MCSA/MCSE

Training Kit

Exam 70-216

Microsoft®

Windows 2000 Network Infrastructure Administration

Microsoft Press

Учебный
курс
MCSA/MCSE

Сертификационный экзамен 70-216

Администрирование сети на основе

Microsoft®
Windows 2000

Официальное пособие Microsoft для самостоятельной подготовки

3-е издание, исправленное

Москва 2004

РУССКАЯ РЕДАКЦИЯ

УДК 004
ББК 32.973.26–018.2
М59

Microsoft Corporation

М59 Администрирование сети на основе Microsoft Windows 2000. Учебный курс **MCSA/MCSE:** Пер. с англ. 3-е изд., испр.— М.: Издательско-торговый дом «Русская Редакция», 2004. — 416 **стр.:** ил.

ISBN 5–7502–0148–1

Учебный курс, посвященный сетевой инфраструктуре Windows 2000, содержит основные сведения об организации сетей на базе этой ОС, позволяет освоить навыки по установке и настройке ее основных сетевых компонентов. В книге рассматриваются сетевые протоколы и такие сетевые службы Windows 2000, как DNS, WINS, DHCP и RRAS. Немало внимания уделено вопросам безопасности — вы научитесь использовать протокол IPSec и политики безопасности, а также планировать структуру безопасности сети в целом.

Учебный курс адресован всем, кто хочет получить исчерпывающие знания в области планирования, развертывания и конфигурирования сетей на основе Windows 2000. Помимо теоретических сведений книга содержит упражнения и контрольные вопросы, облегчающие освоение материала. Вы сможете самостоятельно подготовиться к экзамену по программе сертификации Microsoft (Microsoft Certified System Engineer. MCSE) № 70-216: Implementing and Administering a Microsoft Windows 2000 Network Infrastructure.

Богато иллюстрированное издание состоит из 13 глав, одного приложения, словаря терминов и предметного указателя.

УДК 004
ББК 32.973.26–018.2

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

ISBN 1–57231–904–6 (англ.)
ISBN 5–7502–0148–1

Содержание

Об этой книге

Мы рады представить вам учебный курс MCSE «Администрирование сети на основе Microsoft Windows 2000». Он поможет вам понять принципы планирования сетевой инфраструктуры на основе Windows 2000. В книге описаны сетевые протоколы и службы и проведен их сравнительный анализ, что поможет вам выбрать нужный в соответствии с требованиями вашей организации. Кроме того, здесь рассказано об интеграции с сетями Novell NetWare на основе совместимых с IPX/SPX протоколов. Наибольшее внимание уделяется описанию самого популярного в Интернете протокола — TCP/IP — эффективного средства для построения сетей масштаба предприятия. Здесь описаны возможности и настройка протокола TCP/IP, а также служб NetBIOS, WINS, DHCP и DNS. Кроме того, рассказано о работе со службами маршрутизации и удаленного доступа, в том числе о *виртуальных частных сетях* (virtual private networks, VPN).

Примечание Дополнительную информацию о программе сертификации специалистов Microsoft Certified Systems Engineer см. далее в разделе «Программа сертификации специалистов Microsoft».

Главы учебника подразделяются на занятия, большинство которых содержат упражнения, предназначенные для демонстрации излагаемых методов и приобретения практических навыков. Каждое занятие заканчивается кратким обобщением материала, а глава — вопросами, которые помогут нам проконтролировать уровень ваших знаний и степень усвоения материала.

В разделе «С чего начать» вводной главы книги перечислены аппаратные и программные требования, а также параметры сетевой конфигурации, необходимые для выполнения занятий и упражнений курса. Внимательно прочитайте его, прежде чем изучать материал.

Кому адресована эта книга

Данный курс предназначен тем, кто собирается планировать, устанавливать и поддерживать сети предприятия на основе Windows 2000, или тем, кто желает сдать сертификационный экзамен 70-216.

Для изучения данного курса необходимо:

- знать основы современных сетевых технологий;
- иметь опыт работы администрирования сетей Windows NT 4.0;
- знать материал в объеме курса MSCE по Microsoft Windows 2000 Server.

Справочные материалы

- *Microsoft Windows 2000 Server Resource Kit.* **Microsoft Press.** 1999.
- Справочная система Windows 2000 Server.
- Материалы по Windows 2000, доступные на Web-узле Microsoft по адресу *http://www.microsoft.com/windows2000/guide/server/overview.*

Компакт-диск с дополнительными материалами к курсу

На прилагаемом к книге компакт-диске хранится полная электронная версия книги на английском языке. Кроме того, на компакт-диске вы найдете медиа-файлы для самостоятельной подготовки к сдаче экзамена, толковый словарь терминов и пакеты обновления для русской и оригинальной версии Microsoft Windows 2000 Server и Professional.

Структура книги

- Каждая глава начинается с раздела «В этой главе», содержащего краткий обзор обсуждаемых тем.
- Главы делятся на занятия, большинство из которых содержат упражнения. Выполнив их, вы закрепите свои знания и приобретете практические навыки. Упражнения обозначаются значком на полях.
- Каждую главу завершает раздел «Закрепление материала», вопросы которого помогут вам проверить, насколько твердо вы усвоили материал.
- Приложение «Вопросы и отпеты» содержит вопросы всех глав книги и ответы на них.

Обозначения

- Вводимые вами символы или команды набраны строчными буквами полужирного начертания.
- *Курсив* в операторах указывает, что в этом месте вы должны подставить собственные значения; названия книг и адреса Интернета также набраны *курсивом.*
- Имена файлов, папок и каталогов начинаются с прописных букв (за исключением имен, которые вы задаете сами). Кроме особо оговоренных случаев, для ввода имен файлов и каталогов в диалоговом окне или в командной строке Вы можете использовать строчные буквы.
- Расширения имен файлов набраны строчными буквами.
- Аббревиатуры напечатаны ЗАГЛАВНЫМИ БУКВАМИ.
- Примеры кода, текста, выводимого на экран и вводимого в командной строке, набраны моноширинным шрифтом.
- Необязательные элементы операторов заключены в скобки <>. Например *<имя_файла>* в синтаксисе команды означает, что после команды можно указать имя файла. Сами скобки вводить НЕ надо.
- Обязательные элементы операторов заключены в фигурные скобки {}. Сами скобки вводить НЕ надо.
- Значками на полях помечены конкретные разделы.

Значок	Описание
	Упражнение по закреплению навыков, приобретенных при изучении материала
	Вопросы, отвечая на которые, вы проверите, насколько твердо и безошибочно усвоили изложенный материал. Вопросы обычно сгруппированы в конце главы, ответы см. в приложении «Вопросы и ответы»

Клавиатура

- Знак «+» между названиями клавиш означает, что их следует нажать одновременно. Например, выражение «Нажмите Alt+Tab» обозначает, что нужно нажать клавишу Tab, удерживая нажатой клавишу Alt.
- 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 вам придется сначала нажать клавиши Alt и W вместе, потом отпустить их и нажать клавишу L.
- Команды меню можно выбирать с клавиатуры. Для этого нажмите клавишу Alt (чтобы активизировать меню), а затем последовательно — выделенные или подчеркнутые буквы в названиях нужных вам разделов меню или команд. Кроме того, некоторым командам сопоставлены клавиатурные сокращения (они указаны в меню).
- Флажки и переключатели также можно устанавливать и снимать посредством клавиатуры. Для этого достаточно нажать Alt, а затем клавишу, соответствующую подчеркнутой букве в названии флажка или переключателя. Кроме того, нажимая клавишу Tab, вы можете сделать зону нужного параметра активной, а затем установить или снять выбранный флажок или переключатель, нажав клавишу «пробел».
- Работу с диалоговым окном всегда можно прервать, нажав клавишу **ESC.**

Обзор глав и приложений

Этот курс, предполагающий самостоятельную работу, включает занятия, упражнения и проверочные вопросы, которые помогут вам научиться разрабатывать, реализовывать, администрировать и обслуживать сеть на основе Windows 2000. Курс рассчитан на последовательное изучение «от корки до корки», но не исключена и возможность работы лишь с интересующими вас главами. Советуем в этом случае обращать внимание на раздел «Прежде всего» в начале каждой главы, где указаны предварительные требования для выполнения упражнений.

Ниже кратко описаны главы и приложения учебного курса.

- В разделе «Об этой книге» собраны сведения о содержании учебника и данные о структурных единицах и условных обозначениях, принятых в нем. Внимательно прочитайте его: это поможет вам эффективнее работать с материалами курса, а также выбрать интересующие вас темы. Здесь также приведена информация по установке, необходимая для успешного выполнения упражнений данного курса.
- В главе 1 «Проектирование сети Windows 2000» рассказано об основных сетевых протоколах и службах, используемых при планировании сетевой инфраструктуры.
- В главе 2 «Внедрение TCP/IP» описаны процедуры установки и настройки сетевого протокола TCP/IP.
- В главе 3 «Внедрение NWLink» обсуждаются установка и настройка совместимого с протоколами IPX/SPX сетевого протокола NWLink, обеспечивающего взаимодействие с сетями Novell NetWare.
- В главе 4 «Мониторинг сетевой активности» рассказывается об использовании приложения Network Monitor, входящего в комплект Windows 2000.

- Глава 5 «Внедрение IPSec» посвящена таким вопросам, как активизация, настройка, наблюдение работы IPSec, а также настройка политик и правил IPSec.
- В главе 6 «Разрешение имен узлов в сети» дан обзор различных способов разрешения имен, применяемых в TCP/IP.
- В главе 7 «Внедрение DNS» объясняется, как DNS разрешает имена узлов в локальной сети и в Интернете. В Microsoft Windows 2000 включена расширенная версия DNS.
- В главе 8 «Использование DNS» рассказано о работе с зонами DNS. В частности, здесь обсуждается применение делегированных зон и конфигурирование зон для динамического обновления. Из этой главы вы также узнаете, как настраивать DNS-сервер кэширования и научитесь наблюдать за производительностью DNS-сервера.
- В главе 9 «Внедрение WINS» обсуждается разрешение имён в сети с помощью WINS. Здесь вы также узнаете об основных компонентах службы WINS в Windows 2000, о ее установке и конфигурировании и с решении возникающих при работе с ней проблем.
- В главе 10 «Внедрение DHCP» рассказывается о том, как протокол DHCP применяется для управления и настройки клиентских компьютеров в локальной сети с сервера Windows 2000. Вы узнаете об основных компонентах протокола DHCP, о его установке и конфигурировании как на клиенте, так и на сервере и о решении возникающих при работе с ним проблем.
- В главе 11 «Маршрутизация и удаленный доступ» рассказывается о службе RAS, позволяющей получать доступ к сетевым ресурсам клиентам, которые находятся дома или в дороге. Здесь также описана установка безопасных соединений на основе VPN.
- Главу 12 «Поддержка протокола NAT» мы посвятили протоколу NAT, предоставляющему сети с частными адресами, доступ к Интернет посредством трансляции IP-адресов. Вы также узнаете о том, как средствами протокола NAT настроить общее подключение к Интернету для домашней сети или сети небольшого офиса.
- В главе 13 «Внедрение служб сертификации» рассказывается о сертификатах — центральном элементе Microsoft PKI (инфраструктуры открытого ключа Microsoft), а также об их установке и настройке.
- В главе 14 «Безопасность сети предприятия» описываются возможности системы безопасности Windows 2000, а также рассказывается, как обеспечить максимально надежную безопасность вашей сети.
- В приложении «Вопросы и ответы» приведены ответы на вопросы из упражнений и разделов «Закрепление материала» всех глав учебного курса.
- В словаре терминов приведены определения терминов, которые вам надо знать при внедрении сетей Windows 2000 и управлении ими.

С чего начать

Данный курс предназначен для самостоятельного изучения, поэтому вы можете пропускать некоторые занятия, чтобы вернуться к ним потом. И все же помните, что для выполнения упражнений главы в большинстве случаев надо проделать упражнения предыдущих глав. Чтобы определить, с чего начать изучение курса, обратитесь к таблице.

Если вы	Что делать
готовитесь к сдаче сертификационного экзамена 70-215: Implementing and Administering a Microsoft Windows 2000 Network Infrastructure	см. раздел «Начало работы», а также описание процедур установки далее в этой главе. Затем изучите все главы этой книги
хотите изучить информацию по определенной теме экзамена	см. раздел «Материалы для полготовки к экзаменам»

Материалы для подготовки к экзаменам

В таблицах перечислены темы сертификационного экзамена 70-216: Implementing and Administering a Microsoft Windows 2000 Network Infrastructure и главы настоящего учебного курса, где обсуждаются соответствующие вопросы.

Примечание Конкретная программа любого экзамена определяется Microsoft и может быть изменена без предварительного уведомления.

Установка, настройка, управление, мониторинг и устранение неполадок DNS

Тема	Где обсуждается	
	Глава	Занятие
Установка сервера DNS	7	4
Настройка корневого сервера имен	7	2
Настройка зон	8	1
Настройка DNS-сервера кэширования	8	2
Настройка клиента DNS	7	2
Настройка зон для динамического обновления	8	1
Тестирование сервера DNS	8	2
Делегирование зон в DNS	8	1
Ручное создание записей ресурсов на сервере DNS	7	5
Управление и мониторинг DNS	8	2

Установка, настройка, управление, мониторинг и устранение неполадок DHCP

Тема	**Где обсуждается**	
	Глава	**Занятие**
Установка DHCP-сервера	10	1
Создание и управление областями, суперобластями и многоадресными областями в DHCP	10	2
Настройка DHCP для интеграции с DNS	10	3
Авторизация сервера DHCP для использования в Active Directory	10	4
Управление и мониторинг DHCP	10	5

Настройка, управление, мониторинг и устранение неполадок при работе с удаленным доступом

Тема	**Где обсуждается**	
	Глава	**Занятие**
Настройка удаленного доступа и решение проблем		
Настройка входящих подключений	11	2
Создание политики удаленного доступа	11	2

(см. след. стр.)

Настройка, управление, мониторинг и устранение неполадок при работе с удаленным ДОСТУПОМ *(окончание)*

Тема	Где обсуждается Глава	Занятие
Настройка профиля удаленного доступа	11	2
Настройка VPN	11	4
Настройка многоканальных подключений	11	5
Настройка служб маршрутизации и удаленного доступа для интеграции с DHCP	11	6
Управление и мониторинг удаленного доступа	11	7
	14	**Ч**
Управление безопасностью удаленного доступа		
Настройка протоколов аутентификации	14	2
Настройка протоколов шифрования	4	3
	14	2
Создание политики удаленного доступа	11	2
	14	2

Установка, настройка, управление, мониторинг и устранение неполадок с сетевыми протоколами

Тема	**Где обсуждается Глава**	**Занятие**
Установка, настройка, управление и устранение неполадок с сетевыми протоколами		
Установка и настройка протоколов TCP/IP	2	3
Установка протокола NWLink	3	4
Настройка сетевых привязок	3	4
Настройка фильтров пакетов TCP/IP	2	3
Настройка и решение проблем безопасности	5	2
сетевых протоколов	14	2
Управление сетевым трафиком и наблюдение *за* ним	4	2
	14	3
Настройка и решение проблем с протоколом IPSec		
Активизация IPSec	5	1,2
Конфигурирование IPSec для работы в транспортном режиме	5	3
Конфигурирование IPSec для работы в туннельном режиме	5	3
Настройка политик и правил IPSec	5	3
Управление и мониторинг IPSec	5	4

Установка, настройка, управление, мониторинг и устранение неполадок при работе со службой WINS

Тема	Где обсуждается	
	Глава	Занятие
Установка, настройка и решение проблем при работе со службой **WINS**	9	1-4
Настройка репликации **WINS**	9	4
Настройка разрешения имен с **NetBIOS**	9	1, 2
Управление и мониторинг WINS	9	3, 4

Установка, настройка, управление, мониторинг и устранение неполадок IP-маршрутизации

Тема	Где обсуждается	
	Глава	Занятие
Установка, настройка и решение проблем с протоколами IP-маршрутизации		
Дополнение таблицы маршрутов Windows 2000 статическими маршрутами	2 11	4 4
Внедрение маршрутизации по требованию	11	2
Управление и мониторинг IP-маршрутизации		
Управление и мониторинг граничной маршрутизации	2 11	4 1, 7
Управление и мониторинг внутренней маршрутизации	2 11	4 6
Управление и мониторинг протоколами IP-маршрутизации	2 11	4 1, 7

Установка, настройка и решение проблем с NAT

Тема	Где обсуждается	
	Глава	Занятие
Настройка совместного использования подключения к Интернету	12	2
Установка NAT	12	2, 3
Настройка свойств NAT	12	3
Настройка **интерфейсов NAT**	12	3

Установка, настройка, управление, мониторинг и решение проблем со службами сертификации

Тема	Где обсуждается	
	Глава	Занятие
Установка и настройка центров сертификации (Certificate Authority, CA)	13	2
Создание сертификатов	13	2
Выпуск сертификатов	13	2
Отзыв сертификатов	13	3
Удаление ключей восстановления шифрованной файловой системы (Encrypting File System, EFS)	13	3

Начало работы

Данный курс предназначен для самостоятельного изучения и содержит упражнения и практические рекомендации, которые помогут вам освоить развертывание и администрирование сетей Windows 2000

Для выполнения упражнений вам потребуется один компьютер с Windows 2000 Server. Кроме того, некоторые упражнения требуют наличия двух компьютеров. Если у вас нет возможности воспользоваться вторым компьютером, прочитайте упражнение и попытайтесь понять предпринимаемые действия.

Для изучения этого курса рекомендуется выделить отдельную сеть, чтобы не нарушать работу сети вашего предприятия и пользователей вашего домена. Тем не менее вы можете выполнять упражнения и в существующей сети.

Внимание! При выполнении части упражнений потребуется изменить конфигурацию серверов. Если ваш компьютер подключен к большой сети, это может привести к нежелательным результатам. Перед выполнением такт упражнений предварительно проконсультируйтесь с сетевым администратором.

Аппаратное обеспечение

Компьютер должен соответствовать приведенной далее минимальной конфигурации, а установленное на нем оборудование необходимо выбрать из списка совместимого оборудования Microsoft Windows 2000 Professional Hardware Compatibility List:

- 32-разрядный процессор Pentium с частотой не менее 166 МГц;
- не менее 64 Мб оперативной памяти, если в сети, к которой подключен ваш компьютер, от одного до пяти клиентских компьютеров (рекомендуется 128 Мб);
- один или несколько жестких дисков с 2 Гб свободного пространства;
- 12-скоростной привод CD-ROM (для установки Windows 2000 по сети привод CD-ROM не требуется);
- монитор SVGA с разрешением 800 x 600 (рекомендуется 1024 x 768);
- дисковод для дискет (если ваш CD-ROM не поддерживает загрузку или вы не можете запустить с него программу установки);
- мышь Microsoft или другое совместимое указательное устройство.

Программное обеспечение

Для выполнения практических заданий вам потребуется установить Microsoft Windows 2000 Server.

Подготовка компьютера к выполнению практических заданий

Ниже перечислены основные этапы подготовки вашего компьютера к выполнению заданий этого курса. Если вы ранее не занимались установкой Windows 2000 или другой сетевой ОС, обратитесь к опытному сетевому администратору. После выполнения каждого этапа отметьте галочкой соответствующую строку. Подробные инструкции для выполнения каждого этапа описаны ниже. Итак, кратко:

- создайте установочные дискеты Windows 2000 Server;
- запустите программу установки Windows 2000 Server;
- установите сетевые компоненты;
- установите аппаратное обеспечение.

Примечание Ниже содержатся указания по установке Windows 2000, которые помогут вам подготовить компьютер для выполнения заданий этой книги. Однако обучение установке не входит в цели данного курса. Подробности об установке Windows 2000 Server см. в учебном курсе MSCE, посвященном Microsoft Windows 2000 Server.

Установка Windows 2000 Server

Для выполнения упражнений этого курса необходимо установить Windows 2000 Server. Компьютер, на который вы хотите установить операционную систему, не должен содержать форматированных разделов. Раздел на жестком диске для установки Windows 2000 Server в качестве изолированного сервера рабочей группы можно создать непосредственно в процессе установки Windows 2000 Server.

Для выполнения приведенных ниже инструкций на вашем компьютере должна работать MS-DOS или любая версия Windows. Кроме того, он должен уметь обращаться к каталогу Bootdisk установочного компакт-диска с Windows 2000 Server. Если ваш компьютер настроен для загрузки с CD-ROM, вы можете установить Windows 2000, не используя установочные дискеты.

Внимание! Для установки необходимо четыре дискеты емкостью 1,44 Мб каждая. Запись на дискеты выполняется поверх имеющихся данных; предупреждения о перезаписи вы не получите.

▶ Создание установочных дискет Windows 2000 Server

1. Наклейте на четыре пустые отформатированные дискеты емкостью 1,44 Мб наклейки со следующими надписями:
   - «Установочный диск Windows 2000 Server №1»;
   - «Установочный диск Windows 2000 Server №2»;
   - «Установочный диск Windows 2000 Server №3»;
   - «Установочный диск Windows 2000 Server №4».
2. Вставьте установочный компакт-диск для Microsoft Windows 2000 Server к привода CD-ROM.
3. Если появится сообщение Windows 2000 CD-ROM с запросом на установку или обновление операционной системы до Windows 2000, щелкните кнопку No.

4. Откройте окно командной строки.
5. Введите букву привода CD-ROM в командную строку и нажмите Enter.
6. Сделайте активным каталог Bootdisk, введя в командную строку cd **bootdisk** и нажмите Enter.
7. Если на компьютере, на котором вы создаете загрузочные дискеты, установлена MS-DOS, 16-разрядная версия Windows, Windows 95 или Windows 98, введите в командной строке **makeboot** a: (где a: — имя вашего дисковода) и нажмите Enter. Если на компьютере установлена Windows NT или Windows 2000, введите **makebt32** a: (где a: — имя вашего дисковода) и нажмите Enter. Появится сообщение о том, что будут созданы четыре установочные дискеты для Windows 2000, для чего вам необходимо приготовить четыре пустые отформатированные гибкие дискеты высокой плотности.
8. Нажмите любую клавишу для продолжения. Появится сообщение, что нужно вставить в дисковод дискету, на которую будет записана установочная информация.
9. Вставьте в дисковод пустую отформатированную дискету, надписанную «Установочный диск Windows 2000 Server №1», и нажмите любую клавишу, После создания образа диска Windows 2000 попросит вас вставить вторую, третью и четвертую дискеты.
10. В командной строке введите **exit** и нажмите Enter.

    Выньте дискету из дисковода и компакт-диск из привода CD-ROM.

▶ Запуск программы установки Windows 2000 Server

Примечание При описании этой процедуры предполагается, что на вашем компьютере не установлена ОС, жесткий диск не забит на разделы, а поддержка загрузки с CD-ROM отключена.

---

1. Вставьте дискету, надписанную «Установочный диск Windows 2000 Server №1», и загрузочный диск Windows 2000 Server и перезагрузите компьютер.

   После перезапуска компьютера появится сообщение, что происходит проверка нашей системной конфигурации. Вскоре после этого откроется окно Windows 2000 Setup.

   Обратите внимание на серую строку внизу экрана. В ней сообщается, что происходит проверка компьютера и загрузка Windows 2000 Executive — минимальной версии ядра Windows 2000.

   Вставьте в дисковод дискету №2 (когда увидите соответствующее сообщение) и нажмите Enter.

   Setup произведет загрузку HAL, шрифтов, драйверов шины и других программ, обеспечивающих работу материнской платы, шины и других аппаратных средств вашего компьютера. Кроме того, будут загружены исполнимые файлы Windows 2000 Setup.
2. Вставьте в дисковод дискету №3 (когда увидите соответствующее сообщение) и нажмите Enter.

   Setup произведет загрузку драйверов контроллера дисковода и инициализацию драйверов, обеспечивающих поддержку доступа к дисководу. Во время этого процесса Setup может несколько раз останавливаться.
3. Вставьте в дисковод дискету №4 (когда увидите соответствующее сообщение) и нажмите Enter.

   Будут загружены драйверы периферийных устройств, например, драйвер дисковода и файловых систем, после чего произойдет инициализация Windows 2000 Executive и загрузка оставшихся установочных файлов.

   Если вы устанавливаете пробную версию Windows 2000, программа установки предупредит вас об этом.
4. Прочитав сообщение Setup, нажмите Enter.

Заметьте, что программа установки позволяет нам произвести не только первоначальную установку, но и восстановить поврежденную версию Windows 2000.

X Прочитайте сообщение, содержащееся в окне Welcome To Setup, и нажмите Enter для продолжения установки. Откроется окно License Agreement (Лицензионное соглашение).

6. Прочитайте лицензионное соглашение. Для прокрутки текста пользуйтесь клавишей Page Down.
7. Выберите I Accept The Agreement (Я принимаю соглашение), нажав клавишу F8.

   Откроется окно Windows 2000 Server Setup (Установка Windows 2000 Server), где вам предлагается выбрать область диска (или уже существующий раздел) для установки Windows 2000. На этом этапе вы можете создавать и удалять разделы на нашем жестком диске.

   Если ваш жесткий диск ранее не содержал разделов (как предполагается в этом упражнении), то вы увидите на диске неразмеченное пространство.
8. Убедившись, что выбрано Unpartitioned space (Неразмеченное пространство), нажмите с.

   Появится сообщение, что сейчас будет создан новый раздел, с указанием минимально и максимально возможных размеров этого раздела.
9. **Выбрав** размер раздела (минимум 2 Гб), нажмите **Enter.**

   Новый **раздел** будет назван **C:** New **(Unformatted).**

Примечание На этом этапе вы можете создавать и дополнительные разделы на свободном дисковом пространстве. Тем не менее созданием разделов рекомендуется заниматься после установки Windows 2000, используя оснастку Disk Management.

---

10. Убедившись, что выбран новый раздел, нажмите Enter.

    Появится предложение выбрать файловую систему для нового раздела.
11. Воспользовавшись клавишами управления курсором, выберите Format The Partition Using The NTFS File System (Отформатировать раздел под файловую систему NTFS) и нажмите Enter.

    Setup отформатирует раздел под NTFS, произведет проверку жесткого диска на наличие ошибок, которые могут повлечь сбои в установке, после чего скопирует файлы на диск. Это займет несколько минут.

    По завершении копирования компьютер будет перезагружен.
12. Выньте установочную дискету из дисковода.

Внимание! Если ваш компьютер настроен для загрузки с CD-ROM и поддержка загрузки с CD-ROM не была отключена в BIOS, то при перезагрузке программа установки будет запущена с самого начала. В этом случае выньте компакт-диск из привода CD-ROM и перезагрузите компьютер.

---

13. Программа установки скопирует дополнительные файлы, после чего перезагрузит ваш компьютер и запустит мастер установки Windows 2000.

► Графический режим установки

Примечание С этого момента Setup начинает работать в графическом режиме.

I. В окне мастера установки Windows 2000 щелкните кнопку Next (Далее) для сбора информации о компьютере.

Setup произведет конфигурирование папки и разрешений NTFS для файлов ОС. После этого будет выполнен поиск устройств, подключенных к компьютеру, а также установка и конфигурирование драйверов этих устройств. Это займет несколько минут.

2. Убедившись, что системные и пользовательские параметры и раскладка клавиатуры, указанные в окне Regional Settings (Региональные настройки), соответствуют нужному вам языку и региону, щелкните Next.

Примечание Чтобы изменить региональные настройки после того, как Windows 2000 уже установлена, дважды щелкните значок Regional Options на панели управления (Control Panel).

---

3. Введите ваше имя в поле Name (Имя) и имя вашей организации в поле Organization (Организация), затем щелкните Next.

Примечание Если откроется окно Your Product Key (Ключ продукта), введите в него ключ продукта, который указан на желтой наклейке на задней стороне коробки установочного компакт-диска Windows 2000 Server.

Откроется окно Licensing Modes (Режимы лицензирования), предлагая вам выбрать режим лицензирования. По умолчанию устанавливается режим лицензирования Per Server (На сервер). Setup попросит вас ввести количество приобретенных для этого сервера лицензий.

4. Щелкните переключатель Per Server Number Of Concurrent Connections (Число одновременных соединений для одного сервера) и установите число одновременных соединений равным 5 (для этого введите 5 в соответствующее поле). Далее щелкните Next.

Внимание! Для изучения курса рекомендуется выбрать параметр Per Server Number Of Concurrent Connections и задать число одновременных подключений равным 5. Тем не менее число одновременных соединений не должно превышать количества имеющихся у вас лицензий. Вы можете также использовать режим лицензирования Per Seat вместо Per Server.

Откроется окно Computer Name And Administrator Password (Имя компьютера и административный пароль). Обратите внимание, что имя компьютера сгенерировано на основе имени вашей организации.

5. В поле Computer Name (Имя компьютера) введите **server1.**

Вы увидите имя компьютера. Оно состоит из прописных букв вне зависимости от того, использовали ли вы при вводе строчные или прописные буквы.

Внимание! Если ваш компьютер подключен к сети, для задания имени компьютера обратитесь к администратору.

На протяжении всего курса учебный компьютер в вопросах и упражнениях будет обозначаться именем Server1. Если вы назвали свой сервер по-другому, вместо имени Server1 подставляйте имя вашего сервера.

6. В поля Administrator Password (Пароль администратора) и Confirm Password (Подтверждение пароля) введите строчными буквами **password** и щелкните кнопку Next. Пароль чувствителен к регистру, поэтом/ убедитесь, что слово **password** было набрано именно строчными буквами.

Для изучения этого курса пароль администратора **password** вполне подходит. В реальных ситуациях для пароля администратора рекомендуется выбирать более сложное

...ий было бы трудно угадать). В частности, Microsoft реко-
...чал прописные и строчные буквы, а также числа и другие
...).

...ft Components (Компоненты Windows 2000), **в котором пере-**
...енты Windows 2000.

...ополнительные компоненты после установки Windows 2000.
...ите значок Add/Remove Programs (Установка и удаление про-
...вления. Пока же вам нужно установить только компоненты,
...ию. Дополнительные компоненты вы будете устанавливать поз-
...урса.

...овки на вашем компьютере был обнаружен модем, откроется окно
...rmation (Информация о модеме).

...но Modem Dialing Information, введите в него код региона или горо-
...ext.

... Date And Time Settings (Настройки даты и времени).

Работа многочисленных служб Windows 2000 основана на настройках даты
Поэтому, чтобы избежать проблем в будущем, необходимо указать правиль-
...й пояс и регион.

...вильные параметры даты, времени и часового пояса, щелкните Next.
...тся окно Network Settings (Сетевые настройки), и будут установлены сетевые
...мпоненты.

Завершение установки сетевых компонентов

Сетевые компоненты — неотъемлемая часть Windows 2000 Server. При их настройке существуют большие возможности выбора. Пока вам нужно установить только основные сетевые компоненты, а дополнительные вы установите во время выполнения упражнений курса.

1. Убедившись, что на странице Networking Settings (Сетевые параметры) выбран параметр Typical Settings, шелкните Next. Начнется установка сетевых компонентов.

   Выбор параметра Typical Settings означает, что будут установлены компоненты, используемые для осуществления и предоставления доступа к сетевым ресурсам. Кроме того, протокол TCP/IP будет автоматически запрашивать IP-адрес у сервера DHCP.

   Откроется окно Workgroup Or Computer Domain (Рабочая группа или домен) с запросом, хотите ли вы включить ваш компьютер в рабочую группу или домен.

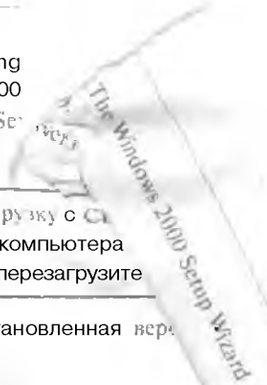
2. Убедившись, что в окне Workgroup Or Computer Domain выбран переключатель No. This Computer Is Not On A Network or Is On A Network Without A Domain (Компьютер не подключен к сети или входит в сеть без доменов) и в качестве имени рабочей группы указано WORKGROUP, шелкните Next.

   Откроется окно Installing Components (Установка компонентов), в котором изображается статус выполняемых опреаций по установке и настройке оставшихся компонентов ОС. Это займет несколько минут.

   Затем откроется окно Performing Final Tasks (Выполнение завершающих задач), в котором изображается статус выполняемых операций по завершению копирования файлов, внесению и сохранению изменений в конфигурации и удалению временных файлов. Если аппаратное обеспечение вашего компьютера ненамного превосходит минимальные требования, для завершения этой фазы установки может понадобиться более 30 минут.

По завершении установки откроется окно Completing (Завершение работы мастера установки Windows 2000

3. Выньте установочный компакт-диск с Windows 2000 Se... кните кнопку Finish (Готово).



Внимание! Если ваш компьютер поддерживает загрузку с CD установочный компакт-диск, то после перезагрузки компьютера запустится снова. В этом случае выньте CD-ROM и перезагрузите

После перезагрузки будет запущена только что установленная вер... Server.

▶ Завершение установки аппаратных средств

Сейчас вы выполните поиск устройств Plug and Play, не обнаруженных на стадиях установки.

1. Войдите *к* систему, нажав Ctrl+Alt+Delete.
2. *В* диалоговом окне Enter Password (Ввод пароля) введите **administrator** в поле Us... (Имя пользователя) и **password** — в поле Password (Пароль).
3. Щелкните ОК.
4. Если Windows 2000 найдет устройства, которые не были обнаружены при устанс... откроется окно мастера Found New Hardware (Обнаруженные устройства), сообщая в, что Windows 2000 устанавливает соответствующие драйверы.

   Если откроется окно мастера Found New Hardware, убедитесь, что флажок Restart The Computer When J Click Finish (Перезагрузить компьютер после окончания установки) не выбран, н щелкните кнопку Finish для завершения работы мастера Found New Hardware,

   Откроется окно Configure Your Server (Настройка вашего сервера), позволяющее вам конфигурировать множество различных параметров и служб.
5. Выберите I Will Configure This Server Later (Настроить сервер позднее) и щелкните кнопку Next (Далее).
6. В следующем окне сбросьте флажок Show This Screen At Startup (Показывать это окно при запуске).
7. Закройте окно Configure Your Server.

   Установка Windows 2000 Server завершена, и вы зарегистрированы с учетной записью Administrator.

Примечание Для правильного завершения работы Windows NT Server *к* меню Start выберите команду Shut Down и следуйте инструкциям на экране.

Для выполнения упражнений, требующих работы в сети, компьютеры должны иметь возможность связываться друг с другом. Первый компьютер с именем Server1 должен быть *первичным контроллером домена* (primary domain controller, PDC) Domain I. В большинстве процедур этого курса второй компьютер булет выполнять функции клиента или рядового сервера.

Примечание Если ваши компьютеры являются частью большой сети, обратитесь к сетевому администратору и проверьте, не входят ли имена компьютеров, доменов и другая введенная при установке информация в конфликт с текущими сетевыми параметрами. В случае конфликта попросите администратора присвоить вашим компьютерам другие значения и используйте их, изучая этот курс.

Программа сертификации специалистов Microsoft

Программа сертификации специалистов Microsoft (Microsoft Certified Professional, MCP) — отличная возможность подтвердить наши знания современных технологий и программных продуктов этой фирмы. Лидер отрасли в области сертификации Microsoft разработала современные методы тестирования. Экзамены и программы сертификации подтвердят вашу квалификацию разработчика или специалиста по реализации решений на основе технологий и программных продуктов Microsoft. Сертифицированные Microsoft профессионалы квалифицируются как эксперты и высоко ценятся на рынке труда.

Программа сертификации специалистов предлагает восемь типов сертификации по разным специальностям.

- **Сертифицированный специалист Microsoft (Microsoft Certified Professional, MCP)** — предполагается глубокое и доскональное знание по крайней мере одной операционной системы Microsoft. Сдав дополнительные экзамены, кандидаты подтвердят свое право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.
- **Сертифицированный специалист Microsoft + Интернет (MCP + Internet)** — должен разбираться в планировании систем защиты, установке и конфигурировании серверных продуктов, управлении ресурсами сервера, расширении возможностей сервера средствами сценариев *интерфейса общего шлюза* (Common Gateway Interface, CGI) и *интерфейса прикладного программирования сервера Интернета* (Internet Server Application Programming Interface, ISAPI), мониторинге работы сервера, анализе его производительности и устранении неисправностей.
- **Сертифицированный специалист Microsoft + Site Bulding (MCP + Site Bulding)** — планирование, создание, поддержка и управление Web-узлами с применением технологий и продуктов Microsoft.
- **Сертифицированный системный инженер Microsoft (Microsoft Certified Systems Engineer)** — умение эффективно планировать, развертывать, сопровождать и поддерживать информационные системы на базе Microsoft Windows 95, Microsoft Windows NT и интегрированного семейства серверных продуктов Microsoft BackOffice.
- **Сертифицированный системный инженер Microsoft + Интернет (MCSE + Internet)** — развертывание и сопровождение многофункциональных решений для интрасети и Интернета, включая программы просмотра, представительские серверы, базы данных, системы сообщений и коммерческие компоненты. Кроме того, сертифицированные по этой специальности инженеры должны уметь управлять Web-узлом и проводить его анализ.
- **Сертифицированный администратор баз данных Microsoft (Microsoft Certified Database Administrator, MCDBA)** — разработка физической структуры, логических моделей данных, создание физических БД, создание служб доступа к данным с использованием T-SQL, управление и поддержка БД, настройка и управление системой защиты, мониторинг и оптимизация БД, а также установка и настройка Microsoft SQL Server.
- **Сертифицированный разработчик программных решений на основе продуктов Microsoft (Microsoft Certified Solution Developer, MCSD)** — разработка и создание прикладных приложений с применением инструментальных средств, технологий и платформ Microsoft, включая Microsoft Office и Microsoft BackOffice.
- **Сертифицированный преподаватель Microsoft (Microsoft Certified Trainer, MCT)** — теоретическая и практическая подготовка для ведения соответствующих курсов в авторизованных учебных центрах Microsoft.

Преимущества программы сертификации Microsoft

Программа сертификации Microsoft — один из самых строгих и полных тестов оценки знаний и навыков ft области проектирования, разработки и сопровождения программного обеспечения. Сертифицированными специалистами Microsoft становятся лишь те, кто демонстрирует умение решать конкретные задачи, применяя продукты компании. Программа тестирования позволяет не только оценить квалификацию специалиста, но и служит ориентиром для всех, кто стремится достичь современного уровня знаний в этой области. Как и любой другой тест или экзамен, сертификация Microsoft является показателем определенного уровня знаний специалиста, что важно при трудоустройстве.

Для специалистов. Звание Microsoft Certified Professional даст вам следующие преимущества:

- официальное признание знаний и опыта работы с продуктами и технологиями Microsoft;
- доступ к технической информации о продуктах Microsoft через защищенную область Web-узла MCP;
- членство MSDN Online Certified Membership, обеспечивающее доступ к лучшим техническим ресурсам, сообществу MCP и другим полезным ресурсам и службам (некоторые из элементов узла MSDN Online доступны лишь на английском языке, *а к* некоторых странах — недоступны вообще); для получения растущего списка услуг, доступных сертифицированным членам, обратитесь на Web-узел MSDN;
- эмблемы, свидетельствующие, что вы имеете квалификацию сертифицированного специалиста Microsoft;
- приглашения на конференции, семинары и мероприятия, предназначенные для специалистов Microsoft;
- сертификат «Microsoft Certified Professional»;
- подписку на различные издания Microsoft, содержащие ценную техническую информацию о продуктах и технологиях Microsoft.

Кроме того, в зависимости от типа сертификации и страны, сертифицированные специалисты получают:

- годовую подписку на ежемесячно распространяемые компакт-диски Microsoft TechNet Technical Information Network;
- годовую подписку на программу бета-тестирования продуктов Microsoft (вы бесплатно получите до 12 компакт-дисков с бета-версиями новейших программных продуктов компании **Microsoft).**

Для работодателей и организаций. Сертификация позволяет быстро окупить затраты на технологии Microsoft и извлечь максимум прибыли из этих технологий. Исследования показывают, что сертификация сотрудников по программам Microsoft:

- быстро окупается за счет стандартизации требований к обучению специалистов и методов оценки их квалификации;
- позволяет увеличить эффективность обслуживания клиентов, повысить производительность труда и снизить расходы на сопровождение ОС;
- обеспечивает надежные критерии найма специалистов и их продвижения по службе;
- предоставляет методы оценки эффективности труда персонала;
- обеспечивает гибкие методы переподготовки сотрудников для обучения новым технологиям;
- позволяет оценить партнеров — сторонние фирмы.

Требования к соискателям

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

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 компании Microsoft.

Сертифицированный специалист Microsoft — кандидаты на это звание сдают экзамен по работе с одной из операционных систем. Кандидат может сдать дополнительные экзамены, которые подтвердят его право на работу с продуктами Microsoft BackOffice, инструментальными средствами или прикладными программами.

Сертифицированный специалист Microsoft + Интернет — кандидаты на это звание сдают экзамен по ОС Microsoft Windows NT Server 4.0. поддержке TCP/IP и экзамены по Microsoft Internet Information Server.

Сертифицированный специалист Microsoft + **Site Building** — кандидаты на это звание сдают два экзамена по основам технологий Microsoft Front Page, Microsoft Site Server и Microsoft Visual InterDev.

Сертифицированный системный инженер Microsoft — кандидаты на это звание сдают экзамены по технологии ОС Microsoft Windows, сетевым технологиям и технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.

Сертифицированный системный инженер Microsoft + Интернет — кандидаты на это звание сдают семь экзаменов по операционным системам и два — по выбору,

Сертифицированный администратор баз данных Microsoft — кандидаты на это звание сдают три ключевых экзамена и один — по выбору.

Сертифицированный разработчик программных решений на основе продуктов Microsoft — кандидаты сдают дна экзамена по основам технологии ОС Microsoft Windows и два — по технологиям интегрированного семейства серверных продуктов Microsoft BackOffice.

Сертифицированный преподаватель Microsoft — надо подтвердить свою теоретическую и практическую подготовку для ведения соответствующих курсов в авторизованных учебных центрах Microsoft. Более подробные сведения о сертификации по этой программе вы получите в компании Microsoft по телефону (800) 636-7544 (в США и Канаде) или по адресу *http://www.microsoft.com/train_cert/mct/*За пределами США и Канады обращайтесь в местные отделения компании Microsoft.

Подготовка к экзаменам

Рекомендуются три режима подготовки: самостоятельная работа, интерактивный режим, а также занятия с инструктором в авторизованных центрах подготовки.

Самостоятельная подготовка

Самостоятельная подготовка — наиболее эффективный метод подготовки для инициативных соискателей. Издательства «Microsoft Press» и «Microsoft Developer Division» предлагают весь спектр учебных пособий для подготовки к экзаменам по программе сертификации специалистов Microsoft. Учебные курсы для самостоятельного изучения, адресованные специалистам компьютерной отрасли, содержат теоретические и практические материалы, мультимедийные презентации, упражнения и необходимое ПО. Все эти пособия позволяют наилучшим образом подготовиться к сдаче сертификационных экзаменов.

Интерактивная подготовка

Интерактивная подготовка средствами Интернета — альтернатива занятиям в учебных центрах. Вы можете выбрать наиболее удобный распорядок занятий в виртуальном классе, где научитесь работать с продуктами и технологиями компании Microsoft и подготовитесь к сдаче экзаменов. Интерактивное обучение охватывает множество курсов Microsoft — от обычных официальных до специальных, доступных лишь в интерактивном режиме. Интерактивные ресурсы доступны круглосуточно в сертифицированных центрах подготовки.

Сертифицированные центры технического обучения Microsoft

Сертифицированные центры технического обучения Microsoft (Certified Technical Education Center, CTEC) — самый простой способ пройти курс обучения под руководством опытного инструктора и стать сертифицированным специалистом, Microsoft CTEC — всемирная сеть учебных центров, которые позволяют специалистам повысить свой технический потенциал под руководством сертифицированных инструкторов Microsoft.

Список центров CTEC в США и Канаде можно получить, обратившись на Web-узел компании Microsoft по адресу *http://www.microsoft.com/CTEC/default.htm* (на русском языке: *http://www.microsoft.com/rus/CTEC/default.htm*).

Техническая поддержка

Мы постарались сделать все от нас зависящее, чтобы и сам учебный курс, и прилагаемый к нему компакт-диск не содержали ошибок. Если все же у вас возникнут вопросы или вы захотите поделиться своими предложениями или комментариями, обращайтесь в издательство Microsoft Press по одному из этих адресов.

Электронная почта TKINPUT@MICROSOFT.COM

Почтовый адрес: Microsoft Press
Attn:MCSE Training Kit-Microsoft Windows 2000 Professional Editor
One Microsoft Way
Redmond,WA98052-6399

Издательство «Microsoft Press» публикует постоянно обновляемый список исправлений и дополнений к своим книгам по адресу *http://mspress.mkrosoft.com/support/.*

Учтите, что по указанным почтовым адресам техническая поддержка не предоставляется. Для получения подробной информации о технической поддержке программных продуктов Microsoft обращайтесь на Web-узел компании Microsoft по адресу *http://www.microsofr.com/support/* или звоните в службу Microsoft Support Network Sales по телефону (800) 936-3500 — в США.

Подробнее о получении полных версий программных продуктов Microsoft вы можете узнать, позвонив в службу Microsoft Sales по телефону (800) 426-9400 или по адресу *www.microsoft.com.*

ГЛАВА 1

Проектирование сети Windows 2000

В этой главе

Мы расскажем о планировании сети Windows 2000, а также познакомим вас с важными особенностями разработки плана внедрения сети. Кроме того, вы узнаете о различных сетевых протоколах, используемых Microsoft Windows 2000, и их взаимосвязи с сетевыми службами. .

Прежде всего

Для изучения материалов этой главы предварительных требований нет.

Занятие 1 Обзор сетевых служб

Microsoft Windows 2000 предоставляет множество полезных функций, служб и технологий, расширяющих возможности работы в сетях. Для использования сетевых служб необходимо правильно внедрить соответствующие технологии в вашей сети. Например, для работы службы каталогов Active Directory требуется установить протокол TCP/IP.

На этом занятии мы рассмотрим следующие сетевые службы Windows 2000:

- Domain Name System **(DNS);**
- Dynamic Host Configuration Protocol (DHCP);
- **Windows** Internet Name Service (WINS).

Вы узнаете о способах организации удаленного доступа в сеть с использованием оснастки Routing and Remote Access (Маршрутизация и удаленный доступ) из состава служб удаленного доступа Windows 2000 (RRAS) и об использовании транслятора сетевых адресов (NAT). Также мы расскажем о принципах обеспечения безопасности посредством служб сертификации — Microsoft Certificate Services.

Изучив материал этого занятия, вы сможете:

- ✓ пояснить назначение служб DNS, DHCP и WINS;
- ✓ описать службу RRAS,
- ✓ описать преимущества транслятора сетевых адресов;
- ✓ рассказать о возможностях служб сертификации.

Продолжительность занятия – около 40 минут.

Протокол TCP/IP

Windows 2000 поддерживает множестве протоколов, однако основным является TCP/IP. Он по умолчанию устанавливается вместе с Windows 2000 как основной сетевой протокол. Большинство сетевых служб Windows 2000 используют именно TCP/IP, а для некоторых, например, Internet Information Server (IIS) и Active Directory, он просто необходим. TCP/IP — это маршрутизируемый протокол, применяемой во многих ГВС, включая Интернет. Другие протоколы, такие, как NetBEUI, разработаны исключительно для нужд ЛВС и поэтому не позволяют подключаться к Интернету. Важно учесть это при планировании сети.

Служба DNS

Хотя поиск и подключение к узлам (компьютерам или любым другим устройствам, использующим TCP/IP) осуществляются по протоколу IP, для удобства пользователей вместо трудно запоминаемых цифр применяются дружественные имена. Например, имя ftp.microsoft.com запомнить проще, чем IP-адрес — 172.16.23.55. *Система доменных имен* (Domain Name System, DNS) позволяет использовать иерархические дружественные имена, упрощающие поиск компьютеров и других ресурсов к IP-сети.

DNS используется в Интернете в качестве стандарта имен для поиска компьютеров, работающих по протоколу IP. До внедрения DNS для обнаружения ресурсов в сетях TCP/IP включая Интернет, использовались файлы HOSTS. Сетевые администраторы вручную вводили привязки имен к IP-адресам в файл HOSTS, который компьютеры затем использовали для разрешения имен.

Протокол DHCP

Протокол Dynamic Host Configuration Protocol (DHCP) упрощает администрирование и управление IP-адресами всети TCP/IP. автоматизируя процесс конфигурации адресов для сетевых клиентов. DHCP-сервером считается любой компьютер с запущенной службой DHCP. Windows 2000 Server включает службу DHCP Server, позволяющую компьютеру выполнять функции DHCP-сервера и конфигурировать клиентские компьютеры в сети (рис. 1-1).

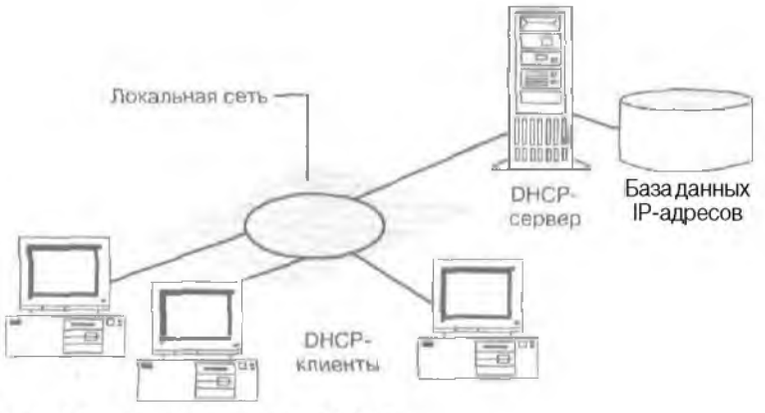


Рис. 1-1. Основная модель DHCP

Служба DHCP Server для Windows 2000 также поддерживает:

- интеграцию со службами Active Directory и DNS;
- оптимизированный **мониторинг и** статистическую отчетность;
- дополнительные возможности. включаемые поставщиком. и пользовательские классы:
- выделение адресов многоадресной рассылки;
- динамическое обнаружение DHCP-сервера.

В сети TCP/IP каждый компьютер должен иметь уникальный IP-адрес. Без использования DHCP настройку IP-адресов для всех новых, перемешенных из одной подсети в другую и удаленных компьютеров придется выполнять вручную. При внедрении DHCP эти процессы становятся централизованными и выполняются автоматически.

Реализация DHCP в Windows 2000 настолько тесно связана с WINS и DNS. что сетевым администраторам необходимо рассмотреть возможность объединения всех этих служб при планировании сети. Для взаимодействия серверов DHCP с клиентами сетей Microsoft требуется служба разрешения имен. Помимо обычного разрешения имен в сети Windows 2000 для поддержки Active Directory задействована служба DNS. Сети на основе Windows NT 4.0 и более ранних клиентов должны использовать серверы WINS. В смешанных сетях Windows 2000/NT 4.0 требуются обе службы — WINS и DNS.

Служба **WINS**

Windows Internet Name Service (WINS) — это система разрешения имен, используемая в Windows NT Server 4.0 и более ранних ОС. WINS предоставляет распределенную базу данных для регистрации имен компьютеров (по сути имен NetBIOS) и сопоставления этих имен с IP-адресами в маршрутизируемой сетевой среде. При управлении маршрутизируемой сетью WINS является лучшим способом разрешения имен NetBIOS. WINS уменьшает количество локальных широковещательных рассылок. применяемых для разрешения имен, и упрощает поиск систем в удаленных сетях. В динамической DHCP-среде IP-адреса узлов могут часто меняться. Служба WINS динамически регистрирует изменения привязок IP-адресов к именам компьютеров.

Разрешение имен

Независимо от того, какая из служб, WINS или DNS, используется в вашей сети, разрешение имен является важной частью сетевого администрирования. Хотя Windows 2000 для определения привязок IP-адресов к именам узлов главным образом применяет DNS, поддержка WINS для этой цели по-прежнему сохранена.

Разрешение имен позволяет подключаться к ресурсам и осуществлять поиск в сети, используя понятные имена, например «printer1» или «fileserver1», вместо IP-адресов. Кроме того, совершенно бессмысленно запоминать IP-адреса при использовании DHCP, так как в этом случае IP-адреса узлов меняются с течением времени. Интеграция DHCP и служб разрешении имен позволяет даже при динамическом изменении IP-адреса найти компьютер по имени. При подключении к компьютеру fileserver1 из другого узла сети вы все равно можете использовать имя «fileserver1» вместо обновленного IP-адреса, так как WINS отслеживает все изменения **IP-адресов,** связанные с этим именем.

Общие сведения об удаленном доступе

Служба Routing and Remote Access Service (RRAS) в Windows 2000 позволяет удаленным клиентам прозрачно подключаться к удаленному серверу; такое подключение называется «точка-точка». В результате удаленные клиенты, дозвонившись до сервера, получают доступ к ресурсам, как если бы они были физически подключены к его сети. В Windows 2000 удаленный доступ предоставляется двумя способами:

- **по телефонной линии** — клиент удаленного доступа использует инфраструктуру телефонной сети для создания временного физического или виртуального канала с портом сервера удаленного доступа. После создания временного физического или виртуального канала согласовываются остальные параметры подключения;
- **по виртуальной частной сети** (Virtual private network, VPN) — VPN-клиент использует транзитную IP-сеть для создания виртуального соединения «точка-точка» с VPN-сервером удаленного доступа. После установления виртуального подключения согласовываются остальные параметры подключения.

Удаленное подключение по телефонной линии

Служба RRAS принимает входящие телефонные подключения и перенаправляет пакеты между клиентами удаленного доступа и сетью, к которой подключен сервер удаленного доступа. Удаленное соединение состоит из клиента удаленного доступа, инфраструктуры ГВС и сервера удаленного доступа (рис. 1-2),

Рис. 1-2. Удаленное подключение по телефонной линии

Протоколы удаленного доступа

Управляют параметрами подключения и передачей данных по каналам ГВС. Протокол, по которому могут взаимодействовать пользователи, зависит от ОС и сетевых протоколов, установленных на сервере удаленного доступа и клиенте. Служба RRAS поддерживает три типа протоколов удаленного доступа:

- Point-to-Point Protocol (PPP) — стандартизованный набор протоколов, обеспечивающий надежную защиту, поддержку множества протоколов и межплатформенное взаимодействие;
- Serial Line Internet Protocol (SLIP) — используется устаревшими серверами удаленного доступа;
- Asynchronous NetBEUI (AsyBEUI) — протокол службы удаленного доступа Microsoft, известный также как асинхронный NetBEUI; применяется устаревшими клиентами удаленного доступа под управлением Windows NT, Windows 3.1, Windows for Workgroups, MS-DOS и LAN Manager.

