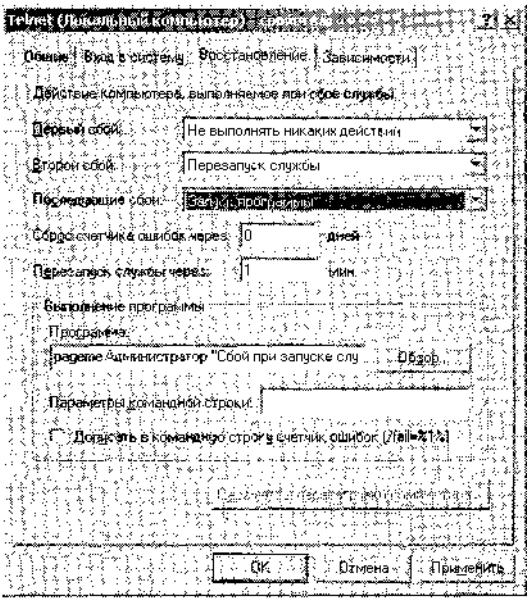


Рис. 12-30. Настройка поведения при сбое службы на вкладке *Восстановление*

При сбое службы возможны четыре варианта поведения:

- *Не выполнять никаких действий* (Take No Action);

в *Перезапуск службы* (Restart The Service);

- *Запуск программы* (Run A Program);
- *Перезагрузка компьютера* (Restart The Computer).

Единичный сбой службы может быть просто случайностью, например служба не смогла загрузиться из-за того, что другая служба, от которой она зависит, не была инициализирована. Возможных причин масса, в том числе временное замедление доступа к диску или необходимость для другой службы закончить запись в файл журнала перед завершением запуска. Поэтому при первом сбое стоит просто перезапустить службу.

Если служба сбоит регулярно, можно попробовать опять перезапустить ее, запустить программу, которая сообщит об отказе службы, либо перезагрузить компьютер, чтобы проверить, не обусловлена зависимость особой ситуацией в ОС.

Лабораторная работа. Настройка служб

Вы настроите зависимость службы и параметры восстановления на Computer 1.

Упражнение 1. Настройка зависимости службы

Вы попытаетесь запустить службу *Сервер папки обмена*. Не забывайте о зависимости служб.

1. На Computerl в меню **Пуск (Start)** правой кнопкой щелкните Мой компьютер (My **Computer)** и в контекстном меню выберите **Управление** (Manage).
2. Раскройте узел **Службы и приложения (Computer Management, Services And Applications)** и выберите **Службы (Services).**
3. Найдите в списке службу **Сервер папки обмена (Clipbook)** и двойным щелчком откройте окно свойств.

4. Измените **Тип запуска (Startup Type)** с **Отключено (Disabled)** на **Авто (Automatic)** и щелкните **Применить (Apply).**
5. Щелкнув ***Пуск (Start),*** *попытайтесь запустить службу: Появится* сообщение об ошибке: **Не удалось запусить дочернюю службу (The dependency** service or **group failed to start).**
6. Выберите вкладку **Зависимости (Dependencies),** чтобы выяснить зависимости службы *Сервер папки обмена.* Видно, что для работы *Сервера папки обмена* нужно запустить службы **Служба сетевого DDE (Network DDE)** и **Диспетчер сетевого DDE (Network DDE** *DSDM). Закройте диалоговое окно* свойств службы *Сервер папки обмена* щелчком OK.
7. Найдите значок службы **Диспетчер сетевого DDE** и дважды щелкните его. В окне свойства измените **Тип запуска** с **Отключено** на **Авто** и щелкните Применить.
8. Запустите службу щелчком кнопки Пуск. Щелкнув OK, закройте диалоговое окно свойств службы **Диспетчер сетевого DDE.**
9. Аналогичным образом запустите *Службу сетевого DDE.*
10. Правой кнопкой щелкните службу **Сервер папки обмена,** а затем щелчком Пуск запустите ее. На этот раз служба запустится.