Протоколы ЛВС применяются клиентами удаленного доступа для использования ресурсов сети, к которой подключен сервер удаленного доступа. Служба удаленного доступа Windows 2000 поддерживает протоколы TCP/IP, IPX, AppleTalk и NetBEUI.

► Настройка сервера удаленного доступа и маршрутизации

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Routing And Remote Access (Маршрутизация и удаленный доступ).

   Откроется одноименная оснастка.

2. Щелкните правой кнопкой сервер на левой панели и выберите в контекстном меню команду Configure And Enable Routing And Remote Access (Настроить и включить маршрутизацию и удаленный доступ) (рис. 1-3).

   Откроется окно мастера настройки маршрутизации, который поможет вам настроить сервер удаленного доступа.

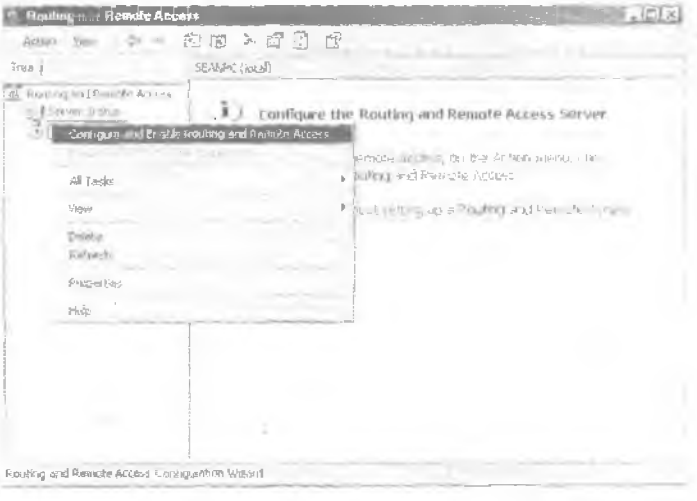


Рис. 1-3. Создание сервера маршрутизации и удаленного доступа

Преобразование сетевых адресов

Существуют два типа IP-адресов: открытые и частные. Открытые адреса назначаются вам поставщиком услуг Интернета (Internet service provider, ISP) для подключения к Интернету. Для внутренних узлов организации, не нуждающихся в прямом доступе к Интернету, требуются IP-адреса, не дублирующие уже выделенные открытые адреса. Чтобы решить эту проблему адресации, разработчики Интернета зарезервировали часть IP-адресов и назвали ее частным адресным пространством. Таким образом, IP-адрес из частного адресного пространства не может быть назначен в качестве открытого адреса; IP-адреса внутри частного адресного пространства назывются частными адресами. Использование частных IP-адресов помогает защитить сеть от взлома.

Поскольку InterNIC никогда не выделит IP-адрес в частном адресном пространстве для общего пользования, в маршрутизаторах Интернета невозможно существование маршрутов для частных адресов. Частные адреса из Интернета недоступны, поэтому при использовании частных IP-адресов вам понадобится какой-то прокси или сервер для преобразования IP-адресов из частного адресного пространства вашей локальной сети в открытые IP-адреса, допускающие маршрутизацию. Другой вариант — преобразовывать частные адреса в соответствующие открытые адреса при помощи Network Address Translator (NAT) перед их представлением в Интернете. Трансляция сетевого адреса для подключения частных сетей малых офисов к Интернету иллюстрируется на рис. 1-4.

Преобразование сетевых адресов (NAT) позволяет скрыть во внешних сетях IP-адреса внутренней сети путем преобразования внутренних IP-адресов во внешние открытые адреса. Это сокращает затраты на регистрацию IP-адресов, позволяя использовать во внутренней сети множество незарегистрированных IP-адресов, преобразуя их в несколько IP-адресов, имеющих внешнюю регистрацию. Таким образом скрывается структура внутренней сети, что снижает риск несанкционированного доступа извне.

Рис. 1-4. Подключение частной сети к Интернету

Службы сертификации

Проектирование системы безопасности для защиты конфиденциальной и частной информации вашей организации требует разработки набора решений, соответствующих определенным сценариям риска. В Windows 2000 реализовано несколько технологий, которые помогут вам разработать схему безопасности. Одна из них — службы сертификации, или Microsoft Certificate Services. Вы можете использовать службы сертификации для создания и управления *центрами сертификации* (Certificate Authority, CA), ответственными за выпуск цифровых сертификатов.

Цифровые сертификаты – это электронные реквизиты, применяемые для проверки подлинности пользователей, организаций и компьютеров. Сертификат:

- содержит личную информацию, помогающую идентифицировать владельца;
- содержит цифровую подпись законного владельца и сведения о выдавшем сертификат центре;
- не поддается взлому и подделке;
- может быть аннулирован центром сертификации в любое время, например, если сертификат неправильно используется или украден;
- может быть проверен на действительность в издавшем его центре.

Цифровые сертификаты применяют для обеспечения самых разных функций безопасности, например:

- защиты электронной почты;
- безопасною взаимодействия клиентов с Web-серверами;
- подписания исполняемого кода для его распространения в сетях общего пользования;
- проверки подлинности при регистрации в локальных и удаленных сетях;
- проверки подлинности с использованием протокола IPSec.

Службы сертификации предоставляют предприятиям простые средства установки центров сертификации. Службы сертификации включают модуль политики по умолчанию, ответственный за выпуск сертификатов для таких объектов предприятия, как пользователи, компьютеры и службы.

Резюме

В Windows 2000 реализованы технологии, расширяющие возможности сетей TCP/IP, Хотя для поиска узлов и подключения к ним протокол TCP/IP применяет IP-адреса, клиентам гораздо удобнее запоминать дружественные имена. За счет использования иерархических дружественных имен служба DNS упрощает поиск компьютеров и других ресурсов в сети IP. Протокол DHCP упрощает администрирование и управление IP-адресами в сети TCP/IP, автоматизируя процесс конфигурации адресов для клиентов сети. WINS предоставляет распределенную базу данных для регистрации имен компьютеров (по сути, имен NetBIOS) и сопоставления этих имен с IP-адресами в маршрутизируемой сетевой среде. Средствами службы RRAS клиенты могут прозрачно подключаться к серверу удаленного доступа и его сети.

Занятие 2. Разработка плана развертывания сети

Внедрение новых технологий в сетевую среду предприятия требует разработки, планирования, утверждения и финансирования. Для получения максимальной выгоды от Windows 2000 к процессу планирования структуры сети следует отнестись ответственно. До того как вы начнете планировать развертывание Windows 2000, вам надо хорошо изучить все ее возможности, чтобы далее их использовать по своему усмотрению. Это поможет увеличить продуктивность выполняемой персоналом вашей организации работы и снизить *совокупную стоимость владения* (total cost of ownership, TCO). На этом занятии вы научитесь разрабатывать план внедрения сети Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ описать семейство ОС Windows 2000;
- ✓ описать фазы жизненного цикла проекта по планированию структуры сети;
- ✓ выбрать аппаратные и программные средства для сети;
- ✓ выбрать сетевой протокол и интегрировать в сеть устаревшие системы.

Продолжительность занятия — около 40 минут.

Обзор операционных систем

Выбор ОС при планировании сети Windows 2000 обусловлен требованиями пользователей и вашего бизнеса. Например, если на серверах вашей сети будут выполняться приложения, требующие интенсивной работы процессора и памяти, то наилучшее решение — ОС Windows 2000 Advanced Server. Вам надо определить краткосрочные и стратегические цели организации и затем решить, какие технологии Windows 2000 наиболее важны,

Windows 2000 Professional

Это настольная ОС, расширяющая возможности Windows NT в области безопасности и отказоустойчивости, она унаследовала от Windows 98 легкость в управлении, поддержку множества устройств и PnP. Windows 2000 Professional можно установить путем обновления любой ОС, начиная с Windows NT Workstation 3.5l и до Windows 98. Минимальные системные требования Windows 2000 Professional:

- **Pentium-совместимый процессор** с тактовой **частотой не ниже 133 МГц** — Windows 2000 Professional поддерживает до двух процессоров;
- 64 **Мб** ОЗУ — большее количество памяти повышает быстродействие системы;
- **жесткий диск объемом не менее** 2 **Гб** — для установки самой ОС Windows 2000 Professional на вашем жестком диске должно быть свободно минимум 650 Мб.

Windows 2000 Server

Включает основанные на открытых стандартах службы каталогов, Web, приложений, коммуникаций, файлов и печати, отличается высокой надежностью и простотой управления, поддерживает новейшее сетевое оборудование для интеграции с Интернетом. В Windows 2000 Server реализованы:

- службы Internet Information Services 5.0 (IIS);
- среда программирования Active Server Pages (ASP);
- XML-интерпретатор;
- архитектура DNA;

- модель COM+;
- мультимедийные возможности;
- поддержка приложений, взаимодействующих со службой каталогов;
- **Web-папки;**
- печать через Интернет.

Минимальные аппаратные требования Windows 2000 Server:

- **Pentium-совместимый процессор с тактовой частотой не ниже 133 МГц** — Windows 2000 Server поддерживает до 4 процессоров;
- 128 Мб **ОЗУ** (рекомендуется 256 Мб). Большее количество памяти значительно увеличивает быстродействие системы. Windows 2000 Server поддерживает ОЗУ объемом до 4 Гб;
- **2 Гб свободного дискового пространства** — для установки Windows 2000 Server требуется около 1 Гб. Дополнительное место на диске необходимо для установки сетевых компонентов.

Windows 2000 Advanced Server

Эта ОС, по сути, представляет собой новую версию Windows NT Server 4.0 Enterprise Edition. Windows 2000 Advanced Server — идеальная система для работы с требовательными к ресурсам научными приложениями и приложениями электронной коммерции, где очень важны масштабируемость и высокая производительность. Аппаратные требования для Windows 2000 Advanced Server не отличаются от требований для Windows 2000 Server, однако эта более мощная ОС включает дополнительные возможности:

- балансировку сетевой нагрузки;
- поддерживает ОЗУ объемом до 8 Гб на системах с Intel Page Address Extension (PAE);
- поддерживает до 8 процессоров.

Windows 2000 Datacenter Server

Это серверная ОС, еще больше расширяющая возможности Windows 2000 Advanced Server. Поддерживает до 32 процессоров и больший объем ОЗУ, чем любая другая ОС Windows 2000;

- до 32 Гб для компьютеров с процессорами Alpha;
- до 64 Гб для компьютеров с процессорами Intel.

Вопрос об установке Windows 2000 Data'center Server следует рассматривать только в том случае, если вам требуется поддерживать системы *оперативной обработки транзакций* (online transaction processing, OLTP), крупные хранилища данных или предоставлять услуги Интернета.

Фазы развертывания сети

Цель планирования сети Windows 2000 — убедиться, что сеть выполняет все требуемые функции. Фазы жизненного цикла планирования сети перечислены ниже.

1. **Анализ.** Выясните цели и задачи проекта. Это поможет вам разработать сеть требуемой пропускной способности, удовлетворяющую требованиям безопасности и выделенного бюджета.
2. Разработка. Оцените инфраструктуру Windows 2000, включающую DNS, WINS, DHCP и сетевые протоколы. Структура сети должна учитывать взаимодействие систем между собой и с другими сетями.
3. **Тестирование.** Внедрите в производственную среду пилотную версию с небольшим числом пользователей для проверки работоспособности сети. Основываясь на результатах тестового выпуска, откорректируйте вашу сеть для достижения необходимой функциональности и стабильности сетевого окружения.

4. **Развертывание.** Это финальная фаза разработки сети Windows 2000. После того как ваша сеть протестирована с помощью пилотной версии, можно приступать к ее внедрению на всем предприятии. Создайте план восстановления системы после сбоя и предоставьте необходимые учебные материалы пользователям и персоналу группы поддержки.

Выбор аппаратных средств

Проблемы совместимости с устройствами и программами могут поставить под угрозу надежность и качество системы. Если это требуется, проверьте аппаратную и программную совместимость с Windows 2000 на странице *http://www.microsoft.com/windows2000/default.asp*.

Перед внедрением сети Windows 2000 обязательно выполните инвентаризацию конфигурации компьютеров и параметров BIOS. Также не забудьте задокументировать конфигурацию всех периферийных устройств, версии драйверов, пакетов исправлений и другую информацию о ПО и программно-аппаратных средствах. Кроме того, создайте и установите стандартные конфигурации для серверов и клиентов вашей системы, включая директивы о минимальном и рекомендуемом быстродействии процессора, объеме ОЗУ, жестких дисков и требования дополнительных устройств, таких, как приводы CD-ROM и источники бесперебойного питания (ИБП).

Убедитесь также, что такие компоненты сети, как концентраторы и кабели, удовлетворяют вашим потребностям в скорости передачи. Если вам необходимо пересылать по сети видео и звуковую информацию, то позаботьтесь, чтобы кабели и коммутаторы имели высокую пропускную способность. Некоторые удаленные пользователи не создают большой нагрузки на сеть. Например, удаленные пользователи, работающие с файлами Microsoft Word или Microsoft Excel, не создают такую большую нагрузку для RRAS-сервера, как пользователи, оперирующие базами данных или бухгалтерскими системами. Поэтому в большинстве ситуаций подойдут 10-мегабитные кабели категории 3 в сочетании с концентраторами того же класса; 100-мегабитные устройства категории 5 потребуются только для приложений, значительно загружающих сеть. Зафиксируйте фактическую пропускную способность вашей сети при низкой, средней и высокой нагрузках.

Взаимодействие с устаревшими системами

Многие сети разнородны, то есть в них применяются разные ОС и сетевые протоколы. Если, например, ваши компьютеры, оснащенные Windows 2000, должны взаимодействовать с мэйнфреймами, системами UNIX или другими сетевыми ОС, во время планирования тщательно продумайте особо важные для организации вопросы взаимодействия.

К тому же Windows 2000 Server предоставляет для взаимодействия с другими ОС шлюзовые службы, позволяющие получать доступ к ресурсам других сетей. Например, служба Gateway Service for NetWare (GSNW) позволяет клиентам сети Windows 2000 взаимодействовать со службой каталогов Novell Directory Services (NDS), использовать сценарии регистрации в ОС Novell версии 4.2 или старше, а также аутентифицировать пользователей на серверах Novell.

Выбор сетевых протоколов

В некоторых сетях применяется несколько протоколов. Например, в небольшой сети Ethernet может использоваться протокол NetBEUI и качестве основного протокола ЛВС и протокол TCP/IP для взаимодействия с Интернетом. Кроме того, в сетях, включающих серверы Novell NetWare и Windows NT, обязательно работают протоколы IPX/SPX и TCP/IP. Вы должны знать используемые в вашей сети сетевые протоколы и уметь по возможности заменять или удалять некоторые из них более эффективными протоколами из состава

Windows 2000. Например, при обновлении клиентских ОС до Windows 2000 Professional иногда следует удалить протокол IPX/SPX из вашей сети.

Windows 2000 содержит более функциональный набор протоколов TCP/IP, чем предыдущие версии Windows. Для использования Active Directory и расширенных возможностей Windows 2000 стоит применять протоколы семейства TCP/IP. Постарайтесь упростить вашу сеть и использовать только протокол TCP/IP.

В Windows 2000 для просмотра параметров вашей сети и информации о протоколах щелкните правой кнопкой мыши значок My Network Places (Мое сетевое окружение) на рабочем столе и выберите в контекстном меню команду Properties (Свойства).

Резюме

Для получения максимальной выгоды от внедрения Windows 2000 при планировании сети необходимо правильно выбрать серверную ОС Windows 2000. Процесс развертывания сети предприятия включает следующие фазы: анализ, разработку, тестирование и развертывание. Перед внедрением Windows 2000 задокументируйте набор программных и аппаратных средств для всех использующихся в вашей сети клиентов и серверов. Также рассмотрите вопросы взаимодействия с другими сетями и определите наиболее подходящие протоколы.

Занятие 3. Протоколы, поддерживаемые Windows 2000

При планировании сети подробно рассмотрите условия взаимодействия пользователей. Сетевые протоколы напоминают языки, различные по лексике, орфографии и пунктуации. Сетевой протокол в процессе общения компьютеров играет роль языка для общения людей. Используемый в сети протокол определяет, как настраиваются и посылаются по сетевому кабелю пакеты (блоки данных). Поэтому не поленитесь ответить на следующие вопросы.

- Подключаются ли пользователи сети к серверам Novell NetWare? Клиенты, подключенные к серверам NetWare, должны применять протокол NWLink. Клиенты под управлением Windows должны использовать протокол NWLink, даже если сервер NetWare сконфигурирован для работы с протоколом TCP/IP.
- Используются ли в вашей сети маршрутизаторы? Протокол NetBEUI не маршрутизируемый. Для компьютеров, объединенных в сети маршрутизаторами, необходимо применять маршрутизируемые сетевые протоколы, такие, как TCP/IP или NWLink.
- Подключены ли вы к Интернету? Для клиентов, подключенных к Интернегу, следует использовать протокол TCP/IP.

Для работы некоторых дополнительных аппаратных или программных средств иногда требуются соответствующие протоколы. Если вы хотите внедрить Active Directory или IIS либо предоставить клиентам доступ в Интернет, установите протокол TCP/IP. На этом занятии описано семейство протоколов TCP/IP, а также некоторые другие протоколы, которые вы можете применить в Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ описать разные сетевые архитектуры;
- ✓ описать сетевые протоколы, применяемые в Windows 2000.

Продолжительность занятия — около 30 минут.

TCP/IP

Это стандартизованный набор протоколов, разработанный для применения в крупных сетях. TCP/IP — маршрутизируемый протокол, то есть пакеты данных могут коммутироваться (перенаправляться в другую подсеть) на основе адреса назначения пакета. Маршрутизация TCP/IP обеспечивает отказоустойчивость, то есть способность компьютера или ОС реагировать на аварийные ситуации, вызванные, например, отключением энергии или отказом аппаратуры, гарантируя при этом сохранность данных. При сбое в сети пакеты TCP/IP передаются по другому маршруту.

Хотя TCP/IP разрабатывался для объединения разнородных сетей, сейчас он широко используется для высокоскоростной связи между сетями. Семейство протоколов TCP/IP применяется в Windows 2000 в качестве стандартного сетевого транспорта. Подробнее об архитектуре, установке и конфигурации TCP/IP рассказано в главе 2.

Преимущества реализации TCP/IP в Windows 2000

В Windows 2000 производительность TCP/IP оптимизирована для сетей с высокой пропускной способностью.

Поддержка **больших окон**

Под размером окна в коммуникациях на базе TCP понимают максимальное количество пакетов, которое можно послать, перед тем как придет подтверждение о приеме первого из них. Размер окна обычно фиксирован и устанавливается вначале сеанса связи передающего и принимающего узлов. При использовании поддержки больших окон размер окна пересчитывается динамически и может увеличиться, если в течение долгого сеанса происходит обмен большим количеством пакетов. Это увеличивает пропускную способность и позволяет одновременно передавать по сети больше пакетов данных.

Выборочные подтверждения

При выборочном подтверждении получатель вправе оповещать о потере или повреждении конкретных пакетов или запрашивать повторную передачу только необходимых пакетов. Это позволяет сети быстро восстанавливаться после временной перегрузки или взаимных помех, так как повторно пересылаются только поврежденные пакеты. В предыдущих версиях TCP/IP при возникновении сбоев отправителю приходилось повторно передавать все пакеты, посланные после поврежденного. Выборочные подтверждения уменьшают количество повторно передаваемых пакетов, что позволяет повысить производительность и эффективность использования сети.

Оценка времени обмена данными

Под *временем обмена данными* (Round Trip Time, RTT) понимается время на двустороннюю передачу сообщения между отправителем и получателем при TCP-подключении. Оценка RTT — это метод расчета времени прохождения пакета и настройки оптимального времени повторной передачи пакетов. Производительность сети зависит в том числе и от времени ожидания утерянных пакетов. Точная оценка RTT поможет правильно задать на каждом узле значения времени простоя, чтобы узел не запрашивал повторную передачу пакета, пока не истечет указанный интервал времени. Чем лучше синхронизация, тем выше производительность протяженных двусторонних сетей, таких, как ГВС, например, связывающая континенты или использующая каналы радио- или спутниковой связи.

Поддержка **IPSec**

IPSec — идеальная платформа для защиты сетевых коммуникаций. IPSec обеспечивает безопасную передачу информации между компьютерами, шлюзами безопасности или между шлюзом безопасности и узлом. В Windows 2000 Server управление системной политикой тесно интегрировано с IPSec для обеспечения шифрования при обмене данными. Клиенты могут использовать связь с шифрованием, регулируемую групповой политикой, — стражем, защищающим передаваемую по сети информацию. Так как IPSec интегрировал в ОС, он проще в настройке и управлении, чем обладающие аналогичной функциональностью надстройки ОС.

Службы обмена информацией конфигурируются с использованием политики IPSec, которая может быть настроена на компьютере локально или назначена с использованием Active Directory средствами групповой политики (рис. 1-5). При применении Active Directory узлы на этапе запуска определяют наличие политики, извлекают ее параметры и периодически проверяют ее обновления. Политика IPSec регулирует доверительные отношения между компьютерами. Проще всего реализовать доверительные отношения доменов Windows 2000 на основе протокола Kerberos 5. Готовые политики IPSec предписывают доверять компьютерам в том же домене или в других доверенных доменах Windows 2000.

Каждый принимаемый и отправляемый на уровне IP (сетевом) пакет называется дейтаграммой. Каждая IP-дейтаграмма содержит IP-адрес отправителя и IP-адрес получателя. Любая IP-дейтаграмма, обрабатываемая на уровне IP, сравнивается с набором фильтров групповой политики, настраиваемой администратором для компьютера, пользовате-

ля, группы или целого домена. Уровень IP может воздействовать на дейтаграмму следующим образом:

- предоставить дейтаграмме службы IPSec;
- передать дейтаграмму далее без изменений;
- отбросить дейтаграмму.

Рис. 1-5. Реализация групповой **политики с использованием Active Directory**

Поскольку IPSec обычно шифрует весь IP-пакет, то при перехвате IPSec-дейтаграммы, переданной после *сопоставления безопасности* (security association, SA), в дейтаграмме практически не останется незашифрованной исходной информации. В перехваченных данных могут быть проанализированы или прочитаны, например, с помощью Network Monitor только отдельные части пакета — Ethernet- и IP-заголовки. Таким образом, обеспечивается высокий уровень безопасности IP-транзакций. Протоколу IPSec посвящена глава 5.

Качество обслуживания

Один из способов гарантировать обслуживание сетевых запросов мультимедийных приложений в сети TCP/IP — каждому подключению выделить требуемую часть пропускной способности сети.

Качество обслуживания (Quality of Service, QoS) позволяет сетевым администраторам эффективно использовать существующие ресурсы и гарантировать важным приложениям высококачественное обслуживание без необходимости расширения или модернизации сетей. Применение QoS упрощает управление сетями и снижает затраты. Набор компонентов QoS в составе Windows 2000 взаимодействует с разными QoS-механизмами в таких сетевых устройствах, как маршрутизаторы и концентраторы. Таким образом, администратор получает представление о том, какие приложения используются в данный момент и какие ресурсы им требуются, не рассчитывая привязки между реальными пользователями, сетевыми портами и адресами. Если известен характер взаимодействия узла с сетью, ресурсами можно управлять более эффективно.

В состав Windows 2000 включены следующие компоненты QoS:

- **API-интерфейс GQoS** — подмножество API-интерфейса WinSock 2, позволяющее приложениям вызывать службы GQoS напрямую из ОС, не требуя знания лежащих в основе механизмов;

- **поставщик** услуг QoS — отвечает на запросы API-интерфейса GQoS. Предоставляет сигнальный протокол резервирования ресурсов Resource Reservation Protocol (RSVP) и поддержку политики QoS в Kerberos. Также вызывает механизмы контроля трафика;
- **служба Admission Control Service (ACS) и протокол Subnet Bandwidth Manager (SBM) — управляет общими сетевыми ресурсами посредством стандартного сигнального протокола;**
- инфраструктура управления трафиком — включает планировщик пакетов и маркер для управления трафиком драйверов и сетевых плат, не обладающих собственными планировщиками пакетов. Для управления трафиком в Windows 2000 предусмотрены такие дополнительные механизмы, как служба Integrated Services over Slow Links (ISSLOW) и Asynchronous Transfer Mode (ATM).

Microsoft тесно сотрудничает с Cisco, что позволяет создавать эффективные службы QoS, а также с Cisco. Extreme Networks, Intel, Sun, 3Com и другими, работающими *к* области стандартизации RSVP.

NWLink

Это Microsoft-совместимый IPX/SPX протокол для Windows 2000. Применение NWLink полезно, если в сети выполняются несколько клиентских или серверных программ Novell NetWare, использующих WinSock или протокол NetBIOS поверх IPX/SPX. WinSock — это API-интерфейс, позволяющий Windows-приложениям применять транспортные протоколы. Протокол NWLink может работать на компьютерах с Windows 2000 Server или Windows 2000 Professional.

Сам протокол NWLink не предоставляет компьютеру с Windows 2000 доступ к общим файлам или принтерам сервера NetWare. Также он не позволяет компьютеру с Windows 2000 выступать в роли сервера печати или файлового сервера для клиента NetWare. Для доступа к файлам или принтерам сервера NetWare надо задействовать *перенаправитель* (redirector), такой, как клиент для сетей NetWare в Windows 2000 Professional или служба шлюза NetWare в Windows 2000 Server. Протокол NWLink включен в состав обеих ОС Windows и устанавливается автоматически вместе с клиентом и службой шлюза для NetWare. Протокол NWLink подробно рассматривается в главе 3.

Служба шлюза для сетей NetWare

Служба Gateway Service for NetWare (GSNW), использующая протокол NWLink, предоставляет доступ к службам файлов, печати и каталогов NetWare. Она действует как шлюз, через который несколько клиентов могут обращаться к ресурсам NetWare. Средствами GSNW вы можете подключить компьютер с Windows 2000 Server *к* серверам NetWare, использующим регистрационную базу данных, или серверам Novell NDS. Кроме того, для обращения к ресурсам NetWare нескольких Windows-клиентов разрешается использовать GSNW как обычный шлюз: для этого не требуется установка специального клиентского ПО.

GSNW поддерживает прямой доступ *к* службам NetWare с компьютера под управлением Windows 2000 Server таким же образом, как клиент для NetWare поддерживает прямой доступ с клиентского компьютера. Дополнительно GSNW поддерживает сценарии регистрации NetWare.

Примечание GSNW включена в состав только Windows 2000 Server и Windows 2000 Advanced Server.

Клиент для сетей NetWare

Как и GSNW, служба Client Service for NetWare (CSNW) использует протокол NWLink и предоставляет доступ к службам файлов, печати и каталогов NetWare. Однако вместо тою

чтобы выступать в роли шлюза для клиентов, CSNW позволяет клиентам напрямую подключаться к ресурсам NetWare, использующим регистрационную базу данных, или серверов Novell NDS. Служба CSNW также поддерживает сценарии регистрации NetWare и включена только в состав Windows 2000 Professional.

Протокол NetBEUI

Протокол NetBIOS Enhanced User Interface (NetBEUI) разрабатывался как протокол для небольших ЛВС, содержащих 20-200 компьютеров. NetBEUI — не маршрутизируемый протокол, поскольку в нем не реализован сетевой уровень. NetBEUI включен в состав Windows 2000 Server и Windows 2000 Professional и используется в основном для поддержки рабочих станций, не обновленных до Windows 2000.

Протоколы AppleTalk

Это набор протоколов, разработанный Apple Computer, Inc. для связи компьютеров Apple Macintosh. Windows 2000 поддерживает все протоколы AppleTalk, что позволяет этой ОС выступать в роли маршрутизатора и сервера удаленного доступа сетей Macintosh. Для работы с протоколом AppleTalk предоставляется соответствующая служба доступа к файлам и принтерам.

Windows 2000 поддерживает весь стек протоколов AppleTalk и программные средства маршрутизации, то есть сервер Windows 2000 теперь может подключаться к сетям Macintosh и обеспечивать маршрутизацию для них.

Протокол Data Link Control

Этот протокол был разработан для объединения мэйнфреймов IBM. Он не проектировался как основной протокол персональных компьютеров в сети. Зачастую его используют для печати на сетевых принтерах Hewlett-Packard. Выбор DLC для применения в сетевых принтерах обусловлен тем, что его кадры удобно дизассемблировать и всю функциональность DLC можно легко запрограммировать в ПЗУ. Впрочем, возможности DLC ограничены, поскольку он не способен напрямую взаимодействовать с уровнем *интерфейса транспортного драйвера* (Transport Driver Interface, TDI). Устанавливайте DLC только для выполнения его основной задачи — отправки данных с сервера печати на сетевой принтер Hewlett-Packard. Клиентам, посылающим задания печати на сетевой принтер, он не нужен — DLC требуется только на сервере печати.

Стандарт IrDA

Ассоциация Infrared Data Association (IrDA) определила группу двусторонних высокоскоростных беспроводных протоколов для обмена информацией в инфракрасном диапазоне, обычно называемых IrDA. Протоколы IrDA обеспечивают взаимодействие компьютеров со множеством устройств: камерами, принтерами, *персональными цифровыми помощниками* (personal digital assistants, PDAs) и др.

Резюме

TCP/IP — это стандартизованный набор протоколов, разработанный для применения в крупных сетях. TCP/IP — маршрутизируемый протокол: пакеты данных могут коммутироваться (перенаправляться в другую подсеть) на основе адреса назначения пакета. Маршрутизация TCP/IP обеспечивает отказоустойчивость. Windows 2000 поддерживает протоколы NWLink, NetBEUI, AppleTalk, DLC, IrDA.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Предположим, вы вручную настраиваете TCP/IP для новых компьютеров и компьютеров, перемещенных из одной подсети в другую. Вы хотите упростить управление TCP/IP-адресами и назначать их автоматически. Какая сетевая служба Windows 2000 для этого применяется?

2. У вас имеется сервер с процессором Alpha, ОЗУ объемом 8 Гб и восемью процессорами, Вы хотите предоставить службу доступа к файлам 400 членам вашего предприятия. Какую ОС Windows 2000 лучше выбрать для этого и почему?

3. Вы хотите подключить сервер Windows 2000 к сети Macintosh, использующей протокол AppleTalk, и обеспечить ее маршрутизацию. Какой протокол следует установить?

ГЛАВА 2

Внедрение TCP/IP

В этой главе

Здесь вкратце обсуждается история стека протоколов TCP/IP и стандарты Интернета, а также рассматриваются утилиты TCP/IP. Вы научитесь присваивать IP-адреса различным TCP/IP-сетям с одинаковым идентификатором сети, изучите базовые концепции и процедуры реализации полсетей и надсетей. Изучив материал данной главы, вы сможете определить, когда следует создавать полсети, как и когда использовать маску подсети по умолчанию, как создать собственную маску подсети и диапазон действительных IP-адресов для каждой подсети.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server.

Занятие 1 Основы стека протоколов TCP/IP

Стек протоколов TCP/IP — промышленно стандартизованный пакет протоколов для ГВС. В Microsoft Windows 2000 имеется расширенная поддержка как самого стека протоколов TCP/IP, так и набора служб для управления и коммуникации в IP-сетях. На этом занятии мы познакомим нас с терминологией TCP/IP, расскажем об основных принципах работы и стандартах Интернета. Кроме того, вы узнаете об интеграции Windows 2000 и TCP/IP.

Изучив материал этого занятия, вы сможете:

- ✓ описать стек протоколов TCP/IP и ею преимущества в Windows 2000;
- ✓ описать привязку пакета протоколов TCP/IP к четырехуровневой модели;
- ✓ описать порядок передачи данных протоколами TCP и UDP.

Продолжительность занятия — около 45 минут.

Преимущества протокола TCP/IP

Все современные ОС поддерживают протокол TCP/IP; помимо этого, основная часть трафика в большинстве крупных сетей передается по протоколу TCP/IP. Пакет протоколов TCP/IP считается стандартом Интернета. Кроме того, существует множество стандартных коммуникационных утилит, обеспечивающих доступ и передачу данных между разнородными системами. Некоторые из них, например протокол FTP и Telnet, включены в Windows 2000 Server. TCP/IP-сети легко интегрируются с Интернетом. Протокол TCP/IP хорошо проработан и содержит много утилит, повышающих удобство применения, производительность и безопасность. Для взаимодействия TCP/IP-сетей и сетей, основанных на других транспортных протоколах, например ATM или AppleTalk, используются шлюзы. Добавив TCP/IP в систему Windows 2000, вы получите;

- технологию, позволяющую соединять разнородные системы. — TCP/IP поддерживает маршрутизацию и, используя шлюзы, способен работать с сетями на основе других транспортных протоколов;
- надежную, масштабируемую, платформо-независимую структуру — TCP/IP поддерживает интерфейс Winsock, идеально подходящий для разработки клиент-серверных приложений для Winsock-совместимых стеков;
- доступ к ресурсам Интернета — после подключения к Интернету можно создать виртуальную частную сеть или экстрасеть, обеспечив недорогой удаленный доступ.

Кроме того, клиенты Macintosh теперь могут применять протокол TCP/IP для доступа к общим ресурсам сервера Windows 2000, на котором выполняется служба File Services for Macintosh [AFP (AppleShare File Server) over IP]. Это значительно упрощает сетевое взаимодействие с компьютерами Macintosh.

Коммуникационные протоколы TCP/IP Windows 2000

Одна из важных особенностей Windows 2000 — возможность подключения к Интернету и разнородным системам. Кроме того, к Windows 2000 реализованы усовершенствованные возможности защиты, которые разрешается использовать при подключении к системе по сети. Для поддержки этих возможностей в версию TCP/IP для Windows 2000 добавлены следующие протоколы и технологии:

- технология IP **Security (IPSec)** — используется для шифрования сетевого трафика TCP/IP. IPSec обеспечивает безопасный обмен данными между удаленными клиентами и частными корпоративными серверами предприятий по виртуальной частной сети;
- **протокол Point-to-Point Tunneling Protocol (PPTP)** — как и IPSec, позволяет создавать защищенные виртуальные частные сети. Помимо стека протоколов TCP/IP, протокол PPTP также поддерживает многие другие сетевые протоколы, например: IP, Internetwork Packet Exchange (IPX) и NetBIOS Enhanced User Interface (NetBEUI);
- **протокол Layer Two Tunneling Protocol (L2TP)** — представляет собой комбинацию протоколов PPTP и Layer 2 Forwarding (L2F). L2F — это транспортный протокол, позволяющий серверам удаленного доступа разделять удаленный трафик на пакеты протокола Point to Point Protocol (PPP) и передавать по PBC-соединениям серверу L2F (маршрутизатору).

Кроме того, для сохранения инвестиций и уменьшения риска, связанных с управлением разнородными средами, Microsoft реализовала в Windows 2000 поддержку устаревших систем и протоколов, в том числе:

- AppleTalk;
- Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX);
- NetBEUI.

Эти проколы облегчают управление разнородными средами и упрощают переход к транспортной платформе TCP/IP на основе Windows 2000 — более гибкой и обладающей расширенными возможностями.

Новшества стека протоколов TCP/IP

В Windows 2000 реализованы некоторые новые возможности стека протоколов TCP/IP, в том числе:

- поддержка больших окон, что повышает производительности системы при передаче в течение длительного интервала времени большого числа пакетов;
- избирательные подтверждения, позволяющие системе быстро восстанавливаться после перегрузки — отправителю надо пересылать лишь пакеты, не полученные конечной системой;
- улучшенная функция оценки времени обмена данными;
- улучшенная функция назначения приоритета трафика для требовательных приложений.

Утилиты TCP/IP

Windows 2000 включает несколько утилит TCP/IP.

- **Утилиты передачи данных.** Windows 2000 поддерживает несколько разных протоколов передачи данных, основанных на IP, включая FTP, HTTP и Common Internet File System (CIFS).
- Telnet. Для управления UNIX-узлами традиционно используется утилита Telnet — текстовый интерфейс, аналогичный интерфейсу командной строки, с которым можно работать по IP-сети. В Windows 2000 имеются клиент и сервер Telnet.
- **Утилиты печати.** Windows 2000 способна отправлять задания печати напрямую на принтеры, поддерживающие протокол IP. Кроме того, две утилиты TCP/IP позволяют отправлять задания печати и получать сведения о состоянии TCP/IP-принтеров. Line Printer Remote (LPR) отправляет задания печати на компьютер, работающий под управлением службы Line Priming Daemon (LPD). Line Printer Queue (LPQ) позволяет получить сведения о состоянии очереди печати на узле под управлением службы LPD.
- **Диагностические утилиты.** В Windows 2000 имеется несколько утилит для устранения проблем с пакетом протоколов TCP/IP, в том числе PING, Ipconfig, Nslookup и Tracert.

Архитектура пакета протоколов TCP/IP

Протоколы TCP/IP обеспечивают сетевую поддержку для подключения всех узлов и обеспечивают соблюдение стандартов, касающихся соединения компьютеров и взаимодействия сетей. Стек протоколов TCP/IP имеет 4 уровня: сетевой, Интернета, транспортный и прикладной (рис. 2-1).

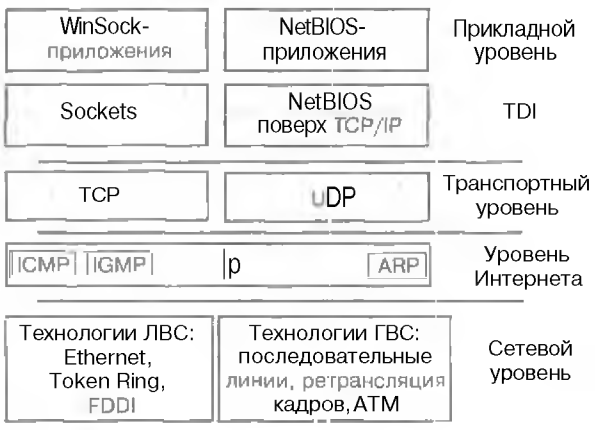


Рис. 2-1. Четыре уровня стека протоколов TCP/IP

Прикладной уровень

Верхним уровнем модели является прикладной, предоставляющий приложениям доступ к сети. Он соответствует сеансовому, прикладному и представительскому уровням модели OSI. В прикладном уровне работает множество стандартных утилит и служб TCP/IP:

- протокол **HTTP** — используется для большинства WWW-коммуникаций. Windows 2000 включает клиента (Internet Explorer) и сервер HTTP (Internet Information Server, IIS);
- **протокол FTP** — служба Интернета, обеспечивающая передачу файлов между компьютерами. Клиенты FTP в Windows 2000: Internet Explorer и утилита командной строки FTP. IIS включает сервер FTP;
- **протокол SMTP** — применяется почтовыми серверами для передачи электронной почты. IIS может посылать сообщения, используя SMTP;
- **протокол Telnet** — протокол эмуляции терминала, применяемый для подключения к удаленным узлам сети. Telnet позволяет клиентам удалено запускать приложения: кроме того, он упрощает удаленное администрирование. Реализации Telnet, доступные практически для всех ОС, облегчают интеграцию в разнородных сетевых средах. В Windows 2000 включены клиент и сервер Telnet;
- DNS — набор протоколов и служб TCP/IP-сети, позволяющий применять понятные имена, построенные с соблюдением иерархии, вместо IP-адресов узлов. На сегодняшний день DNS получила широкое распространение в Интернете и во многих корпоративных сетях. Работая с Интернетом при помощи Web-браузера, приложения Telnet, утилиты FTP или другой аналогичной утилиты TCP/IP, вы, скорее всего, обращаетесь именно к DNS-серверу. Windows 2000 также включает DNS-сервер;
- **протокол SNMP** — позволяет централизованно управлять узлами сети, например серверами, рабочими станциями, маршрутизаторами, мостами и концентраторами. Кроме того, SNMP можно использовать для конфигурирования удаленных устройств, мониторинга производительности сети, выявления ошибок сети и попыток несанкционированного доступа, а также для аудита использования сети.

API-интерфейсы сетевых **приложений**

Для взаимодействия со службами стека протоколов TCP/IP последний предоставляет сетевым приложениям два интерфейса: Winsock и NetBIOS поверх TCP/IP (NetBT).

- **WinSock.** Версия широко распространенного API-интерфейса Sockets, реализованная в Windows 2000. API-интерфейс Sockets представляет собой стандартный механизм доступа к службам дейтаграмм и сеансов по протоколу TCP/IP
- **NetBIOS.** Стандартный API-интерфейс, используемый в среде Windows для межпроцессной коммуникации. Хотя NetBIOS обеспечивает стандартный механизм коммуникации с протоколами, использующими службы именования и сообщений NetBIOS, например TCP/IP и NetBEUI, в Windows 2000 он применяется преимущественно для поддержки старых приложений.

Транспортный уровень

Транспортные протоколы позволяют организовать связь между компьютерами с обязательным установлением логического соединения (TCP) или без такового (UDP). Протокол TCP обеспечивает приложениям, разово пересылающим большие объемы информации или требующим подтверждения получения данных, надежную связь с обязательным установлением логического соединения. Протокол UDP обеспечивает связь без установления логического соединения и не гарантирует доставку пакетов. Приложения, использующие UDP, разово передают небольшой объем данных. За надежность доставки данных отвечает приложение. Транспортный уровень четырехуровневой модели соответствует транспортному уровню модели OSI.

Уровень Интернета

Протоколы уровня Интернета инкапсулируют пакеты в дейтаграммы Интернета и управляют необходимыми алгоритмами маршрутизации. Реализуемые уровнем Интернета функции маршрутизации необходимы для взаимодействия компьютеров с другими сетями. Уровень Интернета в четырехуровневой модели соответствует сетевому уровню модели OSI и включает пять протоколов:

- Address Resolution Protocol (ARP) — позволяет определить физические адреса узлов;
- Reverse Address Resolution Protocol (RARP) — обеспечивает обратное разрешение адреса на принимающем узле (в версии TCP/IP, реализованной Microsoft, протокол RARP отсутствует; впрочем, он есть в альтернативных системах и упомянут нами для полноты картины);
- Internet Control Message Protocol (ICMP) — позволяет компьютерам обмениваться сообщениями об ошибках связи;
- Internet Group Management Protocol (IGMP) — информирует маршрутизаторы о доступности членов группы многоадресной рассылки;
- IP — адресует и направляет пакеты.

Сетевой уровень

В основе модели лежит уровень сетевого интерфейса. Все локальные, общегородские и глобальные сети, а также сети удаленного доступа, например Ethernet, Token Ring, FDDI и ARCnet, предъявляют различные требования к кабелям, передаче сигналов и кодированию данных. Уровень сетевого интерфейса в четырехуровневой модели соответствует канальному и физическому уровням модели OSI и отвечает за прием и передачу кадров — пакетов информации, пересылаемых по сети в виде отдельных блоков. Сетевой уровень передает и получает кадры из сети.

ГВС-технологии TCP/IP

Стек протоколов TCP/IP поддерживает две основные группы ГВС-технологий.

1. Последовательные линии, в том числе аналоговые линии удаленного доступа, цифровые и выделенные линии.

   TCP/IP-трафик обычно передается по последовательным линиям с применением протоколов SLIP или PPP. Поддержка этих протоколов в Windows 2000 Server обеспечивается службой Routing And Remote Access Service (RRAS). По сравнению с протоколом SLIP протокол PPP обеспечивает более высокую степень безопасности и предоставляет более полные возможности по управлению конфигурацией и определению ошибок. Поэтому он рекомендуется для связи по последовательным линиям.
2. Сети, основанные на коммутации пакетов, включая X.25, ретрансляцию кадров и асинхронный режим передачи (ATM).

Примечание SLIP-сервер в Windows 2000 отсутствует. Служба **RRAS** не принимает **входящие** соединения клиентов SLIP.

Протокол TCP

Это надежная служба передачи данных с обязательным установлением логического соединения. Информация передается сегментами, и узлам требуется предварительно установить соединение. В TCP данные пересылаются в виде потока байт.

Надежность передачи обеспечивается присвоением каждому передаваемому сегменту порядкового номера. Если сегмент разбивается на более мелкие части, порядковые номера позволяют принимающему узлу узнать, все ли части сегмента получены. При получении данных принимающий узел в течение определенного периода времени должен вернуть подтверждение. Если отправитель не получает подтверждение, он повторяет передачу информации. Поврежденные сегменты получающим узлом отбрасываются. Так как при этом подтверждение не отсылается, отправитель передает сегмент еще раз.

Протокол IP

Протокол TCP разделяет данные на дискретные пакеты и гарантирует их доставку, однако фактически доставка информации осуществляется протоколом IP. На уровне IP входящие и исходящие пакеты называются дейтаграммами. При передаче пакета с сетевого уровня в его заголовок добавляются поля дейтаграмм IP. Они перечислены к таблице.

Поле	Функция
Исходный IP-адрес	Содержит IP-адрес отправителя дейтаграммы
Конечный IP-адрес	Содержит IP-адрес получателя дейтаграммы
Протокол	Указывает получающему узлу протокол, которому следует передать сообщение, — TCP или UDP
Контрольная сумма	Используется для проверки целостности полученного пакета
Время жизни (Time to Live, TTL)	Указывает период времени в секундах, по истечении которого пересылаемая дейтаграмма отбрасывается. Это предотвращает бесконечную циркуляцию пакетов по сети. Каждый маршрутизатор, через который проходит пакет, уменьшает время TTL на единицу. По умолчанию время TTL в Windows 2000 составляет 128 секунд

Протокол UDP

Протокол UDP — служба дейтаграмм, не требующая установления логического соединения и не гарантирующая доставку и строгую последовательность пакетов. В UDP контрольные суммы необязательны, что позволяет передавать данные по высоконадежным сетям без излишней нагрузки на процессоры компьютеров и ресурсы сети. Протокол UDP используется приложениями, не требующими подтверждения получения данных. Такие программы разово передают небольшой объем данных. С использованием протокола UDP пересылаются широковещательные пакеты.

В качестве примера служб и приложений, использующих протокол UDP, можно назвать DNS, RIP и SNMP.

Резюме

Стек протоколов TCP/IP — промышленно стандартизованный пакет протоколов для глобальных вычислительных сетей. Добавив TCP/IP в систему Windows 2000, вы получите определенные преимущества, в том числе большие совместимость, надежность, масштабируемость и безопасность. В Windows 2000 имеется ряд утилит, позволяющих подключаться к другим TCP/IP-узлам, а также устранять проблемы с TCP/IP.

Стек протоколов TCP/IP включает 4 уровня: сетевой, Интернета, транспортный и прикладной. Протокол IP работает на уровне Интернета и поддерживает многие ЛВС- и ГВС-технологии, в том числе Ethernet, Token Ring, ретрансляцию кадров и ATM. IP не требуется устанавливать соединение, он адресует и маршрутизирует пакеты между узлами. Так как доставка пакетов не гарантируется, протокол IP ненадежен.

Протокол TCP, работающий на транспортном уровне, обеспечивает протоколу IP надежную доставку данных с обязательным установлением логического соединения. После установки связи TCP передает приложениям данные, используя уникальные номера портов. Альтернативой TCP считается протокол UDP — не требующая логического соединения служба дейтаграмм, не гарантирующая доставку пакетов. Протокол UDP используется приложениями, которым не надо подтверждать получение данных.

Занятие 2. Адресация IP-протокола

Всем узлам и сетевым компонентам, взаимодействующим по протоколу TCP/IP, необходим уникальный IP-адрес. Сети TCP/IP обычно делятся на три основных класса с предопределенными размерами. Системные администраторы могут разбить крупную сеть на несколько небольших подсетей, разделив IP-адрес с помощью маски подсети на две части. Одна из частей будет идентифицировать (узел) компьютер, а другая часть — сеть, к которой он относится. Каждый узел TCP/IP идентифицируется логическим IP-адресом. IP-адрес — это адрес сетевого уровня, не зависящий от адреса канального уровня (например, от MAC-адреса платы сетевого интерфейса). На этом занятии вы узнаете об IP-адресации в сетях TCP/IP.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение **IP-адреса;**
- ✓ преобразовать IP-адрес из двоичного формата в десятичный;
- ✓ перечислить классы IP-адресов.

Продолжительность занятия — около 30 минут.

IP-адрес

Это 32-разрядное число, уникально идентифицирующее узел (компьютер или другое устройство, например принтер или маршрутизатор) в сети TCP/IP. Обычно IP-адреса выражаются в десятичном формате — четыре числа, разделенных точками, например 192.168.123.132.

Для обеспечения эффективной работы глобальной сети на основе TCP/IP, состоящей из набора подсетей, маршрутизаторам, передающим пакеты данных между сетями, не требуется знать точное местоположение узла, которому предназначен пакет информации. Маршрутизаторы знают лишь о принадлежности узла к определенной сети и используют информацию из своих таблиц маршрутизации для построения маршрута доставки пакета в сеть конечного узла. После доставки в конечную сеть пакет пересылается соответствующему узлу. Поэтому IP-адрес состоит из двух частей: идентификатора сети и идентификатора узла.

Идентификатор сети

Уникально определяет TCP/IP-узлы, расположенные в одной и той же сети. Для взаимодействия друг с другом все узлы одной сети должны иметь одинаковый идентификатор сети. Если маршрутизаторы соединяют сети так, как показано на рис. 2-2, уникальный идентификатор сети требуется каждому ГВС-соединению:

- сети 1 и 2 — маршрутизируемые;
- сеть 3 — ГВС-соединение между маршрутизаторами;
- сети 3 необходим идентификатор сети, чтобы интерфейсам между двумя маршрутизаторами удалось присвоить уникальные идентификаторы узлов.

Примечание Если вы собираетесь подключить сеть к Интернету, вам потребуется получить часть IP-адреса, содержащую идентификатор сети. Таким образом гарантируется уникальность идентификатора IP-сети. Для регистрации доменного имени и получения номера IP-сети обратитесь к своему поставщику услуг Интернета.

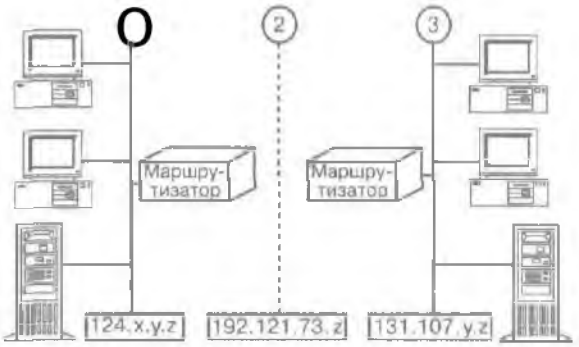


Рис. 2-2. **Маршрутизаторы,** соединяющие **сети**

Идентификатор узла

Определяет узел внутри сети. В сети, определяемой идентификатором сети, все идентификаторы узлов должны быть уникальными. IP-адрес указывает местоположение системы в сети аналогично тому, как уличный адрес определяет местоположение дома в городе (рис. 2-3).

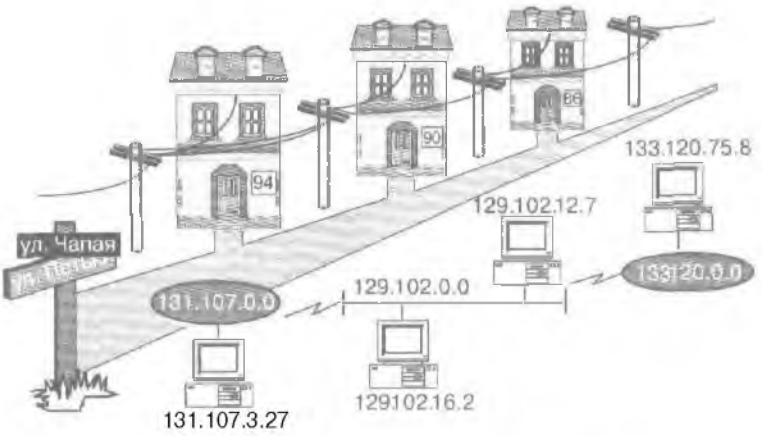


Рис. 2-3. **Узлы и сетевые компоненты,** взаимодействующие по протоколу **TCP/IP**

Десятично-точечная нотация

Существует дна формата ссылок на IP-адрес — двоичный и десятичный с разделением точками. Как показано на рис. 2-4. длина каждого IP-адреса равна 32 битам; сам адрес состоит из четырех 8-разрядных секций (октетов). Например, IP-адрес 192.168.I23.I32 в двоичном виде выглядит как 11000000.10101000.01111011.10000100. Числа в десятичной системе счисления, разделенные точками, — это октеты, преобразованные из двоичного в десятичное представление. Октеты представляют десятичные числа от 0 до 255. Порядок деления 32 бит IP-адреса на идентификаторы сети и узла показан на рис. 2-4.

y. z.

Пример: 3.24

Рис. 2-4. Порядок составления IP-адреса

Примечание Идентификатор сети не может быть ранен 127. Этот номер зарезервирован для возвратной петли и диагностических функций.

Преобразование IP-адреса из двоичного формата в десятичный

В части администрирования TCP/IP вы должны уметь преобразовывать битовые значения октета из двоичного представления в десятичное. В двоичном формате каждому биту октета соответствует десятичное значение. Равный нулю бит всегда имеет нулевое значение; равный единице можно преобразовать в десятичное значение. Бит низшего разряда представляет десятичное значение числа 1, а бит высшего разряда — десятичное значение числа 128. Наибольшее десятичное значение октета равно 255 — в этом случае все биты равны 1 (рис. 2-5).

Рис. 2-5. Все биты равны единице, что в результате дает 255

Ниже показано преобразование бит октета из двоичного кода в десятичный формат.

Двоичный код	Значения бит	Десятичное значение
00000000	0	0
00000001	1	1
00000011	1+2	3
00000111	1+2+4	7
00001111	1+2+4+8	15
00011111	1+2+4+8+16	31
00111111	1+2+4+8+16+32	63
01111111	1+2+4+8+16+32+64	127
11111111	1+2+4+8+16+32+64+128	255

Классы адресов

Адреса Интернета назначаются группой InterNIC *(http://www.infernic.net)* — организацией, управляющей Интернетом. Все IP-адреса делятся на классы, наиболее распространенными из которых являются классы A, B и C. Существуют также классы D и E, однако конечные пользователи обычно не работают с ними. Для каждого класса адресов применяются разные миски подсети по умолчанию. Класс IP-адреса можно определить по его первому октету. Ниже описаны диапазоны IP-адресов классов A, B и C.