Упражнение 2. Настройка параметров восстановления службы

Вы намеренно вызовете сбой службы **Telnet,** чтобы посмотреть, как она отреагирует на сбой.

1. На Computerl в меню **Пуск (Start)** правой кнопкой щелкните **Мой компьютер (My Computer)** и в контекстном меню выберите **Управление (Manage).**
2. Раскройте узел **Службы и приложения (Computer Management, Services And Applications)** и выберите **Службы (Services).**
3. Двойным щелчком откройте окно свойств службы **Telnet.**
4. Измените **Тип запуска (Startup Type)** с **Отключено (Disabled)** на **Авто (Automatic).**
5. На вкладке **Восстановление (Recovery)** в поле со списком **Первый сбой (First Failure)** выберите **Перезапуск службы (Restart The Service).**
6. Щелчком OK закройте окно свойств **Telnet.**
7. Щелкните службу **Telnet** правой кнопкой и выберите **Пуск (Start).** Служба **Telnet** запустится.
8. Нажмите комбинацию Ctrl+Alt+Del и выберите **Диспетчер задач. (Task Manager).** Откроется окно **Диспетчер задач (Task Manager).**
9. На вкладке **Процессы (Processes)** выберите процесс **Tlntsvr.exe** и нажмите кнопку **Завершить процесс (End Process).** Служба **Telnet** остановится.
10. Подождите минутку и вновь взгляните на список процессов на вкладке. В списке снова появилось **Tlntsvr.exe,** так как служба автоматически перезапустилась.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данного занятия. Если вы не сумеете ответить на вопрос, повторите соответствующий материал. Ответы для самопроверки — в приложении «Вопросы и ответы» в конце главы.

1. Вы устанавливаете новое приложение, которое также устанавливает на компьютере свою службу. При первом запуске приложения происходит сбой. В журнале событий обнаруживается сообщение об ошибке, информирующее, что служба не запускается из-за сбоя входа в систему. Что следует предпринять?
   a. Предоставить учетной записи право *Вход в качестве службы* (Logon As A Service).
   b. В учетной записи изменить пароль, не меняя имя.

c. Проверить имя пользователя в учетной записи, используемой для запуска службы.
d. Предоставить учетной записи административные полномочия.

2. Вы устанавливаете новое приложение, которое также устанавливает на компьютере свою службу. При первом запуске приложения происходит сбой. При проверке зависимостей новой службы оказалось, что необходимая служба не запущена. Однако политика безопасности требует, чтобы службы оставались отключенными, пока другое приложение не потребует их запуска. Какой параметр выбрать для зависимой службы, чтобы она запустилась?
   a. Авто.
   b. Авто, но с приостановкой службы.
   c. Вручную.
   d. Отключено.
3. Вы устанавливаете новое приложение на рядовой сервер. Приложение сообщает, что устанавливает на компьютер службу. В процессе установки службы предлагается указать имя пользователя и пароль для запуска службы. Вы задали имя *DOMAIN\\$ervicel,* однако при попытке первый раз запустить приложение происходит сбой. Вы предполагаете, что учетная запись получила недостаточные полномочия для запуска службы. Что следует предпринять?
   a. На рядовом сервере предоставить учетной записи Service 1 право *Вход в качестве службы* (Log On As A Service).
   b. В домене предоставить учетной записи Service 1 право *Вход в качестве службы* (Log On As A Service).
   c. На рядовом сервере предоставить учетной записи Servicel право *Вход в качестве пакетного задания* (Log On As A Batch Job).
   d. В домене предоставить учетной записи Servicel право *Вход в качестве пакетного задания* (Log On As A Batch Job).

Резюме

- Запуск одних служб часто зависит от наличия и работы других служб. Если служба не запускается, рекомендуется проверить, запущены ли службы, от которых она зависит.
- При устранении неполадок запуска служб нужно проверить имя пользователя, пароль и наличие права *Вход в качестве службы* (Log On As A Service).
- Можно настроить параметры восстановления службы так, чтобы получать сообщения о неудачном запуске службы.