- Адреса класса A присваиваются сетям с очень большим количеством узлов. Маска подсети сетей класса A по умолчанию — 255.0.0.0; первый октет адреса изменяется в диапазоне от 0 до 126. Например, адрес 10.52.36.11 относится к классу A, поскольку его первый октет (число 10) попадает в диапазон с 1 по 126 включительно.
- Адреса класса B присваиваются сетям среднего и большого размера. Маска подсети сетей класса B по умолчанию — 255.255.0.0; первый октет адреса изменяется в диапазоне от 128 до 191. Например, адрес 172.16.52.63 относится к классу B, поскольку его первый октет (число 172) попадает в диапазон со 128 по 191 включительно.
- Адреса класса C присваиваются небольшим ЛВС. Маска подсети сетей класса C по умолчанию — 255.255.255.0; первый октет адреса изменяется в диапазоне от 192 до 223. Например, адрес 192.168.123.132 относится к классу C, поскольку его первый октет (число 192) попадает в диапазон со 192 по 223 включительно.

Класс адреса определяет биты, используемые для идентификатора сети и идентификатора узла (рис. 2-6). Кроме того, класс адреса определяет возможное число сетей и количество узлов в сети.

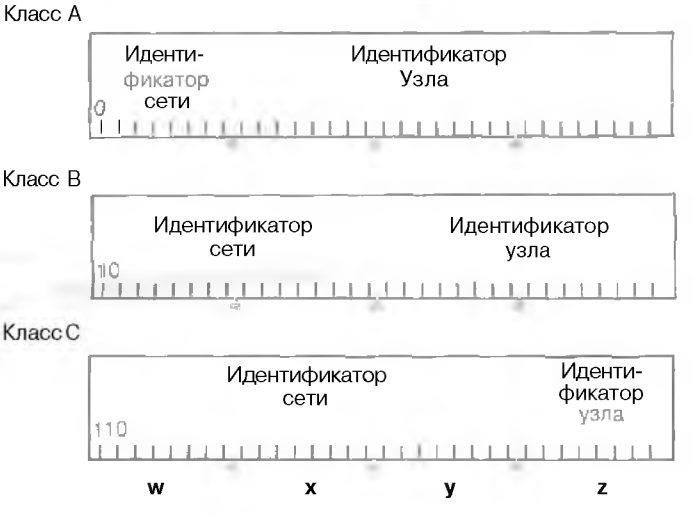


Рис. 2-6. Установка бит для каждого класса IP-адреса

Различия между классами A, B и C проиллюстрированы на рис. 2-7.

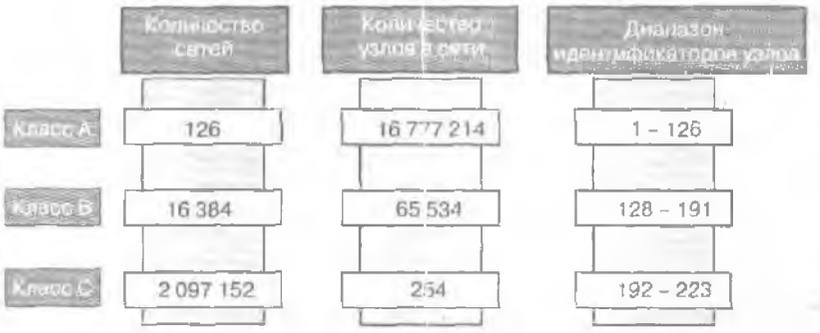


Рис. 2-7. Влияние класса адреса на сеть

Рекомендации по назначению **IP-адресов**

Правил присвоения IP-адресов не существует, однако всегда следует назначать действительные идентификаторы сетей и узлов. Задавая их, помните:

- идентификатор сети никогда не равен 127. Этот идентификатор зарезервирован для возвратной петли и диагностических функций;
- любой бит идентификаторов сети и узла не может быть равен 1. Иначе адрес рассматривается как широковещательная передача, а не идентификатор узла;
- все биты идентификаторов сети и узла не могут быть равны 1. Иначе адрес рассматривается как «только эта сеть»;
- в локальной сети идентификаторы узлов должны быть уникальными;
- каждому ГВС-соединению и каждой сети необходим уникальный идентификатор сети. Для подключения сети к Интернету необходимо получить идентификатор сети;
- каждому узлу TCP/IP, включая интерфейсы с маршрутизаторами, требуется уникальный идентификатор узла. Идентификатор узла, используемый маршрутизатором, — это IP-адрес, настроенный как шлюз рабочей станции по умолчанию;
- для каждого узла сети TCP/IP необходимо определить маску подсети — либо маску подсети по умолчанию (при отсутствии подсетей), либо пользовательскую маску подсети (применяется, если сеть разделена на подсети). Маска подсети — 32-разрядный адрес, используемый для блокировки или «маскировки» части IP-адреса с целью различения идентификаторов сети и узла. Это позволяет стеку TCP/IP определить, где находится IP-адрес — в локальной или удаленной сети. Маска подсети по умолчанию зависит от класса адреса (рис. 2-8).

Класс узлов	Биты, используемые для маски подсети				Десятичное точечное значение
A	11111111	00000000	00000000	00000000	255.0.0.0
B	11111111	11111111	00000000	00000000	255.255.0.0
C	11111111	11111111	11111111	00000000	255.255.255.0

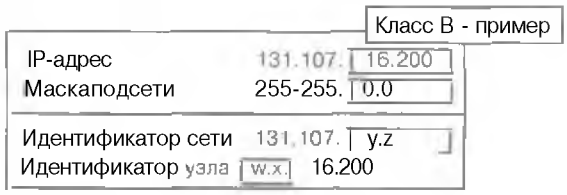


Рис. 2-8. **Пример маски подсети, используемой** для IP-адреса класса B

Резюме

IP-адреса идентифицируют все узлы TCP/IP и необходимы любому узлу или сетевому компоненту, использующему протокол TCP/IP. IP-адрес определяет идентификаторы сети и узла. Длина IP-адреса — 32 бита; он состоит из четырех восьмиразрядных полей (октетов). Существует пять классов IP-адресов. Узлам присваиваются адреса классов A, B и C. Каждый класс адресов включает сети разных размеров.

Существует несколько рекомендаций, которым нужно следовать при назначении действительных IP-адресов. Для взаимодействия узлов друг с другом сетевой идентификатор всех узлов одной сети должен быть одинаковым. Всем узлам TCP/IP, включая интерфейсы с маршрутизаторами, требуются уникальные идентификаторы узлов.

Занятие 1 Установка и настройка протокола TCP/IP

Сейчас мы расскажем об установке и настройке протокола Microsoft TCP/IP. Если на нашем компьютере не установлен пакет протоколов TCP/IP, выполните описанную ниже процедуру.

Изучив материал этого занятия, вы сможете:

- ✓ настроить параметры TCP/IP;
- ✓ назвать некоторые распространенные утилиты TCP/IP;
- ✓ рассказать о фильтровании пакетов.

Продолжительность занятия — около 15 минут.

Установка пакета протоколов TCP/IP

TCP/IP можно использовать в разных сетевых средах — от небольших ГВС-сетей до Интернета. Если Windows 2000 Setup обнаружит сетевой адаптер, протокол TCP/IP будет установлен по умолчанию. Таким образом, TCP/IP необходимо устанавливать, если по умолчанию применяется другой сетевой протокол или если вы удалили TCP/IP из параметров соединения в папке Network and Dial-Up Connections (Сеть и удаленный доступ к сети).

Практикум: установка протокола TCP/IP

Установите протокол TCP/IP для локального подключения. Для выполнения данного упражнения необходимы полномочия администратора.

▶ **Задание: установите протокол TCP/IP для подключения по локальной сети**

1. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Network And Dial-Up Connections (Сеть и удаленный доступ к сети).
   Откроется одноименное окно.
2. Щелкните значок Local Area Connection (Подключение по локальной сети) правой кнопкой и выберите в контекстном меню команду Properties (Свойства).
   Откроется диалоговое окно свойств локального подключения.
3. Щелкните кнопку Install (Установить).
   Откроется окно Select Network Component Type (Выбор типа сетевого компонента).
4. Щелкните Protocol (Протокол), затем кнопку Add (Добавить).
   Откроется окно Select Network Protocol (Выбор сетевого протокола).
5. Выберите Internet Protocol (TCP/IP) и щелкните OK (рис. 2-9).
   Пакет протоколов TCP/IP будет установлен и добавлен в список компонентов в окне свойств локального подключения
6. Щелкните кнопку Close (Закрыть).

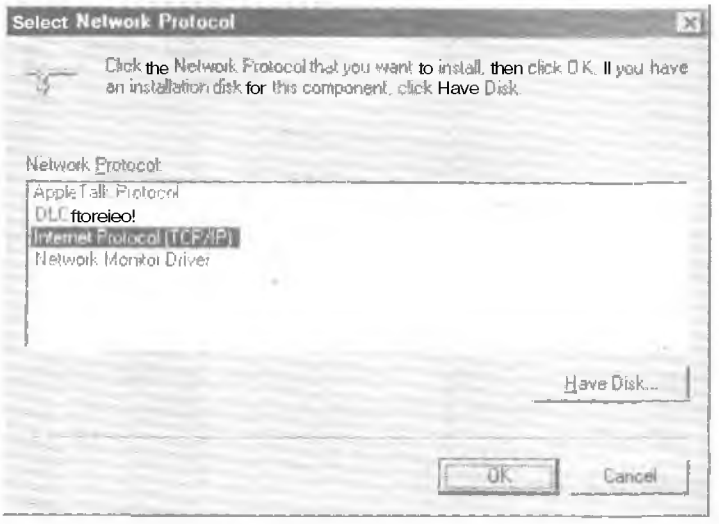


Рис. 2-9. Выбор протокола TCP/IP

Настройка протокола TCP/IP

Если вы впервые устанавливаете в сети протокол TCP/IP, вам стоит разработать подробный план IP-адресации в ней. Схема адресации сети, не подключенной к Интернету, содержит общедоступные либо частные адреса. Впрочем, для взаимодействия с Интернетом вы, скорее всего, создадите несколько общедоступных IP-адресов — они требуются устройствам, подключенным к Интернету напрямую. Группа InterNIC выделяет общедоступные адреса поставщикам услуг Интернета, которые, в свою очередь, выделяют адреса желающим установить соединение с Интернетом, Назначенные таким способом IP-адреса гарантированно уникальны и заносятся в маршрутизаторы Интернета, обеспечивающие трафик конечным узлам.

Кроме того, для защиты внутренних адресов вашей сети от проникновения из Интернета можно реализовать схему закрытой адресации, сконфигурировав для всех компьютеров закрытой сети (или интрасети) частные адреса. Системы с частными адресами недоступны из Интернета, поскольку частные адреса не пересекаются с общедоступными.

В Windows 2000 IP-адреса разрешается назначать динамически посредством протокола DHCP; кроме того, вы можете воспользоваться функцией *автоматической частной IP-адресации* (Automatic Private IP Addressing, API PA) или настроить параметры TCP/IP вручную. Выбор этих параметров обусловлен функциями компьютера. Например, внутренним серверам сети организации, взаимодействующим с клиентами, IP-адрес следует назначить вручную. Тем не менее настройку параметров TCP/IP для основной массы клиентов стоит выполнять динамически, с помощью DHCP-сервера.

Динамическое конфигурирование

По умолчанию компьютеры с Windows 2000 пытаются получить конфигурационные параметры TCP/IP от сервера DHCP в вашей сети (рис. 2-10). Если для вашего компьютера заданы статические параметры TCP/IP, можно реализовать динамическое конфигурирование TCP/IP.

▶ **Настройка компьютера для динамического конфигурирования параметров TCP/IP**

1. Раскройте меню Start\Settings и щелкните ярлык Network And Dial-Up Connections.
2. Щелкните значок Local Area Connection правой кнопкой и выберите в контекстном меню команду Properties.
3. На вкладке General (Общие) выберите в списке протоколов TCP/IP и щелкните кнопку Properties.

   Для соединений других типов перейдите на вкладку Networking (Сеть).
4. Щелкните переключатель Obtain An IP Address Automatically (Получить IP-адрес автоматически), затем — OK.

Ручная настройка

Некоторым серверам, например DHCP-, DNS- и WINS-серверам, IP-адрес необходимо назначать вручную. Если в вашей сети нет DHCP-сервера, вам придется вручную сконфигурировать компьютеры, использующие TCP/IP, для работы со статическим IP-адресом.

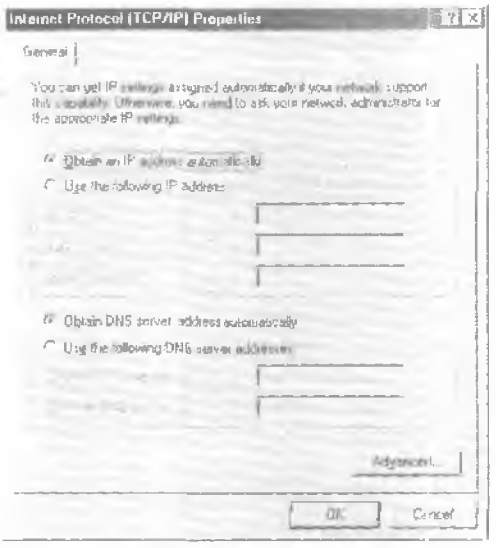


Рис. 2-Ю. Настройка автоматическою получения параметров TCP/IP

▶ **Настройка компьютера для использования статического IP-адреса**

1. Раскройте меню Start\Settings и выберите пункт Network And Dial-Up Connections.
2. Щелкните значок Local Area Con lection правой кнопкой и выберите в контекстном меню команду Properties.
3. На вкладке General укажите TCP/IP и щелкните кнопку Properties.
4. Щелкните переключатель Use The Following IP Address (Использовать следующий IP-адрес).

Затем укажите IP-адрес, маску подсети и адрес шлюза по умолчанию. При наличии в сети сервера **DNS** можно настроить систему для использования DNS.

▶ **Настройка компьютера для использования DNS**

1. Щелкните переключатель Select The Following DNS Server Addresses (Использовать следующие адреса DNS-серверов).

2. В полях Preferred DNS Server (Предпочтительный DNS-сервер) и Alternate DNS Server (Альтернативный DNS-сервер) укажите адреса основного и дополнительного серверов DNS (рис. 2-11).

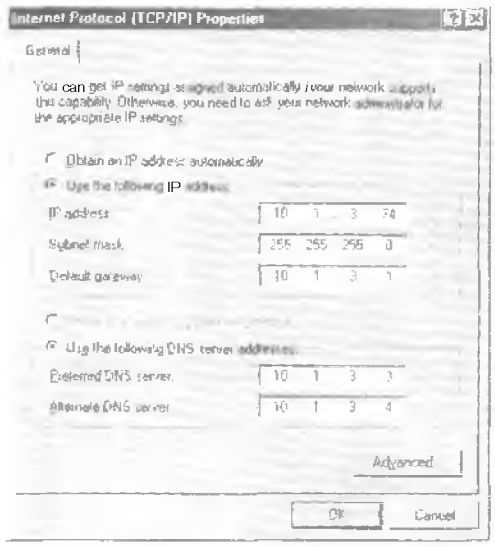


Рис. 2-11. Ручная настройка параметров TCP/IP

Кроме того, вы можете настроить дополнительные IP-адреса и шлюзы по умолчанию.

► **Настройка дополнительных IP-адресов и шлюзов по умолчанию**

1. В окне свойств протокола TCP/IP щелкните кнопку Advanced (Дополнительно).
2. На вкладке IP Settings (Параметры IP) в области IP Addresses (IP-адреса) щелкните кнопку Add (Добавить).
3. В полях IP Address (IP-адрес) и Subnet Mask (Маска подсети) введите IP-адрес и маску полсети и щелкните OK.
4. Повторите пункты 2 и 3 для каждого IP-адреса, который требуется добавить, и щелкните OK.
5. На вкладке IP Settings в области Default Gateways (Основные шлюзы) щелкните кнопку Add.
6. В полях Gateway (Шлюз) и Metric (Метрика) введите IP-адрес шлюза по умолчанию и метрику, затем щелкните кнопку Add.

   Кроме того, чтобы создать собственную метрику для данного соединения, можно ввести значение метрики в окне Interface Metric.
7. Повторите пункты 5 и 6 для каждого IP-адреса, который требуется добавить, затем шелкните OK.

Примечание Процесс конфигурирования клиента для использования сервера WINS описан в главе 9.

Автоматическое присвоение частных IP-адресов

Еще один вариант настройки TCP/IP — использование функции APIPA, если сервер DHCP недоступен. В предыдущих версиях Windows настройка IP-адресов осуществлялась вручную или динамически средствами DHCP. Если клиент не мог получить IP-адрес от сервера DHCP, сетевые службы для него были недоступны. В отсутствие сервера DHCP функция APIPA автоматически назначает клиентам неиспользуемые IP-адреса.

APIPA назначает клиенту адрес из диапазона 169.254.0.1 — 169.254.255.254 с маской подсети 255.255.0.0. Выделенный клиенту адрес применяется, пока не будет обнаружен сервер DHCP.

Проверка параметров TCP/IP с помощью утилит Ipconfig и ping

Вам необходимо регулярно проверять и тестировать конфигурацию протокола TCP/IP, чтобы гарантировать, что компьютер способен соединяться с другими TCP/IP-узлами и сетями. Для проверки параметров протокола TCP/IP можно воспользоваться утилитами Ipconfig и ping.

Утилита Ipconfig позволяет из командной строки просмотреть параметры конфигурации TCP/IP системы, включая IP-адрес, маску подсети и адрес шлюза по умолчанию. Это удобно, если вам требуется определить, инициализирована ли конфигурация, или выявить идентичные IP-адреса.

▶ Запуск Ipconfig из командной строки

1. Откройте окно командной строки.
2. Введите **Ipconfig** и нажмите Enter.

На экране отобразится конфигурационная информация TCP/IP (рис. 2-12).

Рис. 2-12. Просмотр конфигурационной информации TCP/IP с помощью утилиты Ipconfig

Утилита ping — диагностическое средство, тестирующее конфигурации TCP/IP и выявляющее ошибки соединений. Для определения доступности и работоспособности конкретного узла утилита ping использует сообщения эхо-запрос и эхо-ответ протокола ICMP. Как и утилита Ipconfig, ping работает из командной строки. Синтаксис команды таков:

ping *IP-адрес*

При успешном запросе к узлу на экран выводится информационное сообщение (рис. 2-13).

Рис. 2-13. **Отклики, выводимые** утилитой ping

Настройка фильтрования пакетов

Фильтрование пакетов IP позволяет реализовать функции защиты на основе данных об источнике, месте назначения и типе трафика IP. Благодаря этому вы можете задать триггеры IP- и IPX-трафика, которые будут защищать систему от нежелательного трафика или пропускать данные без фильтрования.

Например, с целью снижения объема трафика к определенным системам можно ограничить для сети типы входящего и исходящего доступа. Создаваемые вами фильтры пакетов не должны быть слишком строгими или нарушать функциональность сетевых протоколов компьютера. Например, на компьютере с Windows 2000 в качестве Web-сервера выполняется служба Internet Information Services (MS) и сконфигурированы фильтры, допускающие исключительно Web-трафик, поэтому вы не сможете выполнить к данной системе запрос с помощью утилиты ping.

Фильтрование пакетов IP может выполняться по:

- номеру порта TCP;
- номеру порта UDP;
- номеру протокола IP

Практикум: настройка фильтрования пакетов IP

Вы настроите на компьютере с Windows 2000 Server фильтрование пакетов TCP/IP для локального подключения.

▶ **Задание: включите фильтр** пакетов **TCP/IP**

1. Раскройте меню Start\Settings и щелкните ярлык Network And Dial-Up Connections.
2. Щелкните значок Local Area Connection правой кнопкой и выберите в контекстном меню команду Properties.
3. В окне свойств выберите протокол TCP/IP и щелкните кнопку Properties.

   Откроется окно свойств TCP/IP.
4. Щелкните кнопку Advanced (Дополнительно).

   Откроется окно Advanced TCP/IP Settings (Дополнительные параметры TCP/IP).

5. Перейдите на вкладку Options (Параметры), выделите в списке пункт TCP/IP Filtering (Фильтрация TCP/IP) и щелкните кнопку Properties.

   Откроется окно TCP/IP Filtering (рис. 2-14).

6. Пометьте флажок Enable TCP/IP Filtering (All Adapters).

   Теперь вы можете задать фильтрование пакетов протоколов TCP, UDP и IP. Для этого щелкните переключатель Permit Only (Только), затем — кнопку Add (Добавить) под списком TCP Ports (TCP-порты), UDP Ports (UDP-порты) или IP Protocols (IP-протоколы).

   Например, вы можете:

   - отключить все порты, кроме TCP-порта с номером 23, — будет разрешен лишь Telnet-трафик;
   - отключить на выбранном Web-сервере все порты, кроме TCP-порта с номером 80, — таким образом, вы позволите серверу обрабатывать лишь Web-трафик протокола TCP.

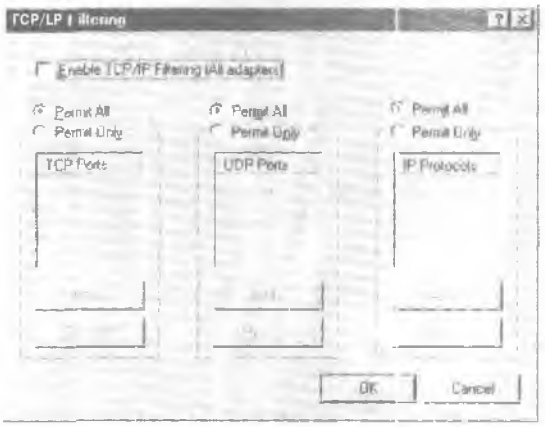


Рис. 2-14. Настройка фильтров пакетов TCP/IP в окне TCP/IP Filtering (Фильтрация TCP/IP)

Внимание! При отключении всех портов, кроме 80, будут заблокированы все сетевые подключения, осуществляемые по этим портам.

7. Щелкайте кнопку OK, чтобы закрыть все открытые окна.

Резюме

Если Windows 2000 Setup обнаружит сетевой адаптер, будет автоматически установлен протокол TCP/IP. Кроме того, пакет протоколов TCP/IP можно установить вручную. TCP/IP разрешается настроить для автоматического получения IP-адреса или задать его параметры вручную. Для снижения объема трафика к определенным системам стоит включить фильтрование пакетов.

Занятие 4. Основные принципы IP-маршрутизации

Маршрутизация представляет собой процесс выбора пути доставки пакетов и считается основной функцией протокола IP. Маршрутизатор (зачастую называемый шлюзом) — устройство, пересылающее пакеты из одной физической сети в другую. При получении маршрутизатором пакета сетевой адаптер передает дейтаграммы на уровень протокола Интернета. Протокол IP проверяет конечный адрес дейтаграммы, сравнивает его с таблицей IP-маршрутизации и принимает решение, куда следует переслать пакет. Здесь рассматриваются базовые концепции IP-маршрутизации.

Изучив материал этого занятия, вы сможете:

- ✓ дополнить таблицу маршрутизации Windows 2000 статическими маршрутами;
- ✓ управлять и нести мониторинг внутренней и граничной маршрутизации.

Продолжительность занятия — около 40 минут.

Основы маршрутизации

Маршрутизатор обеспечивает взаимодействие и связь ГВС и ЛВС, а также позволяет соединять разнородные ЛВС. Каждый пакет, пересылаемый по ЛВС, включает заголовок, содержащий поля с исходным и конечным адресами. Маршрутизаторы сопоставляют заголовки пакетов сегменту ЛВС и выбирают наилучший путь передачи пакета, оптимизируя производительность сети. Например, если пакет передается от компьютера А компьютеру С (рис. 2-15), наилучший маршрут включает лишь один транзит. Если по умолчанию компьютер А использует маршрутизатор 1, пакет будет перенаправлен через маршрутизатор 2. Компьютеру А будет сообщен оптимальный маршрут, по которому следует передавать пакеты компьютеру С. После того как найдены все маршруты, пакет передается следующему маршрутизатору (это называется *транзитом*), пока тот не прибудет на конечный узел. Если маршрут не найден, исходному узлу направляется сообщение об ошибке.

Рис. 2-15. Маршрутизация пакета между компьютерами А и С

Для выбора маршрута уровень протокола Интернета обращается к таблице маршрутов в памяти (рис. 2-16).

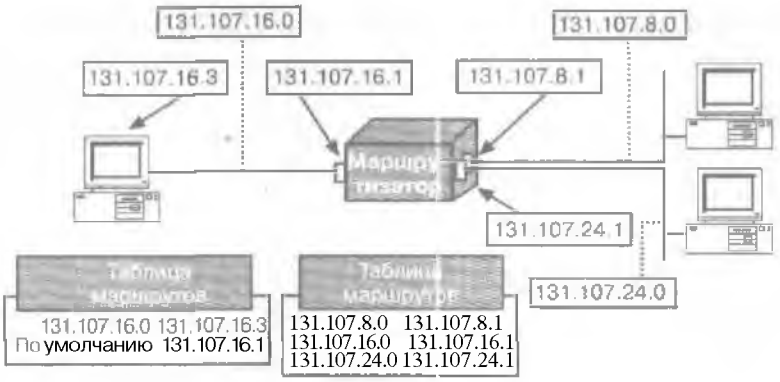


Рис. 2-16. Уровень IP обращается к таблице маршрутов

Данная таблица содержит записи с IP-адресами интерфейсов маршрутизатора к другим сетям, с которыми тот может взаимодействовать. Таблица маршрутов — это набор записей, называемых *маршрутами* (routes), содержащих информацию о местоположении сетевых идентификаторов промежуточных сетей. Таблица маршрутизации компьютера с Windows 2000 формируется автоматически на основе конфигурации протокола TCP/IP. Чтобы просмотреть таблицу маршрутов, введите в командной строке route print (рис. 2-17).

Рис. 2-17. Просмотр таблицы маршрутов в режиме командной строки

Примечание Таблица маршрутов имеется не только у маршрутизаторов. Узлы также обладают такими таблицами для выбора оптимального пути передачи пакетов.

Статическая и динамическая IP-маршрутизация

Методы получения маршрутизаторами сведений о маршрутах зависят от типа IP-маршрутизации, реализованной маршрутизатором: статической или динамической. Статическая маршрутизация — функция протокола IP, допускающая использование только статических таблиц маршрутов. Статические маршрутизаторы требуют, чтобы таблицы маршрутов формировались и обновлялись вручную. Для добавления статических записей в таблицу служит команда route.

Чтобы добавить или обновить статический маршрут, выполните команду	Описание
route add [*сеть*] **mask** [*маска_подсети*] [*шлюз*]	Добавляет маршрут
route **-p add** [*сеть*] **mask** [*маска_подсети*] ***[шлюз]***	Добавляет постоянный маршрут
route delete [*сеть*] [*шлюз*]	Удаляет маршрут
route change *[сеть]* [*шлюз*]	Изменяет маршрут
route print	Отображает таблицу маршрутов
route -f	Очищает все маршруты

Практикум: обновление таблицы маршрутов

Дополните таблицу маршрутов Windows 2000 статическими маршрутами.

▶ **Задание: обновите таблицу маршрутов**

1. Откройте **окно** командной **строки.**
2. Введите **route add** ***IP-адрес*** **mask** ***маска_подсети шлюз,*** чтобы добавить маршрут, который позволит компьютерам одной **сети** взаимодействовать с узлом другой сети.

   Например, чтобы добавить маршрут, который позволит компьютерам сети 10.107.24.0 **взаимодействовать** с узлом сети 10.107.16.0, в командной **строке** введите **route add** 10.107.24.0 **mask** 255.255.255.0 10.107.16.2 (рис. 2-18).

Рис. 2-18. Добавление статического маршрута

Использование динамической маршрутизации

Если маршрут изменяется, статические маршрутизаторы не сообщают друг другу об этом; кроме **того, они** не обмениваются маршрутами с динамическими маршрутизаторами. Динамическая же маршрутизация подразумевает автоматическое обновление таблицы маршрутов, упрощая администрирование. Тем не менее при использовании **динамической** маршрутизации в больших сетях увеличивается объем трафика.

Протоколы маршрутизации

Динамическая маршрутизация — функция протоколов маршрутизации, например Routing Information Protocol (RIP) и Open Shortest Path First (OSPF). Протоколы маршрутизации периодически обмениваются информацией о маршрутах к известным сетям между динамическими маршрутизаторами. Если маршрут изменяется, маршрутизаторы автоматически уведомляются об этом. На серверах Windows 2000 для каждой сети должен быть установлен свой сетевой адаптер. Кроме того, вам следует установить и настроить службу RRAS, поскольку по умолчанию одновременно с Windows 2000 протоколы динамической маршрутизации не устанавливаются. Реализация IP-маршрутизации описана в главе 11.

Windows 2000 включает два основных протокола IP-маршрутизации, выбор которых зависит от размера и топологии сети, а также от других факторов.

Протокол RIP

Это протокол дистанционно-векторной маршрутизации, обеспечивающий совместимость и предыдущими версиями RIP-сетей. Позволяет RIP-маршрутизаторам обмениваться информацией о маршрутах и сообщать друг другу о любых изменениях в конфигурации сети. RIP передает информацию соседним маршрутизаторам и периодически рассылает широковещательные пакеты, включающие всю информацию о маршрутах, которой обладает маршрутизатор. Это позволяет синхронизировать таблицы маршрутов всех маршрутизаторов сети.

Протокол OSPF

Это протокол маршрутизации, использующий информацию о состоянии каналов. Позволяет маршрутизаторам обмениваться информацией о маршрутизации и создавать карту сети, определяющую оптимальный путь к каждой из сетей. По мере обновления базы данных состояния каналов таблица маршрутов перестраивается. С увеличением размера БД о состоянии каналов растут требования к памяти и увеличивается время вычисления маршрута. Для решения этой проблемы масштабирования OSPF разделяет сеть на группы непрерывных сетей, называемых областями. Области соединяются друг с другом через область магистрали. Магистральный маршрутизатор в OSPF — это маршрутизатор, соединенный с областью магистрали. Магистральными считаются маршрутизаторы, соединенные с двумя и более областями. Тем не менее маршрутизаторы магистрали не должны работать маршрутизаторами границы области. Маршрутизаторы, у которых все сети соединены с магистралью, называют внутренними.

Каждый маршрутизатор отвечает за БД состояния каналов только для тех областей, которые присоединены к нему. Граничные маршрутизаторы области (ГМО) соединяют область магистрали с другими областями (рис. 2-19).

Рис. 2-19. Структура области OSPF

Среда маршрутизации OSPF лучше всего подходит для большой или очень большой динамической IP-сети с несколькими путями, например: сети крупной кампании, университетского городка, всемирной корпоративной или университетской сети. Для управления внутренними и граничными маршрутизаторами необходимо:

- убедиться, что для ГМО заданы параметры (место назначения, маска сети), определяющие границы соответствующей области;
- убедиться, что фильтрование источника и маршрута на ГМО не слишком строгое и не блокирует передачу соответствующих маршрутов автономной системе OSPF. Фильтрование внешнего источника и маршрута конфигурируется на вкладке External Routing окна свойств протокола OSPF;
- убедиться, что все маршрутизаторы ABR либо физически подсоединены к магистрали, либо подсоединены к ней логически через виртуальное соединение. В сети не должно быть маршрутизаторов «черного хода» — маршрутизаторов, которые соединяют две области, минуя магистраль.

▶ **Администрирование маршрутизатора**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Routing And Remote Access (Маршрутизация и удаленный доступ).
2. В дереве консоли щелкните правой кнопкой узел Server Status (Состояние сервера) и выберите в контекстном меню команду Add Server (Добавление сервера).
3. В окне Add Server выполните одну из следующих операций.
   - Щелкните переключатель The Following Computer (Указанный ниже компьютер) и введите имя компьютера или IP-адрес сервера.
   - Щелкните переключатель All Routing And Remote Access Servers In The Domain (Все компьютеры маршрутизации и удаленного доступа) и затем укажите домен, содержащий сервер, который требуется администрировать. Щелкните кнопку OK и выберите сервер.
   - Щелкните переключатель Browse The Active Directory (Обзор Active Directory). Затем шелкните кнопку Next и в окне Find Routers Or Remote Access Servers (Поиск: Маршрутизаторы и серверы удаленного доступа) пометьте флажки напротив серверов, которые требуется найти. Щелкните OK и выберите сервер.
4. Вы сможете администрировать удаленный сервер, когда он появится в дереве консоли.

Резюме

Маршрутизаторы передают пакеты между сетями. Уровень протокола Интернета обращается к таблице маршрутов в памяти. Таблица маршрутов содержит записи с IP-адресами интерфейсов маршрутизаторов к другим сетям. Статические маршрутизаторы требуют, чтобы таблицы маршрутов формировались и обновлялись вручную. При динамической маршрутизации маршрутизаторы автоматически получают уведомления об изменении маршрутов.

Закрепление материала

Прицеленные ниже вопросы помогут нам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Опишите пакет протоколов TCP/IP.
2. Назовите утилиты TCP/IP, используемые для проверки и тестирования конфигурации протокола TCP/IP.
3. Опишите назначение маски подсети.
4. Назовите минимальное число областей в промежуточной сети OSPF.
5. Что такое внутренний маршрутизатор?
6. Что такое граничный маршрутизатор?
7. Назовите административную утилиту Windows 2000, позволяющую управлять внутренними и граничными маршрутизаторами.

ГЛАВА 3

Внедрение NWLink

В этой главе

Эта глава посвящена вопросам взаимодействия Microsoft Windows 2000 с Novell NetWare. в том числе установке и настройке протокола NWLink.

Прежде всего

Для изучения материалов этой главы необходимо:

- выполнить установочные процедуры, описанные во вводной главе.

Занятие 1. Знакомство с NWLink

Для совместного использования ресурсов в сети Novell NetWare на компьютерах в сети Windows 2000 необходимо установить протокол, совместимый с базовым протоколом сетей NetWare — Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX). NWLink — это Microsoft-реализация IPX/SPX-совместимого протокола, позволяющая компьютерам с Windows 2000 подключаться к службам NetWare. На этом занятии вы познакомитесь с протоколом NWLink.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить назначение протокола NWLink;
- ✓ представить некоторые **из** компонентов, **используемых для** взаимодействия Windows 2000 с Novell NetWare;
- ✓ определять архитектуру NWLink.

Продолжительность занятия — около 25 минут.

Взаимодействие с NetWare

Windows 2000 предоставляет протоколы и службы, в том числе IPX/SPX/NetBIOS-совместимый транспортный протокол (NWLink), Windows 2000 Gateway Service for NetWare (GSNW) и Windows 2000 Client Service for NetWare (CSNW), позволяющие интегрировать сети Windows 2000 с сетями Novell NetWare. Эти протоколы и службы позволяют создавать сетевую среду, состоящую из серверов, использующих как Windows 2000, так и NetWare. Для перемещения учетных записей пользователей, групп, файлов и разрешений из NetWare в Windows 2000 в составе последней предусмотрено средство Directory Services Migration Tool for NetWare.

Ниже приведен список служб Windows 2000 Server, доступных компьютерам с Windows 2000, для взаимодействия с сетями и серверами Novell NetWare. Некоторые из них включены в Windows 2000 Server, в то время как другие являются самостоятельными продуктами.

- **IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink)** - фундамент NetWare-совместимых служб платформы Windows 2000. Протокол NWLink включен в Windows 2000 Server и Windows 2000 Professional.
- **GSNW**— служба шлюза для NetWare, которая входит по все серверные редакции Windows 2000. Она позволяет компьютеру с Windows 2000 Server связываться на прикладном уровне с компьютерами, использующими NetWare 3.2 или более поздней версии. Также включена поддержка сценария входа в систему. Кроме того, эту службу применяют для создания шлюзов к ресурсам NetWare, позволяющих компьютерам с клиентским ПО Microsoft получать доступ к ресурсам NetWare. GSNW более подробно рассматривается на занятии 2.
- **Directory Service Migration Tool** — позволяет перемещать учетные записи, группы, файлы и разрешения с сервера NetWare в службы каталогов Active Directory для Windows 2000. В Windows 2000 этот инструмент заменил NetWare Convert Tool. Он без сбоев осуществляет перемещение как системной базы данных NetWare, так и служб домена NetWare в автономную БД и позволяет администраторам корректировать учетную информацию до переноса в Active Directory (рис. 3-1).

Рис. 3-1. **Перенос учетных сведений из NetWare Domain Services в Windows 2000**

- File and Print Services for NetWare — служба доступа к файлам и принтерам сетей NetWare позволяет клиентам NetWare использовать IPX/SPX-совместимый транспортный протокол для передачи по сети заданий печати на серверы печати Windows 2000. Эта служба является отдельным продуктом и не требует внесения каких-либо изменений на клиентах NetWare.

Интегрирование NetWare 5.0 и Windows 2000 Server

Как и Windows 2000, NetWare 5.0 использует в качестве основного протокола TCP/IP, по умолчанию протокол IPX даже не устанавливается. Ни CSNW, ни GSNW не поддерживают доступ к ресурсам NetWare по протоколу IP. Следовательно, при применении NWLink для подключения к серверам NetWare 5.0 вы должны включить IPX на серверах NetWare 5.0.

NWLink и Windows 2000

Протокол NWLink предоставляет сетевые и транспортные протоколы для обеспечения связи с файловыми серверами NetWare; он требуется для подключения к серверам NetWare посредством GSNW или CSNW. Чтобы войти в сеть NetWare с компьютера Windows 2000 Professional, необходимо использовать CSNW или другой NetWare-клиент, например Novell Client for Windows 2000. Помимо этого, вы можете задействовать шлюзовой вариант межсетевого соединения, установив GSNW на сервер Windows 2000. CSNW и GSNW обсуждаются далее в этой главе.

Поскольку NWLink совместим со спецификацией NDIS, на компьютере с Windows 2000 разрешается одновременно использовать и другие наборы протоколов, например TCP/IP. NWLink может привязываться к нескольким сетевым адаптерам с различными типами кадров. При работе в небольших немаршрутизируемых сетях NWLink требует минимальной настройки, а в иных случаях и вообще ее не требует.

NetBIOS и Windows Sockets

NWLink поддерживает два API-интерфейса, NetBIOS и Windows Sockets (WinSock), позволяющие компьютерам с Windows 2000 взаимодействовать с клиентами и серверами NetWare, а также с любыми другими компьютерами, использующими NWLink. Поскольку NWLink поддерживает NetBIOS, он позволяет взаимодействовать со всеми NetBIOS-приложениями, включая Microsoft Systems Management Server, SNA Server, SQL Server и Exchange Server. WinSock-интерфейс NWLink позволяет клиентским компьютерам на базе Windows, где установлен только NWLink, работать с приложениями, использующими сокеты, например Microsoft Internet Explorer.

Архитектура NWLink

NWLink предоставляет полный набор протоколов транспортною и сетевого уровней для интеграции в среду NetWare. В табл. 3-1 описаны подпротоколы и компоненты NWLink.

Табл. 3-1. Подпротоколы NWLink

Протокол	Описание	Драйвер
IPX	Одноранговый сетевой протокол, обеспечивает передачу дейтаграмм без установления логического соединения и управляет выделением адресов и маршрутизацией пакетов данных внутри и между сетями	NWLNKIPX.SYS
SPX и SPXII	Предоставляет службы передачи с установлением логического соединения	NWLNKSPX.SYS
Router Information **Protocol (RIP)**	Предоставляет службы обнаружения маршрута и маршрутизаторов	**NWLNKIPX.SYS**
ServiceAdvising Protocol (SAP)	Собирает и распространяет имена и адреса служб	NWLNKIPX.SYS
NetBIOS	Обеспечивает совместимость с NetBIOS для **IPX/SPX**	**NWLNKNB.SYS**
Forwarder	Поддерживает	NWLNKFWD.SYS IPX маршрутизатор

На рис. 3-2 изображена структура NWLink в Windows 2000, а также указаны файлы, реализующие соответствующий протокол.

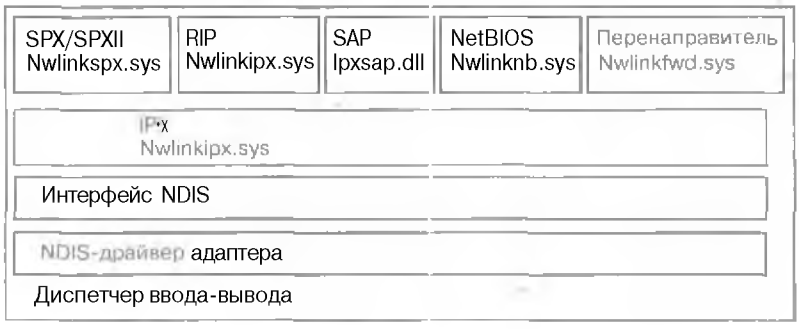


Рис. 3-2. NWLink в архитектуре Windows 2000

IPX

IPX — одноранговый сетевой протокол, предоставляющий службы передачи дейтаграмм без установления логического соединения и управляющий выделением адресов и маршрутизацией пакетов данных внутри и между сетями. Если логическое соединение не устанавливается, при передаче пакетов не требуется каждый раз создавать сеанс — пакеты просто посылаются по каналу связи. Передачу без установления соединения лучше применять, когда данные генерируются нерегулярно, короткими пакетами.

Поскольку при связи по IPX соединение не устанавливается, этот протокол не обеспечивает управление потоком и не подтверждает прием пакетов дейтаграммы. IPX допускает, что они прибудут неповрежденными, и не гарантирует, что они дойдут до адресата в требуемой последовательности. Впрочем, поскольку при передаче данных по ЛВС ошибки возникают редко, IPX удобен для поставки данных короткими пакетами в рамках локальных сетей.

NWLink позволяет разрабатывать приложения, использующие WinSock и *удаленные вызовы процедур* (remote procedure call, RPC) по WinSock. IPX поддерживает NetBIOS, Named Pipes, Mailslots, службу Network Dynamic Data Exchange (NetDDE), RPC поверх NetBIOS и др. NWLink также поддерживает другие приложения, использующие IPX посредством прямого хостинга. Последний позволяет компьютерам взаимодействовать по IPX в обход уровня NetBIOS, что помогает снизить нагрузку на сеть и повысить производительность.

SPX

Это транспортный протокол, предоставляющий службы, ориентированные на соединения, для IPX. Служба, ориентированная на соединение, первоначально дополнительно загружает сеть за счет формирования сеанса, а затем выполняет свою работу, как и службы, не требующие соединения. Следовательно, протокол SPX наилучшим образом подходит для утилит, которым необходимо длительное соединение. SPX обеспечивает надежную доставку благодаря упорядочению, подтверждению и проверке успешной доставки пакетов к любому месту назначения в сети. Это реализуется путем запроса у адресата подтверждения о приеме данных. Верификационный ответ должен содержать значение, соответствующее контрольной сумме, подсчитанной на основе данных до их отправки. Сравнивая эти значения, SPX убеждается не только в том, что пакет данных достиг адресата, но и в том, что он пришел туда неповрежденным. SPX может отслеживать передачу последовательностей отдельных пакетов. Если на запрос подтверждения приема не получен ответ, SPX повторно передаст его до 8 раз. Если ответа не последует, SPX полагает, что соединение было прервано.

SPX также предусматривает механизм групповой передачи пакетов, в котором не требуется упорядочивать и подтверждать получение каждого отдельного пакета. За счет однократного подтверждения приема группы пакетов в большинстве сетей IPX можно снизить сетевой трафик. Помимо этого, механизм группировки пакетов отслеживает утерянные пакеты и повторно передает только их, а не всю группу. В Windows 2000 режим группировки пакетов включен по умолчанию.

SPXII

Это доработанный вариант SPX, отличающийся лучшей производительностью в сетях с высокой пропускной способностью. Вот в чем SPXII превосходит SPX.

- SPX1I допускает обработку большего количества неподтвержденных пакетов, чем SPX. SPX не допускает существования более одного неподтвержденного пакета, а в SPX1I количество неподтвержденных пакетов согласовывается участниками соединения.
- SPXII предусматривает использование пакетов большего размера. Максимальный размер пакета SPX равен 576 байтам, в то время как SPXII способен использовать пакеты любой длины, допускаемой в базовой ЛВС. Например, в сетях Ethernet пакеты SPXII могут иметь размер до 1518 байт.

RIP

NWLink использует протокол RIPX — Router Information Protocol (RIP) поверх IPX — для реализации служб поиска маршрута и маршрутизатора, используемых SPX и NBIPX. RIP обрабатывает IPX-трафик и поддерживает таблицу маршрутов. R1P выполняется на уровне, соответствующем прикладному уровню модели OSI. Код протокола RIP находится в файле NWLNKIPX.SYS.

NWLink включает RIP-протокол для Windows-клиентов и для компьютеров с Windows 2000 Server, на которых не установлена служба Routing and Remote Access Service (RRAS). Эти компьютеры не отправляют пакеты, как это делают маршрутизаторы. — для определения адресата пакетов они используют таблицу R1P. RIP-клиенты, например рабочие станции, выявляют оптимальный маршрут к сети IPX с определенным номером посредством широковещательного запроса маршрута GetLocalTarget. Каждый маршрутизатор, способный достичь адресата, отвечает на запрос GetLocalTarget, выдавая соответствующий маршрут. Основываясь на RIP-откликах от локальных маршрутизаторов, посылающая станция выбирает наилучший маршрут для перенаправления IPX-пакета.

SAP

Service Advertising Protocol (SAP) — механизм, при помощи которого IPX-клиенты собирают и распространяют названия и адреса служб, выполняющихся на IPX-узлах. SAP-клиенты используют SAP-вещание, только если невозможно выполнить запросы к системной БД NetWare или NetWare Domain Services. SAP-клиенты посылают следующие типы сообщений:

- запрашивают имя и адрес ближайшего сервера требуемого типа, транслируя SAP-запрос GetNearestServer.
- запрашивают имя и адрес всех служб или служб определенного типа, транслируя запрос базовой службы.

Для Windows-клиентов и компьютеров с Windows 2000 Server, на которых не установлен IPX-маршрутизатор, в составе NWLink имеется поднабор SAP-протоколов.

NetBIOS поверх IPX

В целях упрощения выполнения в IPX сетях приложений, базирующихся на NetBIOS, NetBIOS поверх IPX (NWLNKNB.SYS) предоставляет следующие стандартные NetBIOS-службы:

- NetBIOS Datagram Services — приложения используют службы дейтаграмм NetBIOS для быстрой связи без установления соединения. Эти службы необходимы для работы почтовых ящиков и для проверки подлинности пользователей;
- NetBIOS Session Services — службы сеансов NetBIOS обеспечивают надежную, основанную на соединении связь между приложениями и поддерживают совместное использование файлов и принтеров;
- NetBIOS Name Service — управление именами включает обработку запросов, регистрацию и освобождение NetBIOS-имен.

Перенаправитель

Это компонент режима ядра, устанавливаемый вместе с NWLink. Впрочем, перенаправитель (Forwarder) применяется, только если сервер Windows 2000 используется в качестве IPX-маршрутизатора, выполняющего службу RRAS.

После активизации ПО IPX-маршрутизатора перенаправитель обрабатывает пакеты в связке с IPX Router Manager и фильтрующим компонентом. Перенаправитель получает информацию о конфигурации от IPX Router Manager и хранит таблицу наилучших маршрутов. Получив входящий пакет, перснаправитель передает его фильтрующему драйверу для проверки на входных фильтрах. Получив исходящий пакет, перенаправитель также сначала передает его фильтрующему драйверу. Если пакет не пройдет исходящий фильтр, го он не отсылается. Возвращенный фильтром пакет перенаправляется по соответствующему интерфейсу.

Резюме

NWLink — 32-разрядная реализация пакета протоколов IPX/SPX, разработанная Microsoft. IPX — одноранговый сетевой протокол, предоставляющий службы передачи дейтаграмм, не устанавливающие логическое соединение; также управляет адресацией и маршрутизацией пакетов. SPX — транспортный протокол, выполняемый поверх IPX; предоставляет службы, устанавливающие логическое соединение поверх IPX. Перснаправитель взаимодействует с диспетчером маршрутов IPX и фильтрующим компонентом для оптимального выбора маршрута пересылки пакетов.

Занятие 2. Использование Gateway Service for NetWare

GSNW позволяет сетевым клиентам Microsoft (LAN Manager, MS-DOS, Windows for Workgroups, Windows 9x, Windows NT/2000) получать доступ к службам сервера NetWare через сервер Windows 2000. На этом занятии вы изучите порядок установки и способы использования службы шлюза для NetWare.

Изучив материал этого занятия, вы сможете:

- ✓ устанавливать GSNW;
- ✓ включать шлюзы в Windows 2000.

Продолжительность занятия — около 30 минут.

Общие сведения о службе шлюза для NetWare

Средства GSNW позволяют создать шлюз, через который компьютеры Microsoft-клиентов, не имеющие клиентского ПО Novell NetWare, смогут обращаться к файлам и службам печати на серверах NetWare. Вы вправе создать шлюзы для ресурсов, находящихся как в Novell NDS, так и на серверах с системной БД NetWare (bindery). Эти ресурсы включают тома, каталоги, объекты с карты каталога, принтеры и очереди печати. Пользователи, работающие локально на компьютерах с Windows 2000 Server, могут использовать GSNW для получения прямого доступа к файлам NetWare и ресурсам печати, находящимся в Novell NDS и на серверах с системной БД NetWare. GSNW зависит от NWLink и работает совместно с этим протоколом.

Что такое GSNW и шлюзы

GSNW действует как мост между протоколом NetBIOS, применяемым в сети Windows, и NetWare Core Protocol (NCP), используемым в сети NetWare. Когда шлюз активизирован, сетевые клиенты, применяющие клиентское ПО Microsoft, могут получить доступ к NetWare-файлам и принтерам, не устанавливая и не запуская на своем компьютере клиентское ПО NetWare (рис. 3-3).

Для организации доступа к файлам сервер, выполняющий роль шлюза, подключает один из своих дисков к тому NetWare и затем открывает совместный доступ к этому диску для клиентов Microsoft. Для создания подключения с сервером NetWare файловый шлюз использует учетную запись NetWare на компьютере с Windows 2000 Server. Это подключение выглядит на Windows 2000 Server, как сетевой диск. После открытия совместного доступа к сетевому диску он выглядит для клиентов Windows, как и любой другой общий ресурс на Windows 2000 Server.

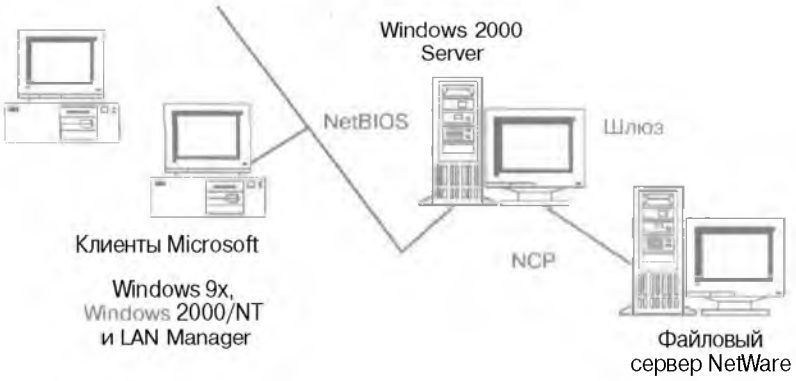


Рис. 3-3. **Конфигурация файлового шлюза**

Предположим, вы хотите создать шлюз между компьютером AIREDALE (выполняющим GSNW) и папкой \\NW4\Server1\Org_Unit. Org\Data в Novell NDS на NetWare-сервере Nw4. При активизации шлюза надо указать \\NW4\Server1\Org_Unit.Org\Data в качестве ресурса NetWare, а затем — общее имя ресурса для клиентов Microsoft — Nw_Data. Затем клиенты Microsoft смогут ссылаться на этот ресурс как на \\AIREDALE\Nw_Data.

После установки межсетевое соединение будет прервано только в следующих случаях: при выключении компьютера, использующего Windows 2000 Server; если администратор отключит общий ресурс или блокирует шлюз, а также если доступ к серверу NetWare будет прерван из-за неполадок в сети.

Примечание Поскольку запросы от подключенных к сети Microsoft-клиентов обрабатываются через шлюз, доступ осуществляется медленнее, чем при прямом обращении к сети NetWare. На компьютеры, которым требуется частый доступ к ресурсам NetWare, рекомендуется установить клиентское ПО NetWare.

Установка GSNW

Вы можете установить GSNW одновременно с Windows 2000 Server или позже, Для установки и настройки GSNW требуются полномочия администратора.

▶ **Установка Gateway Service for NetWare**

1. В окне Control Panel (Панель управления) дважды щелкните значок Network and Dial-Up Connections (Сеть и удаленный доступ к сети).
2. Щелкните правой кнопкой значок Local Area Connection (Подключение по локальной сети) и выберите в контекстном меню команду Properties (Свойства).
3. На вкладке General (Общие) щелкните кнопку Install (Установить).
4. В окне Select Network Component Type (Выбор типа сетевого компонента) щелкните Client (Клиент), затем — кнопку Add (Добавить).
5. В окне Select Network Client (Выбор сетевого клиента) щелкните Gateway (And Client) Service For NetWare [Службы шлюза (и клиента) для NetWare], затем щелкните OK.

Одновременно с GSNW будет установлен NWLink, если он еще не был установлен на сервере, а также CSNW; в Control Panel добавится значок GSNW. По умолчанию средства для сетей NetWare займут первое место в списке компонентов.

Внимание! Перед установкой GSNW удалите с компьютера любое имеющееся клиентское ПО, совместимое с NetWare Core Protocol, включая клиентское ПО NetWare.

Настройка GSNW

При первом входе в систему после установки GSNW вам будет предложено выбрать дерево и контекст по умолчанию и основной сервер. Дерево и контекст определяют имя NDS и положение имени пользователя, применяемое при регистрации в дереве NDS. Основной сервер — это сервер NetWare, к которому вы будете автоматически подключены при входе в систему, если ваша сеть не использует Novell NDS. Дерево и контекст по умолчанию задают только в среде Novell NDS, в остальных случаях надо указать основной сервер.