Пример из практики

Вы работаете в компании Tailspin Toys, штаб-квартира которой находится в Арканзасе, а филиал — в Делавэре. Арканзас и Делавэр соединены линией T1. Единственное подключение к Интернету находится в Арканзасе. Сеть Tailspin Toys, в которой работает 300 человек, состоит из одного домена. ИТ-отдел расположен в Арканзасе.

Вы — администратор сети компании. Пользователи и другие администраторы сообщают о неполадках в сети, и нужно решить, какие средства диагностики лучше всего использовать для устранения неполадок.

Ниже приведены пять разных отчетов. Для каждого из отчетов нужно выбрать соответствующие средства. Выберите между полной и облегченной версией *Сетевого мони-*

тора (Network Monitor), утилитой Netstat, командой Ping, тестами вкладки DNS **Наблюдение (Monitoring),** кнопкой **Исправить (Repair),** установкой сетевого моста и настройкой служб. Укажите причину, объясняющую ваш вьхбор. Может быть, не понадобится использовать все возможные варианты ответов.

1. Пользователь в Арканзасе жалуется, что не может выйти в Интернет. Вы попросили его проверить локальный шлюз командой ping и результат оказался отрицательным. Другие пользователи не испытывают проблем с подключением.
2. Все пользователи компании сообщают о невозможности подключиться к Интернету, однако доступ к ресурсам компании сохраняется.
3. Администратор сети в Делавэре хочет узнать, как наилучшим образом создать в сети новый сегмент с другой физической топологией, не приобретая аппаратный маршрутизатор.
4. Администратор сети в Делавэре сообщает, что на сервере не запускается служба стороннего производителя. Он предпринял несколько попыток запустить службу, но безуспешно.
5. Администратор в Арканзасе подозревает, что сервер поражен вирусом или троянской программой. Похоже, что эта программа открывает определенный порт. Как определить, какой порт использует потенциально опасный процесс?

Резюме главы

- Поддержка сети под управлением Windows Server 2003 — одна из важнейших ежедневных задач.
- Самый простой и быстрый способ получить сведения о состоянии сетевого интерфейса сервера — вкладка **Сеть (Networking)** в окне **Диспетчере задач (Task Manager).**
- Консоль *Производительность* (Perfomance) используется для настройки оповещений. Оповещения добавляют информацию в журнал *Приложение* (Application).
- Утилита Netstat служит для наблюдения за сетевым трафиком, а команда Netstat -O позволяет определить идентификатор процесса (PID), который открыл порт. Идентификаторы процессов отображаются и в *Диспетчере задач* (Task Manager).
- Полная версия *Сетевого монитора* (Network Monitor), входящая в состав Microsoft Systems Management Server, позволяет записывать трафик между любыми компьютерами локального сегмента.
- Триггеры сетевого монитора инициируют оповещение при определенных показаниях счетчиков либо при достижении определенного уровня заполнения буфера.
- Устраняя неполадки связи с Интернетом, проверяют IP-конфигурацию клиента, параметры DNS и серверы пересылки.
- Кнопка **Исправить (Repair)** на странице свойств сетевого адаптера позволяет выполнять множество операций по устранению неполадок связи.
- Сетевой мост позволяет объединить несколько сетей в единую сеть.
- Запуск некоторых служб зависит от наличия и работоспособности других служб. Информация об этих зависимостях отображается на вкладке **Зависимости (Dependencies)** службы.
- Параметры восстановления службы позволяют определить, что должно выполняться в случае одного или нескольких сбоев службы: перезапуск службы, запуск программы или перегрузка компьютера.

Рекомендации по подготовке к экзамену

Прежде чем сдавать экзамен, повторите основные положения и термины, приведенные ниже, чтобы выяснить, какие темы нужно проработать дополнительно.

Основные положения

- Запомните, какие средства лучше всего подходят для быстрого наблюдения за сетью, а какие требуют времени на установку и настройку, но дают больше информации.
- Научитесь использовать оповещения для наблюдения за определенными характеристиками сети и правильно настраивать их.
- Нужно понимать, что устранение неполадок подключения к Интернету — многосторонняя проблема, корни-которой могут уходить к клиенту или серверу. Поэтому надо знать, где начинать и заканчивать.
- Нужно знать, как настраивать службы, с запуском которых наблюдаются затруднения.