▶ **Выбор основного сервера**

1. В окне Control Panel дважды щелкните значок GSNW.
2. Щелкните переключатель Preferred Server (Основной сервер) и в поле Select Preferred Server (Другой) введите основной сервер.

   Если вы не хотите указывать основной сервер, не заполняйте поле Select Preferred Server. В этом случае вам будет предложено указывать имя основного сервера при каждом входе в систему.

Рис. 3-4. Диалоговое окно **Gateway** Service for **NetWare**

Вы можете выбрать дерево и контекст по умолчанию или основной сервер, но не оба этих варианта одновременно. (В среде Novell NDS задается дерево и контекст по умолчанию.) Выбрав дерево и контекст по умолчанию, вы сохраните возможность доступа к серверам, использующим системную БД NetWare.

▶ **Выбор дерева и контекста по умолчанию**

1. В окне Control Panel дважды щелкните значок GSNW.
2. Щелкните переключатель Default Tree And Context (Дерево и контекст по умолчанию) и заполните поля Tree (Дерево) и Context (Контекст).

Занятие 3. Использование Client Service for NetWare

Сетевые клиенты Microsoft получают доступ к серверу NetWare через сервер Windows 2000, на котором запущена служба GSNW. Компьютеры с Windows 2000 могут обращаться к ресурсам на сервере NetWare в качестве клиентов посредством встроенного компонента — Client Service for NetWare (CSNW). В ходе этого занятия вы научитесь устанавливать и использовать CSNW.

Изучив материал этого занятия, вы сможете:

- ✓ устанавливать CSNW;
- ✓ пояснить преимущества и недостатки CSNW.

Продолжительность занятия — около 15 минут.

Взаимодействие с NetWare

CSNW обеспечивает подключение клиентов к NetWare, а GSNW работает в качестве шлюза, через который множество клиентов могут обращаться к ресурсам NetWare. Обе эти службы зависят от протокола NWLink и работают совместно с ним. NWLink автоматически устанавливается вместе с псренаправителем (редиректором). CSNW использует часть кода GSNW.

После подключения диска к тому NetWare компьютеры с Windows 2000 Professional используют учетную запись NetWare для создания подтвержденного соединения с NetWare-сервсром. Например, такая запись применяется для подключения компьютера А (выполняющего CSNW) с томом \\T\Volname.Orgunit.Org\Folder, где T — имя дерева Novell NDS, Volname.Orgunit.Org — путь к имени тома в Novell NDS, а Folder — подкаталог тома Volname. В Windows Explorer выберите в меню Tools (Сервис) команду Map Network Drive («Подключить сетевой диск). Для подключения также можно использовать утилиту командной строки net use. После подключения диска с помощью команды net use соединение может прерваться только при выключении компьютера с Windows 2000 Professional или при возникновении неполадок сети, прерывающих доступ к NetWare-серверу. Сетевой диск будет повторно подключен при следующем входе в систему.

Выбор между CSNW и GSNW

Если вам необходимо поддерживать разнородную среду, включающую серверы Windows 2000 и серверы NetWare, используйте CSNW. Если вы хотите постепенно перейти от NetWare к Windows 2000 или упростить администрирование, примените GSNW.

Преимущества CSNW

В сравнении со службой шлюза применение CSNW имеет значительные преимущества.

- **CSNW Service позволяет организовать доступ на уровне пользователей, а не на уровне** ресурсов. Средства CSNW позволят вам предоставить доступ к индивидуальным домашним каталогам на томах NetWare. Пользователи могут затем подключить сетевые диски к своим домашним каталогам и любым дополнительным томам, для которых у них есть полномочия.

- CSNW работает быстрее, чем шлюз. CSNW напрямую связывается с сервером NetWare, избегая задержек, вызванных запросами через шлюзовой сервер.

Недостатки CSNW

- **CSNW требует обслуживать несколько учетных записей для каждого пользователя.** Для каждого пользователя надо создать и поддерживать отдельные учетные записи для Windows 2000 и для NetWare. Впрочем, этого можно избежать, если вы дополнительно применяете такой продукт, как Novell Client for Windows 2000. В среде Windows NT 4.0 для этого можно задействовать Directory Service Manager.
- **CSNW требует больших затрат по установке и управлению. При использовании CSNW вы должны установить и обслуживать дополнительное клиентское ПО на каждом компьютере с Windows 2000** Professional.
- CSNW требует установки протокола IPX на всех компьютерах сети. Серверы Windows 2000 и серверы NetWare 5.0 используют в качестве основного протокола TCP/IP. Однако CSNW нужен протокол IPX (через NWLink) и иногда — IPX-маршрутизация во всей сети.

Настройка CSNW

Вместе с CSNW автоматически устанавливается NWLink — IPX/SPX/NetBIOS-совместимый транспортный протокол. Для установки CSNW на компьютере с Windows 2000 Professional необходимы полномочия администратора. При массовом развертывании Windows 2000 Professional и CSNW можно применить режим автоматической установки.

▶ **Установка Client Service for NetWare**

1. В панели управления дважды щелкните значок Network and Dial-Up Connections.
2. Щелкните правой кнопкой локальное подключение, для которого вы хотите установить CSNW, и выберите в контекстном меню команду Properties (Свойства).
3. На вкладке General (Общие) щелкните кнопку Install (Установить).
4. В окне Select Network Component Type (Выбор типа сетевого компонента) щелкните Client (Клиент), затем — кнопку Add (Добавить).
5. В окне Select Network Client (Выбор сетевого клиента) щелкните Client Service For NetWare, затем — OK.

Резюме

Windows 2000 содержит клиентское ПО для подключения к серверам NetWare. Средства Client Service for NetWare в составе Windows 2000 Professional и Gateway Service for NetWare в составе Windows 2000 Server позволяют пользователям обращаться к файловым ресурсам и принтерам на серверах NetWare.

Занятие 4 Установка и настройка NWLink

Вы научитесь устанавливать протокол **NWLink, который** включен во все редакции Windows 2000, для соединения с компьютерами **NetWare или** другими совместимыми системами.

Изучив материал этого занятия, вы сможете:

- ✓ установить и настроить протокол NWLink в Windows 2000;
- ✓ объяснить назначение типа кадра и номера сети.

Продолжительность занятия — около 30 минут.

Взаимодействие Windows 2000 Professional с NetWare

Для подключения к ресурсам Novell NDS и серверам NetWare с системной БД в Windows 2000 Professional применяются CSNW и протокол NWLink. Последний является компонентом Windows и включает протокол IPX/SPX.

При обновлении Windows 9x или Windows NT 4.0 Workstation до Windows 2000 Professional можно оставить в ОС клиент Novell Client 32. Windows 2000 Professional обновляет компьютеры, использующие Novell Client 32 версий младше 4.7. В ходе обновления до Windows 2000 Professional устанавливается Novell Client 32 версии 4.51. Этот процесс позволяет обновить Novell Client 32 без потерь функциональных возможностей. Для получения полной версии Novell Client для Windows 2000 обратитесь в Novell.

Установка протокола NWLink

При установке Windows 2000 протокол NWLink не устанавливается по умолчанию, как TCP/IP. Впрочем, вы можете установить NWLink позже, как и любой другой протокол.

▶ **Установка NWLink**

1. В панели управления дважды щелкните значок Network and Dial-Up Connections.
2. Щелкните правой кнопкой локальное подключение, для которого надо установить CSNW, и выберите в контекстном меню команду Properties.
3. На вкладке **General** щелкните **Install.**
4. В диалоговом окне Select Network Component Type щелкните Client, затем — кнопку Add.
5. В диалоговом окне Select Network Client щелкните NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, затем — OK.

Чтобы убедиться в корректности работы NWLink, в командной строке наберите ip\route config. Отобразится таблица со сведениями о привязках, для которых сконфигурирован NWLink (рис. 3-5).

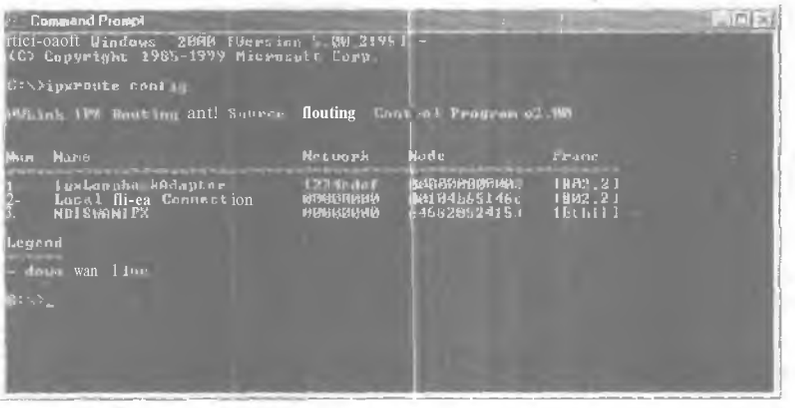


Рис. 3-5. **Информация о привязках NWLink**

Номер внутренней сети

Используется для внутренней маршрутизации, когда компьютер с Windows 2000 обеспечивает функционирование служб IPX. При вычислении наилучшего маршрута для передачи пакетов к требуемому компьютеру может быть найдено несколько маршрутов с одинаковыми метриками. Когда вы определяете уникальный номер внутренней сети, вы создаете виртуальную сеть внутри компьютера. Это обеспечивает оптимальный маршрут между сетью и службами, выполняемыми на компьютере. .

Изменение номера **внутренней сети**

1. В панели управления дважды щелкните значок Network And Dial-Up Connections.
2. Щелкните правой кнопкой локальное подключение и выберите в контекстном меню команду Properties.
3. На вкладке General щелкните NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, затем щелкните кнопку Properties.
4. Наберите номер в поле Internal Network Number (Номер внутренней сети), затем щелкните OK (рис. 3-6).

Примечание Обычно нет необходимости изменять внутренний номер сети.

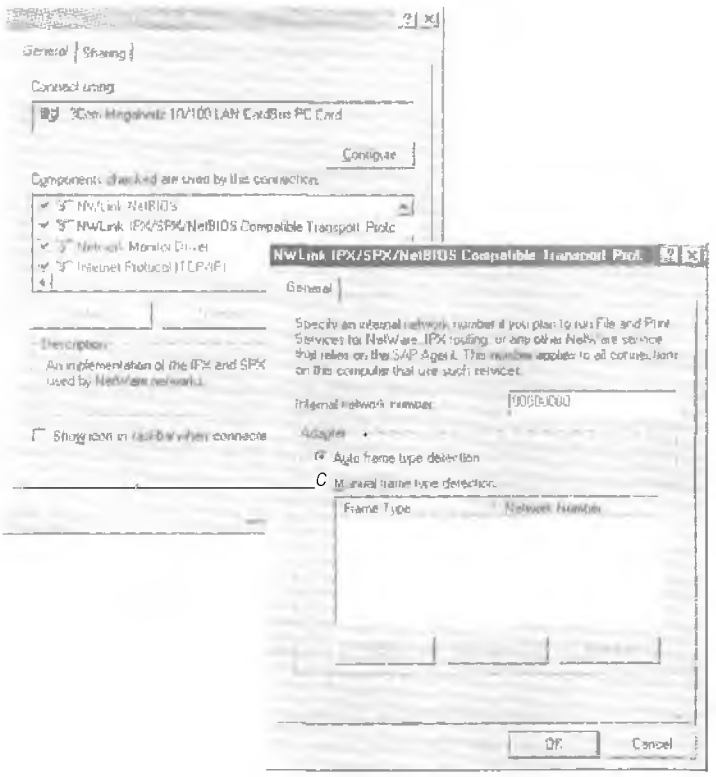


Рис. 3-6. Диалоговое окно NWLink IPX/SPX/NetBIOS Compatible Transport Protocol

Тип кадра и номер сети

Тип кадра определяет способ, которым сетевой адаптер компьютера с Windows 2000 форматирует данные перед передачей их в сеть. Для связи между компьютером с Windows 2000 и сервером NetWare необходимо настроить NWLink IPX/SPX/NetBIOS Compatible Transport Protocol (NWLink) для использования того же типа кадра, какой используется сервером NetWare. В табл. 3-2 приведен список топологий и типов кадров, поддерживаемых NWLink.

Табл. 3-2. Типы кадров NWLink

Тип сети	Поддерживаемые типы кадров
Ethernet	Ethernet II, 802.2, 802.3. 802.2 Subnetwork Access Protocol (SNAP)
Token Ring	802.5 и 802.5 **SNAP**
FDDI	802.2 и **SNAP**

Тип кадра (frame type) определяет формат заголовка и окончания кадра, используемые разными протоколами канального уровня.

В процессе автоматического определения NWLink испытывает все доступные типы кадров из списка связанных с сетевым носителем кадров. Например, в сети Ethernet это будут Ethernet 802.2, Ethernet 802.3, Ethernet II и Ethernet Subnetwork Access Protocol (SNAP). Вместе с откликом от сервера NetWare с одним из этих типов кадров NWLink

сразу получает номер сети, связанный с данным типом кадра для того сетевого сегмента, где находится клиент. Затем NWLink перестраивает свои привязки, используя типы кадра, на которые были получены отклики.

Внешний номер сети — это уникальный номер, представляющий конкретный сетевой сегмент с соответствующим типом кадра. Все компьютеры одного сетевого сегмента, использующие данный тип кадра, должны иметь одинаковый внешний номер сети.

Тип кадра IPX и номер сети задаются при начальной конфигурации сервера NetWare и могут быть автоматически определены в Windows 2000 средствами протокола NWLink. Рекомендуется всегда автоматически конфигурировать тип кадра и номер сети.

Иногда функция автоопределения выбирает для адаптера неправильные значения типа кадра и номера сети. Поскольку она использует отклики от компьютеров того же сетевого сегмента, то, если компьютер ответит некорректно, могут быть выбраны неправильные значения. Это происходит, если неверно настроен какой-либо компьютер в сегменте сети. При выборе неправильных значений вы можете вручную изменить тип кадра для NWLink и номер сети для данного адаптера. В Windows 2000 тип кадра и номер сети должны соответствовать аналогичным параметрам сервера NetWare. Для автоматического определения номера сети задайте номер сети равным 0000000.

▶ **Изменение номера сети и типа кадра**

1. В панели управления дважды щелкните значок Network and Dial-Up Connections.
2. Щелкните правой кнопкой локальное подключение и выберите команду Properties.
3. На вкладке General щелкните NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, затем щелкните кнопку Properties
4. В списке Frame Type (Тип кадра) укажите требуемый тип кадра.
5. В поле Network Number (Номер сети) наберите номер сети, затем щелкните OK.

Внимание! В большинстве случаев изменять значения типа кадра и номера сети не требуется. Если вы зададите неправильные значения, клиент не сможет связаться с сервером NetWare,

Настройка NWLink

Для настройки NWLink нужны полномочия администратора. Вот как привязать NWLink к другому сетевому адаптеру или настроить для ручного изменения типа кадра.

▶ **Настройка NWLink**

1. В панели управления дважды шелкните значок Network and Dial-Up Connections.
2. Щелкните праиой кнопкой локальное подключение и выберите команду Properties.
3. На вкладке General щелкните NWLink IPX/SPX/NetBIOS Compatible Transpori Protocol, затем шелкните кнопку Properties.
4. На вкладке General наберите значение Internal Network Number или оставьте значение по умолчанию - 00000000.
5. Если вы хотите, чтобы Windows 2000 автоматически выбрала тип кадра, щелкните Auto Frame Type Detection, затем — кнопку OK. Пропустите пункты 6–10.

   По умолчанию NWLink автоматически определяет тип кадра, используемый сетевым адаптером, к которому он привязан. Если NWLink не обнаружит сетевого трафика или будут определены множество различных типов кадра помимо 802.2, NWLink выберет тип 802.2.
6. Для задания типа кадра вручную шелкните Manual Frame Type Detection (Ручное определение типа кадра).
7. Щелкните кнопку Add (Добавить).

8. В списке Frame Type (Тип кадра) выберите тип кадра.

   Вы можете определить используемые вашим маршрутизатором внешний и внутренний номера сети и тип кадра, набрав в командной строке команду **ipxroute config**.
9. В поле Network Number (Номер сети) наберите номер сети и щелкните кнопку Add (Добавить).
10. Повторите эти действия для каждого типа кадра, который вы хотите добавить, и щелкните OK.

Практикум: установка и настройка NWLink

Установите и настройте протокол NWLink. Затем измените порядок привязок для него.

▶ Задание 1: установите и настройте протокол NWLink

1. В панели управления дважды щелкните значок Network and Dial-Up Connections
2. Щелкните правой кнопкой локальное подключение и выберите команду Properties.

   Откроется диалоговое окно свойств локального подключения.
3. Щелкните кнопку Add.

   Откроется диалоговое окно Select Network Component Type.
4. Щелкните Protocol (Протокол), затем — кнопку Add.
5. Выберите NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, затем - OK.
6. В окне свойств локального подключения выберите NWLink IPX/SPX/NetBIOS Compatible Transport Protocol, затем щелкните кнопку Properties. На данном этапе вы можете указать, как выбирать тип кадра; автоматически или вручную.

▶ Задание 2; измените порядок привязок для протокола NWLink

1. В панели управления дважды щелкните значок Network and Dial-Up Connections
2. Щелкните подключение, которое надо настроить, и в меню Advanced (Дополнительно) выберите команду Advanced Settings (Дополнительные параметры).
3. На вкладке Adapters And Bindings (Адаптеры и привязки) в списке Binding: For (Привязка для) щелкните протокол NWLink и переместите его вниз списка, щелкая кнопку со стрелкой вниз (рис. 3-7).

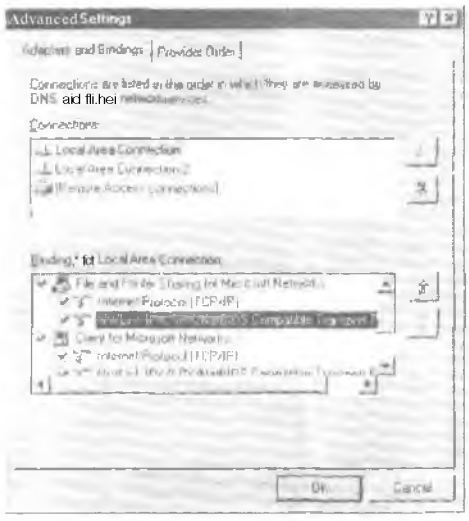


Рис. 3-7. Диалоговое **окно Advanced Settings (Дополнительные параметры)**

Резюме

IPX/SPX — стек протоколов, используемый в сетях Novell. Протокол NWLink, совместимый с IPX/SPX, позволяет Windows 2000 взаимодействовать с сетями Novell. Он автоматически устанавливается вместе с Client Service for NetWare.

Для установки и настройки NWLink надо иметь полномочия администратора. Внутренний номер сети применяется для внутренней маршрутизации, когда компьютер, с Windows 2000 выполняет службы IPX. Тип кадра определяет, каким образом сетевой адаптер форматирует данные перед их передачей по сети. Номер внешней сети — уникальный, представляющий конкретный сегмент сети с соответствующим типом кадра. Все компьютеры одного сетевого сегмента, использующие данный тип кадра, должны иметь одинаковый номер внешней сети.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Что такое NWLink и какое отношение он имеет к Windows 2000?

2. Что такое SPX?

3. Что такое Gateway Service for NetWare?

4. Что надо принять во внимание при выборе между использованием Gateway Service for NetWare и Client Service for NetWare?

5. Для чего предназначена функция автоопределения в NWLink?

ГЛАВА 4

Мониторинг сетевой активности

В этой главе

Сетевые коммуникации играют важную роль в рабочем окружении. По аналогии с процессором или дисками вашего компьютера поведение сети отражается на работе системы в целом. В этой главе рассматриваются вопросы оптимизации работы вашей системы с помощью различных методов анализа сетевой активности, например мониторинга сетевого трафика и использования ресурсов. В состав Microsoft Windows 2000 входят две утилиты для мониторинга сети: System Monitor и Network Monitor. Утилита System Monitor (Системный монитор) для Windows 2000 Professional и Windows 2000 Server отслеживает использование ресурсов и пропускную способность сети. Утилита Network Monitor (Сетевой монитор) для Windows 2000 Server проверяет пропускную способность сети путем записи сетевого трафика. Эта глава посвящена применению Network Monitor для анализа локального трафика.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server.

Занятие 1. Знакомство с утилитой Network Monitor

Microsoft Windows 2000 Network Monitor используется для анализа и обнаружения проблем в ЛВС, например, для выявления ошибок, возникающих в аппаратной и программной частях, когда два или более компьютеров не могут установить связь. Network Monitor позволяет вести журнал сетевой активности, копию которого можно отослать профессиональным сетевым аналитикам или в службу поддержки. Кроме того, разработчики сетевого ПО применяют Network Monitor для мониторинга и отладки своих приложений.

Изучив материал этого занятия, вы сможете:

- ✓ установить Network Monitor;
- ✓ описать преимущества использования Network Monitor.

Продолжительность **занятия** — около 15 минут.

Что такое Network Monitor

Утилита Network Monitor используется для записи данных, переданных и полученных компьютерами сети, и последующего просмотра и анализа этих данных. Кадры и пакеты канального уровня записываются через прикладной уровень и представляются в графическом виде. Кадры и пакеты содержат различную информацию:

- адреса отправителя **и адресата;**
- порядковые номера;
- контрольные суммы.

Утилита Network Monitor расшифровывает эту информацию, позволяя анализировать сетевой трафик и устранять неполадки в сети. Помимо данных канального уровня, Network Monitor «понимает» некоторые данные прикладного уровня, например протоколы HTTP или FTP, Эти данные помогают решить проблемы взаимодействия браузера и Web-сервера.

Практикум: установка Network Monitor

Для записи, просмотра и анализа сетевых кадров необходимо установить утилиту Network Monitor и сетевой протокол под названием Network Monitor Driver (Драйвер сетевого монитора). Сейчас вы установите Network Monitor для Windows 2000 Server.

▶ **Задание 1: установите Network Monitor**

1. Раскройте меню Start\Settings\Control Panel (Пуск\Настройка\Панель управления) и щелкните ярлык Add/Remove Programs (Установка и удаление программ).
2. Щелкните кнопку Add/Remove Windows Components (Добавление и удаление компонентов Windows).
3. В окне мастера компонентов Windows выберите Management And Monitoring Tools (Средства управления и наблюдения) и щелкните кнопку Details (Состав).
4. В окне Management And Monitoring Tools пометьте флажок Network Monitor Tools (Средства сетевого монитора) и щелкните OK (рис. 4-1).
5. В окне мастера компонентов Windows щелкните Next. При необходимости вставьте компакт-диск Windows 2000 или укажите путь к требуемым файлам.
6. Щелкните кнопку Finish (Готово), чтобы завершить установку.

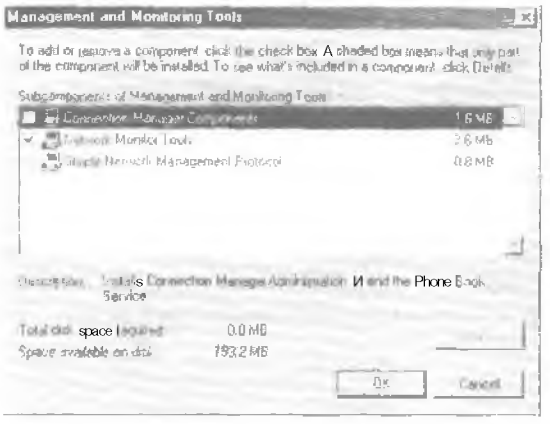


Рис. 4-1. Выбор компонента Network Monitor Tools (Средства **сетевого монитора**)

Примечание Network Monitor включает агент, отвечающий за сбор данных, и утилиту, которая отображает и анализирует эти данные. Обе составляющие автоматически устанавливаются одновременно с Network Monitor Tools.

Драйвер сетевого монитора

Просматривает кадры с сетевого адаптера и передает информацию утилите Network Monitor. Кроме того, драйвер может передавать кадры удаленному администратору, который использует версию Network Monitor из состава Microsoft Systems Management Server.

Примечание При установке драйвера сетевого монитора в утилите System Monitor появляется объект Network Segment.

Установка драйвера не означает установку утилиты Network Monitor. Для просмотра и анализа данных необходимо установить компонент Network Monitor Tools на компьютере с Windows 2000 Server.

► Задание 2: установите драйвер сетевого монитора

1. Раскройте меню Start\Settings\Control Panel и щелкните ярлык Network and Dial-Up Connections (Сеть и удаленный доступ к сети).
2. Щелкните правой кнопкой локальное подключение, мониторинг которого необходимо выполнить, и выберите в контекстном меню команду Properties (Свойства).
3. В окне свойств локального подключения щелкните кнопку Install (Установить).
4. В окне Select Network Component Type (Выбор типа сетевого компонента) щелкните Protocol (Протокол), а затем — кнопку Add (Добавить).
5. Вокне Select Network Protocol (Выбор сетевого протокола) выберите Network Monitor Driver (Драйвер сетевого монитора) и щелкните OK.

   При необходимости вставьте компакт-диск Windows 2000 или укажите путь к требуемым файлам.

Запись сетевых данных

Утилита Network Monitor записывает и анализирует сетевые кадры. Она позволяет записать весь сетевой трафик, проходящий через сетевой адаптер или выбрать некоторое подмножество кадров. Кроме того, утилиту Network Monitor можно заставить отвечать на события в сети. Запись и анализ сетевых данных рассматриваются на занятии 2.

Резюме

Утилита Network Monitor используется для определения и анализа проблем, возникающих в сети. Network Monitor позволяет вести журнал сетевой активности, копию которого можно отослать профессиональным сетевым аналитикам или в службу поддержки.

Занятие 2 Использование Network Monitor

Здесь рассматривается использование Network Monitor для решения проблем, возникающих в сети. При применении Network Monitor вы должны соблюдать следующие правила.

1. Запускайте Network Monitor в периоды минимальной нагрузки на сеть или на непродолжительное время. Это уменьшит потребление ресурсов системы.
2. Записывайте только те статистические данные, которые действительно необходимы. Это ограничит объем информации и поможет быстро найти ошибку.

Изучив материал этого занятия, вы сможете;

- ✓ записывать сетевые данные и исследовать кадры средствами Network Monitor.

Продолжительность занятия — около 40 минут.

Исследование кадров

Утилита Network Monitor записывает кадры, проходящие через сетевой адаптер. Кадры содержат различную информацию:

- название используемого протокола;
- адрес компьютера-отправителя;
- адрес назначения кадра;
- длину кадра.

▶ **Запись сетевых кадров**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Network Monitor.

   При необходимости выберите локальную сеть, для которой по умолчанию будут записываться данные.
2. В меню Capture (Запись) выберите команду Start (Запустить).

Просмотр данных

Записанные сетевые данные можно просмотреть средствами пользовательского интерфейса утилиты Network Monitor (рис. 4-21. Разбирая строку записанных данных и приводя ее к структуре логического кадра. Network Monitor автоматически анализирует некоторые данные. Кроме того, утилита отображает общую статистику по сегменту сети, в том числе сведения о:

- широковещательных кадрах;
- многоадресных кадрах;
- использовании сети;
- количестве полученных байт в секунду;
- количестве полученных кадров в секунду.

Примечание Из соображений безопасности утилита Network Monitor записывает кадры, включая широковещательные и многоадресные, которые посылает или получает только локальный компьютер.

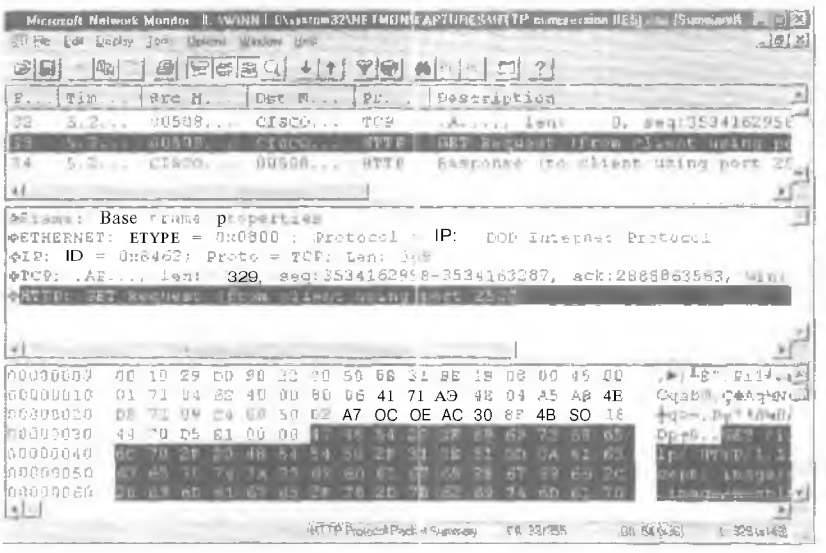


Рис. 4-2. Пользовательский интерфейс Network Monitor

Для копирования кадров в буфер записи (область памяти переменного размера) Network Monitor использует драйвер NDIS. По умолчанию размер буфера равен 1 Мб. При необходимости это значение можно изменить в пределах свободной оперативной памяти.

Примечание Если *наш* сетевой адаптер не поддерживает смешанный режим (при котором через него проходят все кадры, посланные по сети), Network Monitor будет применять локальный режим. В этом случае при записи кадров драйвером NDIS нагрузка на сеть не увеличится. (Перевод адаптера в смешанный режим иногда повышает нагрузку на процессор более чем на 30%.)

Network Monitor отображает статистику первой сотни уникальных сеансов. Чтобы обновить статистику и увидеть информацию о следующих ста сеансах, в меню Capture (Запись) выберите команду Clear Statistics (Очистить статистику). В табл. 4-1 описаны области окна Capture.

Табл. 4-1. Статистика в окне Capture

Область	Показывает
Диаграмма	Графическое представление текущей сетевой активности
Статистика сеанса	Статистика текущего сеанса
Статистика станции	Статистика сеансов, в которых участвовал данный компьютер
Общая статистика	Общая статистика сетевой активности с начала записи

Чтобы записать кадры, полученные с определенных компьютеров, необходимо узнать их адреса и ассоциировать их с именами DNS или NetBIOS. После этого имена требуется сохранить в файле адресов (.adr), который используется для настройки фильтров записи и отображения. Фильтр записи позволяет задать критерий отбора данных. Для настройки фильтра записи служит диалоговое окно Capture Filter (Фильтр записи) (рис. 4-3), которое вызывается соответствующей командой в меню Capture или нажатием клавиши F8.

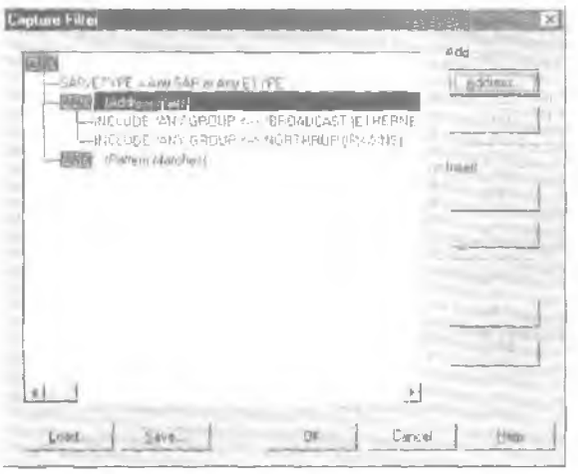


Рис. 4-3. Диалоговое окно Capture Filter (Фильтр записи)

Примечание Фильтры записи существенно увеличивают нагрузку на процессор, так как через них проходит каждый пакет. Иногда использование сложных фильтров приводит к потере кадра.

Чтобы настроить фильтр записи, задайте условия в диалоговом окне Capture Filter, Указав условия соответствия, вы сможете:

- **записывать** кадры, содержащие определенный тип данных;
- записывать кадры, использующие определенный протокол;
- использовать триггер записи для выполнения каких-либо действий.

В табл. 4-2 описаны типы триггеров и условия, которые его запускают.

Табл. 4-2. Описание триггеров записи

Тип триггера	Описание
Nothing (Никогда)	Триггер выключен (по умолчанию)
Pattern Match (Соответствие шаблону)	Триггер включается при совпадении шаблона, выраженного в текстовом или шестнадцатеричном формате
Buffer Space (Место в буфере)	Триггер включается при заполнении на определенный процент буфера записи данными
Pattern Match Then Buffer Space (Соотв. шаблону, затем место в буфере)	Триггер включается при обнаружении в записанном кадре определенной последовательности и последующем заполнении буфера на указанное число процентов
Buffer Space Then Pattern Match (Место в буфере, а затем соотв. шаблону)	Триггер включается при заполнении буфера на указанное число процентов и последующем обнаружении в записанном кадре определенной последовательности
No Action (Только звуковой сигнал)	При соблюдении условий триггера никаких действий не происходит, но компьютер издает звуковой сигнал
Stop Capture (Останов записи)	Останавливает запись при выполнении условий триггера
Execute Command Line (Выполнение команды)	Запускает программу или командный файл при соблюдении условий триггера. Выбирая этот тип триггера, укажите путь к программе или командному файлу

Примечание Если на компьютере установлено несколько сетевых адаптеров, надо либо переключаться между ними, либо запустить несколько экземпляров утилиты Network Monitor. Чтобы переключиться на другой сетевой адаптер, в меню Capture выберите команду Networks (Сети) и укажите нужный адаптер.

Записанные данные можно сохранить. Например, это стоит сделать перед началом следующей записи (чтобы избежать потери данных), если данные будут анализироваться позже или если требуется составить документ об использовании сети и возникших проблемах. При сохранении данные копируются в файл с расширением .cap.

Использование фильтров отображения

По аналогии с фильтрами записи можно использовать фильтр отображения как запрос к базе данных, чтобы указать, какие кадры следует отображать. Фильтр отображения оперирует с записанными данными и не оказывает влияния на содержимое буфера записи. Кадры фильтруются на основе следующих данных:

- адреса отправителя и приемника кадра для канального и сетевого уровней;
- используемого при отправке протокола;
- свойств и значений, содержащихся в пакете (под свойством подразумевается поле данных в заголовке протокола, которые в совокупности определяют его назначение).

Чтобы настроить фильтр отображения, необходимо задать условия в диалоговом окне Display Filter (Фильтр отображения). Вся информация в этом окне отображается в виде дерева решений и является графическим представлением логики работы фильтра. Изменения в определении фильтра отражаются на дереве решений. В табл. 4-3 перечислены различные способы фильтрования.

Табл. 4-3. Типы фильтров отображения

Элемент фильтра	Описание
Protocol (Протокол)	Определяет протокол или его свойства
Address Filter (по умолчанию ANY <——> ANY) (Адрес)	Определяет адреса компьютеров, с которых необходимо записывать данные
Property (Свойство)	Определяет свойства, которые удовлетворяют условию отображения

При настройке фильтров отображения можно использовать логические операторы AND, OR и NOT. Кроме того, в отличие от фильтров записи в выражении разрешается применять более четырех адресов. При отображении записанных данных вся информация о кадрах появляется в окне просмотра кадров. Чтобы отобразить кадры, для отправки которых использовался определенный протокол, измените поле Protocol в диалоговом окне Display Filter (Фильтр отображения). Свойства протокола — это информация, извлеченная из данных этого протокола. Допустим, вы записали много кадров, переданных с помощью протокола Server Message Block (SMB), но хотите исследовать только те кадры, которые применялись для создания каталога на вашем компьютере. В этом случае стоит исследовать кадры, где свойство, отвечающее за команду SMB, эквивалентно созданию каталога. Кроме того, изменив строку ANY < -> ANY в диалоговом окне Display Filter, можно просмотреть кадры, посланные с определенного компьютера.

Просмотр записанных данных

Для просмотра и анализа записанных **данных выполните** следующие действия:

- выполните сеанс, используя IP-адреса отправителя и приемника и номера портов;
- при обнаружении сбросов обратите внимание на порядковые номера и подтверждения, которые им предшествуют;
- с помощью калькулятора определите подтверждения, согласующиеся с посланными данными;
- попытайтесь понять активность, которую вы видите.

  Вам надо установить:
  - повторяет ли отправитель попытки. Если да, обратите внимание на номера попыток и истекшее время. Стандартное число попыток для протокола TCP/IP равно 5. Для других протоколов это значение может отличаться;
  - восстанавливает ли и посылает ли заново отправитель предыдущий пакет;
  - запрашивает ли получатель отсутствующий кадр, подтверждая предыдущий порядковый номер.

Сбросы могут быть вызваны тайм-аутами на уровне TCP или тайм-аутами протоколов более высокого уровня. Сбросы на уровне TCP легко увидеть в трассировке; сложнее найти их причину, возникающую в протоколах более высокого уровня, таких, как SMB.

Например, тайм-аут SMB-чтения иногда длится 45 секунд и вызывает сброс сессии, даже если соединение работает на уровне TCP. С помощью трассировки удается определить компонент, где происходит сбой, поэтому, чтобы определить проблему, в некоторых случаях требуются другие методы выявления неполадок.

Чтобы увидеть последовательность TCP при наличии протокола более высокого уровня, запустите Network Monitor, откройте диалоговое окно Expression (Выражение) (рис. 4-4) и выполните следующий практикум.

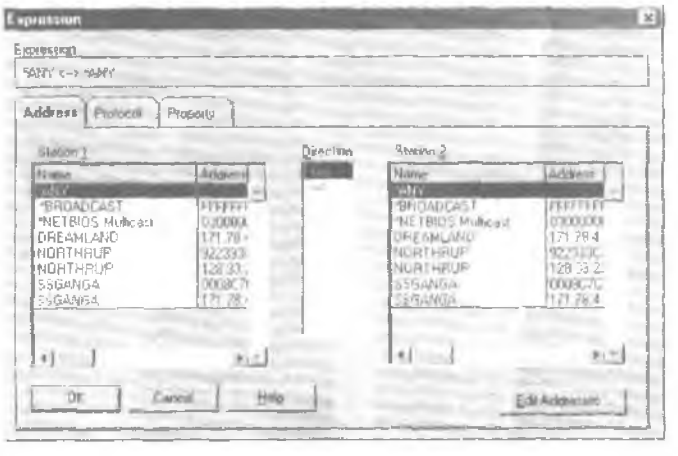


Рис. 4-4. Диалоговое окно Expression

Практикум: запись кадров с помощью Network Monitor

Утилита Network Monitor записывает сетевые кадры из потоков данных в сети и копирует их во временный файл. Используйте Network Monitor для динамического отображения статистики записанных кадров в окне Capture и настройки фильтра записи для отбора кадров, удовлетворяющих определенному критерию.

▶ **Задание: просмотрите последовательность TCP**

1. Запустите Network Monitor.
2. Просмотрите записанные данные.
3. В меню Display (Отображение) выберите команду Options (Параметры).
4. Выберите Auto (based on protocols in the display filter) [Авто (на базе протоколов фильтра отображения)] и щелкните OK.
5. В меню Display выберите команду Filter (Фильтр).
6. Щелкните два раза строку Protocol=Any.
7. На вкладке Protocol щелкните кнопку Disable All (Отключить все).
8. В списке Disabled Protocols (Отключенные протоколы) выберите TCP.
9. Щелкните кнопку Enable (Включить), а затем — OK.
10. В меню Capture (Запись) выберите команду Start (Запустить).

Производительность Network Monitor

Для буфера записи утилита Network Monitor создает файл, проецируемый в память. Чтобы вместить необходимый трафик, буфер записи должен иметь достаточный объем. Кроме того, чтобы уменьшить затраты ОЗУ, в буфере стоит хранить только часть кадра. Например, если нужно записывать данные только из заголовка кадра, сократите размер кадра (в байтах) до размера заголовка. Network Monitor отбросит ненужные данные, экономно используя ОЗУ.

Обнаружение Network Monitor

В целях предотвращения вашей сети от несанкционированного мониторинга Network Monitor обнаруживает другие свои экземпляры, работающие в локальном сегменте сети. При обнаружении другого Network Monitor выдается следующая информация:

- имя компьютера;
- имя пользователя данного компьютера;
- состояние Network Monitor на удаленном компьютере (запущена, записывает или передает);
- адрес адаптера удаленного компьютера;
- версия Network Monitor на удаленном компьютере.

Иногда архитектура сети не позволяет обнаружить другие утилиты Network Monitor, Например, невозможно обнаружить другой Network Monitor, если он отделен от вашего маршрутизатором, который не перенаправляет широковещательные рассылки.

Резюме

Утилита Network Monitor используется для мониторинга потока сетевых данных, то есть всей информации, проходящей через сеть в любой момент времени. Фильтры отображения определяют кадры, которые должны быть отображены. Чтобы настроить фильтр записи, необходимо задать условия в диалоговом окне Capture Filter (Фильтр записи). Записанные сетевые данные можно просмотреть средствами пользовательского интерфейса утилиты Network Monitor. Чтобы вместить необходимый трафик, буфер записи должен иметь достаточный объем.

Занятие 3. Средства администрирования Windows 2000

Windows 2000 содержит различные средства администрирования компьютеров к сети. Службы терминалов. Terminal Services. предоставляют клиентам доступ к Windows *2000* и Windows-приложениям. Путем терминального доступа администраторы могут удаленно администрировать сетевые ресурсы. Кроме того. Windows 2000 содержит протокол SNMP. который используется для мониторинга и обмена информацией между агентом SNMP и программой управления сетью.

Изучив материал этого занятия, вы сможете:

- ✓ настроить сервер терминалов для удаленного администрирования;
- ✓ установить и настроить службу SNMP;
- ✓ описать работу службы SNMP.

Продолжительность занятия — около 25 минут.

Возможности администрирования Windows 2000

Windows 2000 предоставляет срелства локального и удаленного администрирования. Удаленное администрирование подразумевает подключение к компьютеру через сеть для выполнения административных задач. Это позволяет администратору централизованно управлять несколькими компьютерами вместо того, чтобы отдельно настраивать каждый компьютер. Для удаленного администрирования разрешается применять программы сторонних разработчиков или средства из состава Windows 2000.

Службы терминалов

При включении служб терминалов на компьютере Windows 2000 Server необходимо выбрать один из двух режимов: Remote Administration (Режим удаленного управления) или Application Server (Режим сервера приложений) (рис. 4-5).

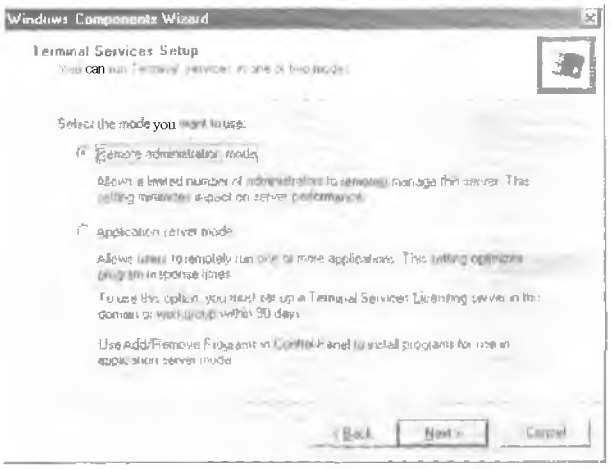


Рис. 4-5. Выбор режима для служб терминалов

Режим сервера приложении позволяет запускать приложения и управлять ими с удаленного компьютера. Интерфейс Windows 2000 и Windows-приложения можно предоставить компьютерам, которые не могут работать в этой ОС. Так как службы терминалов являются встроенным продуктом Windows 2000. разрешается запустить приложение на сервере и предоставить пользовательский интерфейс клиенту, который не может работать в Windows 2000, например компьютеру с Windows 3.11 или Windows CE, подключенному к серверу терминалов.

Для доступа, управления и исправления ошибок клиентов службы терминалов предоставляют режим удаленного администрирования. Режим удаленного управления служит для удаленного администрирования серверов Windows 2000 через любое TCP/IP-соединение, в том числе удаленный доступ, Ethernet, Интернет, беспроводные сети, ГВС и виртуальные частные сети (VPN). Службы терминалов устанавливаются как один из компонентов Windows (рис. 4-6).

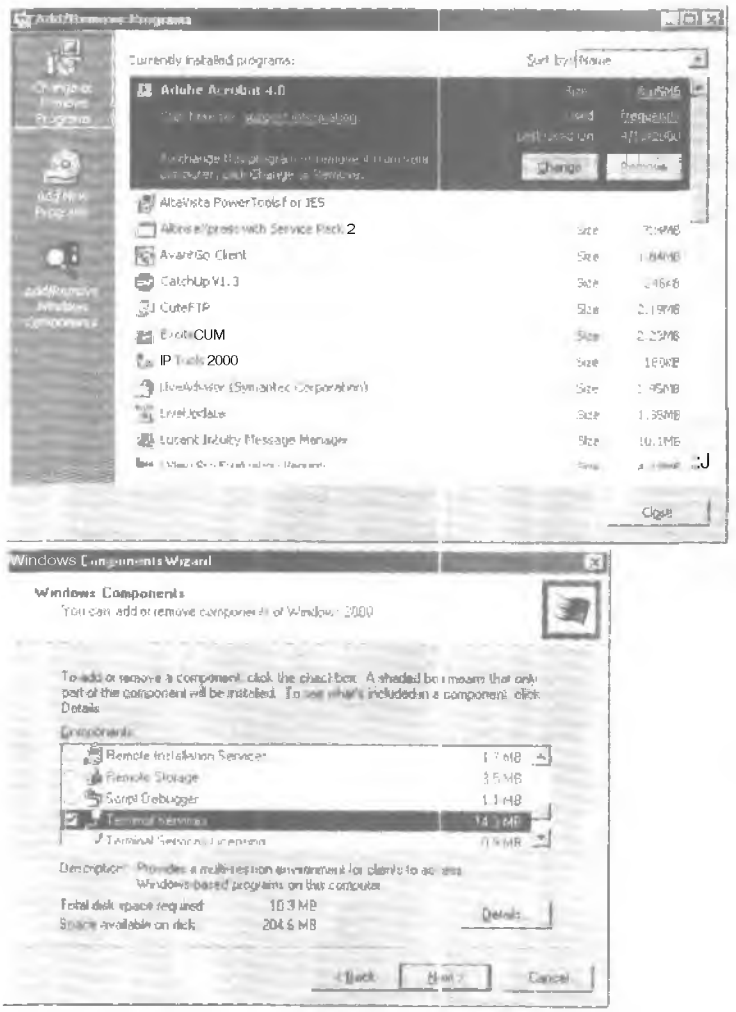


Рис. 4-6. Установка Terminal Services

Использование сервера терминалов

Хотя соединение Remote Desktop Protocol (RDP) автоматически настраивается при установке службы терминалов, можно создать новое подключение. Для каждого сетевого адаптера на сервере терминалов разрешается настроить только одно подключение, однако вы настроите дополнительные подключения RDP, установив сетевой адаптер для каждого подключения вашего компьютера.

▶ **Создание подключения**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Terminal Services Configuration (Настройка служб терминалов).
2. Щелкните правой кнопкой папку Connections (Подключения) и выберите в контекстном меню команду Create New Connection (Создать подключение).

   Откроется окно мастера Terminal Services Connection (Мастер подключения к службам терминалов).
3. Щелкните Next.
4. В первом окне мастера укажите тип подключения, например Microsoft RDP 5.0, и щелкните Next.
5. Выберите уровень шифрования: Low, Medium или High (Низкий, Средний или Высокий). Можно также задать обычную проверку подлинности Windows. Щелкните Next.
6. Задайте параметры и уровень удаленного управления и щелкните Next.
7. Укажите имя подключения, тип протокола, комментарий и щелкните Next.
8. Выберите один или несколько сетевых адаптеров для данного типа протокола, задайте допустимое количество подключений и щелкните Next.
9. Щелкните кнопку Finish.

Службы терминалов поддерживают не более двух параллельных подключений в режиме удаленного администрирования, которые не требуют лицензии. Клиенты службы терминалов потребляют минимальное количество системных ресурсов.

▶ **Предоставление доступа к** серверу **терминалов**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Computer Management (Управление компьютером).
2. Раскройте узел System Tools\Local Users And Groups\Users (Служебные программы\Локальные пользователи и группы\Пользователи).
3. Дважды щелкните объект пользователя, которому надо предоставить доступ.
4. На вкладке Terminal Services Profile пометьте флажок Allow Logon To Terminal Server (рис. 4-7) и щелкните OK.
5. Закройте оснастку Computer Management.
6. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Terminal Services Configuration.
7. В папке Connections (Подключения) выберите Rdp-Tcp.
8. В меню Action (Действие) выберите команду Properties (Свойства).
9. Выберите вкладку Permissions (Разрешения) и добавьте пользователя или группу, который должен иметь разрешения для доступа к данному серверу терминалов.
10. Щелкните OK.
11. Закройте окно Terminal Services Configuration.

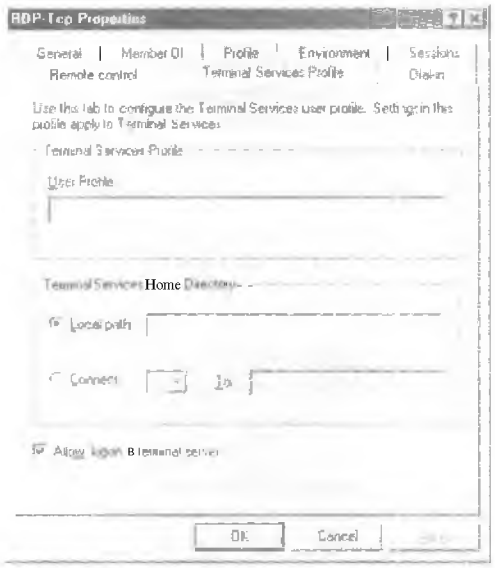


Рис. 4-7. Предоставление доступа к серверу терминалов

Протокол SNMP

Протокол SNMP предназначен для сетевого управления и часто используется для мониторинга и управления компьютерами или другими устройствами (например, принтерами) в TCP/IP-сетях. Этот протокол можно установить и использовать на любом компьютере Windows 2000 с протоколами TCP/IP или IPX/SPX.

► **Установка службы SNMP**

1. Раскройте меню Start\Settings\Control Panel, щелкните ярлык Add/Remove Programs и в открывшемся окне щелкните кнопку Add/Remove Windows Components.
   Откроется окно мастера компонентов Windows.
2. В перечне компонентов выберите Management And Monitoring Tools (Средства наблюдения и управления) и щелкните кнопку Details (Состав).
   Откроется диалоговое окно Management And Monitoring Tools.
3. Пометьте флажок Simple Network Management Protocol и щелкните кнопку OK.
4. В окне мастера компонентов Windows щелкните кнопку Next.
   Мастер установит протокол SNMP
5. Щелкните кнопку Finish.

Системы управления и агенты

Служба SNMP состоит из систем управления и агентов. Под системой управления подразумевается любой компьютер, на котором выполняется управляющее ПО SNMP. Windows 2000 не содержит систем управления, однако множество продуктов сторонних разработчиков, например Sun Net Manager или HP Open View, разработано специально для этого. Система управления запрашивает информацию у агента.

Под агентом подразумевается любой компьютер с Windows 2000, маршрутизатор или концентратор, на котором выполняется программа-агент SNMP (рис. 4-8). Служба Microsoft SNMP содержит только ПО агента, основная функция которого заключается в выполнении команд системы управления.

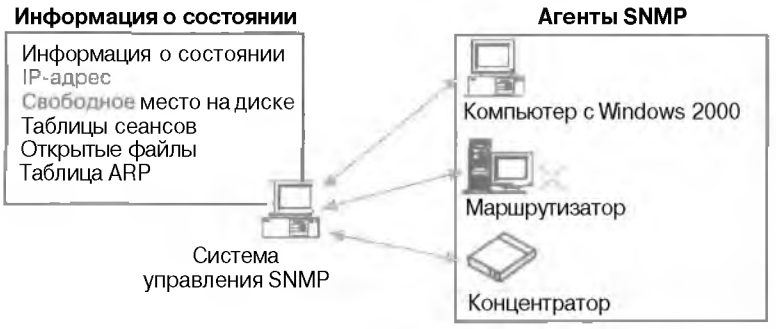


Рис. 4-8. Агент SNMP

Агент Microsoft SNMP позволяет удаленно управлять компьютером с Windows 2000. Агент инициирует только *ловушку* (trap). Ловушка — это сообщение о возникновении на узле некоторого события, переданное системе управления. Программа управления SNMP не обязательно должна выполняться на том же компьютере, что и агент SNMP (рис. 4-9).

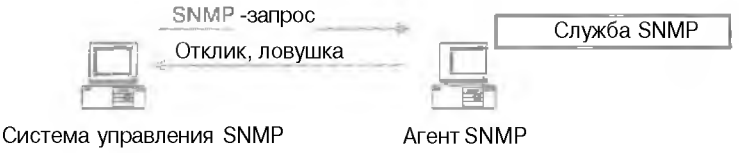


Рис. 4-9. Система управления и агент SNMP

Преимущества SNMP

Средствами диспетчера SNMP можно выполнить мониторинг серверов DHCP, Internet Information Server или WINS. Кроме того, после установки службы SNMP утилита Performance Monitor позволяет просмотреть показания счетчиков производительности TCP/IP: ICMP, TCP, IP, UDP, DHCP, WINS, FTP, Network Interface и Internet Information Server. Утилита Performance Monitor подсчитывает (рис. 4-10):

- активные TCP-соединения;
- UDP-дейтаграммы в секунду;
- ICMP-сообщения в секунду;
- число байт в секунду, проходящих через интерфейс.

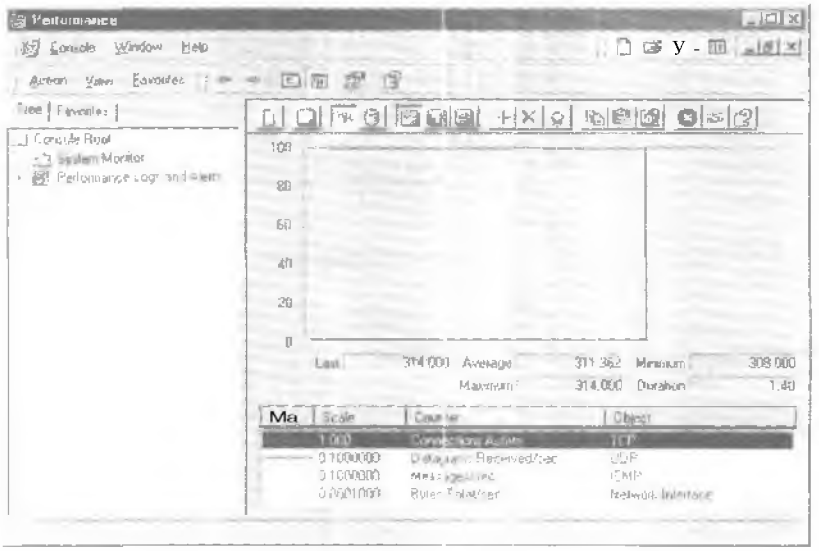


Рис. 4-Ю. Система управления и агент SNMP

Резюме

Протокол SNMP предназначен для управления сетью и широко применяется в TCP/IP-сетях. На его основе взаимодействуют программа управления, запущенная администратором, и программа-агент, выполняемая на узле или шлюзе. Протокол SNMP также применяется для мониторинга и управления узлами и шлюзами при работе в Интернете. Служба Microsoft SNMP позволяет выполнять удаленный мониторинг компьютера с Windows 2000; она обрабатывает запросы с одного или нескольких узлов и отправляет информацию об управлении сетью узлам дискретными блоками, называемыми ловушками. После установки службы **SNMP** утилита Performance Monitor позволяет проверить счетчики производительности TCP/IP.

Закрепление материала

? Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные отпеты см. в приложении «Вопросы и ответы» в конце книги.

1. Какова цель анализа кадров с помощью Network Monitor?

2. Какие данные содержат кадры?

3. Что такое фильтр записи и для чего он используется?

ГЛАВА 5

Внедрение IPSec

В этой главе

Для обеспечения конфиденциальности информации в сети можно воспользоваться протоколом Internet Protocol Security (IPSec), шифрующим сетевой трафик между отдельными или всеми компьютерами сети. IPSec позволяет создавать аутентифицированное и зашифрованное сетевое соединение между двумя компьютерами. Здесь рассказывается об установке, настройке и мониторинге IPSec. Кроме того, вы научитесь настраивать политику и правила IPSec.

Прежде всего

Для изучения материалов этой главы необходимы:

- два компьютера под управлением Microsoft Windows 2000 Server с установленным Network Monitor версии 2.0.

Занятие 1. Знакомство с протоколом IPSec

IPSec — стратегическая технология защиты сетей, предотвращающая проникновение нарушителей в частные сети и на узлы Интернета и сочетающая в себе легкость использования с надежностью. На этом занятии мы рассмотрим технологии, составляющие протокол Internet Protocol Security (IPSec).

Изучив материал этого занятия, вы сможете:

- ✓ описать преимущества использования и архитектуру IPSec.

Продолжительность занятия — около 50 минут.

Протокол IPSec

С развитием Интернета и интрасетей увеличилась потребность в защите информации. Основные проблемы — это зашита сетевого трафика от:

- изменения данных в пути;
- перехвата, просмотра или копирования данных;
- несанкционированного доступа.

IPSec — структура открытых стандартов для обеспечения частной защищенной связи по IP-сетям с помощью криптографических служб безопасности. Реализация IPSec в Microsoft Windows 2000 основана на стандартах, разработанных рабочей группой Internet Engineering Task Force (IETF) IPSec. IPSec выполняет две задачи:

1. защищает пакеты протокола IP;
2. обеспечивает защиту от сетевых атак.

Обе задачи выполняются с помощью основанных на криптографии служб, протоколов безопасности и динамического управления ключами. Такой метод является достаточно мощным и гибким, чтобы обезопасить связи между компьютерами в частной сети, между удаленными узлами, соединенными через Интернет, а также между удаленными клиентами. IPSec также используют для фильтрования пакетов данных в сети.

IPSec основан на сквозной модели защиты. Это означает, что поддержка IPSec требуется лишь на принимающем и передающем компьютерах. Каждый из них управляет защитой со своей стороны, предполагая, что среда передачи данных небезопасна. Маршрутизаторы, переправляющие пакеты между источником и адресатом, для поддержки IPSec не требуются. Подобная модель позволяет успешно развернуть IPSec в имеющейся сети предприятия:

- ЛВС: клиент-сервер, одноранговая сеть;
- ГВС: маршрутизатор-маршрутизатор;
- удаленный доступ: удаленные клиенты и доступ из частных сетей через Интернет.

Всесторонняя защита

Данные должны быть защищены от перехвата, модификации или доступа посторонних лиц. Результатом сетевой атаки может быть простой компьютеров и разглашение секретной информации.

Стратегии зашиты сетей обычно предусматривают только предотвращение нападений извне. При этом используются брандмауэры, зашищенные маршрутизаторы (шлюзы защиты) и аутентификация удаленного доступа. Это называется «зашитой по периметру» и не спасает от нападений изнутри сети.

Методы защиты на уровне пользователей (смарт-карты, аутентификация по протоколу Kerberos версии 5) не позволяют обеспечить адекватную защиту против большинства атак на сетевом уровне, поскольку основаны исключительно на именах пользователей и паролях. Большинство систем являются многопользовательскими. В результате после завершения работы пользователи часто не отключаются от сети, что весьма небезопасно. Если злоумышленник похитит имя пользователя и пароль, зашита на уровне пользователя не предотвратит доступ атакующего к сетевым ресурсам.

Стратегии безопасности на физическом уровне защищают сетевой кабель от несанкционированного подключения и точки доступа к сети от использования. Тем не менее эти стратегии не гарантируют конфиденциальность информации при прохождении данных через несколько сетей (как это происходит в Интернете). Наилучшая защита данных обеспечивается сквозной моделью IPSec: отправитель шифрует данные перед тем, кап передать их по кабелю, а получатель расшифровывает информацию только после приема всех данных. В связи с этим протокол IPSec рекомендуется включить в план многоуровневой зашиты предприятия. Он обезопасит ваши частные данные в открытой среде, шифруя их. Использование IPSec в комбинации с тщательным контролем доступа, внешней защитой и защитой на физическом уровне гарантирует безопасность ваших данных.

Преимущества IPSec

В Windows 2000 протокол IPSec реализован прозрачно для пользователя. Для связи с применением протокола IPSec от пользователей не требуется подключение к одному домену. Они могут находиться в любом из доверенных доменов сети предприятия. Утилита IPSec Management позволяет централизовать администрирование. Администраторы домена создают для обычных сценариев связи политику зашиты. Эта политика, привязанная к политике домена, хранится в службе каталогов.

При регистрации в домене каждый компьютер автоматически загружает его политику защиты, что устраняет необходимость в настройке отдельных систем.

Протокол Windows 2000 IPSec обеспечивает следующие преимущества, позволяющие достичь высокого уровня безопасности связи при низкой цене использования:

- централизованное администрирование политики зашиты;
- прозрачность IPSec для пользователей и приложений;
- гибкость в настройке политики зашиты, что отвечает потребностям разных предприятий;
- наличие служб конфиденциальности, предотвращающих неавторизированный доступ к передаваемым по сети секретным данным;
- наличие служб аутентификации, проверяющих подлинность отправителя и получателя, что позволяет предотвратить использование подложных идентификационных сведений;
- шифрование каждого пакета с использованием информации о времени, что позволяет предотвратить перехват и последующую передачу данных (атаку повтора);
- высокая стойкость ключей и их динамическая смена в процессе коммуникации позволяют защититься от атак;
- безопасные сквозные каналы для пользователей частной сети в пределах одного домена или любого доверенного домена сети предприятия;
- безопасные сквозные каналы, основанные на IP-адресе, между удаленными пользователями и пользователями в любом домене предприятия.

Упрощенное развертывание

Для обеспечения безопасной связи при низкой стоимости владения Windows 2000 упрощает развертывание IPSec.

Интеграция с системой защиты Windows 2000

В качестве доверительной модели протокол IPSec использует безопасный домен Windows 2000. По умолчанию для идентификации и установления доверительных отношений между связывающимися компьютерами политика IPSec применяет обычный метод аутентификации Windows 2000 (аутентификация Kerberos V5). Компьютеры, являющиеся членами домена Windows 2000 или доверенного домена, могут легко создать защищенный канал связи с использованием протокола IPSec.

Централизованное администрирование политики IPSec на уровне Active Directory

Политика IPSec может назначаться через функции групповой политики службы Active Directory. Это позволяет назначить политику IPSec на уровне домена или организационного подразделения, что устраняет административную нагрузку по настройке отдельных компьютеров.

Прозрачность IPSec для пользователей и приложений

Надежная защита, предоставляемая протоколом IPSec, связана с тем, что он реализован на сетевом уровне модели OSI. Такая реализация (рис. 5-1) обеспечивает в стеке TCP/IP защиту протоколов верхнего уровня, например TCP, UDP, HTTP, и даже пользовательских протоколов, пересылающих трафик на уровне протокола IP. Основное преимущество низкоуровневой защиты — все приложения и услуги, использующие для передачи протокол IP, можно защитить средствами IPSec. Таким образом, IPSec — это более совершенная технология по сравнению с механизмами высокоуровневой защиты, например Secure Sockets Layer (SSL), которые действуют только на приложения, предназначенные для работы с ними. Если бы потребовалась защита всех приложений, каждое из них пришлось бы соответствующим образом модифицировать.

Рис. 5-1, Защита на сетевом уровне

Гибкая настройка защиты

Службы безопасности в пределах каждой полигики можно настроить для соответствия большинству требований защиты для сети и трафика данных.

Автоматическое управление ключами

Службы IPSec динамически управляют и обмениваются криптографическими ключами между сообщающимися компьютерами.

Автоматическое согласование параметров защиты

Службы IPSec динамически согласовывают взаимный набор требований защиты между сообщающимися компьютерами, в результате на каждом компьютере не надо задавать одну и ту же политику.

Поддержка инфраструктуры открытого ключа

Использование удостоверений с открытым ключом для аутентификации позволяет проверять подлинность и безопасно связываться с компьютерами, не относящимися к доверенному домену Windows 2000.

Поддержка общих ключей

Если аутентификация по протоколу Kerberos V5 или с использованием сертификатов открытого ключа невозможна, для аутентификации и установления доверительных отношений между сообщающимися компьютерами можно создать общий ключ (общий секретный пароль).

Работа протокола IPSec

Работа протокола IPSec описана ниже и проиллюстрирована на рис. 5-2.

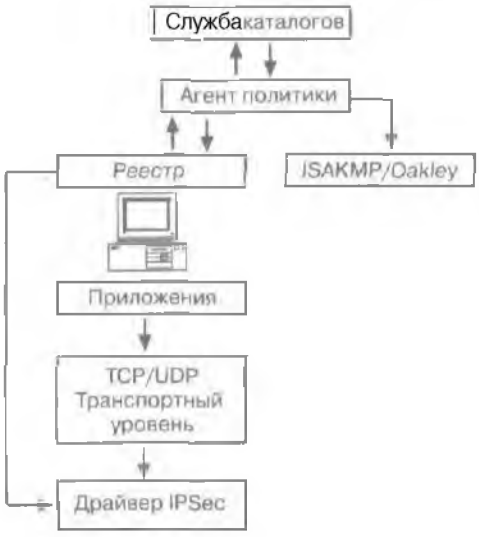


Рис. 5-2. Схема работы протокола IPSec

- Пакет IP сравнивается с IP-фильтром, являющимся частью политики IPSec.
- Политика IPSec может включать несколько дополнительных методов защиты. Драйверу IPSec требуется знать, какой метод использовать для защиты пакета. Для согласования метода и ключа защиты драйвер IPSec опрашивает Internet Security Association and Key Management Protocol (ISAKMP).
- ISAKMP определяет метод защиты и передает его вместе с ключом защиты драйверу IPSec.

- Метод и ключ становятся *сопоставлением безопасности* (security association, SA) IPSec. Драйвер IPSec сохраняет это SA в своей базе данных.
- Обоим сообщающимся компьютерам требуется шифровать или расшифровывать трафик IP, поэтому им необходимо знать и хранить SA.

Архитектура IPSec

Протокол IPSec реализован в Windows 2000 с использованием следующих компонентов:

- агента **политики** IPSec;
- службы ISAKMP/Oakley Key Management;
- драйвера IPSec;
- модели IPSec.

Агент политики IPSec

Это механизм IPSec, находящийся на каждом компьютере с Windows 2000. Агент политики автоматически загружается при запуске компьютера и через заданный в политике IPSec интервал времени выполняет определенные задачи (рис. 5-3).

1. Получает от службы Windows 2000 Active Directory назначенную компьютеру политику IPSec.
2. Если в службе каталогов политики IPSec нет или агент не может подключиться к этой службе, он пытается считать политику из системного реестра компьютера. Если политика IPSec отсутствует и в системном реестре, служба агента политики приостанавливается.
3. При наличии политики IPSec в службе каталогов агент передает ее на компьютер с использованием служб контроля целостности и шифрования данных.
4. Посылает сведения о политике драйверу IPSec, службе ISAKMP/Oakley, а также в системный реестр.

Рис. 5-3. Задачи, выполняемые агентом политики

Служба управления ключами ISAKMP/Oakley

Это механизм IPSec, находящийся на каждом компьютере с Windows 2000, Перед передачей IP-дейтаграмм между двумя компьютерами необходимо определить сопоставление безопасности — набор параметров, указывающий службы безопасности и механизмы (например, ключи и параметры защиты), применяемые для защиты коммуникаций.

ISAKMP централизует управление ассоциацией защиты, сокращая время, необходимое для установления соединения. Протокол Oakley генерирует реальные ключи, используемые для шифрования и дешифровки передаваемых данных. Служба ISAKMP/Oakley выполняет операцию, состоящую из двух этапов.

1. Устанавливает защищенный канал связи между двумя компьютерами. Для этого служба аутентифицирует сущности компьютеров и обменивается данными о ключах, чтобы создать общий секретный ключ, который будет использоваться при шифровании и дешифровке данных.
2. Определяет между двумя компьютерами сопоставление безопасности. Затем оно вместе с общим ключом передается драйверам IPSec обоих компьютеров.

Агент политики автоматически запускает службу ISAKMP/Oakley. Если служба агента не загружена, службу ISAKMP/Oakley невозможно запустить ни автоматически, ни вручную. Когда не удается согласовать безопасность, политику IPSec можно настроить для блокировки или приема незащищенных соединений.

Драйвер IPSec

Драйвер IPSec (IPSEC.SYS) находится на каждом компьютере с Windows 2000 и проверяет все IP-дейтаграммы на соответствие фильтрам из списка, заданного в политике защиты компьютера. Список фильтров определяет компьютеры и сети, требующие защищенных коммуникаций. Если дейтаграмма соответствует какому-либо фильтру, драйвер IPSec передающего компьютера шифрует данные с использованием SA и общего ключа и затем передает зашифрованную информацию на принимающий компьютер. Драйвер IPSec получающего компьютера расшифровывает присланные данные и передает их принимающему приложению.

Примечание Агент политики автоматически запускает драйвер IPSec.

Модель IPSec

На рис. 5-4 изображены два пользователя, работающие на компьютерах с Windows 2000 Server, подключенных к интрасети. На обоих компьютерах задана активная политика IPSec.

1. Алиса запускает на компьютере А FTP-приложение и передает данные Борису на компьютер Б.
2. Драйвер IPSec компьютера А, используя политику, записанную в системный реестр агентом политики, уведомляет службу ISAKMP/Oakley, что для установки связи необходим протокол IPSec.
3. Службы ISAKMP/Oakley компьютеров А и Б определяют обший ключ и согласование безопасности.
4. Драйверы IPSec компьютеров А и Б получают ключ и SA.
5. Драйвер IPSec компьютера А шифрует данные с использованием ключа и передает их на компьютер Б.
6. Драйвер IPSec компьютера Б расшифровывает данные и пересылает их конечному приложению, где их получает Борис.

Примечание Любые маршрутизаторы или коммутаторы на пути между взаимодействующими компьютерами должны участвовать только к пересылке зашифрованных IP-дейтаграмм адресату. Тем не менее, если между сообщающимися компьютерами имеется брандмауэр или другой шлюз зашиты, на нем следует включить пересылку IP-дейтаграмм или создать специальный фильтр, допускающий перенаправление зашифрованных IP-дейтаграмм.

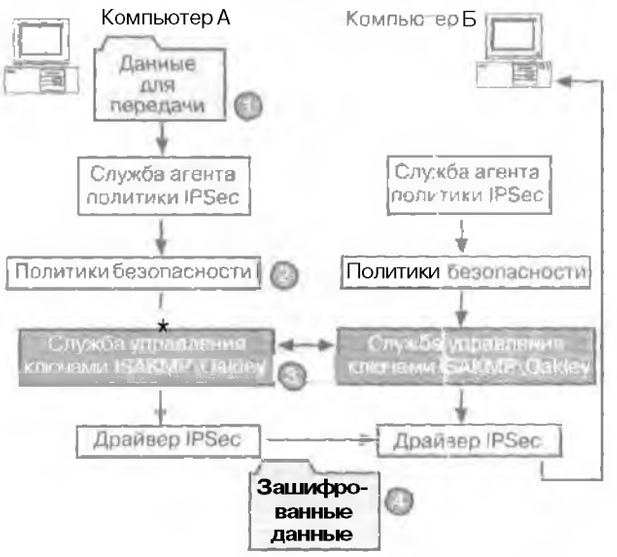


Рис. 5-4. Процесс шифрования данных, пересылаемых между компьютерами с использованием протокола IPSec

Когда следует использовать IPSec

Протокол IPSec шифрует исходящие пакеты, и это сказывается на производительности компьютеров. IPSec осуществляет симметричное шифрование сетевых данных, что очень эффективно. Тем не менее для серверов, поддерживающих множество параллельных сетевых подключений, издержки на шифрование весьма существенны, и поэтому перед внедрением IPSec проверьте, как сервер справится с шифрованием информации, сымитировав сетевой трафик. Кроме того, если для IP-безопасности вы используете аппаратные средства и программные продукты сторонних фирм, не поленитесь провести предварительное тестирование. Для каждого домена можно определить собственную политику IPSec, Политики IPSec позволяют:

- задать тип аутентификации и степень конфиденциальности для обмена данными между клиентами IPSec;
- определить самый низкий уровень безопасности, на котором допускается связь между клиентами с поддержкой IPSec;
- разрешить или заблокировать связь с клиентами, не поддерживающими IPSec;
- потребовать шифрования всех коммуникаций для обеспечения конфиденциальности. Кроме того, вы можете установить соединение без шифрования.

Вот в каких случаях рекомендуется реализовать протокол IPSec:

- одноранговые коммуникации в интрасети вашей организации, например, коммуникации внутри юридического отдела;

- клиент-серверные коммуникации для защиты секретной информации, хранящейся на серверах;
- удаленный доступ по телефонной линии или виртуальной частной сети (для VPN, использующих IPSec совместно с протоколом L2TP, не забудьте создать политики групп, чтобы разрешить автоматическую регистрацию сертификатов IPSec). Подробнее о сертификатах компьютеров для коммуникаций по VPN с использованием L2TP поверх IPSec рассказано в справочной системе Windows 2000;
- защищенные коммуникации «маршрутизатор-маршрутизатор» через ГВС.

Развертывая **защиту сети:**

- определите клиенты и серверы, которые будут использовать IPSec;
- определите, на чем будет основана аутентификация клиента — на доверительных отношениях Kerberos или на цифровых сертификатах;
- опишите все политики IPSec, включая правила и списки фильтров;
- опишите службы сертификатов, необходимые для аутентификации клиентов посредством цифровых сертификатов;
- опишите процессы и стратегии регистрации пользователей для получения сертификатов IPSec.

Резюме

IPSec — структура открытых стандартов для обеспечения частной, безопасной связи по IP-сетям с помощью криптографических служб безопасности. Протокол IPSec прозрачен для пользователей и обеспечивает надежную защиту коммуникации при низкой цене использования.

Архитектура IPSec включает четыре основных компонента; агент политики IPSec, службу управления ключами ISAKMP/Oakley, драйвер IPSec и модель IPSec.

Занятие 2. Настройка IPSec

Для создания и настройки политики IPSec применяется консоль управления. Консоль можно сконфигурировать для централизованного (через Active Directory), локального или удаленного управления политикой компьютера. На этом занятии мы расскажем о настройке протокола IPSec. Кроме того, вы создадите тестовую политику безопасности IP.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о внедрении **IPSec;**
- ✓ настроить политику IPSec;
- ✓ описать различные окна свойств политики IPSec, метода аутентификации, фильтрования IP-пакетов, действий фильтров, а также рассказать о дополнительных задачах IPSec.

Продолжительность занятия - около 30 минут.

Требования к внедрению IPSec

На компьютерах вашей сети должна быть установлена политика IPSec, соответствующая политике защиты сети. Компьютеры одного домена можно организовать в группы и применять политику IPSec к этим группам. Разрешается на компьютерах в различных доменах задавать дополнительные политики IPSec для защиты сетевых коммуникаций.

Внедрение IPSec

Политику IPSec по умолчанию можно просмотреть в оснастке Group Policy (Групповая политика). Политики отображаются в узле IP Security Policies, который расположен в подузле Computer Configuration\ Windows Settings\Security Settings\IP Security Policies (Конфигурация компьютера\Конфигурация Windows\ Параметры безопасности\Политики безопасности IP).

Кроме того, для просмотра политики IPSec можно воспользоваться оснасткой IP Security Policy Management (Управление политикой безопасности IP). Каждая политика IPSec основывается на правилах, определяющих порядок ее применения. Щелкните значок политики правой кнопкой мыши и в контекстном меню выберите команду Properties. На вкладке Rules (Правила) перечислены правила политики. Правила можно разделить на списки фильтров, действия фильтров и дополнительные свойства. Оснастка по умолчанию запускается из меню Administrative Tools и позволяет конфигурировать политику только для локального компьютера. Для централизованного управления политиками нескольких компьютеров добавьте в консоль оснастку IP Security Management.

Настройка политики IPSec:

В первом окне отображаются три предопределенные политики: Client (Respond Only) [Клиент (только ответ)], Secure Server (Require Security) [Безопасность сервера (требовать безопасность)] и Server (Request Security) [Сервер (запрос безопасности)]. По умолчанию ни одна из этих политик не включена (рис. 5-5).

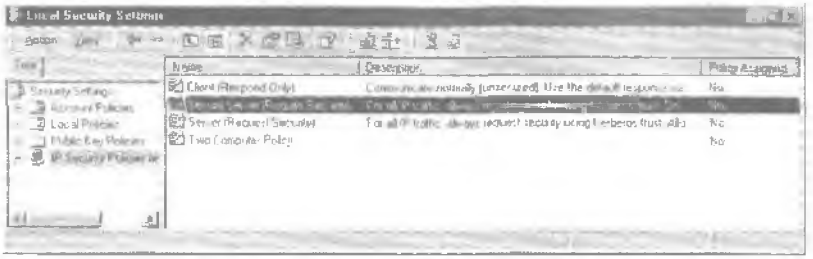


Рис. 5-5. Консоль MMC рядового сервера Windows 2000

Политики по умолчанию не изменяются независимо от того, является ли политика IPSec локальной или хранится в Active Directory как часть политики группы. В этом примере политика IPSec является локальной политикой рядового сервера.

- Политика Client (Respond Only) допускает связь без шифрования данных, но отвечает на запросы IPSec и не отвергает попытки согласовать параметры безопасности. Для аутентификации используется протокол Kerberos V5.
- Политика Server (Request Security) заставляет сервер каждый раз устанавливать защищенную связь. Если с данным компьютером связь пытается установить клиент, не поддерживающий IPSec, сеанс будет разрешен.
- Политика Secure Server (Require Security) требует доверительных отношений Kerberos для всех IP-пакетов, посланных с этого компьютера, за исключением широковещательных и многоадресных пакетов, а также пакетов протокола Resource Reservation Setup Protocol (RSVP) и службы ISAKMP. Данная политика не позволяет устанавливать незащищенную связь с клиентами. В итоге все клиенты, подключающиеся к серверу с политикой IPSec, должны поддерживать IPSec.

Чтобы отредактировать политику, щелкните ее значок правой кнопкой и в контекстном меню выберите команду Properties.

Примечание Одновременно может использоваться лишь одна политика. Если одна и та же политика IPSec назначена в нескольких перекрывающихся группах, действует обычная иерархия групповых политик.

Типы подключений

Вкладка Connection Type (Тип подключения) доступна в диалоговом окне Edit Rule Properties (Свойства: Изменить правило) (рис. 5-6). Кроме того, она отображается в мастере создания правила.

Примечание Все параметры политики можно настраивать средствами различных мастеров; они включены по умолчанию.

Выбор типа подключения для отдельных правил определяет, на какие подключения (через сетевые адаптеры или модемы) распространяется политика IPSec. У каждого правила есть свойство подключения, указывающее, применяется ли правило к ЛВС-подключениям, удаленным подключениям или всем сетевым подключениям.

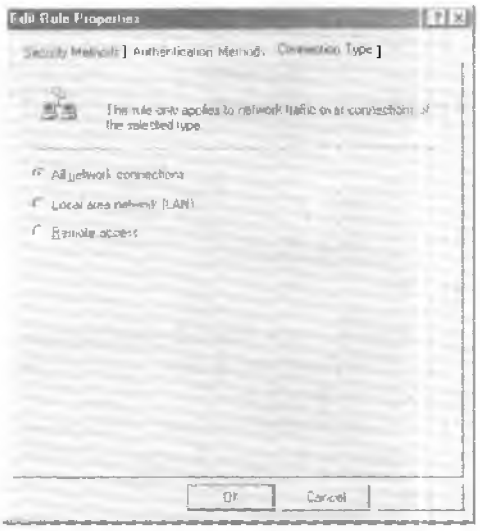


Рис. 5-6. Диалоговое окно свойств правила

Способ проверки подлинности

Определяет порядок проверки подключающихся пользователей и компьютеров. Windows 2000 поддерживает три способа проверки подлинности (рис. 5-7).

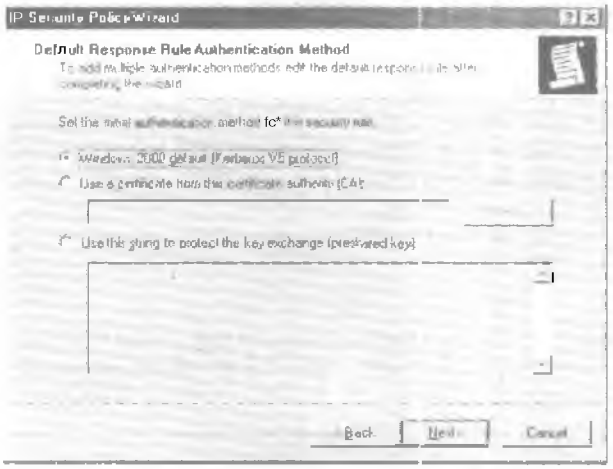


Рис. 5-7. Окно Default Response Rule Authentication Method (Способ проверки подлинности правила отклика по умолчанию)

- **Аутентификация по протоколу Kerberos V5** — используется по умолчанию. При подключении компьютера к доверенному домену протокол Kerberos выдает билет иди виртуальное удостоверение сущности. Этот метод применяется для любых клиентов с установленным протоколом Kerberos V5 (независимо от платформы клиента), состоящих в доверенном домене.
- **Сертификаты** — этот метод требует наличия минимум одного доверенного центра сертификации (ЦС). Windows 2000 поддерживает сертификаты X.509 версии 3, в том чис-

ле сертификаты, создаваемые коммерческими центрами сертификации. Правило может включать несколько методов аутентификации. Это гарантирует, что при согласовании параметров зашиты с клиентом будет найден общий метод.

- Общий ключ — секретный и предварительно согласованный двумя пользователями ключ. Данный метод прост в использовании и не требует, чтобы на клиентской системе выполнялся протокол Kerberos или имелся сертификат. Для применения общего ключа на обоих компьютерах требуется вручную настроить IPSec. Это простой метод аутентификации автономных систем, а также компьютеров, работающих под управлением ОС, отличных от Windows.

Примечание Ключ, полученный при аутентификации, используется *исключительно* для аутентификации: для шифрования или подтверждения подлинности данных он *не* применяется.

Для каждого правила можно определить один или несколько методов аутентификации. Все сконфигурированные методы отображаются в списке в порядке предпочтения. Если первый метод нельзя использовать, предпринимается попытка применить следующий.

Фильтрование пакетов IP

IPSec распространяется на принимаемые и передаваемые пакеты. Исходящие пакеты проверяются на соответствие заданным фильтрам и по результатам сравнения шифруются, блокируются или передаются открытым текстом. Входящие пакеты также проверяются на соответствие фильтрам, и по результатам сравнения производится обмен параметрами безопасности, пакет блокируется или пропускается в систему.

Отдельные фильтры группируются в список, что позволяет группировать и управлять сложными шаблонами трафика как единым именованным списком фильтров, например, «Файловые серверы здания *1*» или «Блокируемый трафик». Списки фильтров при необходимости могут совместно использовать разные правила IPSec одной или разных политик IPSec. Спецификации фильтров устанавливаются отдельно для входящего и исходящего трафика.

- Фильтры входа, распространяющиеся на входящий трафик, позволяют получателю сравнивать трафик со списком фильтров IP, отвечать на запросы об установлении защищенной связи, а также сравнивать трафик с имеющимся соглашением безопасности и расшифровывать защищенные пакеты.
- Фильтры выхода, применяемые к исходящему трафику, вызывают согласование параметров защиты, необходимое для отсылки трафика.

Внимание! Хотя фильтры входа и выхода создаются и используются в списке фильтров, из интерфейса пользователя неясно, какой именно фильтр создается. Тип фильтра определяется адресами отправителя и получателя трафика.

Должен существовать фильтр, покрывающий все сценарии трафика, к которым применяются связанные правила. Фильтр содержит параметры, описанные ниже.

1. Исходный и конечный адрес IP-пакета. Как показано на рис. 5-8, при создании и редактировании фильтра можно определить следующие параметры:
   - My IP Address (Мой IP-адрес) — IP-адрес локальной машины;
   - Any IP Address (Любой IP-адрес) — следует указывать единичный адрес. Протокол IPSec не поддерживает групповые и широковещательные адреса;
   - A Specific IP Address (Определенный IP-адрес) — специфический IP-адрес в локальной сети или в Интернете;

- A Specific IP Subnet (Определенная подсеть IP) — любой IP-адрес в заданной подсети IP.

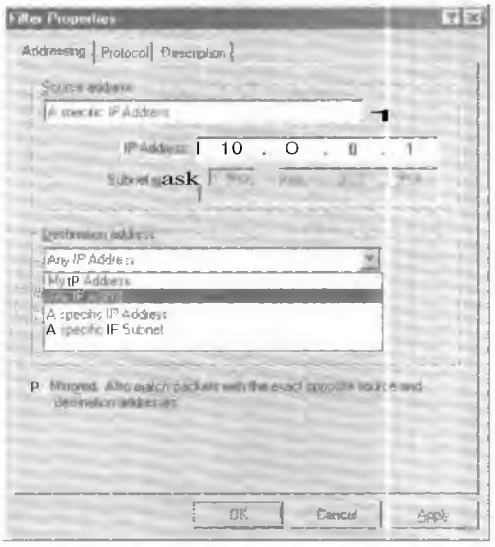


Рис. 5-8. Вкладка Addressing (Адресация) окна свойств фильтра

Примечание IPSec заполняет поле My IP Address только первым привязанным адресом, Если на компьютере установлено несколько сетевых адаптеров, IPSec будет использовать только один из IP-адресов. Клиенты RRAS считаются многоадресными, поэтому IPSec может задать IP-адрес неверно.

2. Протокол, по которому передается пакет. По умолчанию устанавливается такое значение параметра, при котором фильтр покрывает все клиентские протоколы пакета TCP/IP.
В табл. 5-1 перечислены протоколы, доступные на вкладке Protocol (Протокол) диалогового окна свойств фильтра.

Табл. 5-1. Фильтрование протокола

Тип протокола	Описание
ANY	Любой протокол
EGP	Exterior Gateway Protocol
HMP	Host Monitoring Protocol
ICMP	Internet Control Message Protocol
Other	Неопределенный протокол, основанный на номере протокола IP
RAW	Чистые данные поверх IP
RDP	Reliable Datagram Protocol
RVD	MIT Remote Virtual Disk
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XNS-IDP	Xercx NS IDP

3. Исходный и конечный порт протокола для TCP и UDP. По умолчанию устанавливается такое значение параметра, при котором фильтр покрывает все порты. Впрочем, можно указать номер специфического порта.

Задайте свойства фильтра, отредактировав или создав его. Для глобального управления фильтрами следует на управляемом компьютере щелкнуть правой кнопкой в левой панели оснастки. Кроме того, для управления фильтрами можно воспользоваться страницами свойств правил отдельных политик. Мастер создания фильтра позволяет настроить свойства фильтра.

Отражение

Позволяет фильтру сверить пакет с противоположными исходным и конечным адресами. Например, фильтр выхода, у которого исходный адрес задан как IP-адрес, а конечный адрес — как второй компьютер, автоматически создаст фильтр входа, у которого второй компьютер будет указан в качестве исходного адреса, а IP-адрес передающего компьютера — в качестве конечного.

Рис. 5-9. Вкладка Protocol (Протокол) окна свойств фильтра

Примечание Отраженный фильтр не перечислен в списке фильтров. Вместо этого в диалоговом окне свойств фильтра помечается флажок Mirrored (Отраженный).

Если необходимо, чтобы компьютер А всегда безопасно обменивался данными с компьютером Б:

- для пересылки защищенных данных на компьютер Б политика IPSec компьютера А должна включать спецификацию фильтра для любых исходящих пакетов, отсылаемых на компьютер Б;
- для получения защищенных данных с компьютера А политика IPSec компьютера Б должна включать спецификацию фильтра для любых входящих пакетов, присылаемых с компьютера А. Кроме того, на компьютере Б может быть задана политика, в которой активно правило ответа, используемое по умолчанию;
- отражение позволяет компьютерам обмениваться данными без создания специальных фильтров.

Действие фильтра

Определяет, что предпринимает система защиты при срабатывании фильтра: следует ли блокировать или разрешить трафик или согласовать параметры безопасности для данного подключения. Согласование включает поддержку *только* подлинности и целостности данных с использованием протокола *заголовка аутентификации* (authentication header, AH) или поддержку целостности и конфиденциальности данных с использованием протокола Encapsulating Security Payload (ESP). Действие фильтра можно изменять в соответствии с вашими потребностями, что позволяет администратору определить протоколы, требующие подлинности, и протоколы, требующие конфиденциальности.

Можно задать одно или несколько согласованных действий фильтра. Как показано на рис. 5-10, действия фильтра отображаются *к* виде списка, упорядоченного по приоритету. Если согласовать действие фильтра нельзя, система переходит к следующему из заданных действий.

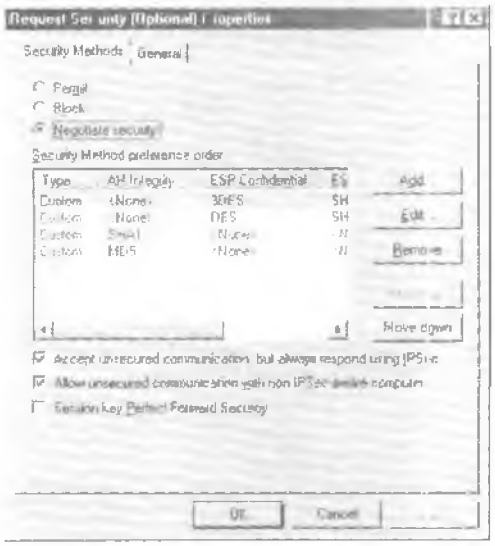


Рис. 5-Ю. Свойства политики Secure Initiator Negotiation

Кроме того, вместо создания пользовательского метода защиты можно выбрать высокий или средний уровень безопасности. При высоком уровне обеспечиваются шифрование и целостность данных. Средний уровень безопасности гарантирует только целостность данных.

Дополнительные задачи IPSec

Чтобы просмотреть дополнительные задачи **IPSec,** щелкните значок IP Security Policy в левой панели правой кнопкой и выберите в контекстном меню команду All Tasks (Все задачи).

- Manage **IP Filter Lists and Filter actions (Управление списками IP-фильтра и действиями** фильтра). Администратор может настраивать фильтры и действия фильтров отдельно от конкретных правил. После создания правила разрешается активировать фильтры и их действия (рис. 5-11).

Рис. 5-11. Вкладка Rules (Правила) окна свойств политики

- Check Policy Integrity (Создать политику безопасности IP). Поскольку Active Directory использует в качестве новейших сведений последние сохраненные данные, при редактировании политики несколькими администраторами возможно нарушение связей между ее компонентами. Например:

  Политика А использует фильтр А

  Политика Б использует фильтр Б

  Это означает, что фильтр А связан с политикой А, а фильтр Б связан с политикой Б.

  Предположим, что Борис отредактировал политику А и добавил правило, использующее фильтр В.

  В это же время Алиса с другого компьютера редактирует политику Б и добавляет правило, также использующее фильтр В.

  Если Алиса и Борис одновременно сохранят изменения, фильтр В может оказаться снизанным и с политикой А, и с политикой Б; тем не менее это маловероятно. Если же политика А будет сохранена последней, она перезапишет ссылку фильтра В на политику Б. Фильтр В будет связан только с политикой А. Это вызовет проблемы в будущем, при изменении фильтра В, так как пользователи политики А получат новые изменения, а пользователи политики В — нет.

  Проверка целостности политики устраняет эту проблему. Проверяются связи во всех политиках IPSec. Рекомендуется выполнить проверку целостности после изменений в политике. Ниже перечислены другие дополнительные возможности IPSec:

- Restore Default Policies (Восстановить политики по умолчанию) — восстанавливает первоначальную конфигурацию политики;
- Import Policies (Импортировать политики) — позволяет импортировать политику с другого компьютера сети;
- Export Policies (Экспортировать политики) — позволяет экспортировать политику на другой компьютер сети.

Практикум: тестирование IPSec

Вы попробуете активировать встроенную политику IPSec и посмотрите, как она блокирует связь, когда передаваемую информацию нельзя защитить. Если оба компьютера с Windows 2000 Server являются членами одного или доверенного защищенного домена Windows 2000 Server, политику IPSec можно использовать для быстрого установления защищенной связи. В противном случае для тестирования вам потребуется создать на каждом компьютере собственную политику IPSec.

► Задание 1: проверьте связь с другим компьютером

1. Запустите утилиту ping, указав IP-адрес другого компьютера.

   Если вы получите четыре отклика, значит вы можете связаться с вашим партнером.

► Задание 2: добавьте IPSec в консоль MMC

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Local Security Policy (Локальная политика безопасности).
2. В дереве консоли выберите IP Security Policies On Local Machine (Политики безопасности IP на «Локальный компьютер»).
3. В правой панели щелкните правой кнопкой значок Secure Server (Require Security) и выберите в контекстном меню команду Properties.
4. В окне свойств щелкните кнопку Add (Добавить).

   Откроется окно мастера правил безопасности.
5. Щелкните кнопку Next.
6. В окне Tunnel Endpoint (Конечная точка туннеля) щелкните Next.
7. В окне Network Type (Тип сети) щелкните Next.
8. В окне Authentication Method (Метод проверки подлинности) щелкните переключатель Use This String To Protect The Key Exchange (Preshared Key) (Использовать данную строку для защиты обмена ключами). Введите в поле ниже MSPRESS и щелкните Next.
9. Щелкните переключатель All IP Traffic (Весь IP-трафик), затем щелкните Next.
10. Щелкните переключатель Require Security (Требовать безопасность), затем щелкните Next.
11. Щелкните кнопку Finish (Готово), чтобы закрыть окно мастера.
12. Теперь, после того как вы добавили жесткий список фильтров, отключите все фильтры по умолчанию.
13. Закройте диалоговое окно Secure Server (Require Security) Properties.
14. Щелкните правой кнопкой значок Secure Server (Require Security) и выберите в контекстном меню команду Assign (Назначить).
15. Запустите утилиту Ping, указав адрес второго компьютера.

    Обратите внимание, что опрос не был успешным.
16. Чтобы связь по сети стала возможной, отключите политику Secure Server (Require Security) с помощью контекстного меню.

Резюме

В Windows 2000 имеется три предопределенные политики — Client (Respond Only), Secure Server (Require Security) и Server (Request Security). Их можно в любое время изменить или удалить. Кроме того, вы можете добавить собственную политику. IPSec позволяет Windows 2000 поддерживать различные методы аутентификации компьютеров и обеспечивать фильтрование IP-пакетов, предоставляя компьютерам возможность устанавливать и отклонять соединения, основываясь на многочисленных правилах и фильтрах.

Занятие 3. Настройка политики и правил IPSec

Протокол IPSec легко настраивается с помощью политик и правил. На этом занятии рассказывается, как этими средствами защитить сеть, принимая во внимание прокси-серверы, трансляцию сетевых адресов (NAT), протокол Simple Network Management Protocol (SNMP), протокол Dynamic Host Configuration Protocol (DHCP), DNS, службу Windows Internet Name Service (WINS), контроллеры домена и т. д.

Изучив материал этого занятия, вы сможете:

- ✓ описать политику и правила IPSec;
- ✓ описать процесс настройки IPSec для работы с брандмауэрами, NAT и прокси-серверами;
- ✓ рассказать об использовании IPSec для защиты сети, включающей контроллеры доменов или протоколы SNMP, DHCP, DNS и WINS.

Продолжительность занятия — около 40 минут.

Защита, основанная на политике

Для защиты связи стали требоваться мощные криптографические методы, но они увеличивают нагрузку по администрированию. Протокол IPSec снижает такую нагрузку, предоставляя возможность администрирования на основе политики. Администратор, отвечающий за защиту сети, вправе настроить политику IPSec для соответствия требованиям безопасности пользователя, группы, приложения, домена, сайта или всего предприятия. В Windows 2000 имеется административный интерфейс. IPSec Policy Management, позволяющий создавать политики IPSec для отдельных компьютеров и их групп в пределах Active Directory.

Политика IPSec

Именованный набор правил и параметров обмена ключами. Политику IPSec можно назначить как политику безопасности домена или отдельного компьютера. При входе в домен компьютер домена автоматически наследует политику IPSec, назначенную домену. Если компьютер не подключен кдомену (например изолированный сервер), политика IPSec хранится и считывается из системного реестра компьютера.

Это обеспечивает большую гибкость в настройке политики зашиты для групп сложных компьютеров или отдельных компьютеров со специфическими требованиями. Например, можно определить единую политику защиты для всех пользователей одной сети или всех пользователей из конкретного отдела. Для создания политик IPSec на рядовых серверах Windows 2000 применяется оснастка IPSec Management (рис. 5-12).

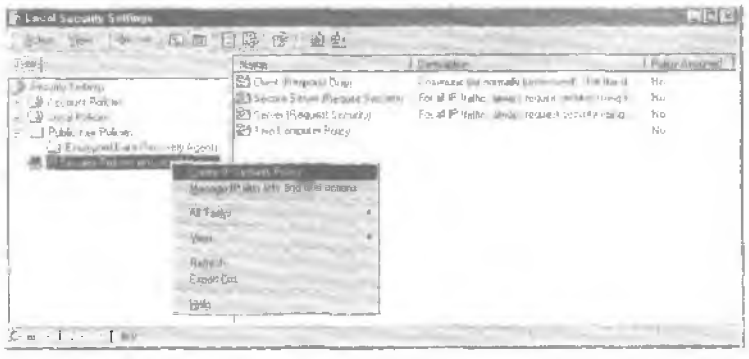


Рис. 5-12. Политики безопасности рядового сервера Windows 2000

Правила

Определяют порядок использования протокола IPSec. Правило содержит список фильтров IP и задает действия, предпринимаемые системой безопасности в случае соответствия пакета определенному фильтру. Правило — это набор:

- IP-фильтров;
- политик согласования параметров связи;
- методов аутентификации;
- атрибутов IP-туннелирования;
- типов адаптеров.

Каждая политика защиты может включать несколько правил. Это позволяет назначать одну политику IPSec нескольким компьютерам с различными сценариями связи. Например, одна политика распространяется на всех пользователей отдела или сети, однако для установки связи может требоваться множество правил: одно будет управлять связью по интрасети, другое — коммуникациями через Интернет, требующими туннелирования, и т. д.

IP-фильтры и спецификации фильтров

Все правила основаны на соответствии пакетов IP-фильтрам. У каждого правила может быть только один активный IP-фильтр. Драйвер IPSec проверяет каждую IP-дейтаграмму на соответствие активному фильтру. При соответствии выполняется действие, определенное в связанном правиле.

Спецификации фильтров

IP-дейтаграммы проверяются на соответствие каждой спецификации фильтра. Спецификации фильтра включают следующие свойства:

- исходный и конечный адрес IP-дейтаграммы, основанный на IP-адресе, имени DNS, определенной сети или подсети;
- протокол — TCP или UDP;
- номера исходного и конечного портов, используемых протоколами TCP и UDP.

Методы защиты и политика согласования

Уровень защиты связи определяется методами зашиты и политикой согласования.

Методы защиты

Каждый метод защиты определяет уникальный уровень зашиты связи. Чтобы повысить вероятность нахождения двумя компьютерами общего метода защиты, в политику согласования параметров связи можно включать несколько методов защиты. Служба ISAKMP/Oakley на каждом компьютере перебирает список методов зашиты в порядке убывания, пока не находит общий метод. Вы можете использовать предопределенный или собственный метод зашиты связи.

- **Высокая степень защиты.** Протокол IP ESP обеспечивает конфиденциальность, целостность и аутентификацию данных, а также защиту против атак повтора.
- **Средняя степень зашиты.** Протокол защиты IP AH обеспечивает целостность и аутентификацию данных, а также зашиту против атак повтора. Конфиденциальность данных не обеспечивается.
- **Настраиваемая зашита.** В дополнение к выбору между ESP и AH опытные пользователи могут сами определить алгоритмы аутентификации, целостности и конфиденциальности данных.

Политика согласования

Это именованный набор методов зашиты. У каждого правила может быть одна активная политика согласования параметров связи. Если два компьютера не могут выбрать общий метод защиты, политику согласования стоит настроить для отказа от связи с другим компьютером или для пересылки данных без шифрования.

Поскольку IPSec не затрагивает исходный заголовок IP, зашифрованные пакеты считаются обычным IP-трафиком и маршрутизируются соответствующим образом. Это верно для режимов как транспортировки, так и туннелирования.

ESP и маршрутизаторы

ESP не шифрует и не аутентифицирует заголовок IP, оставляя его неискаженным. Даже в туннельном режиме, когда первоначальный заголовок IP шифруется, маршрутизация не создает проблем. Для маршрутизации пакета между конечными точками туннеля применяется новый туннельный заголовок IP (оставляемый неискаженным). По достижении точки-адресата пакет аутентифицируется и расшифровывается. Исходный IP-пакет доставляется конечному адресату без аутентификации или шифрования IPSec.

AH и маршрутизаторы

На основе всех полей заголовка IP-пакета протокол AH создает *контрольное значение целостности* (integrity check value, ICV).

Поскольку при пересылке пакетов маршрутизаторы корректируют поля заголовка IP, это может вызывать определенные проблемы. Тем не менее поля, которые могут быть изменены, для вычисления ICV обнуляются. Таким образом, маршрутизаторы иногда изменяют непостоянные поля (время жизни, контрольная сумма и т. д.), не влияя на вычисление ICV. На компьютере-получателе протокол IPSec снова обнуляет изменяемые поля и затем вычисляет контрольную сумму целостности.

Это также верно и для туннельного режима, когда для вычисления ICV используется новый туннельный заголовок IP, а переменные поля обнуляются. На конечном компьютере хеш проверяется, и исходный пакет IP пересылается без дальнейшей аутентификации.

IPSec и брандмауэры

Любые маршрутизаторы или коммутаторы на пути данных между сообщающимися компьютерами лишь переправляют зашифрованные и/или аутентифицированные IP-пакеты к месту назначения. Тем не менее при наличии брандмауэра или фильтрующего маршрутизатора необходимо разрешить перенаправление IP-пакетов для:

- **протокола IP с идентификатором 51 — для пропуска AH-трафика требуется задать фильтры входа и выхода;**
- **протокола IP с идентификатором 50 — для пропуска ESP-трафика требуется задать фильтры входа и выхода;**
- порта номер 500 протокола UDP — для пропуска ISAKMP-трафика требуется задать фильтры входа и выхода.

Помните, что указанные фильтры необходимо определять для пропуска трафика протокола IPSec через брандмауэр только при использовании транспортного режима или в случае, если брандмауэр находится на открытой стороне туннельного сервера. IPSec нельзя использовать таким образом, чтобы брандмауэр применял данный протокол ко всем входящим и исходящим пакетам. Маршрутизатору потребуется создать и поддерживать все SA, связанные с каждым подключением.

Примечание Стандартное фильтрование трафика брандмауэром (фильтрование по портам TCP или UDP) неприменимо к трафику ESP, поскольку номера портов шифруются.

IPSec, NAT и прокси-серверы

IPSec невозможно использовать через NAT или прикладной прокси-сервер. Хотя заголовок IP не изменяется, шифрование и аутентификация не позволяют вносить изменения в другие поля пакета.

NAT

Далее обсуждается, почему протокол IPSec не работает через NAT.

Невозможность различать множественные потоки данных IPSec

Заголовок ESP содержит *индекс параметров защиты* (security parameters index, SPI). Этот индекс используется вместе с адресом назначения IP, присутствующим в стандартных заголовках IP и IPSec, для идентификации сопоставления безопасности IPSec.

В исходящем трафике со шлюза NAT конечный IP-адрес не меняется; тем не менее изменяется исходный IP-адрес. Во входящем трафике на шлюз NAT исходный IP-адрес должен быть привязан к частному IP-адресу. Для корректной работы IPSec также должен быть привязан SPI. Хотя такую привязку и можно осуществить, это потребует корректировки поля индекса параметров защиты. Если поле SPI изменится, ICV станет недостоверным.

Это справедливо и для AH, поскольку индекс параметров зашиты является частью AH и применяется для вычисления ICV.

Невозможность изменять контрольные суммы TCP и UDP

Заголовки UDP и TCP содержат контрольную сумму, включающую исходный и конечный IP-адреса стандартного заголовка IP. Изменение адресов в стандартном заголовке IP сделает недействительной контрольную сумму в заголовках TCP и UDP. Таким образом, NAT не может обновлять заголовки UDP и TCP, поскольку они находятся в зашифрованной части ESP или используются при вычислении ICV.

Прикладные прокси-серверы

Работают на прикладном уровне, поэтому должны поддерживать IPSec и иметь согласование безопасности для каждого клиента IPSec. Это, безусловно, нерационально и не обеспечивается прикладными прокси-серверами.

Прочие рекомендации по настройке IPSec

Здесь приводятся дополнительные рекомендации по настройке IPSec, включая защищенные коммуникации с использованием SNMP и управление службами сервера, такими, как DNS и WINS.

Защита SNMP

Все системы с поддержкой SNMP необходимо сконфигурировать для использования IPSec. Как минимум вам следует настроить политику IPSec таким образом, чтобы она допускала незащищенные коммуникации, если на всех компьютерах с поддержкой SNMP *нельзя* включить поддержку IPSec. В противном случае при установлении защищенного соединения произойдет сбой, и обмен сообщениями SNMP не будет осуществлен.

IPSec не шифрует протокол SNMP автоматически. Единственное исключение — предопределенные политики Secure Initiator и Lockdown, настроенные для автоматической защиты трафика SNMP. Чтобы защитить трафик протокола SNMP, добавьте на компьютере с поддержкой SNMP к новой или имеющейся политике две пары фильтров.

Первая пара предназначается для типичного трафика SNMP (сообщения SNMP) и состоит из одной спецификации фильтра входа и одной спецификации фильтра выхода.

▶ **На вкладке Addressing (Адресация) диалогового окна свойств фильтра**

1. С помощью списка Source address (Адрес источника пакетов) задайте IP-адрес системы управления SNMP.
2. В списке Destination address (Адрес назначения пакетов) выберите My IP Address (Мой IP-адрес) — этот адрес будет преобразован в IP-адрес компьютера, которому назначена политика (агент SNMP).
3. Пометьте флажок Mirrored (Отраженный) для автоматического создания фильтра выхода.

▶ На вкладке **Protocol (Протокол) диалогового окна свойств фильтра**

1. Выберите тип протокола — TCP или UDP (если необходимы оба протокола, создайте дополнительную спецификацию фильтра).
2. В полях From This Port (Пакеты из этого порта) и To This Port (Пакеты на этот порт) введите 161.

Второй набор спецификаций фильтров предназначается для сообщений-ловушек SNMP и включает одну спецификацию входящего фильтра входа и одну спецификацию исходящего фильтра.

▶ **На вкладке Addressing**

1. С помощью списка Source address укажите IP-адрес системы управления SNMP.
2. В списке Destination address выберите My IP Address — этот адрес будет преобразован в IP-адрес компьютера, которому назначена политика (агент **SNMP).**
3. Пометьте флажок Mirrored для автоматического создания фильтра выхода.

▶ **На вкладке Protocol**

1. Выберите тип протокола — TCP или UDP (если необходимы оба протокола, создайте дополнительную спецификацию фильтра).
2. В полях From This Port и To This Port введите **162.**

Система управления или консоль SNMP должны также поддерживать IPSec. Служба SNMP в Windows 2000 поддерживает, но в настоящий момент не включает в себя программное обеспечение для управления протоколом SNMP. Для защиты трафика SNMP с помощью **IPSec** ПО сторонних фирм для управления SNMP должно поддерживать IPSec.

Серверы DHCP, DNS и WINS или контроллеры домена

При включении протокола IPSec на любых серверах, где выполняются указанные службы, определите, все ли клиенты поддерживают IPSec. Убедитесь в совместимости политик, особенно в совместимости параметров аутентификации и согласования. В противном случае согласование безопасности может пройти неудачно, и клиентам не удастся обращаться к сетевым ресурсам.

Когда DNS не поддерживает IPSec

Чтобы в списке фильтров IP можно было указывать DNS-имя компьютера, а не его IP-адрес, в случае если серверы DNS не поддерживают IPSec, необходимо специальным об-

разом настроить политику. Иначе IPSec не сможет преобразовывать DNS-имена компьютеров в действительные IP-адреса. Фильтр требуется настроить так, чтобы трафик между компьютером и сервером DNS не шифровался с использованием IPSec.