Основные термины

Счетчик ~ counter — представление объекта системы. Счетчики служат для мониторинга производительности и выявления затруднений и неполадок в работе системы.

Частота выборки ~ sampling rate — частота, с которой счетчик проверяет выполнение определенных критериев. Чем чаще выполняется выборка, тем точнее результат. Однако при более низкой частоте выборки меньше загружается процессор.

Идентификатор процесса (PID) ~ Process Identifier — уникальный идентификатор работающего в системе процесса.

Триггер ~ trigger — действие, выполняемое, когда значение счетчика достигает порогового значения. Триггеры настраиваются на срабатывание при подходе к пороговому значению сверху или снизу.

Сервер пересылки ~ forwarder — сервер, на который служба DNS пересылает запросы.

Сетевой мост ~ network bridge — соединение, обеспечивающее объединение нескольких сетей в одну.

Зависимость службы ~ service dependency — взаимодействие между службами, при котором одной службе для запуска и нормальной работы необходима другая(ие) служба (ы).

Вопросы и ответы

Занятие 1. Закрепление материала

1. Вам сообщили, что Computerl медленно отвечает на запросы пользователей. Вы решили быстро просмотреть сетевой трафик с помощью окна *Сетевой монитор* (Network Monitor) и выяснить, есть ли на Computerl трафик широковещания. Какой счетчик нужно активизировать?
   a. *Неодноадресных пакетов в интервале* (Nommicasts/Interval).
   b. *Всего одноадр. пакетов в интервале* (Unicasts/Interval).

c. *Отправлено байт в интервале* (Bytes Sent/Interval).

d. *Получено байт в интервале* (Bytes Received/Interval). .

Правильный ответ: а.

2. Вы настроили в оснастке *Журналы и оповещения производительности* (Perfomance Logs And Alerts) оповещение с отправкой сообщения оператору на Computed о слишком высокой загруженности сети на Computerl. Однако Computed не удается принимать сообщения от Computerl. Как активизировать передачу сообщений от Computer! *и прием их на Computer2. (Выберите все подходящие варианты.)*

а. На Computerl запустить Службу сообщений (Messenger).

b. На Computerl запустить службу *Оповещатель* (Alerter).

c. На Computer2 запустить *Службу сообщений* (Messenger).

d. На Computer2 запустить службу *Оповещатель* (Alerter).

Правильные ответы: Ь, с.

3. Вы подозреваете, что компьютер под управлением Windows Server 2003 заражен вирусом и вирус передает данные по сети с сервера через определенный порт. Нужно выяснить, какой процесс использует этот порт. Какая команда, позволит это выяснить?

a. `Nbtstat -RR`.

b. `Nbtstat -r`.

c. `Netstat -a`.

d. `Netstat -o`.

Правильный ответ: `d`.

Занятие 2. Закрепление материала

Три следующих вопроса относятся к схеме сети компании Tailspin Toys (рис. 12-23). Предполагается, *что* вы сетевой *администратор этой компании.*

1. Пользователь из филиала сообщает, что ему не удается с помощью Internet Explorer открыть часто используемый Web-сайт. Эхо-запрос ping указанного адреса с клиентского компьютера в штаб-квартире проходит без проблем, а с клиентского компьютера пользователя — нет. Что предпринять для устранения неполадки? (Выберите все подходящие варианты.)

a. С клиентского компьютера пользователя проверить командой ping адрес назначения.

b. На клиентском компьютере пользователя воспользоваться кнопкой **Исправить (Repair)** для сетевого подключения.

c. На DNS-сервере выполнить тест простым запросом.

d. На DNS-сервере выполнить тест рекурсивным запросом.

Правильные ответы: а, Ь.

2. Вы настраиваете 50 новых клиентских машин в филиале, где другой администратор уже настроил службу DHCR При выходе первого клиентского компьютера в сеть обнаружилось, что.DHCP не предоставляет ни IP-адреса, ни адресов основного и дополнительного DNS-серверов.