Добавьте спецификацию фильтра к соответствующей политике и правилу.

▶ **На вкладке Addressing**

1. В списке Source address выберите My IP Address.
2. С помощью списка Destination address укажите IP-адрес сервера DNS.
3. Пометьте флажок Mirrored для автоматического создания фильтра выхода.

▶ **На вкладке** Protocol

1. В полях From This Port и To This Port введите 53 (это стандартный порт, используемый большинством серверов DNS для связи; укажите здесь любой порт, который служба DNS использует для пересылки трафика).

Кроме того, для данного правила политику согласования следует задать как Do Not Allow Secure Communication: No security methods be configured. Это гарантирует, что DNS-трафик не будет шифроваться с использованием IPSec.

Параметры TCP/IP

Если компьютер, являющийся членом домена, отключится от домена, копия параметров IPSec домена считывается из реестра компьютера. Если компьютер не является членом домена, в системном реестре будет храниться локальная политика fPScc. Параметры TCP/IP позволяют компьютеру, не входящему в домен, использовать IPSec всегда, использовать IPSec по возможности и вообще не использовать IPSec.

Примечание Если компьютер подключен к домену, настройка параметров TCP/IP невозможна.

Практикум: **создание пользовательской** политики **IPSec**

Windows 2000 предоставляет вам для изучения несколько встроенных политик. Тем не менее в большинстве случаев при развертывании IPSec требуется создать собственную политику. Сейчас вы сформируете собственную политику IPSec. Данное упражнение следует выполнять на двух компьютерах.

▶ **Задание 1: создайте собственную политику IPSec**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык Local Security Policy.
2. В левой панели щелкните правой кнопкой значок IP Security Policy On Local Machine.
3. В контекстном меню выберите команду Create IP Security Policy (Создать политику безопасности IP).
4. После запуска мастера щелкните кнопку Next, чтобы продолжить.
5. Введите имя политики. Two Computer **Policy** и щелкните Next.
6. В окне Requests For Secure Connection (Запросы безопасного соединения) не снимайте флажок Default Response Rule (Использовать правило по умолчанию) и щелкните Next.
7. Оставьте способ проверки подлинности по умолчанию для аутентификации по протоколу Kerberos и щелкните Next.
8. Убедитесь, что помечен флажок Edit Properties (Изменить свойства).
9. Щелкните кнопку Finish, чтобы завершить начальную настройку.

10. Откроется окно свойств: *не закрывайте его!*

На данный момент вы еще не создали собственное правило, а лишь настроили свойства правила ответа, используемого по умолчанию.

Опишите назначение правила ответа по умолчанию.

Далее вы будете настраивать политики IPSec вручную, с помощью диалоговых окон и вкладок, без использования мастеров.

► **Задание 2: добавьте новое правило**

1. В нижней части диалогового окна свойств сбросьте флажок Use Add Wizard (Использовать мастер).
2. На вкладке Rules окна свойств щелкните кнопку Add (Добавить).
3. Откроется окно свойств нового правила.

Вы настроите фильтры для обмена данными между компьютерами. Сейчас вы создадите фильтр выхода, указав IP-адрес своего компьютера в качестве исходного адреса и IP-адрес второго компьютера в качестве конечного адреса. Функция отражения автоматически создаст входящий фильтр, подставив соответствующие адреса компьютеров.

► **Задание** 3: добавьте новый **фильтр**

1. Щелкните кнопку Add. Откроется диалоговое окно IP Filter List (Список фильтров IP).
2. В поле Name (Имя) введите имя фильтра — **Host A-Host B Filter.**
3. Сбросьте флажок Use Add Wizard (Использовать мастер).
4. Щелкните кнопку Add.
5. Откроется окно свойств фильтра.
6. В поле Source Address введите конкретный IP-адрес.
7. Добавьте IP-адрес своего компьютера.
8. В поле Destination Address введите конкретный IP-адрес.
9. Добавьте IP-адрес второго компьютера.
10. Щелкните OK и проверьте, добавлен ли ваш фильтр в список Filters (Фильтры) диалогового окна IP Filter List.
11. Щелкните кнопку Close (Закрыть).
12. На вкладке IP Filter List (Список фильтров IP) активизируйте новый фильтр, щелкнув переключатель, расположенный рядом с только что добавленным списком фильтров.

В предыдущем задании вы создали входящий и исходящий фильтры для пакетов связи. Л теперь вы определите действия, предпринимаемые в отношении фильтруемых пакетов.

► **Задание 4: задайте** действие фильтра

1. Перейдите на вкладку Filter Action (Действие фильтра) и сбросьте флажок Use Add Wizard.
2. Щелкните кнопку Add, чтобы задать действие фильтра.
3. Убедитесь, что на вкладке Security Methods (Методы безопасности) помечен флажок Negotiate Security (Согласовать безопасность).
4. Убедитесь, что флажок Allow Unsecured Communication With Non IPSEC Aware Computer (Разрешать связи с компьютерами, не поддерживающими IPSEC) сброшен.
5. Щелкните кнопку Add, чтобы выбрать метод защиты.
6. Выберите Medium (AH) (Средняя безопасность) и щелкните OK.
7. Щелкните OK, чтобы закрыть диалоговое окно задания действия фильтра.
8. Щелкните переключатель, расположенный рядом с созданным фильтром, чтобы активизировать его.

Далее вы зададите порядок установки доверительных взаимоотношений между двумя компьютерами, указав метод аутентификации, который будет использоваться при г опыт-

ке определения соглашения безопасности. Вы воспользуетесь готовым ключом — словом или фразой, которую должны знать оба компьютера для реализации доверительных взаимоотношений. Данный ключ не применяется для шифрования данных и в процессе согласования параметров связи для того, чтобы определить, установят компьютеры доверительные отношения или нет.

▶ Задание 5: выберите метод аутентификации

1. Перейдите на вкладку Authentication Methods (Методы проверки подлинности).
2. Щелкните кнопку Add.
3. Щелкните переключатель Pre-Shared Key (Использовать данную строку для зашиты обмена ключами).
4. Введите в текстовом поле готовый ключ или пароль и щелкните OK.
5. Выберите в списке Pre-Shared Key (Общий ключ) и щелкните кнопку Move Up (Вверх), чтобы данный элемент стал первым.

▶ Задание 6: проверьте параметры туннеля

1. Перейдите на вкладку Tunnel Setting (Параметры туннеля).
2. Убедитесь, что выбран переключатель This Rule Does Not Specify An IPSEC Tunnel (Это правило не указывает туннель IPSEC).

▶ Задание 7: проверьте параметры типа подключения

1. Перейдите на вкладку Connection Type (Тип подключения).
2. Убедитесь, что выбран переключатель All Network Connections (Все сетевые подключения).

▶ Задание 8: завершите создание правила

1. Щелкните кнопку Close, чтобы вернуться к окну свойств политики и завершить создание правила.
2. Убедитесь, что в списке помечено ваше новое правило.
3. Закройте окно свойств политики.

▶ Задание 9: активизируйте новую политику

1. В правой панели консоли управления щелкните значок политики Two Computer Policy правой кнопкой.
2. Щелкните кнопку Assign (Назначьте).
3. В столбце Policy Assigned (Назначенная политика) теперь должно значиться Yes (Да),

▶ Задание 10: протестируйте IPSec

1. Включите политику на обоих компьютерах.
2. Запустите утилиту Ping, указав адрес второго компьютера.
3. Первый опрос обычно проходит неудачно, поскольку на согласование политик требуется время.
4. После того как на компьютерах активируются идентичные политики, вы сможете успешно выполнять тестовые опросы.
5. Включите и отключите политику на одном из компьютеров, чтобы посмотреть, что происходит, если политики не одинаковы,

Резюме

IPSec очень просто настроить с помощью политик и правил. Вы научились защищать сеть их средствами, принимая во внимание прокси-серверы, NAT, протоколы SNMP и DHCP, службы DNS, WINS, контроллеры домена и т. д.

Занятие 4 Мониторинг IPSec

Выяснить, как политики и правила протокола IPSec применяются в вашей сети, можно путем мониторинга IPSec. На этом занятии описаны различные утилиты, предназначенные для этого, — IPSECMON.EXE, Event Viewer. Performance Monitor, Network Monitor и др.

Изучив материал этого занятия, вы сможете:

- ✓ устранить проблемы с IPSec средствами IPSECMON EXE. Event Viewer, Network Monitor или файлов IPSECPA.LOG и OAKLEY.LOG.

Продолжительность занятия — около 30 минут.

Средства управления и устранения проблем IPSec

Здесь описываются утилиты управления и устранения проблем IPSec, доступные в Windows 2000.

Утилиты управления IPSec

- Оснастка IP Security Policy Management применяется для создания и редактирования политик (кроме того, можно воспользоваться утилитой Group Policy Editor).
- Утилита IP Security Management по умолчанию доступна в меню Start\Programs\Administrative Tools.

Средства мониторинга и устранения проблем

Утилита IP Security Monitor (IPSECMON.EXE, рис. 5-13), запускаемая из командной строки, выполняет мониторинг сопоставлений безопасности IP, интервалов смены ключей, ошибок согласования и прочей статистики протокола IP Security.

Статистика IPSec

IP Security Monitor позволяет фиксировать следующую статистику IPSec:

- **Active Associations** (Активные сопоставления) — счетчик активных сопоставлений безопасности;
- **Confidential Bytes Sent/Received** [Послано/получено байт (секретных)] — общее число байт, переданных/полученных по протоколу ESP;
- **Authenticated Bytes Sent/Received** [Послано/получено байт (проверенных)] — общее число байт, переданных/полученных по протоколу AH;
- **Bad Packets** (Сбойных пакетов SPI) — общее число пакетов с неверным SPI. Как мы уже говорили. SPI позволяет сравнивать входящие пакеты с SA. Если SPI неверен, это может означать, что входящее SA истекло, но прибыл пакет, использующий старый SPI. Значение данного счетчика может увеличиваться, если интервалы смены ключей слишком малы и имеется большое количество SA. Поскольку срок действия SA в большинстве случаев истекает, пакет с неверным SPI необязательно указывает на ошибки работы IPSec;

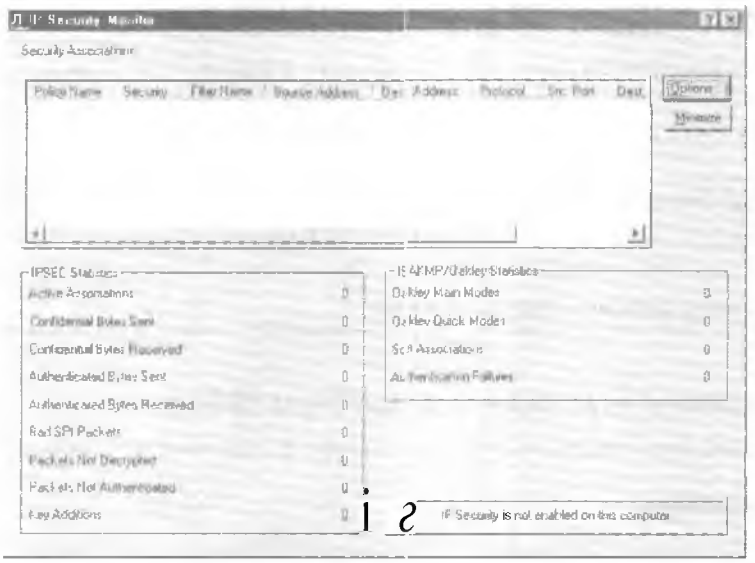


Рис. 5-13. Утилита IP Security Monitor (Монитор IP-безопасности)

- **Packets Not Decrypted** (Незашифрованных пакетов) — общее число пакетов, которые не удалось расшифровать. Как и в случае с пакетами, имеющими неверные SPI, невозможность дешифровки пакета может указывать, что прибыл пакет, для которого истек срок действия SA. При этом также истекает срок действия ключа сеанса, используемого для расшифровки пакета. Невозможность дешифровки не обязательно указывает на ошибки работы IPSec;
- Packets Not Authenticated (Непроверенных пакетов) — общее число пакетов, содержащих данные, которые не удалось проверить. Наиболее вероятная причина этого — истечение срока действия SA;
- **Key Additions** (Дополнения по ключам) — общее число ключей, переданных службой **ISAKMP** драйверу IPSec. Значение данного счетчика отражает общее количество успешных согласований на втором этапе.

Статистика ISAKMP/Oakley

IP Security Monitor позволяет фиксировать следующую статистику ISAKMP/Oakley:

- **Oakley Main** Modes (Главные режимы Oakley) — общее число SA службы ISAKMP, созданных в процессе согласований на первом этапе;
- **Oakley Quick Modes** (Быстрые режимы Oakley) — общее число SA протокола IPSec, созданных в процессе согласований на первом этапе. Поскольку срок окончания действия этих SA может быть разным, значение данного счетчика не обязательно соответствует значению счетчика Oakley Main Modes;
- Soft **Associations** («Мягкие» сопоставления) — общее число согласований на втором этапе, в результате которых данные передавались открытым текстом. Обычно значение данного счетчика отражает число согласований, определенных с участием компьютеров, не поддерживающих IPSec;
- **Authentication Failures** (Сбой проверки подлинности) — общее число ошибок аутентификации сущностей (выполняется по протоколу Kerberos с применением пользовательских сертификатов и определяемых вручную паролей). Значение данного счетчика не аналогично значению счетчика Packets Not Authenticated, который отображает сведения об аутентификации сообщений посредством хеширования.

Примечание Чтобы обнулить значение статистических данных IP Security Monitor, перезапустите агент IP Security Policy Agent.

Performance Monitor включает объекты и счетчики IPSec. Ниже перечислены события, которые можно зарегистрировать и затем проанализировать с помощью Event Viewer:

- события агента политики и драйвера IPSec в системном журнале;
- события Oakley в журнале приложений;
- события ISAKMP (сведения о SA) в журнале зашиты (если включен аудит входа в систему).

Использование Network Monitor

Network Monitor — полезная утилита для устранения проблем IPSec. И ограниченная версия, поставляющаяся с Windows 2000 Server, и полная версия, входящая в состав Microsoft Systems Management Server версии 2.0, включают синтаксические анализаторы для службы ISAKMP и протоколов AH/ESP. Network Monitor перехватывает всю информацию, пересылаемую по сетевому интерфейсу в данный момент времени.

Network Monitor версии 2.0 включает анализаторы для пакетов IPSec. Если протокол IPSec шифрует пакеты, виден только сам пакет, но не его содержимое. Если используется лишь аутентификация пакетов, будут видны и пакет и его содержимое. ESP отображается как протокол IP с номером 50 (десятичное число), а AH — как протокол IP с номером 51 (десятичное число). Служба ISAKMP/Oakley отображается как порт протокола UDP номер 500 (десятичное число).

Примечание Поскольку данные протокола ESP зашифрованы, прочитать их невозможно.

Практикум: просмотр незашифрованного трафика с помощью Network Monitor

Вы перехватите и просмотрите данные, пересылаемые по кабелю между компьютерами. Network Monitor версии 2.0 включает анализаторы для пакетов IPSec и ISAKMP. Network Monitor получает пакет после протокола IPSec, так что, если протокол зашифрует пакет, содержимое последнего не будет видно.

Примечание Данный практикум следует выполнять на обоих компьютерах. Выполняйте следующее задание на них поочередно.

▶ **Задание: просмотрите пакеты целостности IPSec (в формате AH)**

1. Запустите Network Monitor и установите сеть перехвата на MAC-адрес сетевой платы, соединяющей компьютер со второй системой.

   Примечание Для просмотра MAC-адреса сетевого адаптера запустите утилиту ipconfig с параметром /all.

2. В оснастке Local Security Settings назначьте политику Two Computer Policy (созданную в практикуме занятия 3).
3. Начните перехват пакетов с помощью Network Monitor.
4. Запустите утилиту ipsecmon.
5. Запустите утилиту ping, указав IP-адрес второго компьютера.

6. Вам, вероятно, придется повторить это действие, поскольку у ping очень короткое время ожидания, а для определения сопоставления безопасности IPSec между двумя компьютерами требуется определенное время.
7. Остановите и просмотрите записи Network Monitor.
8. Просмотрите ipsecmon.
9. Дважды щелкните первый пакет ICMP.
10. Обратите внимание, что отображаются строки, содержащие заголовки кадра, Ethernet, IP и AH.
11. В области подробных сведений разверните запись IP.
12. Запишите номер протокола IP.

Прокрутите окно подробностей IP вниз и щелкните IP Data: Number Of Data Bytes Remaining = 64 (0x0040). Обратите внимание, что полезные данные IP приведены открытым текстом.

IPSec создал ICV на основе полей IP, ICMP и Data кадра.

Это позволяет IPSec предотвратить перехват данных, их изменение и вторичную отправку плохих данных. Посмотрев на панель Hex, вы увидите еще 32 символа, посланных ping. Используя метод защиты AH, вы гарантируете аутентификацию, но не обеспечиваете шифрование данных пакета. AH лишь предотвращает изменения данных пакета и большей части заголовка IP, например исходного и конечного IP-адресов. В следующем практикуме вы просмотрите пакеты, использующие метод защиты ESP, который шифрует содержимое пакета IP.

Практикум: просмотр зашифрованного трафика с помощью Network Monitor

Вы воспользуетесь Network Monitor, чтобы настроить шифрование ESP и просмотреть зашифрованные пакеты.

► Задание 1: настройте шифрование ESP

1. Отмените политику Two Computer Policy.
2. Переключитесь в режим редактирования, щелкнув значок политики Two Computer Policy правой кнопкой и выбрав в контекстном меню команду Properties.
3. Перейдите вкладку Filter Action.
4. Измените активное действие фильтра.
5. Щелкните кнопку Edit, чтобы скорректировать метод безопасности.
6. Выберите High (ESP).
7. Закройте все диалоговые окна.
8. Назначьте политику Two Computer Policy.

► Задание 2: просмотрите зашифрованные (ESP) пакеты IPSec

1. Начните перехват пакетов с помощью Network Monitor.
2. Запустите утилиту ipsecmon.
3. Запустите утилиту ping, указав IP-адрес второго компьютера.
4. Вам, вероятно, придется повторить это действие, поскольку у ping очень короткое время ожидания, а для определения сопоставления безопасности IPSec между двумя компьютерами требуется определенное время.
5. Остановите и просмотрите записи Network Monitor.
6. Просмотрите ipsecmon.
7. Дважды щелкните кадр ESP.
8. В правой панели отобразятся четыре записи — Frame, Ethernet, IP и ESP. IPSec создал хеш полей ICMP и Data кадра.

9. Разверните раздел IP и запишите протокол IP.
10. Прокрутите окно подробностей IP вниз и щелкните IP Data: Number Of Data Bytes Remaining — 76 (0x004C). Взглянув на панель Hex, вы увидите, что данные зашифрованы.

Практикум: использование диагностических утилит

Вы воспользуетесь диагностической утилитой IPSec Monitor, чтобы проверить, активен ли протокол IPSec, и просмотреть активные SA.

Использование IPSec Monitor

В Windows 2000 Server имеется утилита мониторинга протокола IPSec под названием IPSecmon. Она позволяет просматривать «мягкие» и «жесткие» SA локальных и удаленных компьютеров. IPSecmon не отображает отказавшие SA и другие фильтры.

В меню Start выберите команду Run и затем наберите **ipsecmon [*имя_компьютера*]** Для каждой мягкой или жесткой SA в окне отображается одна строка. Столбец слева, озаглавленный Policy Name (Имя политики), — это имя политики, которая была назначена и выполняется на компьютере. В столбце Negotiation Policy указывается метод защиты, выбранный в процессе согласования параметров связи. Сделана попытка разрешить исходный и конечный IP-адреса в имена DNS.

Кроме того, здесь приведена полная статистическая информация, собираемая с момента последнего запуска компьютера. Обязательно обратите на нее внимание,

- Успешные сопоставления безопасности IPSec первоначально вызовут один главный и один быстрый режимы Oakley. Операции обновления ключей обычно отражаются как дополнительные быстрые режимы.
- Слева отображается общее число принятых/переданных конфиденциальных (ESP) или аутентифицированных (ESP и AH) байт для всех «жестких» SA. Поскольку ESP обеспечивает и конфиденциальность, и аутентификацию данных, увеличиваются значения на обоих счетчиках. Так как AH обеспечивает лишь аутентификацию данных, увеличивается только значение на счетчике переданных аутентифицированных байт.
- Справа отображается общее число «мягких» SA.

► **Задание: убедитесь, активен ли IPSec, и просмотрите активные SA**

1. В Control Panel щелкните значок Network and Dial-Up Connections (Сеть и удаленный доступ к сети).
2. Щелкните значок Local Area Connection (Подключение по локальной сети) правой кнопкой и выберите в контекстном меню команду Properties.
3. Выберите Internet Protocol (TCP/IP), затем щелкните кнопку Properties.
4. Щелкните кнопку Advanced (Дополнительно).
5. Перейдите на вкладку Options (Параметры), выберите IP Security (IP-безопасность) и щелкните кнопку Properties.

   Если компьютер использует локальную политику, ее имя отобразится в поле Use This IP Security Policy. Если используется политика, назначенная через механизмы групповой политики из Active Directory, поля будут недоступны, а имя назначенной политики отобразится в том же поле.

Резюме

Вы научились просматривать используемые в сети политики и правила IPSec средствами таких утилит, как IPSECMON.EXE и Network Monitor. Данные утилиты позволяют вести мониторинг и разрешать проблемы со связью IPSec в сети.

Закрепление материала

? Приведенные ниже вопросы помогут нам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Какая организация стандартизовала протокол IPSec?

2. Опишите отличия криптографии с секретным и открытым ключом.

3. Назовите функции службы ISAKMP/Oakley.

4. Что включает в себя правило?

5. Когда надо исполыовать сертификат открытого ключа?

6. Для чспо применяется IP-фильтр?

ГЛАВА 6

Разрешение имен узлов в сети

В этой главе

В сети и клиент, и сервер должны разрешать удобные для пользователя имена узлов в IP-адреса, применяемые для взаимодействия компьютеров в сети. В этой главе рассказано, как протокол TCP/IP разрешает имена узлов. Это надо знать, если вы проектируете сеть и выбираете механизм разрешения имен и IP-адресов. Расширенные возможности разрешения имен, такие, как *доменная система имен* (Domain Name System, DNS) и *служба имен Интернета для Windows* (Windows Internet Name Service, WINS), будут рассмотрены в следующих главах.

Прежде всего

Для изучения материалов этой главы необходимо:

- изучить главу 2.

Занятие 1. Схемы именования TCP/IP

Протокол IP работает с 32-разрядными IP-адресами узла-источника и узла-приемника, которые трудно запоминать. Человеку гораздо удобнее использовать и запоминать имена, а не IP-адреса. Например, намного проще запомнить www.microsoft.com, чем IP-адрес, связанный с этим Web-узлом. Если имя служит псевдонимом IP-адреса, необходимо обеспечить уникальность этого имени и правильно сопоставить ему соответствующий IP-адрес.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить различные схемы именования, используемые узлами.

Продолжительность занятия — около 10 минут.

Схемы именования Windows 2000

Windows 2000 поддерживает несколько различных типов разрешения имен, включая DNS, WINS, широковещательное разрешение имен и разрешение имен с использованием файлов HOSTS и LMHOSTS. Microsoft Windows 2000 и другие узлы, например UNIX, применяют разные схемы именования. С узлом Windows 2000 может быть связано имя, используемое с приложениями TCP/IP. Узлам UNIX требуется только IP-адрес; указывать имя узла или домена не обязательно.

Для работы в сети каждому узлу TCP/IP надо присвоить IP-адрес. Впрочем, схема именования влияет на то, как обращаются к узлу,

- Например, чтобы выполнить команду NET USE между двумя компьютерами с Windows 2000, пользователь может выбрать, каким образом указать имя компьютера.

  Любой из следующих вариантов верен:

  net use x: *имя_NetBIOS\ресурс*

  net use x: \\10.1.3.74*ресурс*

  net use x: *host.domain.com\ресурс*

  Перед тем как протокол ARP сопоставит IP-адрес аппаратному адресу, имя NetBIOS или имя узла должно быть разрешено в IP-адрес. Если используется IP-адрес, разрешения имени не требуется.

- Чтобы сослаться на узел UNIX, использующий TCP/IP, клиент указывает либо IP-адрес, либо имя узла. Если применяется имя узла, оно разрешается в IP-адрес. Если используется IP-адрес, разрешение имени не требуется, и IP-адрес сопоставляется аппаратному адресу.

Резюме

Узлы Windows 2000 и UNIX могут обозначаться IP-адресом либо именем узла. Windows 2000 и другие сетевые ОС Microsoft также поддерживают имена NetBIOS.

Занятие 2, **Имя узла**

Имя узла упрощает процесс обращения к нему, потому что людям проще запомнить текстовые имена, чем IP-адреса. Имена узлов используются практически во всех средах TCP/IP. На этом занятии рассказано, как работает разрешение имен узлов.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить, как имя узла сопоставляется IP-адресу с помощью файла **HOSTS;**
- ✓ объяснить, как имя узла разрешается в IP-адрес на сервере DNS.

Продолжительность **занятия** — около 20 минут.

Понятие имени узла

Разрешение имени узла — это процесс определения IP-адреса узла по его имени. Имя узла представляет собой псевдоним, присваиваемый IP-узлу и идентифицирующий его в TCP/IP-сети. Имя узла может быть длиной до 255 символов и содержать алфавитно-цифровые символы, дефисы и точки. Одному узлу разрешается присвоить несколько имен.

Программы Windows Sockets (Winsock), например Internet Explorer и служебная программа FTP, могут использовать для обозначения узла, к которому выполняется подключение, любое из двух значений: IP-адрес или имя узла. Если применяется IP-адрес, то необходимость в разрешении имени отпадает. Если же указывается имя узла, то для установления IP-соединения с ресурсом нужно сначала разрешить имя узла в IP-адрес.

Имена узлов могут иметь различные формы. Две наиболее популярные формы — понятное имя и доменное имя. Понятное имя — это псевдоним IP-адреса, назначаемый отдельными пользователями. Доменное имя — это структурированное имя в иерархическом пространстве имен DNS, например www.microsoft.com.

Назначение имени узла

Имя узла — это псевдоним, заданный компьютеру администратором для идентификации узла TCP/IP. Имя узла не обязательно должно совпадать с NetBIOS-именем компьютера; его длина — до 255 символов, и оно состоит из букв и цифр. Один и тот же узел может иметь несколько имен.

Понятное имя узла упрощает обращение пользователя к узлу TCP/IP, его легче запомнить, чем IP-адрес. В сущности, имя узла разрешается применять вместо IP-адреса при использовании утилиты ping или других приложений TCP/IP.

Имя узла всегда соответствует IP-адресу, который содержится в файле HOSTS или в БД на сервере DNS. Клиентам Windows во многих случаях разрешается преобразовывать имена узлов в имена NetBIOS и обратно посредством сервера WINS или файла LM HOSTS.

Утилита hostname может показать имя узла, присвоенное вашей системе. В Windows 2000 по умолчанию имя узла совпадает с именем компьютера.

Разрешение имени узла

Это процесс сопоставления имени узла IP-адресу. Перед тем как IP-адрес разрешается в аппаратное имя, необходимо привязать имя узла к IP-адресу.

В Windows 2000 это делается следующими методами.

- Разрешение имен NetBIOS. NetBIOS определяет интерфейс и протоколы управления и передачи данных сеансового уровня. Для взаимодействия с узлами NetBIOS используется

регистрация имени, освобождение имени и обнаружение имени. Разрешение имени NetBIOS подразумевает сопоставление NetBIOS-имени компьютера его IP-адресу. Способ разрешения имен NetBIOS зависит от конфигурации сети и включает кэш имен NetBIOS, сервер имен NetBIOS, локальное широковещание, файл LMHOSTS, файл HOSTS и DNS.

- **Разрешение имен с помощью файла HOSTS.** Это текстовый файл, хранящийся локально в системе и содержащий имена узлов и соответствующие им IP-адреса (см. также главу 7).
- **Разрешение имен с использованием сервера DNS.** Сервер DNS — это централизованная БД, работающая в режиме реального времени и применяемая в IP-сети для разрешения *полных доменных имен* (fully qualified domain name, FQDN) и других имен узлов в IP-адреса. Windows 2000 также использует DNS-сервер и предоставляет службу DNS-сервера.

Microsoft TCP/IP применяет для разрешения имен узлов любой из способов, перечисленных в табл. 6-1 и 6-2.

Табл. 6-1. Стандартные способы разрешения имен

Стандартный способ разрешения имен	Описание
Локальное имя узла	Заданное компьютеру имя узла; сравнивается с именем целевого узла
Файл HOSTS	Локальный текстовый файл такого же формата, как файл \etc\HOSTS в UNIX. Этот файл сопоставляет имена узлов IP-адресам и обычно применяется для разрешения имен узлов 15 TCP/IP-приложениях
DNS-сервер	Сервер, который поддерживает БД с привязками имен к их IP-адресам

Табл. 6-2. Способы разрешения имен в ОС производства Microsoft

Способ разрешения имен	Описание
Сервер имен NetBIOS	Сервер, реализованный согласно RFC 1001 и 1002 для разрешения компьютерных имен NetBIOS. В продуктах Microsoft это WINS
Локальное широковещание	Широковещание в локальной сети в поисках IP-адресов, соответствующих NetBIOS-именам
Файл LMHOSTS	Локальный текстовый файл, проецирующий IP-адреса на компьютерные NetBIOS-имена узлов Windows

Разрешение имен NetBIOS

Имя NetBIOS — это уникальный 16-разрядный адрес, идентифицирующий ресурс NetBIOS в сети. В процессе разрешения имя NetBIOS преобразуется в IP-адрес. Например, имя NetBIOS используется службой файлов и принтеров для сетей Microsoft на компьютерах с Windows 2000. При загрузке компьютера эта служба регистрирует уникальное имя NetBIOS, основанное на имени компьютера. Компьютеры с протоколом TCP/IP могут использовать разрешение имен локальным широковещанием. Компьютер делает широковещательную рассылку на уровне IP для регистрации своего имени и объявления его в сети. Компьютеры в области широковещания должны соответствующим образом реаги-

ровать на попытки зарегистрировать повторяющееся имя и запросы своего зарегистрированного имени.

Разрешение имен с помощью файла HOSTS

Процесс разрешения имени с использованием файла HOSTS проиллюстрирован на рис. 6-1.

1. Разрешение имени начинается, когда пользователь вызывает WinSock-приложение, указывая имя узла, а не IP-адрес.
2. Windows 2000 проверяет, совпадает ли указанное имя с локальным именем узла. Если эти имена разные, то анализируется файл HOSTS. Если в нем содержится запрошенное имя узла, оно разрешается R IP-адрес.

   Если имя узла не может быть разрешено и никакие другие способы разрешения невозможны, например DNS, сервер имен NetBIOS или файл LMHOSTS, не сконфигурированы, процесс останавливается, и пользователь получает сообщение об ошибке.
3. После разрешения имени узла в IP-адрес производится попытка разрешить IP-адрес целевого узла в аппаратный адрес узла.

   Если целевой узел находится в локальной сети, ARP получает его аппаратный адрес, обратившись в кэш ARP или путем широковещания IP-адреса этого узла. Если целевой узел находится в удаленной сети, ARP получает аппаратный адрес маршрутизатора, который затем перенаправляет запрос целевому узлу.

Рис. 6-1. Сопоставление IP-адреса целевого узла его аппаратному адресу

Разрешение имен с использованием сервера DNS

Сервер DNS — это централизованная база данных, работающая в режиме реального времени, которая применяется в IP-сети для разрешения имен узлов в IP-адреса. Windows 2000 Professional может работать как клиент DNS, а семейство Windows 2000 Server включает службы сервера DNS. Разрешение доменного имени с использованием сервера DNS очень похоже на использование файла HOSTS.

Разрешение имен с использованием сервера DNS производится в два этапа (рис. 6-2).

1. Когда пользователь вводит команду, указывая FQDN или имя узла, то сначала запускается процесс разрешения имени через файл HOSTS. Если IP-адрес не может быть разрешен этим способом, то посылается запрос к серверу DNS, чтобы он разыскал имя узла в БД и сопоставил ему IP-адрес.

   Если DNS-сервер не отвечает на запрос, то направляются дополнительные запросы с интервалом в 1, 2, 2 и 4 секунды. Если DNS-сервер не отвечает на эти пять запросов и

нет никаких других способов разрешения, например посредством сервера имен NetBIOS или файла LMHOSTS, то процесс останавливается, и выдается сообщение об ошибке.

2. После разрешения имени узла ARP получает его аппаратный адрес. Если целевой узел находится в локальной сети, ARP получает его аппаратный адрес, обращаясь в кэш ARP или путем широковещания его IP-адреса. Если целевой узел находится в удаленной сети, то ARP получает аппаратный адрес маршрутизатора, который может перенаправить целевому узлу запрос адреса.

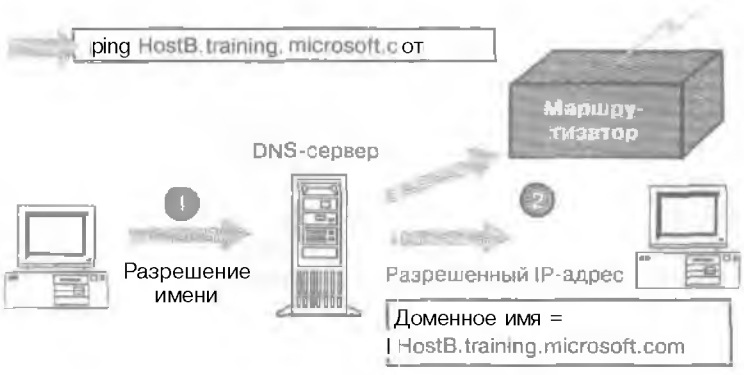


Рис. 6-2. Разрешение имени с использованием сервера DNS

Способы разрешения имен, предлагаемые Microsoft

Windows 2000 можно также настроить для разрешения имен через сервер имен NetBIOS, широковещание или файл LMHOSTS, Если сконфигурированы WINS и LMHOSTS, разрешение выполняется в следующем порядке (рис. 6-3).

1. "Когда пользователь вводит команду, указывая имя узла, Windows 2000 проверяет, не является ли оно локальным. Если это так, имя разрешается и команда выполняется без обращения в сеть.
2. **Если указанное имя узла не** является **локальным** именем **узла,** анализируется файл **HOSTS. После нахождения в** нем имени узла **оно разрешается в IP-адрес.**
3. Если имя узла не может быть разрешено через файл HOSTS, исходный узел посылает запрос указанным для него серверам доменных имен. После нахождения имени узла DNS-сервером оно разрешается в IP-адрес.
4. Если DNS-сервер не может разрешить имя узла, исходный узел проверяет локальный кэш имен NetBIOS перед выполнением трех попыток связаться с сервером имен NetBIOS. Если имя узла найдено в кэше имен NetBIOS или на сервере имен NetBIOS, оно разрешатся в IP-адрес.
5. Если имя узла не может быть разрешено сервером имен NetBIOS, исходный узел генерирует три широковещательных сообщения в локальной сети. После нахождения имени узла в локальной сети оно разрешается в IP-адрес.
6. Если имя узла не разрешено после использования широковещания, анализируется локальный файл LMHOSTS. Если имя узла находится в файле LMHOSTS, оно разрешается в IP-адрес.

   Если ни один из этих методов не разрешил имя узла, единственный способ наладить связь с другим узлом — явно указать его IP-адрес.

Рис. 6-3. Резервные способы разрешения имен

Резюме

Имя узла используется для указания TCP/IP-узла или шлюза по умолчанию. Разрешение имени узла — это процесс сопоставления имени узла IP-адресу, чтобы затем ARP смог разрешить IP-адрес в аппаратный адрес узла.

Занятие 3. Файл HOSTS

Теперь, когда вы получили общее представление о способах разрешения имен узлов, вы изучите файл HOSTS и настроите файл HOSTS для корректного разрешения имен узлов.

Изучив материал этого занятия, вы сможете:

- ✓ сконфигурировать и использовать файл HOSTS.

Продолжительность занятия — около 15 минут.

Общие сведения о файле HOSTS

Файл HOSTS — это статический текстовый файл, используемый для сопоставления имен узлов IP-адресам. Этот файл совместим с файлом HOSTS операционной системы UNIX. Файл HOSTS используется утилитой PING и другими приложениями TCP/IP для разрешения имени узла в IP-адрес. Также этот файл применяется для разрешения имен NetBIOS.

Файл HOSTS должен быть на каждом компьютере. Каждая его запись состоит из IP-адреса и соответствующего ему одного или нескольких имен узлов. По умолчанию в файле HOSTS содержится запись для узла с именем localhost. Этот файл анализируется при любых ссылках на имя узла. Имена узлов в файле читаются последовательно. Наиболее часто используемые имена следует располагать в начале файла.

Примечание Файл HOSTS можно редактировать в любом текстовом редакторе. Он расположен в каталоге \systemroot\System32\Drivers\Etc. Каждая запись ограничена длиной в 255 символов, регистр букв не учитывается.

На рис. 6-4 показан пример файла HOSTS.

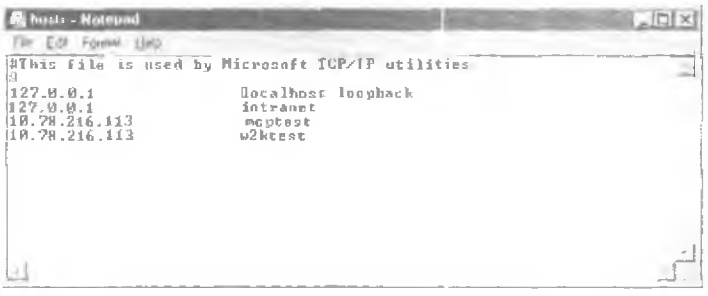


Рис. 6-4. Файл HOSTS

Файл HOSTS имеет несколько особенностей.

- Несколько имен узлов могут соответствовать одному IP-адресу. Для обращения к серверу с IP-адресом 172.16.94.97 достаточно указать его полное доменное имя (rhino.microsoft.com) или мнемоническое имя (rhino). Таким образом, пользователю достаточно запомнить мнемоническое имя rhino, а не полное доменное имя.
- В зависимости от платформы в записях файла HOSTS иногда надо учитывать регистр букв, например для взаимодействия с некоторыми ОС UNIX. Записи файла HOSTS на компьютерах с Windows 2000 не учитывают регистр букв.

Преимущество использования файла HOSTS

Преимущество использования файла HOSTS заключается в том, что его может настраивать пользователь. Каждому пользователю разрешено создавать любые желаемые записи, в том числе легко запоминающиеся мнемонические имена для часто используемых ресурсом. Тем не менее индивидуальное изменение файла HOSTS не очень хорошо подходит для хранения большого числа привязок полных доменных имен.

Практикум: **работа с** файлом **HOSTS и DNS**

Настройте файл HOSTS, затем настроите Windows 2000 для использования DNS. Определите проблемы, связанные с разрешением имен узлов и доменов. В первой части упражнения вы добавите имя узла и соответствующий IP-адрес в файл HOSTS и затем будете использовать этот файл для разрешения имен узлов.

▶ **Задание 1: определите имя локального** узла

1. Откройте окно командной строки.
2. Наберите **hostname и** нажмите Enter.

   Отобразится имя локального узла.

Запустите утилиту ping с именем локального узла, чтобы убедиться, что система может разрешить его имя без использования файла HOSTS.

▶ **Задание 2: проверьте локальное имя** узла **с помощью** ping

1. Наберите **ping** Server1 (где Server1 — имя вашего компьютера) и нажмите Enter.

   Каков отклик?

Произведите следующие действия с Server1, чтобы попытаться выполнить тестовый опрос (ping) локального имени компьютера.

▶ **Задание 3: проверьте локальное имя компьютера с помощью ping**

1. Введите **ping computertwo** и нажмите клавишу Enter.

   Каков отклик?

▶ **Задание *4:* добавьте запись в файл HOSTS на Server 1**

1. Перейдите в каталог файла HOSTS, введя **cd %systemroot%\system32\drivers\etc**.
2. Откройте текстовый редактор для изменения файла HOSTS, введя **notepad hosts.**
3. Добавьте в файл HOSTS запись для computertwo: IP-адрес, затем пробел и имя узла.
4. Сохраните файл и закройте текстовый редактор.

▶ **Задание 5: используйте** файл **HOSTS для разрешения имени**

1. Введите **ping computertwo** и нажмите клавишу Enter.

   Каков отклик?

Резюме

Файл HOSTS — это текстовый файл, который можно редактировать любым текстовым редактором (например, Notepad). Файл HOSTS сопоставляет имена узлов IP-адресам и совместим с файлом HOSTS для ОС UNIX. Если ваша сеть использует файл HOST'S для разрешения имен узлов и вы не можете установить соединение с другим компьютером, указывая его имя узла, вероятная причина — в неправильной записи в файле HOSTS. Поищите в файле HOSTS имя узла другого компьютера, убедитесь, что существует только одна запись для имени узла, и проверьте ее правильность. См. также образец файла HOSTS к папке %SystemRoot%\System32\Drivers\Etc.

Закрепление материала

? Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Что такое имя узла?

2. Каково назначение имени узла?

3. Из чего состоит запись файла HOSTS?

4. Что происходит прежде всего в процессе разрешения имени: разрешение ARP или разрешение имени узла?

ГЛАВА 7

Внедрение DNS

В этой главе

Эта глава посвящена использованию *системы доменных имен* (Domain Name System. DNS) для разрешения имен узлов в локальной сети и Интернете. Microsoft Windows 2000 включает улучшенную версию DNS. Подробности использования DNS в Windows 2000 см. в следующей главе. Цель этой главы — познакомить вас с DNS и объяснить, как внедрить ее в Windows 2000. Вы научитесь определять основные компоненты DNS, устанавливать и настраивать DNS в Windows 2000, устранять неполадки.

Прежде всего

Для изучения этой главы необходимо

- установить Windows 2000 Server и протокол TCP/IP.

Занятие 1. Знакомство с DNS

DNS работает аналогично телефонному справочнику. Каждый компьютер в сети Интернет имеет имя и IP-адрес. Обычно, когда вы хотите связаться с другим компьютером, вы указываете его имя. Затем ваш компьютер соединяется с сервером **DNS,** который находит настоящий IP-адрес по таблице перекрестных ссылок. Этот адрес и используется для связи с удаленным компьютером. Здесь описаны архитектура и структура DNS.

Изучив материал этого занятия, вы сможете:

- ✓ описать структуру, архитектуру и компоненты DNS;
- ✓ описать процесс разрешения имен в DNS.

Продолжительность занятия — около 25 минут.

Основы DNS

До появления DNS имена компьютеров задавались в файле HOSTS, содержавшем список имен и связанных с ними IP-адресов. Этот файл централизованно администрировался, и каждому компьютеру приходилось периодически получать его новую копию. С ростом числа компьютеров этот процесс стал неконтролируемым. В результате была создана DNS, заменившая единый HOSTS-файл распределенной базой данных. Эта **БД** обеспечивает иерархическую структуру имен, распределенное администрирование, расширяемые типы данных, поддерживает практически неограниченный объем данных и обладает высоким быстродействием. DNS — это служба имен для адресов Интернета, которая сопоставляет (транслирует) имена доменов в числовые IP-адреса. Например, имя домена www.microsoft.com транслируется в IP-адрес 207.46.130.149. Этот процесс похож на пользование телефонным справочником, когда по имени человека или по названию организации можно узнать телефонный номер. Аналогично клиент запрашивает имя компьютера, и сервер DNS транслирует его в IP-адрес.

Реализация сервера DNS для ОС производства Microsoft стала частью Windows NT Server 4.0 и продолжает применяться в Windows 2000.

DNS и Windows 2000

Помимо применения в Интернете, DNS — основная служба разрешения имен в Windows 2000. Она спроектирована как высоконадежная иерархическая распределенная и масштабируемая база данных. Клиенты Windows 2000 применяют DNS для разрешения имен и поиска служб, включая поиск контроллеров домена, обслуживающих вход в систему. Версия сервера **DNS** для Windows 2000 обладает уникальными особенностями и полностью совместима с другими стандартными реализациями DNS (см. также главу 8).

Как работает DNS

Задача DNS состоит в трансляции имен компьютеров в IP-адреса (рис. 7-1). В DNS клиенты называются распознавателями, а серверы — серверами имен. DNS использует три основных компонента: распознаватели, серверы имен и пространство имен домена. В простейшем случае распознаватель посылает запросы серверу DNS, который возвращает требуемую информацию либо указатель на другой сервер имен, либо отказ, если запрос не может быть удовлетворен.

В модели OSI DNS располагается на прикладном уровне и применяет протоколы UDP и TCP как протоколы нижнего уровня. Для быстродействия распознаватели сначала обращаются к серверам по протоколу UDP и переходят на TCP в случае потери данных

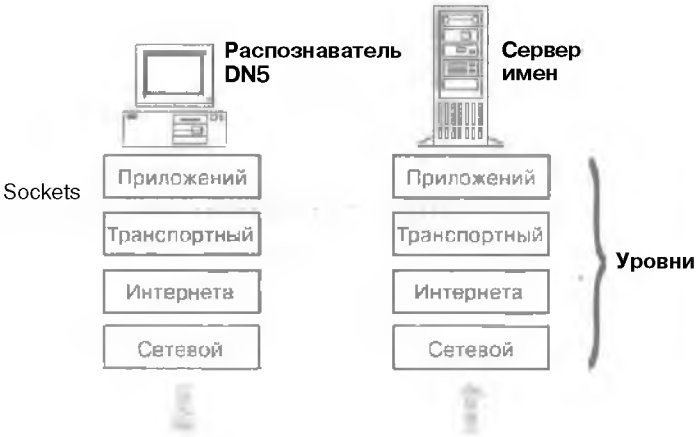


Рис. 7-1. Распознаватели и серверы DNS

Распознаватель

Сообщает клиенту информацию о других компьютерах в сети. Его задача — передать запрос разрешения имени от приложения к серверу DNS. Запрос разрешения имени содержит конкретный вопрос, такой, как IP-адрес Web-узла. Распознаватель может быть встроен в приложение или запускаться как отдельная библиотечная процедура. Распознаватели первоначально посылают запросы по протоколу UDP и переходят на TCP только в случае потери данных.

Сервер имен

Содержит информацию об адресах компьютеров в сети, которая передается клиентам в ответ на запросы. Если сервер не способен разрешить запрос, он может перенаправить его другому серверу DNS. Серверы имен иерархически группируются в домены — логические группы компьютеров в большой сети. Доступ ко всем компьютерам в одной группе контролируется одним сервером.

Структура DNS

Пространство имен домена — иерархическая группировка имен (рис. 7-2).

Корневые домены

Домены определяют различные уровни полномочий в иерархической структуре. Вершина иерархии называется корневым доменом. Ссылка на корневой домен обозначается точкой (.)

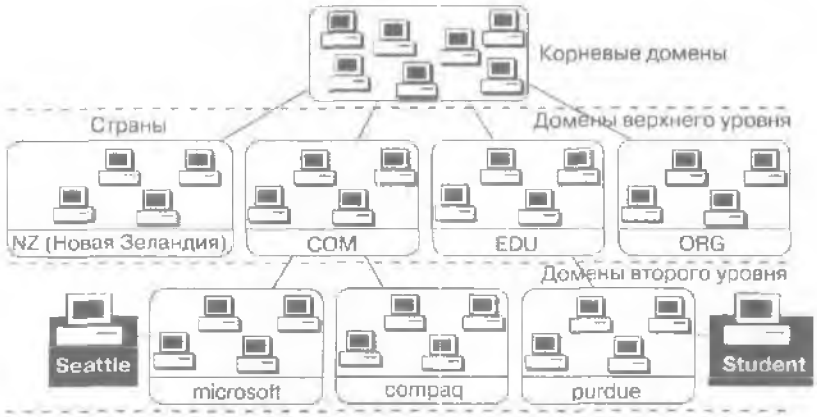


Рис. 7-2. **Уровни в пространстве имен** домена

Домены верхнего уровня

В настоящее время существуют следующие домены верхнего уровня:

- com — коммерческие организации;
- edu — образовательные учреждения;
- org — некоммерческие организации;
- net — организации, предоставляющие услуги на базе Интернета;
- gov — государственные учреждения;
- mil — военные учреждения;
- num — телефонные справочники;
- arpa — используется для регистрации обратного сопоставления IP-адресов, назначенных Internet Assigned Number Authority (IANA) именам доменов DNS для компьютеров, использующих такие адреса в Интернете;
- *xx* — двухбуквенный код страны.

Домены верхнего уровня могут содержать домены второго уровня и узлы.

Примечание Планируется добавление новых доменов верхнего уровня, таких, как firm и web.

Домены второго уровня

Эти домены могут содержать как узлы, так и другие домены, называемые поддоменами. К примеру, домен microsoft.com содержит компьютер ftp.microsoft.com и поддомен dev.microsoft.com. Поддомен dev.microsoft.com может содержать узлы, например ntserver.dev.microsoft.com.

Имена узлов

Имя домена вместе с именем узла образуют *полное доменное имя* (fully qualified domain name, FQDN) компьютера. К имени узла добавляется точка и затем — имя домена. Это может быть, например fileserver1.microsoft.com, где fileserver1 — имя узла, а microsoft.com — имя домена.

Зоны

Зона — административная единица DNS; поддерево в базе данных DNS, которое администрируется отдельно. Зона может состоять как из простого домена, так и из домена с поддоменами. Поддомены зоны также разрешается разбивать на отдельные зоны.

Зона полномочий сервера DNS

Зоной полномочий называется часть пространства имен домена, за которую отвечает один сервер имен. Он хранит все привязки адресов для пространства имен в рамках зоны и обрабатывает клиентские запросы имен. В состав зоны полномочий сервера имен входит минимум один домен — корневой домен зоны. Может существовать и дополнительный сервер DNS, на который копируется информация зоны с основного сервера. Процесс копирования называется передачей зоны.

Как показано на рис. 7-3, домен rnicrosoft.com контролируется несколькими файлами зоны. Часть данных находится в отдельном файле зоны для домена dev.microsoft.com. Разбиение домена на зоны иногда требуется для делегирования управления доменом нескольким группам пользователей и повышения эффективности репликации данных.

Рис. 7-3. Разделение домена на зоны

Роли серверов DNS

Серверы имен DNS настраивают в зависимости от того, как они хранят и поддерживают свои БД имен. Сервер DNS Microsoft бывает как основным, так и дополнительным сервером DNS, в том числе для серверов с другими ОС, например UNIX. Для каждой зоны требуются минимум два сервера DNS — основной и дополнительный. Это необходимо для обеспечения избыточности данных и повышения устойчивости к отказам.

Основные серверы имен

Получают информацию о своей зоне с локальных файлов БД DNS. Если информация в БД изменяется, например происходит передача части зоны другому серверу DNS или добавляются новые узлы, эти изменения необходимо внести на основном сервере DNS, чтобы обновления были отражены в локальном файле зоны.

Дополнительные серверы имен

Получают данные от основных серверов **DNS,** полномочных для их зоны. Процесс копирования файла зоны с основного на дополнительный сервер называется передачей зоны, Существуют три причины для создания дополнительных серверов.

- Избыточность. Необходимо иметь минимум один основной и дополнительный серверы для каждой зоны, при этом компьютеры должны быть по возможности независимы. В общем случае стоит планировать установку этих серверов в различных подсетях, чтобы поддерживать работу DNS даже при отказе одной подсети.
- Быстрый доступ удаленных клиентов. Предусмотрите дополнительный сервер DNS (или основной сервер для поддомена) для обслуживания крупной группы удаленных клиентов. Это избавит клиентов от необходимости использовать медленные линии для разрешения имен.
- Снижение нагрузки. Дополнительные серверы имен снижают нагрузку на основной сервер.

Поскольку информация для каждой зоны хранится в отдельных файлах, ранг серверов определяется по отношению к зоне. Это означает, что конкретный сервер DNS может быть основным сервером для одних зон и дополнительным — для других.

Главные серверы имен

При создании дополнительной зоны для ее сервера имен необходимо указать сервер DNS, от которого первый будет получать данные зоны. Источник данных зоны для дополнительного сервера имен в иерархии DNS называется главным сервером имен. Главный сервер может быть основным или дополнительным сервером данной зоны. При запуске дополнительный сервер связывается со своим главным и запрашивает передачу зоны.

Серверы кэширования

Хотя все DNS-серверы кэшируют запросы, некоторые выделены исключительно для этой цели. Другими словами, в их зону полномочий не входит ни один домен (на них не хранятся никакие файлы зоны). Они содержат лишь данные, накопленные при разрешении запросов.

Имейте в виду, что, когда такой сервер начинает работу, его кэш пуст и заполняется постепенно. Поскольку сервер кэширования не выполняет передачу зоны, трафик между серверами меньше, что особенно важно при использовании медленных линий связи.

Резюме

В DNS получило развитие разрешение имен узлов в Интернете. Клиент или распознаватель посылает запросы серверу имен, который их обрабатывает и сопоставляет имена узлов IP-адресам. Пространство имен домена имеет иерархическую структуру и состоит из корневых доменов, доменов верхнего и второго уровня и имен узлов. Отдельные серверы, ответственные за части пространства имен домена, называют зонами полномочий.

Занятие 2. Процесс разрешения имен и структура файлов DNS

Клиент (распознаватель) может выполнять запросы трех типов: рекурсивные, итеративные и обратные. Серверы DNS хранят информацию в файлах четырех типов: файлах БД, файлах обратного просмотра, кэш-файлах и загрузочных файлах.

Изучив материал этого занятия, вы сможете:

- ✓ пояснить механизм работы рекурсивных, итеративных и обратных запросов;
- ✓ описать, как запросы размешаются в кэше.

Продолжительность занятия — около 10 минут.

Рекурсивные запросы

В отпет на рекурсивный запрос сервер имен должен возвратить требуемые данные либо сообшение об ошибке, если не существуют данные запрашиваемого типа или имя домена. Сервер имен не может переслать рекурсивный запрос другому серверу имен.

Итеративные запросы

В ответ на итеративный запрос сервер имен даст наилучший возможный ответ. Это либо разрешение запроса или ссылка на другой сервер, который, возможно, сумеет ответить на исходный запрос.