Надо устранить неполадки службы DHCP и настроить ее так,'чтобы клиентские компьютеры получили доступ к внутренним ресурсам и к Интернету. Как настроить DHCP-сервер? (Выберите все подходящие варианты.)

a. Настроить DHCP-сервер на предоставление клиентам адреса DNS1.

b. Настроить DHCP-сервер на предоставление клиентам адреса ISPDNS1.

c. Настроить DHCP-сервер на предоставление клиентам адреса DNS2.

d. Настроить DHCP-сервер на предоставление клиентам адреса ISPDNS2.

Правильные ответы: a, c.

3. Пользователь из филиала сообщает, что ему не удается с помощью Internet Explorer открыть часто используемый Web-сайт. При запуске Nslookup с клиентского компьютера в штаб-квартире возвращается правильный адрес, а при выполнении той же команды с клиентского компьютера пользователя возвращается некорректный адрес. Что предпринять, чтобы устранить неполадку? (Выберите все подходящие варианты.)

a. Проверить правильность определения DNS-серверов на клиенте.

b. Выполнить команду Ipconfig /flushdns.

c. Выбрать значок **Сетевые подключения (Network Connections).**

d. Выполнить команду Ipconfig /renew.

Правильные ответы: a, Ь.

Занятие 3. Закрепление материала

1. Вы устанавливаете новое приложение, которое также устанавливает на компьютере свою службу. При первом запуске приложения происходит сбой. В журнале событий обнаруживается сообщение об ошибке, информирующее, что служба не запускается из-за сбоя входа в систему. Что следует предпринять?

a. Предоставить учетной записи право *Вход в качестве службы* (Logon As A Service).

b. В учетной записи изменить пароль, не меняя имя.

c. Проверить имя пользователя в учетной записи, используемой для запуска службы.

d. Предоставить учетной записи административные полномочия.

Правильный ответ: c.

2. Вы устанавливаете новое приложение, которое также устанавливает на компьютере свою службу. При первом запуске приложения происходит сбой. При проверке зависимостей новой службы оказалось, что необходимая служба не запущена. Однако политика безопасности требует, чтобы службы оставались отключенными, пока другое приложение не потребует их запуска. Какой параметр выбрать для зависимой службы, чтобы она запустилась?

a. Авто.

b. Авто, но с приостановкой службы.

c. Вручную.

d. Отключено.

Правильный ответ: c.

3. Вы устанавливаете новое приложение на рядовой сервер. Приложение сообщает, что устанавливает на компьютер службу. В процессе установки службы предлагается указать имя пользователя и пароль для запуска службы. Вы задали имя *DOMAIN\Servicel,* однако при попытке первый раз запустить приложение происходит сбой. Вы предполагаете, что учетная запись получила недостаточные полномочия для запуска службы. Что следует предпринять?

a. На рядовом сервере предоставить учетной записи Service 1 право *Вход в качестве службы* (Log On As A Service).

b. В домене предоставить учетной записи Servicel право *Вход в качестве службы* (Log On As A Service).

c. На рядовом сервере предоставить учетной записи Service 1 право *Вход в качестве пакетного задания* (Log On As A Batch Job).

d. В домене предоставить учетной записи Service 1 право *Вход в качестве пакетного задания* (Log On As A Batch Job).

Правильный ответ: a.

Пример из практики

Вы работаете в компании Tailspin Toys, штаб-квартира которой находится в Арканзасе, а филиал — в Делавэре. Арканзас и Делавэр соединены линией T1. Единственное подключение к Интернету находится в Арканзасе. Сеть Tailspin Toys, в которой работает 300 человек, состоит из одного домена. ИТ-отдел расположен в Арканзасе.

Вы — администратор сети компании. Пользователи и другие администраторы сообщают о неполадках в сети, и нужно решить, какие средства диагностики лучше всего использовать для устранения неполадок.