На рис. 7-4 показаны примеры рекурсивного и итеративного запросов: клиент из корпоративной сети запрашивает у своего DNS-ссрвсра IP-адрес узла www.microsoft.com.

1. Распознаватель посылает рекурсивный запрос IP-адреса для www.microsoft.com локальному серверу DNS. Локальный сервер несет ответственность за разрешение запроса и не может отослать распознавателя к другому серверу DNS.
2. Локальный сервер DNS проверяет свои данные, не находит зоны, соответствующей имени домена, и посылает итеративный запрос адреса www.microsoft.com корневому серверу.
3. Полномочия корневого сервера DNS распространяются на весь корневой домен. Он возвращает IP-адрес сервера DNS для домена com верхнего уровня.
4. Локальный сервер DNS посылает итеративный запрос о www.microsoft.com серверу DNS домена com.
5. Сервер домена com возвращает IP-адрес сервера DNS домена microsoft.com.
6. Локальный сервер DNS посылает итеративный запрос о www.microsott.com серверу DNS домена microsoft.com.
7. Сервер домена microsoft.com возвращает IP-адрес www.microsoft.com.

X. Локальный сервер DNS возвращает клиенту IP-адрес www.microsort.corn.

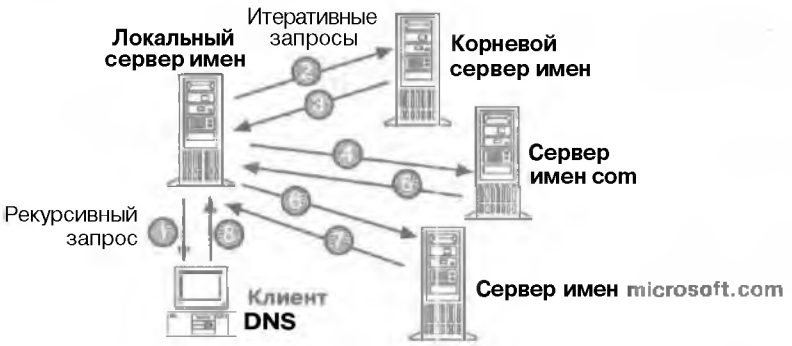


Рис. 7-4. **Рекурсивные и итеративные запросы**

Обратные запросы

При обратном запросе требуется решить обратную задачу: найти имя учла по известному адресу. Поскольку нет корреляции между IP-адресом и именем узла, ответ можно получить, лишь выполнив просмотр по всем доменам.

Для предотвращения полного просмотра всех доменов создан специальный домен in-addr.arpa. Его узлы именуются по номерам десятично-точечного представления IP-адреса. Так, порядок IP-адреса слева направо соответствует порядку справа налево в имени домена, октеты IP-адреса записываются здесь в обратном порядке. При условии соблюдения этой договоренности администрирование нижних ветвей домена in-addr.arpa может быть делегировано организациям, которым присвоены IP-адреса классов A, B и C.

После построения домена in-addr.arpa в него добавляются записи указателей ресурсов (PTR), связывающие IP-адреса с соответствующими именами узлов. Например, чтобы найти имя узла для адреса 157.55.200.51, распознаватель запрашивает у сервера DNS запись PTR для 51.200.55.157.in-addr.arpa. Найденная запись PTR содержит имя узла и соответствующий адрес 157.55.200.51. Эта информация возвращается распознавателю. Административная часть сервера DNS обеспечивает создание записей PTR для узлов.

Кэширование и время жизни

При обработке рекурсивного запроса иногда нужно несколько попыток для его разрешения. Сервер DNS кэширует всю информацию, полученную в этом процессе, и хранит ее в течение времени, указанного в возвращенных данных. Это *время жизни* (Time to Live, TTL). Время жизни для данных задает администратор сервера имен зоны. Малые значения TTL обеспечивают большую достоверность данных в сети, если изменения происходят часто. Впрочем, это увеличивает нагрузку на серверы имен.

После того как данные кэшированы сервером DNS, он должен начать понижать их TTL с первоначального значения, чтобы знать, когда удалить данные из кэша. Если приходит запрос, который может быть разрешен данными кэша, возвращаемое TTL означает время, оставшееся до удаления данных из кэша сервера DNS. Распознаватели клиента также кэшируют данные и учитывают TTL, поэтому они знают, когда данные устаревают.

Конфигурационные файлы DNS

DNS — иерархическая распределенная БД. Сама база состоит из записей ресурсов, которые, в свою очередь, включают имя DNS, тип записи и значения соответствующего типа.

Например, наиболее распространенная запись в базе DNS — адресная запись, включающая имя компьютера и TCP/IP-адрес компьютера.

Для разрешения имен серверы обращаются к файлам зоны (также именуемым файлами БД DNS), содержащим записи ресурсов с описанием ресурсов домена DNS. Например, одни записи ресурсов сопоставляют дружественные имена IP-адресам, а другие, напротив, — IP-адреса дружественным именам.

Начальная запись зоны

Она должна быть первой в любом файле БД, обозначается как SOA (start of authority) и определяет основные параметры зоны DNS. Пример начальной записи зоны:

```
@ IN SOA nameserver.example.microsoft.com
postmaster.example.microsoft.com. (
  1 ; serial number
  3600 ; refresh [1h]
  600 ; retry [10m]
  86400 ; expire [1d]
  3600 ) ; mm TTL [1h]
```

Начальная запись подчиняется следующим правилам:

- символ @ *к* файле базы данных означает «этот сервер»;
- IN означает запись Интернета;
- любое имя узла, не оканчивающееся точкой, будет дополнено именем корневого домена;
- символ @ заменяется точкой в электронном почтовом адресе администратора;
- часть записи, занимающая несколько строк, заключается *в* круглые скобки ().

Запись ресурса сервера имен

Перечисляет дополнительные серверы DNS, обозначается как NS. БД может содержать несколько таких записей.

```
@ IN NS nameserver2.microsoft.com
```

Запись ресурса адреса узла

Связывает имя узла с его IP-адресом, ее тип обозначается A. Такие записи занимают большую часть БД и перечисляют все узлы в зоне.

```
Rhino       IN A 157.55.200.143
localhost   IN A 127.0.0.1
```

Запись ресурса с каноническим именем

Позволяет связать несколько имен узла с одним IP-адресом, ее тип обозначается CNAME. Ее также называют псевдонимом.

```
FileServer1  CNAME  rhino
www          CNAME  rhino
ftp          CNAME  rhino
```

Файл обратного просмотра

Файл z.y.x.w.in-addr.arpa позволяет распознавателю определять имя узла, соответствующее IP-адресу. Файл называется по имени той зоны в in-addr.arpa, для которой он обеспечивает обратный просмотр. Например, файл, обеспечивающий обратный просмотр в сети 157.57.28.0, называется 57.157.in_addr.arpa. Как и обычные базы DNS, этот файл содержит записи SOA и NS, а также записи типа PTR.

Возможность обратного просмотра в DNS имеет большое значение, потому что некоторые приложения основывают защиту информации на проверке имен узлов. Например, если обозреватель Web посылает запрос серверу Web с такой защитой, тот свяжется с сервером DNS и запросит имя клиента по его адресу. Если имени нет в списках доступа к Web-узлу или имя не найдено сервером DNS, запрос будет отклонен.

Примечание Windows 2000 не требует обязательного конфигурирования зон обратного просмотра. Эти зоны требуются некоторым приложениям и иногда упрощают администрирование.

Запись **указателя**

Сопоставляет имя адресу в файле обратного просмотра, ее тип обозначается PTR. При создании записи номера IP записываются в обратном порядке с добавлением фрагмента in-addr.arpa. Например, поиск имени для адреса 157.55.200.51 требует запроса для имени 51.200.55.157.in-addr.arpa.

```
51.200.55.157.in-addr.arpa.  IN  PTR  mailserver1.microsoft.com.
```

Кэш-файл

Записи корневого сервера домена хранятся в файле CACHE.DNS. Кэш-файл с таким именем должен быть на всех серверах имен. Когда сервер разрешает запрос имени за пределами своей юны, он начинает с корневого сервера домена. Пример записей в кэш-файле:

```
                        3600000      IN    NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A           198.41.0.4
```

Кэш-файл содержит информацию об узле, необходимую для разрешения имен за пределами зоны полномочий, а также содержит имена и адреса из базы корневого сервера DNS. Поставляемый в составе Windows 2000 файл находится в папке %SystemRoot%\System32\Dns. Он содержит записи для всех корневых серверов Интернета. Если устанавливается система без доступа в Интернет, этот файл должен быть изменен. В него надо записать информацию о сервере корневого домена частной сети.

Загрузочный файл

Это конфигурационный файл для совместимости с версией **DNS** Berkeley Internet Name Daemon (BIND). Файл содержит информацию об узлах, необходимую для разрешения имен узлов вне зоны полномочий. Этот файл не определен в RFC и не требуется для соответствия стандартам RFC. Windows 2000 поддерживает его для совместимости с традиционными службами DNS на базе UNIX. Загрузочный файл управляет поведением сервера DNS при запуске. Команды в нем должны начинаться с начала строки без пробелов. В табл. 7-1 описаны некоторые команды файла, поддерживаемые Windows 2000.

Табл. 7-1, Команды загрузочного файла

Команда	Описание
directory	Указывает каталог, где могут быть найдены файлы, на которые есть ссылки в загрузочном файле
cache	Указывает файл, позволяющий связаться с серверами корневого домена. Эта команда и файл обязательно должны существовать. Кэш-файл, который может использоваться в Интернете, поставляется с Windows 2000
primary	Указывает подконтрольный серверу домен и файл, содержащий записи ресурсов. В загрузочном файле может быть несколько команд primary
secondary	Указывает подконтрольный серверу домен и список IP-адресов основных серверов, с которых будет обновляться информация о зоне. Здесь также определяется файл для кэширования зоны. В загрузочном файле может быть несколько команд secondary

Табл. 7-2. Примеры команд загрузочного файла

Синтаксис	Пример
directory *[имя каталога]*	directory c:\winnt\system32\dns
cache.*[имя файла]*	cache.cache
primary *[домен] [имя файла]*	primary microsoft.com microsoft.dns primary dev.microsolt.com dev.dns
secondary *[домен] [список узлов] [имя файла]*	secondary test.microsoft.com 157.55.200.100 test.dns

Резюме

Для разрешения имени узла или IP-адреса используются запросы трех типов: рекурсивные, итеративные и обратные. При рекурсивном запросе сервер DNS возвращает только ту информацию, которую он имеет, или сообщение об ошибке. Более типичен итеративный запрос, при котором сервер возвращает требуемую информацию либо отсылает к другому серверу DNS. Третий тип запроса, обратный, предназначен для поиска узла по его IP-адресу.

Серверы DNS хранят информацию в файлах четырех типов: файлах данных, файлах обратного просмотра, кэш-файлах и загрузочных файлах. Windows 2000 и включенная в нее оснастка DNS позволяют конфигурировать эти файлы, используя графический интерфейс (см. главу 8).

Занятие 3. Планирование внедрения DNS

Конфигурация сервера DNS зависит от таких факторов, как размер организации, размещение подразделений и требования по отказоустойчивости. Сейчас мы перечислим основные рекомендации по конфигурации DNS в вашем узле, а также познакомим вас со сценариями, позволяющими оценить ваши знания и планировании сетей перед внедрением DNS.

Изучив материал этого занятия, вы сможете:

- ✓ регистрировать сервер DNS в родительском домене;
- ✓ оценивать количество необходимых для сети серверов имен DNS, доменов и зон.

Продолжительность занятия — около 40 минут.

Основные рекомендации

Хотя Windows 2000 требует для разрешения имен сервер DNS, сам сервер DNS не обязан находиться на сервере Windows 2000. Более того, он даже не должен находиться в той же локальной сети. Для разрешения имен достаточно, чтобы Windows 2000 была настроена для обращения к действующему серверу DNS, поддерживающему необходимые типы записей, например серверу поставщика услуг Интернета. Впрочем, версия DNS для Windows 2000 обладает расширенными возможностями, поэтому вы, возможно, решите установить и настроить собственный сервер DNS. Предположим, вы решили организовать свой собственный сервер DNS.

Если вы независимо от размера организации хотите использовать домен второго уровня, надо сообщить в InterNIC имя домена и IP-адреса по крайней мере двух серверов DNS, обслуживающих домен. Внутри вашей организации вы можете установить дополнительные серверы DNS, независимые от Интернета.

Из соображений надежности и избыточности данных Microsoft рекомендует, чтобы для каждого домена были сконфигурированы минимум два сервера DNS — основной и дополнительный. Основной сервер требуется для поддержки БД, которая реплицируется (копируется) на дополнительный сервер. Такое дублирование позволит обслуживать запросы, даже если один из серверов недоступен. Расписание репликации может быть настроено в зависимости от частоты изменения файлов в домене. С одной стороны, копирование должно быть достаточно частым, чтобы об изменениях знали оба сервера. С другой стороны, частое копирование увеличивает трафик и нагрузку на сервер имен.

Регистрация в родительском домене

После того как вы установили и настроили свой сервер (или серверы) DNS, вам надо зарегистрировать его на сервере DNS в домене верхнего уровня (рис. 7-5). Родительской системе необходимо знать имена и адреса ваших серверов, но ей может потребоваться и другая информация, такая, какдата, с которой домен будет доступен, а также контактные имена и почтовые адреса.

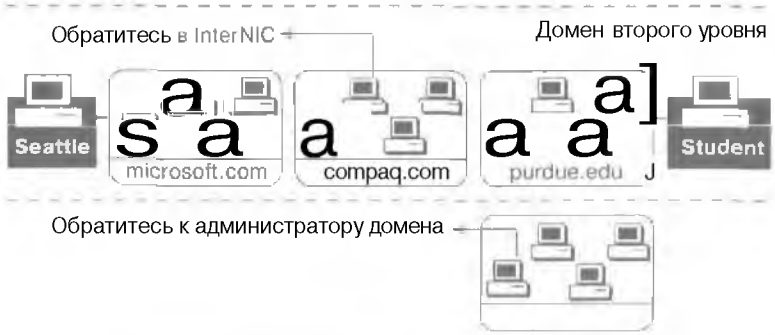


Рис. 7-5. **Регистрация DNS-сервера** в домене верхнего **уровня**

Если вы регистрируетесь на компьютере ниже второго уровня, узнайте у администратора той системы, какую информацию вы должны предоставить.

Практикум: внедрение DNS

Вы ознакомитесь с тремя сценариями установки DNS. В каждом сценарии вам придется оценить необходимое количество серверов DNS, доменов и зон. Каждый сценарий описывает организацию, которая переходит на Windows 2000 и хочет внедрить службу каталогов. Ответьте на ряд вопросов, связанных с проектированием DNS, учитывая конкретные требования. Цель упражнения — оценить ваши знания и проектировании сетей перед установкой DNS. Это станет критерием ваших успехов в изучении курса и поможет вам при проектировании сети DNS.

Сценарий 1. Проектирование DNS для небольшой сети

В небольшой организации меняют старую многопользовательскую систему на компьютер с Windows 2000. Большинство сотрудников подключаются к главному компьютеру через терминалы, некоторые имеют персональные компьютеры с процессорами 486 и Pentium: эти компьютеры не подключены к сети. Оборудование для перехода на новую систему уже приобретено.

Сеть предполагается использовать для совместного использования файлов и принтеров, она также будет включать один сервер БД — Microsoft SQl Server 7 под управлением Windows 2000. Большинство пользователей нуждается в доступе к SQL Server 7. Локальные приложения будут установлены на рабочих станциях, но данные будут храниться на серверах. Организация хочет подключиться к Интернету, чтобы сотрудники могли пользоваться электронной почтой.

Параметры сети перечислены в табл. 7-3.

Табл. 7-3. **Параметры проектируемой** сети

Компоненты	Состав
Пользователи	100 человек
Размещение	Одно здание
Административный персонал	Один штатный администратор
Серверы	2 компьютера Pentium 120 МГц с 32 Мб ОЗУ, диском 3.2 Гб; 1 компьютер Pentium 150 МГц с 128 Мб ОЗУ, выделенный под Exchange Server

(см. след. стр.)

Табл. 7-3. **Параметры проектируемой сети** *(окончание)*

Компоненты	**Состав**
Клиенты	Компьютеры Pentium и 486 с Windows 2000 Professional
Приложения Microsoft	Exchange Server и DNS BackOffice
Использование **сервера**	Совместное использование файлов и принтеров

Проект должен учитывать:

- количество пользователей;
- численность административного персонала;
- размещение подразделений.

Исходя из задач проекта, ответьте на вопросы.

1. Сколько потребуется доменов DNS?
2. Сколько потребуется поддоменов?
3. Сколько потребуется зон?
4. Сколько потребуется основных серверов?
5. Сколько потребуется дополнительных серверов?
6. Сколько потребуется серверов кэширования?

Сценарий 2. Проектирование DNS для сети среднего размера

В организации насчитывается 8795 пользователей. Из них 8000 сосредоточены в четырех головных офисах, остальные — в десяти филиалах в крупнейших городах США. Организация решила перевести локальные сети на Windows 2000 Server. Также решено вести учет пользователей в штаб-квартире компании.

Четыре основных офиса связаны линиями класса TI (рис. 7-6). Филиалы соединены с ними линиями пропускной способностью 56 кбит/с.

Три из четырех основных подразделений действуют независимо друг от друга. Четвертое — штаб-квартира организации. В каждом филиале от 25 до 250 сотрудников, которым требуется доступ ко всем основным сайтам, но они редко связываются с другими филиалами.

Кроме десяти филиалов, в организации есть временное исследовательское подразделение из десяти человек. Сайт этого подразделения состоит из одного сервера, подключающегося к Бостону с использованием маршрутизации по требованию. Ожидается, что подразделение закроется в течение шести месяцев. Для его автономной деятельности требуется только обмен сообщениями.

В основных сайтах будет продолжено использование имеющегося оборудования и оборудования подключенных к ним филиалов. В данный момент загрузка линий связи в пиковое время составляет 60%. Ожидается, что в ближайшие 12–18 месяцев рост сети будет минимальным.

Рис. 7-6. **Линии связи между подразделениями организации**

Параметры сети перечислены в табл. 7-4.

Табл. 7-4, **Параметры проектируемой сети**

Компоненты	Состав
Пользователи	8795 человек
Размещение	4 головных офиса и 10 филиалов в крупнейших городах. **подразделений** за рубежом не предвидится
Административный персонал	Штатные администраторы в четырех основных сайтах, в филиалах администраторы работают по совместительству
Количество серверов DNS	На данный момент неизвестно
Количество серверов кэширования	Сервер кэширования нужен в каждом удаленном подразделении одной зоны
Клиенты	Компьютеры Pentium, 486, 386 с Windows 2000 Professional
Приложения на сервере	**SQL** Server 7. Exchange Server и DNS

Размещение и численность филиалов указаны ниже.

Город	Количество пользователей, чел.
Лос-Анджелес	40
Солт-Лейк-Сити	25
Монреаль	10
Новый Орлеан	25
Канзас-Сити	25
Вашингтон	100
Денвер	200
Майами	75

Проект должен учитывать:

- количество пользователей;
- численность административного персонала;
- размещение **подразделений;**
- скорость и качество связи между подразделениями;
- загрузку каналов **связи;**
- ожидаемые изменения в сети;
- совместное использование деловых приложений.

Исходя из задач проекта, ответьте на вопросы.

1. Сколько потребуется доменов DNS?
2. Сколько потребуется поддоменов?
3. Сколько потребуется зон?
4. Сколько потребуется основных серверов?
5. Сколько потребуется дополнительных серверов?
6. Сколько потребуется серверов кэширования?
7. По данным таблицы расстояний спроектируйте размещение филиалов по зонам. Филиал должен быть в той же зоне, где ближайший головной офис.

Расстояние, миль	Атланта	Бостон	Чикаго	Портленд
Даллас	807	1817	934	2110
Денвер	1400	1987	1014	1300
Канзас-Сити	809	1454	497	1800
Лос-Анджелес	2195	3050	2093	1143
Майами	665	1540	1358	3300
Монреаль	1232	322	846	2695
Новый Орлеан	494	1534	927	2508
Солт-Лейк-Сити	1902	2403	1429	800
Сан-Франциско	2525	3162	2187	700
Вашингтон	632	435	685	2700

Сценарий 3. Проект DNS для большой сети

В компании работают 60 000 сотрудников в различных странах мира. Управление компании расположено в Женеве, кроме того, имеются региональные управления к Нью-Йорке и Сингапуре. Каждое управление полностью контролирует пользователей в своем регионе. Пользователям требуется доступ к ресурсам других регионов. Все три региональных управления связаны линиями TI.

Каждое региональное управление имеет серию бизнес-приложений, которые должны быть доступны во всех точках региона, а также другим региональным управлениям. Основное производство сосредоточено на дочерних предприятиях в Малайзии и Австралии, к которым должны иметь доступ пользователи из других регионов.

Все бизнес-приложения работают на серверах Windows 2000, которые предполагается сконфигурировать как рядовые серверы доменов. Каналы в Сингапуре. Малайзии и Австралии загружены на 90%. В Азии и Австралии расположены десять дочерних фирм.

Так как в некоторых странах действуют ограничения на импорт, решено дать возможность каждой дочерней фирме самой определять состав оборудования и иметь домен в каждой стране. На большинстве недавно приобретенных компьютеров установлена Win-

dows 2000 Professional. При необходимости обоснуйте приобретение дополнительного оборудования. (В табл. 7-5 — только для Азии и Австралии.)

Табл. 7-5, **Параметры проектируемой** сети

Компоненты	**Состав**
Пользователи в Азии и Австралии	25 000 человек, равномерно распределенных по дочерним фирмам
Размещение	Региональное управление в Сингапуре. 10 дочерних фирм в различных странах региона
Административный персонал	Штатные администраторы в главном управлении и на всех дочерних предприятиях
Количество доменов	В настоящий момент неизвестно
Клиенты	Компьютеры Pentium, 486, 386 с Windows 2000 Professional
Приложения на сервере	SQL Server 7, SNA, SMS. почта, DNS

Проект для Азии и Австралии должен учитывать:

- количество пользователей;
- численность административного персонала;
- размещение подразделений;
- скорость и качество связи между подразделениями;
- загрузку каналов связи;
- ожидаемые изменения и сети:
- совместное использование деловых приложений.

Чтобы решить задачи проекта, ответьте на вопросы.

1. Сколько потребуется доменов DNS?
2. Сколько потребуется поддоменов?
3. Сколько потребуется зон?
4. Сколько потребуется основных серверов?
5. Сколько потребуется дополнительных серверов?
6. Сколько потребуется серверов кэширования?

Резюме

Необходимость установки сервера DNS зависит от размера и структуры организации. Для обеспечения полной функциональности Windows 2000 требуется доступ к серверу DNS. Сервер DNS может быть установлен в локальной сети или предоставляться поставщиком услуг Интернета. Реализация DNS в Windows 2000 обладает расширенными возможностями по сравнению с традиционными серверами DNS (см. также главу 8).

Занятие 4. Установка DNS

Сервер Microsoft DNS удовлетворяет требованиям RFC, поэтому он создает и использует стандартные файлы зоны, а также поддерживает все стандартные типы записей ресурсов. Он может взаимодействовать с другими серверами DNS и включает утилиту диагностики NSLOOKUP. Сервер Microsoft DNS тесно интегрирован со службой WINS и администрируется с помощью оснастки DNS. В ходе этого занятия вы установите службу DNS в Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ установить Microsoft DNS Server;
- ✓ использовать утилиту NSLOOKUP для устранения неполадок DNS.

Продолжительность занятия — около 45 минут.

Перед установкой сервера DNS надо правильно настроить протокол TCP/IP. По умолчанию сервер DNS создаст начальную запись зоны, запись имени сервера и запись адреса узла на основе данных в диалоговом окне свойств протокола TCP/IP. Если имена узла и домена не указаны, будет создана только начальная запись зоны.

Практикум: установка службы DNS Server

Установите службу DNS Server, Вы настроите ее на следующем занятии.

Примечание Выполняйте это упражнение на компьютере, который планируете **сделать** сервером DNS.

Перед конфигурированием DNS убедитесь в правильности заданных параметров клиента DNS.

▶ Задание 1: проверьте параметры клиента DNS

1. Щелкните правой кнопкой My Network Places (Мое сетевое окружение) и выберите команду Properties (Свойства).

   Откроется окно Network And Dial-Up Connections (Сеть и удаленный доступ к сети).
2. Щелкните правой кнопкой подключение (обычно это локальное подключение), для которого вы хотите настроить сервер DNS, и выберите команду Properties.

   Откроется окно свойств подключения.
3. Щелкните протокол TCP/IP, затем — кнопку Properties.

   Откроется диалоговое окно свойств TCP/IP.
4. Введите IP-адрес существующего сервера DNS в поле Preferred DNS Server (Предпочитаемый DNS-сервер).

   Вы можете также добавить адрес альтернативного сервера DNS.
5. Если вы хотите указать несколько альтернативных серверов DNS, щелкните кнопку Advanced (Дополнительно), перейдите на вкладку DNS и введите имена серверов в списке DNS Server Addresses (Адреса DNS-серверов).
6. Щелкните OK, чтобы закрыть диалоговое окно свойств TCP/IP.
7. Щелкните OK, чтобы закрыть диалоговое окно свойств подключения.

Задание 2: установите службу DNS Server

1. На панели управления дважды щелкните значок Add/Remove Programs (Установка и удаление программ), затем щелкните Add/Remove Windows Components (Добавление и удаление компонентов Windows).

   Откроется окно мастера компонентов Windows.

2. Щелкните в списке компонентов Networking Services (Сетевые службы), затем кнопку Details (Состав).

   Откроется диалоговое окно Networking Services (Сетевые службы).

3. Пометьте флажок Domain Name System (DNS) и щелкните OK (рис. 7-7).

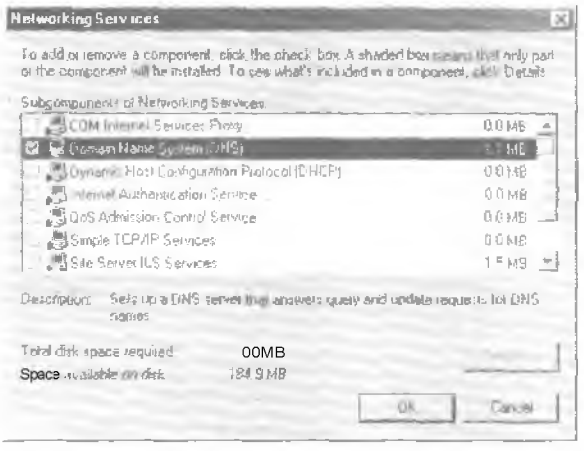


Рис. 7-7. **Доступные для установки сетевые** службы

4. Щелкните Next.

   Windows 2000 установит DNS.

5. Щелкните кнопку Finish (Готово).

Использование утилиты NSLOOKUP для разрешения проблем DNS

NSLOOKUP — полезный инструмент устранения неполадок разрешения имен узлов. При запуске NSLOOKUP отображает имя и IP-адрес сервера DNS, сконфигурированного для нашей системы, и перейдет в интерактивный режим. В этом режиме список доступных команд выдается по команде ?, выход из программы — команда exit. Чтобы получить IP-адрес узла, просто наберите его имя и нажмите Enter. По умолчанию NSLOOKUP использует сервер DNS, указанный в конфигурации компьютера, с которого он запущен, но вы можете переключиться на другой сервер, набран **server** <*имя*>, где *имя* — имя сервера DNS, который вы будете в дальнейшем использовать.

Режимы NSLOOKUP

NSLOOKUP работает в двух режимах — интерактивном и автономном. При однократном обращении используйте автономный режим, при постоянной работе — интерактивный.

Синтаксис NSLOOKUP

Команда NSLOOKUP имеет следующий синтаксис:

```
Nslookup [-параметр ...] [компьютер | -[сервер]]
```

Параметр	Описание
параметр...	Задает одну или несколько команд nslookup как параметры командной строки. Каждый параметр состоит из дефиса (-) и следующей за ним без пробелов команды, а также в некоторых случаях знака равенства (=) и значения
компьютер	Получает сведения о заданном компьютере с использованием текущего сервера или сервера, заданного Параметром *сервер* (если этот параметр указан). Если компьютер задан IP-адресом, а тип запроса — A или PTR, отобразится имя компьютера. Если компьютер задан именем без замыкающей точки, имя текущего домена будет добавлено к указанному имени. Это зависит от состояния параметров команды set: domains, srchlist, defname и search. Чтобы получить сведения о компьютере не из текущего домена, в конец имени надо добавить точку. Если в командной строке введен дефис <-) вместо имени компьютера, команда nslookup перейдет в интерактивный режим
сервер	Задает сервер имен DNS. Если параметр *сервер* не указан, используется текущий сервер DNS.

► Использование NSLOOKUP в автономном режиме

1. Измените свойства окна командной строки для отображения 50 строк.

   Как показано на рис. 7-8, это можно сделать на вкладке Layout (Расположение) в свойствах окна. Вы должны установить это значение на будущее для всех запусков окна командной строки; это потребуется на следующих занятиях.

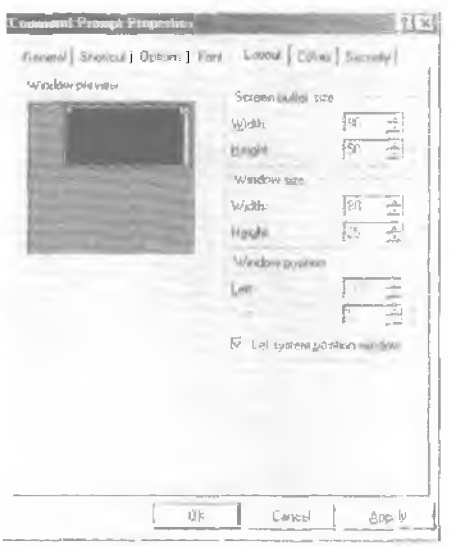


Рис. 7-8. Диалоговое окно свойств командной строки

2. Введите следующую команду

   nslookup *узел*

   где *узел* — имя узла в вашем домене.

NSLOOKUP вернет IP-адрес компьютера *узел,* так как информация о нем есть в БД сервера DNS.

3. Введите exit для выхода из командной строки.

▶ **Использование NSLOOKUP в интерактивном режиме**

1. Введите **nslookup** и нажмите Enter.
   Появится приглашение ввода >.
2. Введите **set all.**
   Появится список текущих значений всех параметров NSLOOKUP.
3. Измените время паузы до 1 и количество попыток до 7 (рис. 7-9).

```
Set t1=1
Set ret=7
```

4. Введите set all. чтобы убедиться, что параметры изменились.
5. Вводите имена других компьютеров по очереди. Нажимайте Enter после каждого имени.
6. Введите **exit** для выхода из программы.

Рис. 7-9. Установка **паузы и** количества **попыток в NSLOOKUP**

Резюме

Microsoft DNS совместим с другими серверами DNS. Перед установкой службы DNS Server убедитесь в правильной конфигурации протокола TCP/IP на сервере Windows 2000. Основным диагностическим инструментом для DNS является утилита NSLOOKUP. Она позволяет просматривать записи ресурсов серверов DNS.

Занятие 5 Настройка DNS

Существует два способа администрирования Microsoft DNS Server: с помощью утилиты DNS Manager и прямое редактирование конфигурационных файлов DNS. Здесь описаны средства администрирования DNS.

Изучив материал этого занятия, вы сможете:

- ✓ администрировать сервер DNS;
- ✓ создать файл зоны и заполнить его записями ресурсов.

Продолжительность занятия — около 60 минут.

Настройка свойств сервера DNS

Основной инструмент для управления серверами DNS и Windows 2000 — консоль DNS (рис. 7-10). Так как сервер DNS первоначально не имеет информации о пользовательской сети, он устанавливается сначала как сервер кэширования Интернета. Это значит, что первоначально сервер содержит информацию только о корневых серверах Интернета. Чтобы добиться эффективной работы, для большинства конфигураций нужно предоставить дополнительную информацию. Чтобы открыть консоль DNS, раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык DNS.

Рис. 7-10. Консоль DNS

▶ Добавление зоны DNS

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык DNS.
2. Щелкните имя вашего сервера, затем выберите в меню Action (Действие) команду New Zone (Добавление новой зоны).
3. Следуйте инструкциям мастера.

   Вы можете создать одну или более зон следующего типа:

- Active Directory-integrated (Интегрированная в Active Directory) — включает механизм Active Directory для хранения и репликации файлов описания зоны. Данные *зоны* хранятся как объект Active Directory, а репликация происходит в процессе репликации домена;
- Standard primary (Основная) — вы должны создать основную зону в вашем пространстве имен, если не используете Active Directory;
- Standard secondary (Дополнительная) — дополнительная зона помогает сбалансировать загрузку основных серверов и обеспечивает отказоустойчивость.

4. Укажите, создаете ли вы зону прямого или обратного просмотра. Если вы создаете зону *прямого* (Forward) просмотра, укажите имена зоны и файла зоны. Если вы создаете зону *обратного* (Reverse) просмотра, укажите идентификатор сети или имя зоны и залайте файл зоны.
5. Щелкните кнопку Finish (Готово) для завершения работы мастера.

Ручная настройка DNS

Сервер DNS можно настроить прямым редактированием файлов в каталоге *\systemroot*\System32\Dns. кула конфигурационные файлы устанавливаются по умолчанию. Администрирование производится в текстовом редакторе аналогично традиционным DNS (рис. 7-11). В этом случае службу DNS надо перезапустить.

Добавление зон и доменов DNS

Первый шаг в настройке сервера DNS — определение иерархии доменов и зон. После этого соответствующую информацию надо внести в конфигурационные файлы DNS из консоли DNS.

Добавление основных и дополнительных зон

Вы можете добавлять основные и дополнительные зоны из консоли DNS (рис. 7-12). После того как вы введете информацию о зоне, оснастка DNS создаст имя файла зоны по умолчанию. Если такой файл уже существует в каталоге DNS, консоль DNS автоматически импортирует его записи.

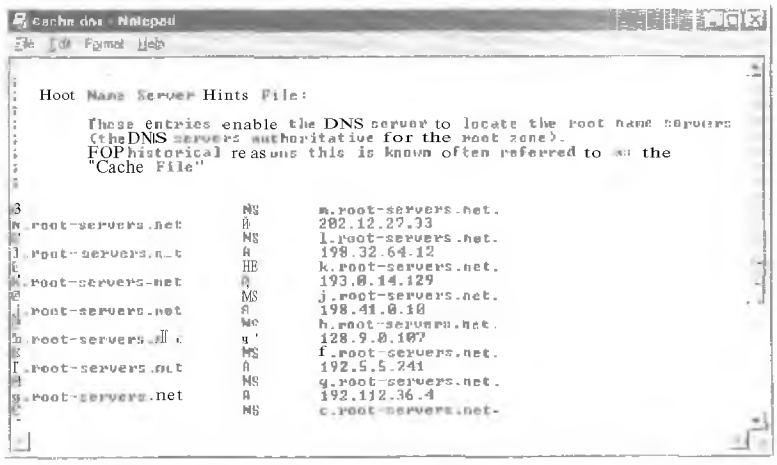


Рис. 7-11. *Редактирование* файла **CACHE.DNS**

Рис. 7-12. Создание новой зоны из консоли DNS

Вся информация основной зоны хранится на том компьютере, где она создается. При создании основной зоны вы не нуждаетесь ни в какой информации, кроме имени зоны. Дополнительные зоны получают информацию с главного сервера к процессе передачи зоны. Поэтому, когда вы создаете дополнительную зону, вы должны указать имена зоны и главного сервера.

После того как файлы описания зоны записаны на сервер, можно добавить в эти зоны поддомены. Если необходимо наличие нескольких уровней поддоменов, создавайте их последовательно. В системном реестре существует раздел для каждой зоны, которая будет создана на сервере. Они расположены в разделе KEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zones.

Каждая зона имеет свой параметр, который содержит имя файла БД и показывает, будет ли сервер DNS основным или дополнительным. Например, для зоны dev.volcano.com существует запись в реестре HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Zones\dev.volcano.com.

Настройка свойств зоны

После добавления зоны можно отредактировать ее свойства, перечисленные к табл. 7-6.

Табл. 7-6. **Свойства зоны**

Вкладка	Описание
General (Общие)	Задает файл зоны, где хранятся записи ресурсов, и указывает, будет ли сервер основным или дополнительным
SOA record (Начальная запись зоны)	Задает информацию о передаче зоны и имя почтового ящика администратора сервера имен
Notify (Уведомление)	Указывает, будет ли посылаться уведомление дополнительному серверу при изменении данных на основном. Также применяется для повышения безопасности указанием дополнительных серверов, которые могут обращаться к серверу

Табл. 7-6. **Свойства зоны** *(окончание)*

Вкладка	Описание
WINS	Позволяет серверу обращаться к службе **WINS** для разрешения имен. Здесь может быть указан список поисковых WINS-серверов. **WINS**-серверы разрешается установить только для этого сервера, щелкнув флажок Settings Only Affect Local Server. Иначе дополнительные серверы будут связываться с теми же WINS-серверами

Практикум: настройка сервера DNS

Вы добавите основную зону с сервера DNS. Выполняйте упражнение на сервере DNS.

▶ **Задание:** добавьте зону на **сервере**

1. В консоли DNS щелкните правой кнопкой имя вашего компьютера и выберите команду New Zone.

   Откроется окно мастера создания новой зоны.
2. Щелкните Next, выберите Standard Primary (Основная), затем еще раз щелкните Next.
3. Щелкните переключатель Forward Lookup Zone (Зона прямого просмотра), затем Next.
4. В поле Name (Имя) введите zonel.org (имя вашей зоны).
5. Щелкните переключатель Create A New File With This File Name (Создать новый файл), затем — Next.

   Имя файла будет Zonel.org.dns, где zonel.org — имя вашей зоны.
6. Щелкните кнопку Finish (Готово), чтобы создать новую зону.

   В папке Forward Lookup Zones появится ваш новый файл описания зоны (рис. 7-13).

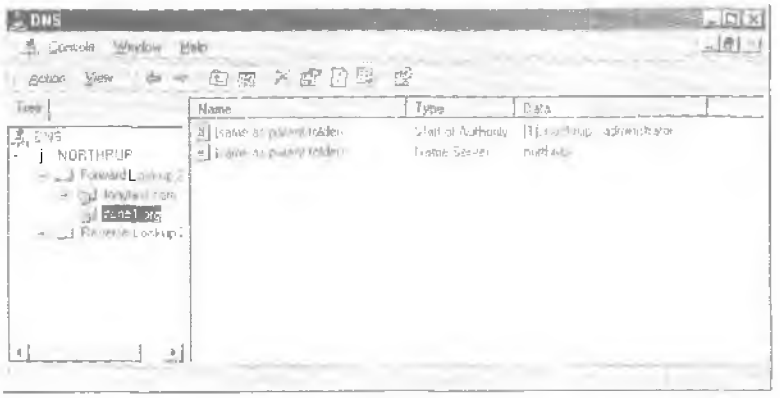


Рис. 7-13. Добавление зоны в папку зон прямого просмотра

Добавление записей ресурсов

После завершения конфигурации зон и доменок можно добавлять записи ресурсов. Чтобы создать новый узел, щелкните правой кнопкой название зоны или поддомена и выберите команду New Host (Создать узел) (рис. 7-14). Просто введите имя узла и щелкните кнопку Add Host (Добавить узел) — адресная запись узла будет создана.

Рис. 7-14. Добавление нового узла

Чтобы создать запись другого типа, щелкните правой кнопкой название зоны или поддомена и выберите команду Other New Record (Другие новые записи). Затем выберите тип создаваемой записи ресурса. В диалоговом окне отображаются разные поля в зависимости от типа записи (рис. 7-15).

Рис. 7-15. Выбор типа создаваемой записи

Настройка обратного просмотра

Чтобы найти имя узла по IP-адресу, надо создать файл обратного просмотра для каждой сети, где есть узлы из базы DNS. Процедура добавления зоны обратного просмотра идентична добавлению зоны любого другого типа, за исключением задания имени зоны. Например, если адрес узла 198.231.25.89, он должен быть представлен в домене in-addr.arpa как 89.25.231.198.in-addr.arpa. Кроме того, чтобы найти имя узла по адресу, к DNS надо доба-

вить файл описания зоны для 89.25.231.198.in-addr.arpa. Все записи ресурсов указателей (PTR) для сети 198.231.25.0 должны быть добавлены в этот файл обратного просмотра.

Резюме

Настройка сервера DNS в Windows 2000 начинается с определения структуры доменов и зон. По завершении конфигурирования зон и поддоменов можно добавлять записи ресурсов. Чтобы находить имя узла по IP-адресу, нужно создать зону обратного просмотра для каждой сети, *к* которой есть узлы из БД DNS.

Закрепление материала

7 Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. и приложении «Вопросы и ответы» в конце книги.

1. Назовите три компонента DNS.

2. Опишите разницу между основным, дополнительным и главным серверами.

3. Перечислите три причины, по которым может потребоваться дополнительный сервер имен.

4. В чем разница между доменом и зоной?

5. Чем отличаются итеративные и рекурсивные запросы?

6. Перечислите файлы, необходимые для работы версии **DNS** для Windows 2000.

7. Опишите назначение загрузочного файла сервера DNS.

ГЛАВА 8

Использование DNS

В этой главе

Вы научитесь работать с зонами системы доменных имен — Domain Name System (DNS), узнаете о применении делегированных зон и конфигурировании зон для динамического обновления. Мы также расскажем, как конфигурировать DNS-сервер кэширования и наблюдать за производительностью DNS-сервера.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Microsoft Windows 2000 Server с протоколом TCP/IP и службой DNS.

Занятие 1. Работа с зонами

Серверы обращаются к своим зонам (называемым также файлами базы данных DNS) для разрешения имен. Зоны содержат записи ресурсов, которые представляют собой информацию, ассоциированную с DNS-доменом. Например, одни записи ресурсов описывают привязки дружественных имен к IP-адресам, а другие — привязки IP-адресов к дружественным именам. Некоторые записи ресурсов содержат информацию не только о серверах в DNS-домене, но и определяют домен, указывая полномочные серверы для данной зоны. На этом занятии вы научитесь конфигурировать DNS-зоны для Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ делегировать зону для DNS;
- ✓ настроить зону для динамического обновления.

Продолжительность занятия — около 20 минут.

Делегирование зон

БД DNS может быть разделена на несколько зон. *Зона* — это часть БД DNS, содержащая записи ресурсов с именами владельцев, принадлежащих непрерывной области пространства имен DNS. Файлы зон хранятся на DNS-серверах. Один DNS-сервер можно настроить так, что он не будет обслуживать зоны совсем или будет обслуживать одну или несколько зон. Каждая зона закреплена за определенным доменным именем, которое ссылается на корневой домен зоны. Зона содержит информацию обо всех именах, которые оканчиваются именем корневого домена зоны. DNS-сервер считается полномочным для имени, если он загружает зону, содержащую это имя. Первая запись в любом файле зоны — *начальная запись ресурса* (Start Of Authority, SOA). Запись SOA определяет первичный DNS-сервер для зоны как лучший источник данных внутри зоны и как сущность, обрабатывающую обновления зоны.

Имена внутри одной зоны могут быть также делегированы другой зоне (зонам). *Делегирование* — это процесс назначения полномочий отдельной сущности для части пространства имен DNS. Эта сущность может быть другим подразделением, отделом или рабочей группой вашей организации. Технически делегирование означает передачу полномочий всей части вашего пространства имен DNS другим зонам. Делегирование представляет запись сервера имен, которая указывает делегированную зону и DNS-имя полномочного сервера для этой зоны. При разработке DNS основной целью было организовать делегирование через множество зон. Вот главные причины делегирования пространства имен DNS:

- необходимость делегировать управление DNS-доменом некоторому числу подразделений внутри организации;
- необходимость распределять нагрузку по обслуживанию одной большой БД DNS между несколькими серверами имен, чтобы увеличить скорость разрешения имен наряду с обеспечением отказоустойчивости среды DNS;
- необходимость принять во внимание организационную структуру узлов, включив их в соответствующие домены.

Записи ресурсов сервера имен облегчают делегирование, идентифицируя DNS-серверы для каждой зоны. Они присутствуют в зонах как прямого, так и обратного просмотра. Когда DNS-серверу необходимо перечень делегирование, он обращается к ресурсным записям сервера имен для DNS-серверов в целевой зоне. На рис. 8-1 управление домена microsoft.com делегировано через две зоны — microsoft.com и mydomain.microsoft.com.

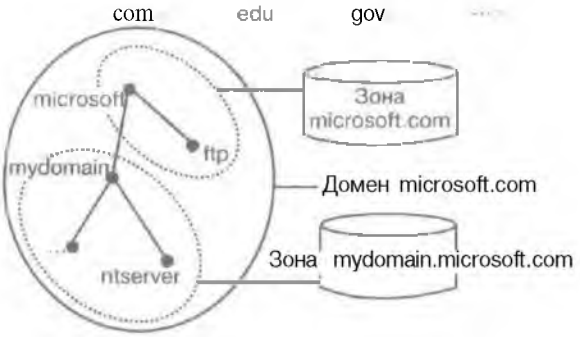


Рис. 8-1. Домен microsoft.com делегирован через две зоны

Примечание Если для делегированной зоны существует несколько записей серверов имен, идентифицирующих несколько DNS-серверов, доступных для запроса, то Windows 2000 DNS-сервер выберет ближайший DNS-сервер, вычислив время обмена данными для каждого DNS-сервера.

Что такое DNS-зоны и домены

Серверы имен домена хранят информацию о части пространства имен домена, называемой зоной. Сервер имен домена обладает полномочиями для отдельной зоны или нескольких зон. Понять различие между зоной и доменом не всегда легко.

Зона — это просто часть домена. Например, домен microsoft.com может содержать все данные о microsoft.com, marketmg.microsoft.com, development.microsoft.com. Однако зона microsoft.com содержит информацию только о microsoft.com и ссылается на полномочные серверы имен для поддоменов. Зона microsoft.com может содержать данные для поддоменов microsoft.com, если они не были делегированы другому серверу. Например, marketing.microsoft.com может обслуживать свою делегированную зону. Родитель, microsoft com, может обслуживать development.microsoft.com. Если не существует поддоменов, то зона и домен, по существу, одно и то же. В этом случае зона содержит все данные о домене.

Примечание Все домены (или поддомены), которые выступают как часть делегирования соответствующей зоны, должны быть созданы в текущей зоне до делегирования. При необходимости сначала добавьте домены к зоне с помощью оснастки DNS.

▶ **Делегирование зоны**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык DNS.
2. В дереве консоли щелкните правой кнопкой зону или поддомен и выберите команду New Delegation (Создать делегирование) (рис. 8-2).

   Откроется окно мастера делегирования.
3. Щелкните Next.
4. В окне Delegated Domain Name (Имя делегируемого домена) наберите имя делегируемого домена, затем щелкните Next.

5. В окне Name Servers (Серверы имен) щелкните Add (Добавить), чтобы указать имена и IP-адреса DNS-серверов, которые будут содержать делегированную зону, затем щелкните Next.
6. Щелкните кнопку Finish (Готово), чтобы закрыть окно мастера делегирования.

Настройка зон для динамического обновления

Первоначально служба DNS поддерживала только статические изменения в БД зоны. Из-за этих ограничений, введенных разработчиками, добавлять, удалять или модифицировать записи ресурсов мог только системный администратор DNS вручную. Например, после того как системный администратор DNS редактировал запись зоны на основном сервере, исправленная БД зоны распространялась на дополнительные серверы в процессе передачи зоны. Этот способ удобен, если количество изменений невелико и обновления вносятся не так часто, однако его сложно реализовать.

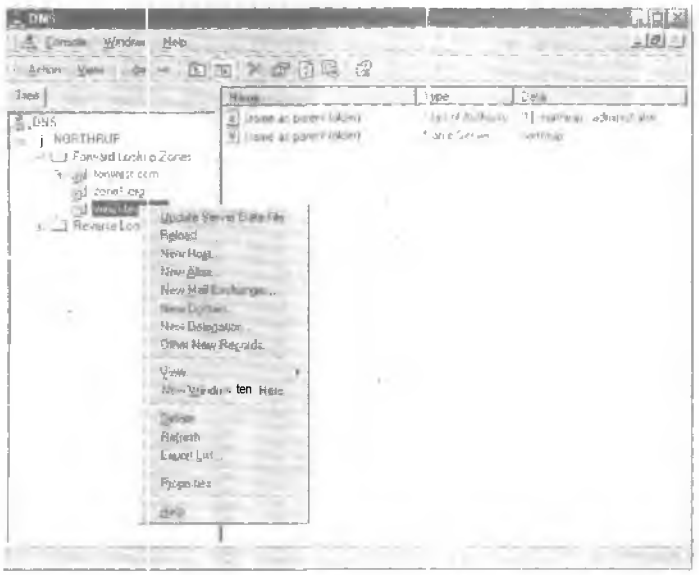


Рис. 8-2. Добавление нового сервера делегирования

Windows 2000 обеспечивает динамическое обновление как клиента, так и сервера. Динамическое обновление позволяет клиентскому компьютеру регистрировать и динамически обновлять свои записи ресурсов с помощью DNS-сервера при любом их изменении. Это исключает ручное администрирование записей зоны, особенно для клиентов, которые часто изменяют свое местоположение и используют для получения IP-адреса сервер DHCP.

По умолчанию компьютеры с Windows 2000, имеющие статический IP-адрес, пытаются динамически зарегистрировать узел и указательные записи ресурса для IP-адресов, используемых Б сетевых подключениях этих компьютеров. Динамические обновления передаются в следующих случаях:

- в результате добавления, удаления или модификации IP-адреса в конфигурации свойств любого настроенного сетевого подключения;
- после автоматического получения IP-адреса от DHCP-сервера одним из имеющихся сетевых подключений, например, когда компьютер запускается или когда используется команда ipconfig /renew;

- в результате применения команды ipconfig /registerdns для принудительного обновления имени клиента в DNS;
- при включении питания компьютера.

Требования к динамическому обновлению

Для DNS-серверов служба DNS позволяет разрешать или запрещать динамическое обновление по зонам для каждого сервера, настроенного для загрузки стандартной основной либо встроенной в каталог зоны. По умолчанию клиентский компьютер с любой версией Windows 2000 динамически обновляет свои записи ресурсов в DNS, если на нем установлен TCP/IP. Если DNS-зоны хранятся в Active Directory, DNS по умолчанию настраивается для динамического обновления.

Примечание В Windows 2000 DNS-сервер поддерживает динамическое обновление. DNS-сервер, поставляемый с Windows **NT** Server 4.0, этого не делает.

Перед запросом на выполнение динамического обновления необходимо выполнить проверку некоторых условий. Каждая проверка должна осуществляться до обновления. После выполнения всех проверок основной сервер зоны может обновлять свои локальные зоны. Вот некоторые примеры таких проверок:

- необходимая запись ресурса или набор записей уже существуют или используются перед обновлением;
- необходимая запись ресурса или набор записей ресурсов не существуют или не используются перед обновлением;
- запросчик разрешил начать обновление определенной записи ресурса или их набора.

Чтобы клиентский компьютер регистрировался и обновлялся динамически с помощью DNS:

- установите или обновите клиентский компьютер до Windows 2000;
- установите Windows 2000 DHCP-сервер в вашей сети для выделения IP-адресов клиентским компьютерам.

Практикум: включение динамического обновления

Разрешите DNS-клиентам регистрироваться и динамически обновлять свои записи ресурсов с помощью DNS-сервера, включив динамическое обновление для зоны DNS.

Задание: включите **динамическое** обновление

скройте меню Start\Programs\Administrative Tools и щелкните ярлык DNS.
поется консоль администратора DNS.
- консоли щелкните правой кнопкой вашу зону и выберите команду Properties.
' диалоговое окно свойств зоны (рис. 8-3).
w Dynamic Updates (Динамическое обновление) выберите Yes (Да).
', чтобы закрыть окно свойств зоны.
ль администратора DNS.

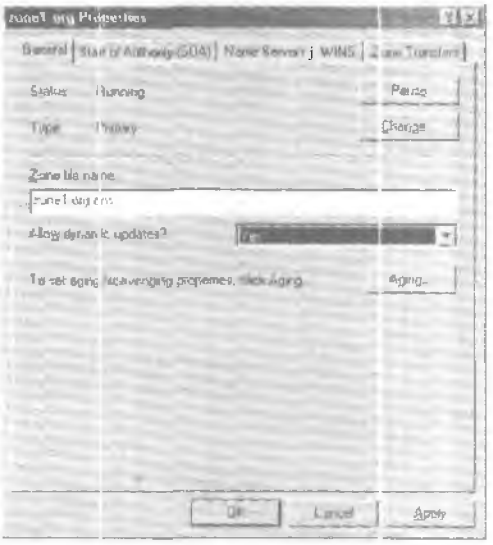


Рис. 8-3. Диалоговое окно свойств зоны

Резюме

Делегирование — это процесс назначения полномочий для части пространства имен DNS отдельной сущности. Записи ресурсов серверов имен облегчают делегирование, отождествляя DNS-сервер с каждой зоной. Они присутствуют как в зоне прямого, так и обратного просмотра. Windows 2000 поддерживает динамическое обновление клиента и сервера. Динамическое обновление позволяет DNS-клиентам регистрироваться и динамически обновлять свои записи ресурсов с помощью DNS-сервера, если происходят какие-либо изменения.

Занятие 2 Работа с DNS-серверами

Поскольку DNS-серверы имеют решающее значение в большинстве конфигураций; за ними необходимо постоянно наблюдать. Вы узнаете, как обслуживать DNS-сервер и проводить мониторинг его работы. Также вы научитесь настраивать сервер кэширования.

Изучив материал этого занятия, вы сможете:

- ✓ конфигурировать сервер кэширования;
- ✓ обслуживать и вести мониторинг DNS-сервера.

Продолжительность занятия — около 15 минут.

Серверы DNS и кэширование

DNS-серверы обрабатывают запросы клиентов, используя рекурсию или итерации. Они исследуют пространство имен DNS и, найдя необходимую информацию, сохраняют ее в кэше. Кэширование позволяет ускорить разрешение имен DNS и сократить сетевой трафик при обработке запросов часто используемых имен.