Ниже приведены пять разных отчетов. Для каждого из отчетов нужно выбрать соответствующие средства. Выберите между полной и облегченной версией *Сетевого монитора* (Network Monitor), утилитой Netstat, командой Ping, тестами вкладки DNS **Наблюдение (Monitoring),** кнопкой **Исправить (Repair),** установкой сетевого моста и настройкой служб. Укажите причину, объясняющую ваш выбор. Может быть, не понадобится использовать все возможные варианты ответов.

1. Пользователь в Арканзасе жалуется, что не может выйти в Интернет. Вы попросили его проверить локальный шлюз командой ping и результат оказался отрицательным. Другие пользователи не испытывают проблем с подключением.

   Правильный ответ: лучше всего использовать кнопку Исправить (Repair), поскольку у этого пользователя скорее всего нарушена связь с сетью. Так как у других пользователей проблем нет, неполадка, скорее всего, носит единичный характер.

2. Все пользователи компании сообщают о невозможности подключиться к Интернету, однако доступ к ресурсам компании сохраняется.

   Правильный ответ: тесты вкладки DNS Наблюдение (Monitoring) помогут убедиться, что DNS-сервер получает правильные ответы от сервера, которому он пересылает запросы.

3. Администратор сети в Делавэре хочет узнать, как наилучшим образом создать в сети новый сегмент с другой физической топологией, не приобретая аппаратный маршрутизатор.

   Правильный ответ: лучше всего использовать сетевой мост, чтобы соединить вместе две разнородные сети.

4. Администратор сети в Делавэре сообщает, что на сервере не запускается служба стороннего производителя. Он предпринял несколько попыток запустить службу, но безуспешно.

   Правильный ответ: проверьте параметры службы, особенно зависимости и права на вход в систему.

5. Администратор в Арканзасе подозревает, что сервер поражен вирусом или троянской программой. Похоже, что эта программа открывает определенный порт. Как определить, какой порт использует потенциально опасный процесс?

   Правильный ответ: командой Netstat -o определить используемые порты. Затем в Диспетчере задач (Task Manager) можно найти идентификатор процесса (PID), чтобы выяснить, что это за процесс.

Предметный указатель

ДЖ. С. МЭКИН (J. C. Mackin) Дж. С. Макин (MCSA, MCSE, MCT) - писатель, редактор, консультант и преподаватель. Написал несколько книг, среди которых курс по Internet Security and Acceleration Server 2000. Имеет звание магистра телекоммуникаций и управления сетями.

Йен МЭКЛИН (Ian McLean) Йен Маклин (MCSE, MCDBA, MCT) обладает 35-летним опытом работы в промышленности, торговле и образовании. Он начал свою карьеру как инженер по электронике, позже Йен занимался заочным обучением, а потом занимал должность профессора в университете. В настоящее время работает на собственную консалтинговую компанию. Написал 14 кних и множество научных и технических статей. С сетями Йен вплотную познакомился в начале 1980-х, а с сетевыми операционными системами Microsoft работает с 1997 года.

Дж, С. Макин, Йен Маклин

Внедрение, управление и поддержка сетевой инфраструктуры Microsoft Windows Server 2003

Перевод с английского под общей редакцией А. **Р. Врублевского**

Редактор **С. В. Дергачев**

Компьютерный дизайн и подготовка иллюстраций Е. Р. **Данилов**

Технический редактор **Н.** Г. **Тимченко**

Дизайнер обложки **Е. В. Козлова**

Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
123317, Москва, ул. Антонова-Овсеенко, д. 13. Тел.: (095) 256-5120, тел./факс: (095) 256-4541.
e-mail: info@rasedit.ru, http://www.rusedit.ru

• «.РУССКАЯ РЕДАКЦИЯ

При участии ООО ПФ «Сашко»

Подписано в печать 07.10.2004 г. Тираж 2 500 экз. Заказ № 5005. Формат 70x1001/16. Физ. п. л. 39

Отпечатано с готовых диапозитивов во ФГУП ИПК
«Ульяновский Дом печати». 432980, г. Ульяновск, ул. Гончарова, 14