DNS-серверы выполняют рекурсивные запросы со стороны клиентов, которые временно кэшируют записи ресурсов. Записи ресурсов в кэше содержат информацию, полученную от полномочных для доменных имен DNS-серверов. Позже, когда другие клиенты посылают новые запросы информации о кэшированной записи ресурса, DNS-сервер для ответа на запрос берет искомые данные из кэша.

Когда информация кэшируется, то всем записям ресурсов в кэше задается *время жизни* (Time To Live, TTL). Пока оно не истечет, DNS-сервер продолжает хранить в памяти и использовать кэшированные записи ресурсов. Значение TTL, заданное в записи SOA, по умолчанию составляет 3 600 секунд (1 час), но его можно увеличить или, если необходимо, настроить индивидуально для каждой записи ресурса.

Запуск DNS-сервера кэширования

Хотя все DNS-серверы способны кэшировать выполненные ими запросы, DNS-сервер кэширования только выполняет запросы, сохраняет в кэше ответы и возвращает результаты. Эти серверы не полномочны для любых доменов, и хранящаяся на них информация ограничена кэшем, накопленным при разрешении запросов. Удобно, что серверы кэширования не создают трафика, связанного с передачами зон, поскольку не содержат каких-либо зон. Впрочем, есть и недостаток: когда сервер запускается, на нем нет кэшированной информации, и он должен собрать ее при выполнении запросов.

Установка DNS-сервера кэширования

1. Установите службу DNS Server на вашем компьютере.

   При установке DNS-сервера рекомендуется вручную настраивать TCP/IP и задавать статический IP-адрес.

2. Не настраивайте DNS-сервер для загрузки какой-либо зоны.

   Сервер кэширования может быть полезен в сайте, где требуется локальная функциональность DNS, но не надо создавать отдельный домен или зону. DNS-серверы кэширования не содержат зон и не обладают полномочиями для какого-либо домена. Они содержат лишь локальный серверный кэш имен, накопленный в ходе выполнения рекурсивных запросов со стороны клиентов.

3. Убедитесь, что корневые ссылки сервера верно настроены и обновлены.

Во время запуска DNS-серверу необходим список *корневых ссылок* (root hints). Эти ссылки представляют собой записи серверов имен (name server, NS) и адресов (address, A) для корневых серверов.

Вы можете настроить корневые ссылки на вкладке Root Hints (Корневые ссылки) диалогового окна свойств сервера DNS в консоли администратора DNS (рис. 8-4).

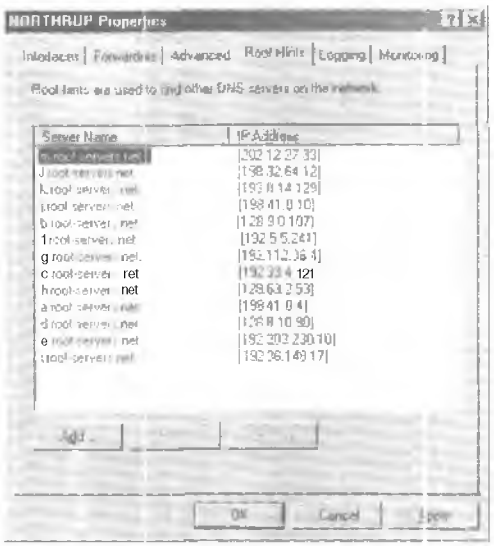


Рис. 8-4. Вкладка Root Hints (Корневые ссылки) окна свойств DNS-сервера

Мониторинг производительности DNS-сервера

Поскольку DNS-серверы очень важны в большинстве конфигураций, наблюдение за их производительностью может быть полезно при прогнозировании, оценке и оптимизаиии быстродействия DNS-сервера. На основе собранных данных вы легко выявите падение производительности сервера ниже приемлемого уровня и периоды пиковой нагрузки. Windows 2000 Server включает набор счетчиков производительности DNS-сервера, которые можно применять и в системном мониторе (System Monitor) для наблюдения за различными параметрами активности сервера.

Практикум: тестирование простого запроса на сервере DNS

Задействуйте консоль администратора DNS для тестирования запроса на вашем DNS-сервере.

▶ **Задание: протестируйте запрос на вашем DNS-сервере**

1. Раскройте меню Start\Programs\Administrative Toots и щелкните ярлык DNS.
2. В дереве консоли щелкните правой кнопкой DNS-сервер и выберите команду Properties.
3. Перейдите на вкладку Monitoring (Наблюдение) (рис. 8-5).

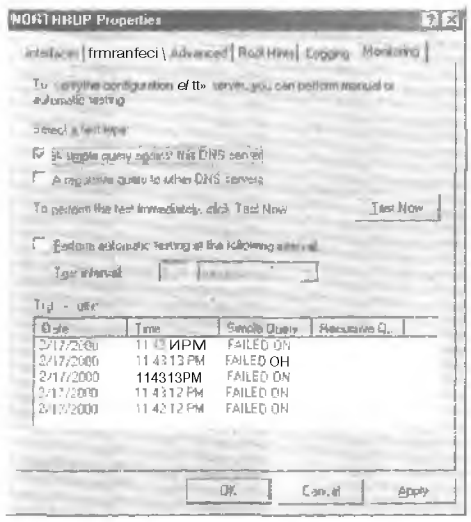


Рис. 8-5. Вкладка Monitoring (Наблюдение) диалогового окна свойств DNS-сервера

4. Пометьте флажок A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу).
5. Щелкните кнопку Test Now (Тест).
   Результаты теста появятся в списке ниже.
6. Щелкните OK, чтобы закрыть диалоговое окно свойств DNS-сервера.

Счетчики производительности DNS-сервера

Windows 2000 Server включает набор счетчиков производительности DNS-сервера, которые можно использовать для наблюдения за различными параметрами активности сервера, такими, как:

- общая статистика производительности DNS-сервера, например общее количество запросов и ответов, обработанных сервером;
- счетчики UDP (User Datagram Protocol) или TCP (Transmission Control Protocol) для измерения запросов и ответов DNS, обработанных с использованием каждого из этих транспортных протоколов;
- счетчики динамических обновлений и безопасных динамических обновлений для измерения действий по регистрации и обновлению, генерируемых динамическими клиентами;
- счетчики использования памяти для измерения использования системной памяти и схем выделения памяти, создаваемых DNS-сервером Windows 2000;
- счетчики рекурсивного просмотра для измерения запросов и ответов, когда служба DNS использует рекурсию для просмотра и полного сопоставления имен DNS для запрашивающих клиентов;
- счетчики просмотра WINS для измерения запросов и ответов WINS-серверов, когда служба DNS использует средства просмотра WINS;
- счетчики зонных передач, включая отдельные счетчики для измерений следующих величин: все зонные передачи (AXFR), добавочные зонные передачи (1XFR) и активность уведомлений при обновлении зон DNS.

Удаленное управление DNS-серверами

DNS — это стандартная служба имен Интернета и **TCP/IP,** позволяющая клиентам вашей сети регистрироваться на сервере, где работает служба DNS, и разрешать доменные имена. Эти имена могут быть использованы для поиска и доступа к ресурсам, предоставляемым другими компьютерами в Интернете. Средства администрирования из комплекта Windows 2000 Server и Windows 2000 Advanced Server позволяют удаленно управлять сервером с любого компьютера, где работает Windows 2000.

Средства администрирования Windows 2000 включают оснастки для консоли управления Microsoft (MMC) и другие утилиты для управления компьютером с Windows 2000 Server, не входящие в Windows 2000 Professional.

Резюме

Хотя все серверы имен DNS кэшируют разрешаемые ими запросы, серверы кэширования только выполняют запросы, кэшируют ответы и возвращают результаты. Достоинство серверов кэширования в том, что они не создают сетевого трафика, связанного с передачами зон, поскольку не содержат зон. Windows 2000 Server предлагает набор счетчиков производительности DNS-сервера, которые применяются в системном мониторе для наблюдения за различными параметрами активности сервера. Для наблюдения за работой DNS-сервера можно использовать вкладку Monitoring диалогового окна свойств DNS-сервера в консоли администратора DNS или средства администрирования для удаленного управления сервером с любого компьютера Windows 2000.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответс гвующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Сколько зон способен обслуживать один DNS-сервер?

2. Какие преимущества получают DNS-клиенты от динамического обновления в Windows 2000?

3. Назовите достоинства и недостатки DNS-сервера кэширования.

4. Назовите три счетчика производительности DNS.

ГЛАВА 9

Внедрение WINS

В этой главе

В сети, полностью состоящей из компьютеров с Microsoft Windows 2000, использовать серверы WINS (Windows Internet Name Service) не требуется. Тем не менее В большинстве TCP/1P-сетей, где работают компьютеры с устаревшими архитектурами (Windows NT 4.0, Windows 98, или Windows 95), WINS-серверы необходимы. Здесь рассказывается о внедрении WINS в сети вашей организации.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server и протокол TCP/IP.

Занятие 1. Знакомство с WINS

Служба WINS предоставляет распределенную базу данных, позволяющую регистрировать и запрашивать динамические привязки NetBIOS-имен компьютеров и групп вашей сети. WINS привязывает имена NetBIOS к IP-адресам и предназначена для устранения проблем преобразования имен NetBIOS в маршрутизируемых средах. WINS наилучшим образом подходит для разрешения имен NetBIOS в маршрутизируемых средах, использующих NetBIOS поверх TCP/IP.

Изучив материал этого занятия, вы сможете:

- ✓ описать связь между NetBIOS и TCP/IP;
- ✓ описать преимущества использования службы WINS;
- ✓ описать новые возможности Windows 2000, связанные с NetBIOS.

Продолжительность занятия - около 15 минут.

Разрешение имен NetBIOS

Здесь описываются базовые концепции и методы разрешения имен NetBIOS. Основная цель данного раздела — помочь вам глубже понять функциональность WINS — обусловлена прежде всего тем, что предыдущие версии Windows, например Windows NT 4.0, а также некоторые Windows-приложения используют имена NetBIOS для идентификации сетевых ресурсов.

Общие сведения о NetBIOS

NetBIOS разработан в 1983 г. Sytek Corporation для IBM как протокол, позволяющий взаимодействовать приложениям по сети. NetBIOS определяет (рис. 9-1):

- сеансовый интерфейс;
- протокол управления сеансом/передачей данных.

Интерфейс NetBIOS — API-интерфейс уровня представления, позволяющий пользовательским приложениям передавать протоколам более низких уровней команды сетевого ввода-вывода и управляющие команды. Любая программа, использующая API-интерфейс NetBIOS для коммуникаций, способна выполняться по любому протоколу, поддерживающему данный интерфейс. Такая возможность обеспечивается средствами программного обеспечения сеансового уровня (например, протокола NetBIOS Frame Protocol или протокола NetBT), которое выполняет операции сетевого ввода-вывода, необходимые для поддержки набора команд интерфейса NetBIOS.

NetBIOS предоставляет команды и поддерживает следующие службы:

- регистрацию и проверку сетевых имен;
- установку и завершение сеанса связи;
- надежную передачу данных с обязательным установлением логического соединения;
- ненадежную передачу данных с использованием дейтаграмм без обязательного установления логического соединения;
- мониторинг и управление вспомогательным протоколом (драйвером) и адаптером.

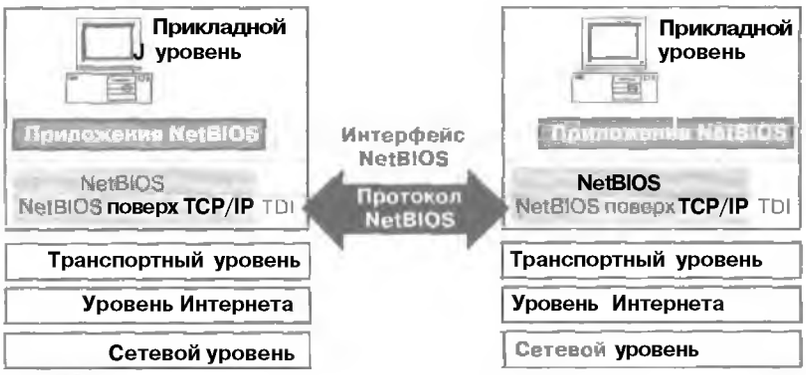


Рис. 9-1. Сетевая связь NetBIOS поверх TCP/IP

Имена NetBIOS

Имя NetBIOS — уникальный 16-разрядный адрес, идентифицирующий ресурс NetBIOS в сети. Имена NetBIOS могут быть как уникальными (монопольными), так и групповыми (общими). Уникальные обычно применяются для взаимодействия со специфическим процессом системы, а групповые — для одновременной рассылки информации нескольким компьютерам. В качестве примера процесса, использующего имя NetBIOS, можно назвать службу доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks), выполняющуюся на компьютере с Windows 2000. При запуске системы данная служба регистрирует уникальное имя NetBIOS, основываясь на имени вашего компьютера. Служба доступа к файлам и принтерам использует следующий формат имени NetBIOS: имя компьютера длиной 15 символов плюс 16-й символ (0x20). Если имя компьютера короче 15 символов, служба дополняет его соответствующим числом пробелов.

Разрешение имен NetBIOS — процесс преобразования имени компьютера NetBIOS в его IP-адрес. Перед тем как IP-адрес удастся преобразовать в аппаратный адрес (MAC-адрес сетевого адаптера), надо преобразовать NetBIOS-имя заданной системы в соответствующий IP-адрес. Версия пакета протоколов TCP/IP, реализованная Microsoft, использует несколько способов разрешения имен NetBIOS. Тем не менее конкретный механизм преобразования зависит от типа узла NetBIOS, сконфигурированного для конечной системы. Типы узлов NetBIOS определены в RFC 1001, «Protocol Standard for a NetBIOS Service on a TCP/UDP Transport; Concepts and Methods» (табл. 9-1).

Табл. 9-1. Типы узлов NetBIOS

Тип узла	Описание
B-узел (широковещательный)	Использует широковещательные запросы имен NetBIOS для регистрации и разрешения имен. B-узел характеризуется двумя основными проблемами: 1) широковещание затрагивает каждый узел в сети; 2) маршрутизаторы обычно не пересылают широковещательный трафик, и поэтому разрешение **имен NetBIOS** ограничивается лишь локальной сетью
P-узел (соединение равноправных узлов ЛВС, одноранговый узел)	Использует сервер имен NetBIOS, например сервер WINS, для разрешения имен NetBIOS. P-узел не рассылает широковещательные запросы, а обращается напрямую к серверу имен

(см. след. стр.)

Табл. 9-1. Типы узлов NetBIOS (*окончание*)

Тип узла	Описание
M-узел (смешанный)	Комбинация B-узла и P-узла. По умолчанию любой M-узел функционирует как B-узел. В случае если M-узел не в состоянии разрешить какое-то имя посредством широковещания, он запрашивает сервер имен NetBIOS
H-узел (гибрид)	Комбинация P-узла и B-узла. По умолчанию любой H-узел функционирует как P-узел. Если H-узел не в состоянии разрешить имя через сервер имен NetBIOS, он преобразует имя с помощью широковещательной рассылки

Компьютеры Windows 2000 по умолчанию функционируют как B-узлы; после того как для них определен WINS-сервер, они начинают функционировать в качестве H-узлов. Для разрешения удаленных NetBIOS-имен Windows 2000 также может использовать файл локальной БД адресов под названием LMHOSTS. Он хранится в папке %systemroot%\System32\Drivers\Etc. Кроме того, в этом каталоге находится образец файла LMHOSTS (LMHOSTS.SAM).

Файл LMHOSTS

Статический ASCII-файл, используемый для преобразования имен NetBIOS в IP-адреса удаленных компьютеров с Windows NT, а также других NetBIOS-компьютеров. На рис. 9-2 показан пример файла LMHOSTS.

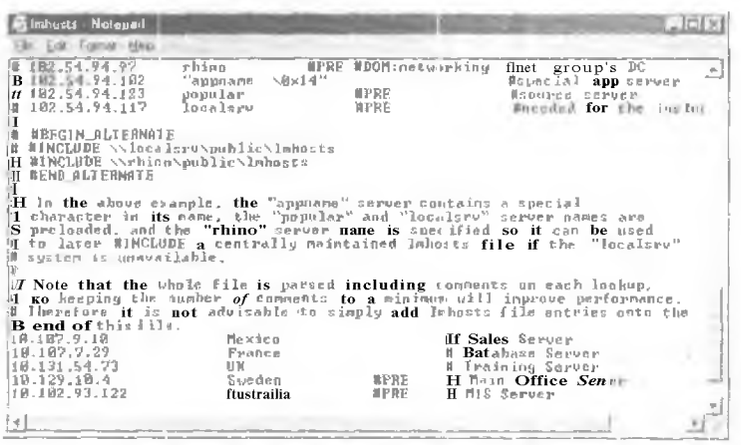


Рис. 9-2. Файл LMHOSTS

Предопределенные ключевые слова

В файле LMHOSTS также содержатся предопределенные ключевые слова, которым предшествует символ #. При использовании файла LMHOSTS в устаревшей системе NetBT, например в LAN Manager, эти директивы будут рассматриваться исключительно в качестве комментариев, поскольку они начинаются с символа #. Допустимые ключевые слова файла LMHOSTS перечислены в табл. 9-2.

Табл. 9-2. Ключевые слова файла LMHOSTS

Предопределенное ключевое слово	Описание
#DOM:[*имя_домена*]	Позволяет осуществлять некоторые функции лочена. например проверку регистрации в домене при подключении через маршрутизатор. синхронизацию учетных записей и просмотр ресурсов
#PRE	Определяет записи файла, предварительно загружаемые в кэш имен в качестве постоянных элементов. Такие элементы позволяют снизить объем широковещательного трафика в сети, поскольку разрешение имен осуществляется с использованием кэша. а не широковещательных рассылок и файла LMHOSTS. Записи с префиксом #PRE автоматически помешаются *в* кэш в процессе инициализации. Кроме того. их можно поместить в кэш имен вручную, выполнив в окне сеанса MS-DOS команду nbtstat-R
#NOFNR	Блокирует использование запросов на разрешение имен. управляемых NetBIOS. в устаревших UNIX-системах на основе LAN Manager
#BEGIN_ALTERNATE #END **ALTERNATE**	Определяет избыточный список альтернативных местоположений файлов LMHOSTS. Для обеспечения доступа к удаленным файлам #INCLUDE при указании пути рекомендуется использовать UNC-имя файла. Разумеется, наряду с UNC-именем в файле LMHOSTS должна присутствовать *соответствующая* привязка «IP-адрес/имя NetBIOS»
#INCLUDE	Ищет и загружает записи NetBIOS из файла LMHOSTS, отличного от файла. используемого по умолчанию. Обычно файл #INCLUDE — это центральный совместно используемый файл LMHOST
#MH	Добавляет несколько записей для компьютера с несколькими сетевыми адаптерами

Общие сведения о WINS

WINS устраняет необходимость применения широковещания для разрешения имен NetBIOS и предоставляет динамическую БД, содержащую привязки имен компьютеров к IP-адресам. WINS — это усовершенствованный сервер имен NetBIOS (NBNS), разработанный Microsoft с целью снижения широковещательного трафика, вызываемого реализацией NetBT на основе B-узлов. WINS применяется для регистрации NetBIOS-имен локальных и удаленных систем и преобразования этих имен в IP-адреса.

Выгода от использования WINS очевидна. Важнейшее преимущество — пересылка клиентских запросов на разрешение имен непосредственно WINS-серверу. Если сервер WINS может разрешить имя, он отсылает соответствующий IP-адрес непосредственно клиенту. Таким образом, отпадает потребность в широковещании и снижается объем сетевого трафика. При отсутствии сервера WINS для разрешения имени клиент WINS может воспользоваться широковещанием. Еще одно преимущество заключается в динамическом обновлении БД WINS, то есть информация этой БД всегда актуальна. Это устраняет потребность в файле LMHOSTS. Кроме того. WINS предоставляет возможность просмотра ресурсов сети и других доменов.

Для установления связи между двумя NetBIOS-компьютерами необходимо преобразовать NetBIOS-имя конечной системы в IP-адрес. Это связано с тем, что для коммуникаций стек протоколов **TCP/IP** использует IP-адреса, а не имена NetBIOS. Вот как происходит разрешение имен (рис. 9-3).

1. В среде WINS при запуске клиент WINS регистрирует свою привязку «имя NetBIOS/IP-адрес» на соответствующем сервере WINS,
2. После того как клиент WINS выполняет команду для связи с другим компьютером, вместо широковещания по локальной сети запрос на разрешение имени пересылается непосредственно серверу WINS.
3. Если сервер WINS находит в своей БД привязку «имя NetBIOS/IP-адрес» для конечной системы, он возвращает WINS-клиенту IP-адрес конечного компьютера. Поскольку привязки «имя NetBIOS/IP-адрес» обновляются в БД WINS динамически, содержащаяся в ней информация всегда соответствует текущему положению дел.

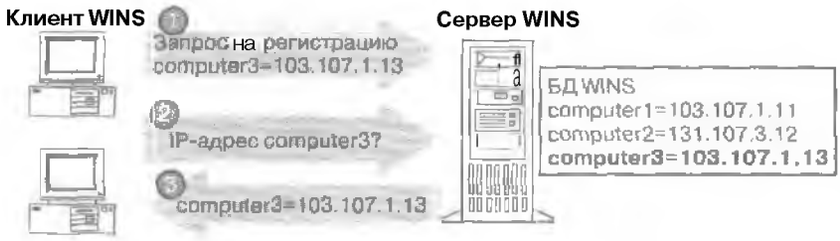


Рис. 9-3. Разрешение имен с использованием WINS

WINS и Windows 2000

До появления Windows 2000 всем ОС семейств MS-DOS и Windows для работы с сетью требовался интерфейс службы имен NetBIOS. С выходом Windows 2000 потребность в наличии интерфейса NetBIOS для работы с сетью отпала, поскольку теперь вы можете отключать протокол NetBT для отдельных сетевых подключений. Данное средство предназначено только для компьютеров, регистрирующих и разрешающих имена с использованием DNS и устанавливающих соединения с другими компьютерами, на которых NetBT отключен, с применением компонентов Client for Microsoft Networks (Клиент для сетей Microsoft) и File and Print Sharing for Microsoft Networks (Служба доступа к файлам и принтерам для сетей Microsoft). Так, протокол NetBT можно отключать на системах, выполняющих в вашей сети специализированные или защищенные функции, например на прокси-сервере в защищенной брандмауэром среде, где поддержка NetBT не требуется или нежелательна.

В качестве еще одного примера можно назвать среду, где компьютеры и программы поддерживают использование DNS. Причем эти компьютеры и программы можно сконфигурировать для работы под управлением Windows 2000 и других операционных систем, не требующих имен NetBIOS, например некоторых версий UNIX. Тем не менее в большинстве сетей до сих пор необходима интеграция устаревших ОС, требующих имен NetBIOS, и компьютеров с Windows 2000. В связи с этим Microsoft реализовала в Windows 2000 поддержку имен NetBIOS по умолчанию, упрощающую взаимодействие с устаревшими ОС, которым такие имена необходимы. Такая поддержка обеспечивается, как правило, одним из двух методов.

- По умолчанию на всех компьютерах с Windows 2000, использующих TCP/IP, устанавливается клиент для разрешения и регистрации имен NetBIOS.

Поддержка регистрации и разрешения имен осуществляется через NetBT и при желании ее можно отключить вручную.

- На компьютерах с Windows 2000 Server устанавливается сервер WINS. Служба WINS позволяет эффективно управлять сетями на основе NetBT.

Резюме

Некоторые приложения и предыдущие версии Windows используют имена NetBIOS для идентификации сетевых ресурсов. Служба WINS — это усовершенствованный сервер имен NetBIOS, разработанный Microsoft с целью снижения широковещательного трафика, вызываемого реализацией NetBT на основе B-узлов. Преимущества использования WINS очевидны. Важнейшее из них — снижение объема широковещательного трафика в результате пересылки клиентских запросов на разрешение имен напрямую WINS-серверу.

Занятие 2. Разрешение имен с использованием WINS

WINS использует стандартные методы регистрации, обновления и освобождения имен. На этом занятии описываются различные фазы преобразования имени NetBIOS в IP-адрес с использованием службы WINS.

Изучив материал этого занятия, вы сможете:

- ✓ описать регистрацию, обновление, высвобождение, запрос и разрешение имени с использованием службы WINS.

Продолжительность занятия — около 25 минут.

Разрешение имен NetBIOS с использованием WINS

Если клиенту требуется установить соединение с другим компьютером той же сети, он сначала обращается к серверу WINS для разрешения IP-адреса конечной системы с использованием информации о привязках «имя NetBIOS/IP-адрес», хранящейся в БД сервера. Реляционный процессор БД сервера WINS обращается к базе данных с индексно-последовательным доступом. Она представляет собой реплицированную БД, содержащую привязки «имя NetBIOS/IP-адрес» для компьютеров сети. Для входа в сеть клиент WINS должен зарегистрировать имя и IP-адрес своего компьютера на сервере WINS. При этом в БД WINS создаются записи для всех служб NetBIOS, выполняющихся на клиентской системе. Так как эти записи обновляются каждый раз, когда клиент входит в сеть, информация, хранимая в БД WINS, остается точной.

Служба WINS разрешает и поддерживает имена NetBIOS по аналогии с реализацией B-узлов. Метод обновления имени для каждого типа узлов NetBIOS, использующего сервер имен NetBIOS, уникален. Служба WINS — это расширение стандартов RFC 1001 и RFC 1002. Процесс разрешения имени NetBIOS показан на рис. 9-4.

Регистрация имени

Для каждого клиента WINS задается IP-адрес основного сервера WINS и при желании дополнительного сервера WINS. При запуске клиент регистрирует имя NetBIOS и IP-адрес своего компьютера на определенном для него сервере WINS. Сервер WINS заносит привязку «имя NetBIOS/IP-адреса» для клиентской системы в свою БД.

Обновление имени

Все имена NetBIOS регистрируются временно. Это означает, что, если система, владеющая именем NetBIOS, прекратит его применение, позднее это имя может использоваться другим компьютером.

Высвобождение имени

Каждый клиент WINS отвечает за продление срока аренды своего зарегистрированного имени. Если имя больше использоваться не будет (например при выключении компьютера), клиент WINS отправляет серверу WINS запрос на высвобождение имени.

Запрос на определение имени и разрешение имени

После регистрации имени NetBIOS и IP-адреса своего компьютера на сервере WINS клиент WINS может устанавливать связь с другими системами, получая с сервера WINS IP-адреса других NetBIOS-систем. Все WINS-коммуникации осуществляются с применением направленных дейтаграмм UDP через порт 137 (служба имен NetBIOS).

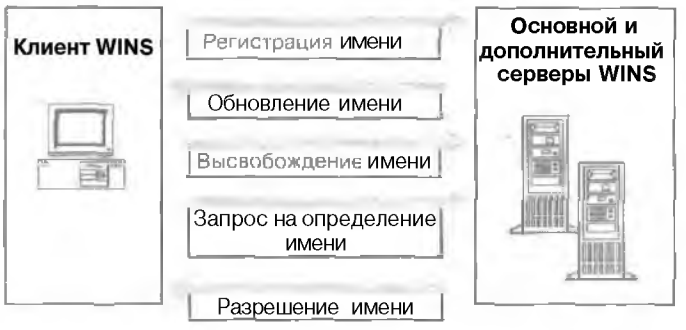


Рис. 9-4. Разрешение имен между клиентами и сервером WINS

Регистрация имен

В отличие от реализации NetBT на основе B-узлов, когда регистрация имен осуществляется посредством широковещания, клиенты WINS регистрируют свои имена NetBIOS на серверах службы WINS.

При инициализации клиент WINS регистрирует свое NetBIOS-имя, напрямую отсылая запрос на регистрацию сконфигурированному для этого клиента серверу WINS. Имена NetBIOS регистрируются при запуске приложений и служб, например Workstation, Server и Messenger.

Если WINS-сервер доступен и требуемое имя не зарегистрировано другим клиентом WINS, клиенту возвращается сообщение об успешной регистрации имени. Сообщение включает сведения о периоде, на который NetBIOS-имя выдсляется клиенту. Этот период указывается как время жизни (TTL). Процесс регистрации имени проиллюстрирован на рис. 9-5.

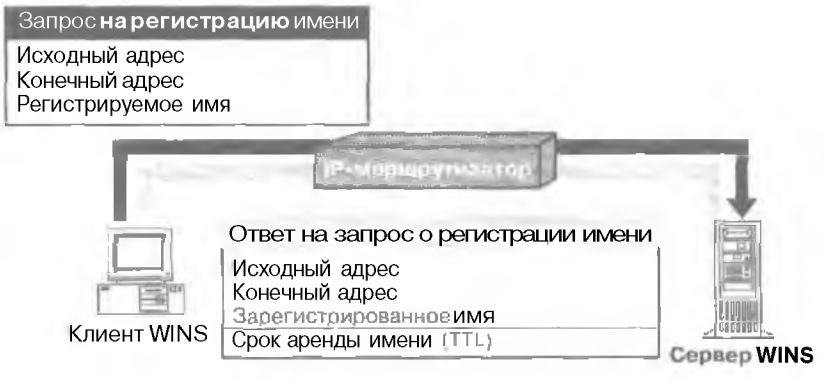


Рис. 9-5. Процесс регистрации имени

Если обнаружено идентичное имя

При попытке клиента зарегистрировать имя, идентичное имеющемуся в БД WINS, сервер WINS посылает вызов компьютеру, владеющему именем в настоящий момент. Вызов отправляется три раза с интервалом 500 мс в форме запроса на определение имени.

Если на компьютере, владеющем искомым именем, установлено несколько сетевых адаптеров, сервер WINS проверяет все IP-адреса данной системы, пока не получит ответ или не переберет все адреса.

После успешного ответа системы, владеющей именем в настоящий момент, сервер WINS посылает клиенту WINS, пытающемуся зарегистрировать имя, отрицательный ответ. Если же владелец имени не отвечает, сервер WINS посылает клиенту WINS, пытающемуся зарегистрировать имя, положительный ответ.

Если сервер WINS недоступен

Клиент WINS трижды пытается обнаружить основной сервер WINS. Если основной сервер не обнаружен, запрос на регистрацию имени передается дополнительному серверу WINS (если таковой определен). При недоступности обоих серверов клиент WINS может попытаться зарегистрировать свое NetBIOS-имя посредством широковещания.

Обновление имен

Чтобы продолжать использовать выделенное ему имя NetBIOS, клиенту необходимо периодически обновлять срок аренды имени, до того как тот истечет. В случае если клиент не продлит аренду имени, сервер WINS делает это имя доступным для других клиентов WINS.

Продление аренды имени

Для использования старого NetBIOS-имени клиент должен продлять срок аренды до истечения последнего. Если клиент не обновил период аренды, сервер WINS делает NetBIOS-имя доступным для получения другими клиентами.

Запрос на продление аренды имени

Клиенты WINS должны продлевать регистрацию имен до того, как истечет интервал времени, отведенный для продления аренды имени. Этот интервал определяет срок, в течение которого сервер хранит регистрацию в качестве активной записи БД WINS. При обновлении регистрации клиент WINS посылает серверу WINS запрос на обновление имени. Он включает IP-адрес и имя NetBIOS, которые необходимо обновить. Сервер WINS отсылает в ответ подтверждение, содержащее новый интервал, в течение которого требуется продлить регистрацию имени. Обновление NetBIOS-имени клиентом WINS состоит из нескольких этапов.

1. По прошествии половины интервала TTL клиент WINS пытается продлить срок аренды, запросив основной сервер WINS.
2. Если основной сервер WINS не продлил аренду, клиент WINS попробует повторно обновить имя через 10 минут и в случае неудачи будет пытаться продлить аренду с помощью основного сервера WINS каждые 10 минут на протяжении 1 часа. Если по прошествии часа клиент не сможет продлить аренду имени, используя основной сервер WINS, он переключится "на дополнительный сервер.
3. В случае если клиенту не удастся продлить срок аренды с помощью дополнительного сервера WINS, он попробует повторно обновить имя через 10 минут и в случае неудачи будет пытаться продлить аренду с помощью дополнительного сервера WINS каждые 10 минут на протяжении 1 часа. После неудачных попыток обновить регистрационное

имя на дополнительном сервере WINS в течение часа клиент переключится на основной сервер. Этот процесс продолжается до тех пор, пока не истечет интервал TTL или пока не будет продлен срок аренды имени.

4. При успешном **продлении аренды имени** клиентом **WINS интервал TTL** на сервере **WINS** обнуляется.
5. Если клиент WINS не сможет в течение интервала TTL продлить срок аренды имени ни на основном, ни на дополнительном сервере WINS, имя высвобождается.

Процесс продления срока аренды старого имени NetBIOS клиентом WINS проиллюстрирован на рис. 9-6.

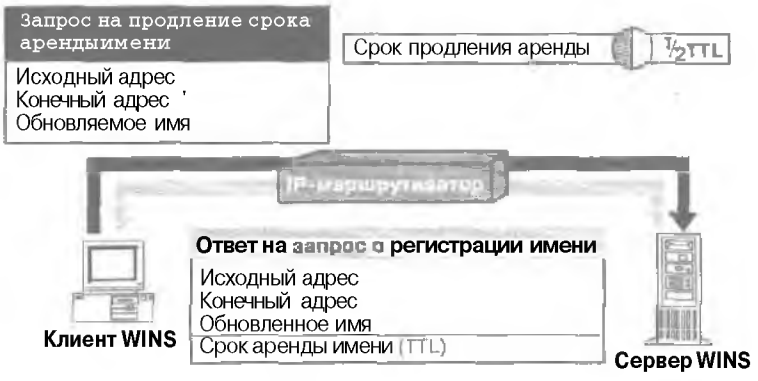


Рис. 9-6. Продление срока аренды старого имени NetBIOS

Освобождение имени

Если NetBIOS-имя больше не требуется, клиент WINS сообщает серверу WINS об освобождении имени. При корректном выключении клиент WINS отсылает серверу запрос, включающий IP-адрес клиента и его NetBIOS-имя, на освобождение каждого зарегистрированного имени. Это позволяет серверу сделать данные имена доступными для других клиентов (рис. 9-7).

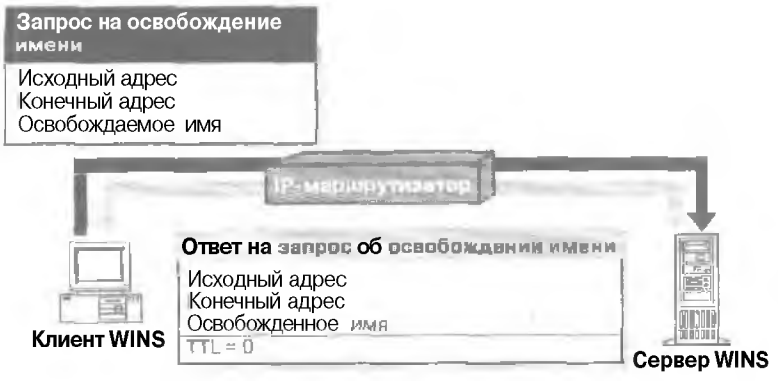


Рис. 9-7. Запрос на освобождение имени

При получении запроса на освобождение имени сервер WINS проверяет наличие указанного имени в своей БД. Если в БД будет обнаружена ошибка или к зарегистрированному имени окажется привязанным другой IP-адрес, сервер WINS откажет клиенту в освобождении имени. В противном случае сервер подтвердит освобождение имени и отме-

тит в БД это имя как освобожденное. Ответ об освобождении имени включает NetBIOS-имя и значение TTL, равное 0.

Разрешение имен

Одним из распространенных способов разрешения имен NetBIOS в IP-адреса является использование серверов имен NetBIOS, например службы **WINS.** По умолчанию все новые узлы WINS конфигурируются как H-узлы NetBT. Перед широковещанием для всех привязок «имя NetBIOS/IP-адрес» обязательно задается сервер имен NetBIOS. Процесс разрешения имени описан ниже и проиллюстрирован на рис. 9-8.

1. При выполнении команды Windows NT, например net use, кэш NetBIOS-имен клиентской системы проверяется на наличие привязки «NetBIOS-имя/IP-адрес», соответствующей конечному компьютеру.
2. Если клиент не может разрешить имя, используя кэш, он посылает запрос на определение имени непосредственно своему основному серверу WINS.

   При недоступности основного сервера WINS клиент отошлет запрос еще дважды. Затем он переключится на дополнительный сервер WINS.

   Если любой из серверов WINS (основной или дополнительный) разрешит имя, он пошлет клиенту ответ с IP-адресом, соответствующим запрошенному NetBIOS-имени.
3. Если ни один из серверов WINS не сможет разрешить имя, клиент получит сообщение о том, что запрошенное имя не существует, и начнет широковещательную рассылку в сети.

   Если клиенту не удалось разрешить искомое имя ни с помощью серверов WINS, ни посредством широковещания, стоит воспользоваться файлом LMHOSTS, файлом Hosts или службой DNS.

Рис. 9-8. Проверка БД сервера имен NetBIOS на наличие привязки «NetBIOS-имя/IP-адрес»

Резюме

Служба WINS использует стандартные методы регистрации, обновления и высвобождения имен. Для использования старого NetBIOS-имени клиент должен продлять срок аренды до истечения последнего. Если NetBIOS-имя больше не требуется, клиент **WINS** сообщает серверу WINS об освобождении имени.

Занятие 3. Внедрение WINS

Для взаимодействия по протоколу TCP/IP в сетях, серверы которых работают под управлением Windows 2000 Server, а компьютеры — под управлением Windows 2000 Professional, протокол NetBIOS не нужен. В связи с этим изменением служба WINS необходима в большинстве сетей; впрочем, в некоторых случаях она может и не требоваться. На этом занятии вы узнаете о внедрении службы WINS в вашей сети.

Изучив материал этого занятия, вы сможете:

- ✓ установить и настроить сервер и клиент WINS;
- ✓ устранить неполадки WINS;
- ✓ управлять и вести мониторинг службы WINS.

Продолжительность занятия — около 40 минут.

Когда необходимо использовать WINS

Принимая решение о необходимости использования WINS, решите для себя следующие вопросы.

- **Имеются ли в вашей** в сети **какие-либо устаревшие компьютеры или приложения, требующие имен NetBIOS?**

  Помните, что всем устаревшим ОС производства Microsoft (предыдущие версии MS-DOS, Windows и Windows NT) требуется поддержка имен NetBIOS. Microsoft Windows 2000 — первая ОС, которой не требуются имена NetBIOS. Таким образом, для поддержки и предоставления устаревшим приложениям базовых служб доступа к файлам и служб печати нам может потребоваться внедрить в своей сети службу WINS.

- **Все ли компьютеры в вашей сети настроены и способны поддерживать другие типы именования сетевых ресурсов, например DNS?**

  Именование сетевых ресурсов — по-прежнему одна из жизненно важных служб, обеспечивающая поиск компьютеров и ресурсов в сети, даже если имена NetBIOS не требуются. Перед тем как отключить службу WINS или поддержку имен NetBIOS, убедитесь, что все компьютеры и программы вашей сети могут работать, используя другую службу именования сетевых ресурсов, например DNS.

- **Является ли ваша сеть одиночной подсетью или она маршрутизирована многочисленными подсетями?**

  Если ваша сеть — небольшая ЛВС, занимающая один физический сетевой сегмент и включающая не более 50 клиентов, вы, вероятно, сможете обойтись и без сервера WINS.

Когда следует использовать серверы WINS

Прежде чем внедрить службу WINS в своей сети, определите требуемое число WINS-серверов. В сети необходим лишь один сервер WINS, поскольку запросы на разрешение имен представляют собой направленные дейтаграммы и могут маршрутизироваться. Два сервера WINS позволят создать отказоустойчивую систему. Если один сервер окажется недоступным, для разрешения имен клиенты смогут воспользоваться вторым сервером. Кроме того, учтите следующие особенности.

- Встроенного ограничения на число WINS-запросов, обрабатываемых сервером WINS, не существует. В большинстве случаев сервер способен обрабатывать 1500 запросов на регистрацию имен и 4500 запросов на определение имени в минуту.
- На каждые 10 000 клиентов WINS рекомендуется иметь один основной и один резервный сервер WINS.
- Производительность многопроцессорных систем приблизительно на 25% выше, поскольку для каждого из процессоров запускается отдельный поток WINS.
- Если регистрация изменений в БД отключена (с помощью оснастки WINS), регистрация имен осуществляется намного быстрее. Тем не менее в случае отказа системы есть риск потерять несколько последних обновлений БД.

Требования WINS

Перед установкой WINS необходимо убедиться, что сервер и клиенты соответствуют конфигурационным требованиям. В TCP/IP-сети на основе сервера Windows NT Server или Windows 2000 Server службу WINS следует установить минимум на одном из компьютеров (он не обязательно должен выполнять функции контроллера домена). Для сервера необходимо определить IP-адрес, маску подсети, шлюз по умолчанию и прочие параметры TCP/IP. Их может автоматически назначать сервер DHCP; тем не менее рекомендуется задать все параметры вручную.

Необходимо, чтобы клиент WINS работал под управлением следующих ОС:

- Windows 2000;
- **Windows NT Server** 3.5 **или** последующих версий;
- Windows NT Workstation 3.5 или последующих версий;
- Windows 98;
- Windows 95;
- Windows for Workgroups 3.11, использующей Microsoft TCP/IP-32;
- Microsoft Network Client 3.0 for MS-DOS;
- LAN Manager 2.2c for MS-DOS.

Для клиента следует также определить IP-адрес основного и при желании дополнительного сервера WINS.

▶ **Установка службы WINS на сервер с Windows 2000**

1. В окне Control Panel дважды щелкните значок Add/Remove Programs.
2. Щелкните **значок Add/Remove Windows Components.**

   Запустится **мастер** Windows Component Wizard.
3. В списке Components окна Windows Components щелкните Networking Services и затем — кнопку Details.

   Откроется диалоговое окно Networking Services.
4. Пометьте флажок Windows Internet Name Service (WINS) и щелкните OK. Далее щелкните кнопку Next.

Использование статических привязок

Привязки «имя-адрес» можно добавлять в БД WINS двумя способами.

- динамически — для регистрации, освобождения и продления срока аренды своих NetBIOS-имен клиенты с поддержкой WINS обращаются напрямую к серверу WINS;
- вручную — с помощью консоли WINS или утилит командной строки.

Статические записи полезны, только если вам требуется добавить в БД сервера WINS привязку «имя-адрес» для компьютера, не использующего WINS напрямую. Например, и некоторых сетях серверы с ОС сторонних фирм не могут зарегистрировать имя NetBIOS на сервере WINS. И хотя эти имена удается добавлять или разрешать посредством файла LMHOSTS или запроса к серверу DNS, вы, вероятно, захотите добавить и БД WINS статические привязки «имя-адрес».

► **Создание статической привязки**

1. Раскройте меню Start\Programs\Administrative Tools и выберите пункт WINS.
2. В консоли WINS раскройте узел вашего сервера WINS и щелкните Active Registrations (Активныерегистрации).
3. В меню Action (Действие) выберите команду New Static Mapping (Создать статическое сопоставление).

   Откроется диалоговое окно Add Static Mapping (рис. 9-9).
4. В поле Computer Name (Имя компьютера) введите NetBIOS-имя компьютера.
5. В поле NetBIOS Scope (Область NetBIOS) при желании можно указать для компьютера идентификатор области NetBIOS (если таковой используется). В противном случае оставьте это поле пустым.

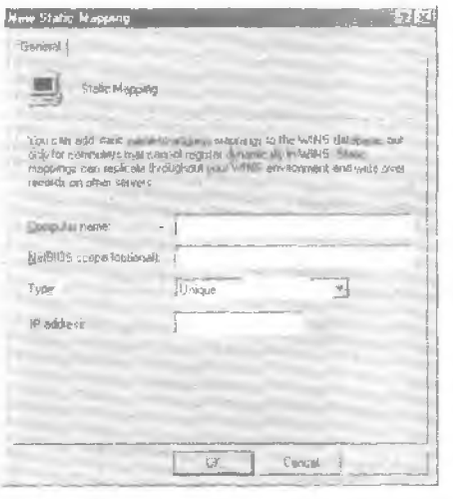


Рис. 9-9. Диалоговое окно Add Static Mapping (Новое статическое отображение)

6. В списке Type (Тип) выберите один из поддерживаемых типов записи: Unique (Уникальный), Group (Группа), Domain Name (Имя домена), Internet Group или Multihomed (Многосетевой) (см. табл. 9-3).
7. В поле IP Address введите адрес компьютера.
8. Щелкните кнопку Apply (Применить), чтобы добавить в БД статическую запись.

   Вы также можете добавлять дополнительные статические записи. Для добавления записи каждый раз щелкайте кнопку Apply; завершив добавление, щелкните кнопку Cancel (Отмена).
9. Щелкните OK, чтобы закрыть диалоговое окно Add Static Mapping.

Табл. 9-3. Типы статической привязки адреса

Тип	Описание
Unique	Уникальное имя, привязанное к одному IP-адресу
Group	Также называется «обычной» группой. Добавляя в группу запись с использованием оснастки WINS, укажите имя компьютера и IP-адрес. IP-адреса членов групп не хранятся в БД WINS, и поэтому число членов в группе не ограничено. Для взаимодействия с членами групп используются широковещательные пакеты
Domain Name	Привязка «NetBIOS-имя/IP-адрес», 16-й байт которой равен 0x1C. В привязке этого типа может храниться до 25 адресов членов домена. Для 26-го и следующих записей WINS перезаписывает адреса реплик или, если таковых нет, перезаписывает наиболее старые записи
Internet Group	Определяемые пользователем группы, создаваемые для объединения ресурсов, например принтеров, для упрощения доступа и просмотра. В записи этого типа может храниться до 25 адресов. И все же динамический член группы не заменяет статического члена группы, добавляемого через оснастку WINS или посредством импорта файла LMHOSTS
Multihomed	Уникальное имя, способное обладать несколькими адресами. Привязка этого типа применяется для компьютеров с несколькими сетевыми платами и включает до 25 адресов. Для 26-го и последующих адресов WINS перезаписывает адреса реплик или, если таковых нет, перезаписывает наиболее старые адреса

Практикум: настройка клиента WINS

При наличии компьютеров-клиентов DHCP-сервер можно сконфигурировать для предоставления им конфигурационной информации WINS. Кроме того, клиенты WINS можно конфигурировать и вручную. IP-адреса одного или нескольких WINS-серверов, определенные для клиента WINS вручную, переопределяют соответствующие параметры DHCP-сервера.

▶ **Задание:** задайте **для клиента WINS IP-адреса одного или нескольких серверов WINS**

1. Откройте окно Network And Dial-Up Connections.
2. Щелкните значок Local Area Connection (Подключение по локальной сети) правой кнопкой и выберите в контекстном меню команду Properties.
   Откроется окно свойств локального подключения.
3. В списке выберите TCP/IP и щелкните кнопку Properties.
   Откроется диалоговое окно свойств TCP/IP.
4. Щелкните кнопку Advanced (Дополнительно) и перейдите на вкладку WINS (рис. 9-10).
5. Щелкните кнопку Add (Добавить), укажите в диалоговом окне TCP/IP WINS Server (WINS-сервер TCP/IP) адрес своего WINS-сервера и затем снова щелкните кнопку Add.
   Введенный вами адрес сервера WINS будет добавлен в список дополнительных параметров TCP/IP,
6. Щелкните OK, чтобы закрыть окно Advanced TCP/IP Settings.
7. Щелкните OK, чтобы закрыть окно Internet Protocol (TCP/IP) Properties.
8. Щелкните OK, чтобы закрыть окно Local Area Connection Properties.

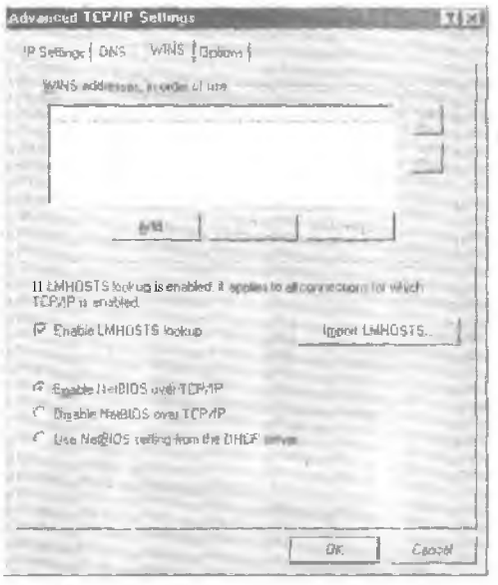


Рис. 9-10. Служба WINS на клиенте Windows 2000

Устранение неполадок WINS

Ниже перечислены вероятные индикаторы распространенных проблем WINS:

- администратор не может подключиться к серверу WINS средствами консоли WINS;
- служба TCP/IP NetBIOS Helper на клиенте WINS отключилась и не может перезапуститься;
- служба WINS не функционирует и не может перезапуститься.

Первое, что необходимо сделать для устранения проблем с WINS, — убедиться, запущены ли соответствующие службы. Это можно сделать как на сервере, так и на клиенте WINS.

▶ **Проверка работы служб**

1. Убедитесь, что служба WINS выполняется на сервере.
2. Убедитесь, что на клиентах выполняются службы Workstation, Server и TCP/IP NetBIOS Helper.

Если службы не запускаются должным образом, воспользуйтесь административной утилитой Computer Management (Управление компьютером), чтобы просмотреть состояние требуемых служб, и затем попытайтесь запустить их вручную. Если служба не запускается, воспользуйтесь утилитой Event Viewer (Просмотр событий) для просмотра журнала событий системы и определите причину сбоя.

Примечание Для службы TCP/IP NetBIOS Helper, выполняющейся на клиентах WINS, в колонке, отображающей состояние служб, должно быть указано Started (Выполняется). На серверах WINS значение Started должно отображаться для службы Windows Internet Name Service (WINS).

Наиболее распространенная проблема клиентов WINS — отказ при разрешении имен. Если клиент не смог разрешить имя, для выявления источника проблемы попробуйте ответить на следующие вопросы.

- **Может ли клиентский компьютер использовать WINS и корректно ли он настроен?**

  Первым делом убедитесь, что клиент настроен для использования и TCP/IP, и WINS. Настраивать параметры TCP/IP можно вручную (администратором) или динамически, средствами сервера DHCP, предоставляющего клиентским системам конфигурационные сведения TCP/IP. В большинстве случаев компьютеры с устаревшими версиями ОС Microsoft могут использовать службу WINS сразу после того, как на клиенте будет установлен и настроен пакет протоколов TCP/IP. В Windows 2000 администраторы имеют возможность по желанию отключать NetBT для отдельных клиентов. Если вы отключите протокол NetBT, клиент не сможет использовать WINS.

Примечание Если сервер WINS не отвечает на прямой тестовый опрос командой Ping. источником неполадок, скорее всего, являются проблемы связи между клиентом и сервером WINS.

- **Произошел ли отказ в разрешении имени NetBIOS или DNS?**

  Имена NetBIOS содержат не более 15 знаков и в отличие от имен DNS не структурированы. Имена DNS обычно длиннее NetBIOS-имен и разделены точками на части, соответствующие уровням доменов. Например, короткое имя NetBIOS «PRINT-SRV1» и длинное имя DNS «print-srv1.example.microsoft.com» указывают на один и тот же компьютер с Windows 2000 (сетевой сервер печати), настроенный для использования обоих имен. Если клиент в предыдущем примере воспользовался бы коротким именем, для разрешения имени Windows 2000 сначала бы была задействованы службы имен NetBIOS, такие, как широковещательные рассылки WINS или NetBT. Если же клиенту не удалось разрешить имя DNS (или имя с точечной нотацией), причиной сбоя, вероятнее всего, явилась бы служба DNS.

Наиболее распространенная проблема серверов WINS — невозможность разрешить запрашиваемое клиентом имя. В этом случае на сбой указывают следующие ситуации:

- сервер отсылает клиенту отрицательный ответ, например сообщение, что имя не найдено;
- сервер отправляет клиенту положительный ответ, но содержащаяся в нем информация не соответствует действительности.

Если вы установили, что проблема WINS не связана с клиентом, ответьте еше на один вопрос.

- **Может ли сервер WINS обслуживать клиента?**

  На сервере WINS, который не может найти запрашиваемое клиентом имя, воспользуйтесь утилитой Event Viewer или консолью управления WINS и убедитесь, что служба WINS запущена. Если служба выполняется, посмотрите, имеется ли запрошенное клиентом имя в БД сервера WINS.

Если сервер WINS отказывает или регистрирует ошибки целостности БД, можно попробовать восстановить БД WINS. Для резервного копирования БД WINS воспользуйтесь консолью управления **WINS.** Сначала вам будет предложено указать конечный каталог, в который будет произведено резервное копирование. По умолчанию архивирование БД выполняется каждые три часа. В случае нарушения целостности БД WINS вы легко можете восстановить *её.* Наиболее простой способ восстановления БД локального сервера — тиражирование данных с партнера по репликации. Если повреждены лишь определенные записи, вы можете тиражировать соответствующие нормальные записи WINS. Репликация записей выполняется на все серверы **WINS.** Если изменения тиражируются быстро, наилучший способ восстановить БД локального сервера WINS — воспользоваться партнером по репликации, но при условии, что ею БД включает новейшие данные.

Управление и мониторинг WINS

Консоль WINS полностью интегрирована с консолью MMC, мощным и удобным для пользователя программным средством, которое можно настраивать «под себя». Поскольку все административные утилиты сервера, входящие в состав Windows 2000 Server, являются частью MMC, работать с ними значительно проще, они функционируют более предсказуемо и отличаются общим внешним видом. Кроме того, некоторые полезные возможности WINS, которые в предыдущих версиях Windows NT Server настраивались исключительно через реестр, теперь удастся конфигурировать с помощью графического интерфейса. К ним относится возможность блокировки записей по определенному владельцу или партнеру по репликации WINS (данная функция ранее называлась Persona Non Grata), а также возможность переопределения статических привязок (данная функция ранее называлась Migrate On/Off). Сейчас мы расскажем об управлении и мониторинге службы WINS с помощью консоли WINS.

Просмотр статистики сервера WINS

В целях мониторинга производительности необходимо периодически просматривать статистику сервера WINS. По умолчанию статистика автоматически обновляется каждые 10 минут. При желании обновление статистики можно также отключить — для этого в окне свойств сервера WINS следует снять флажок Automatically Update Statistics Every (Автоматически обновлять статистику каждые).

▶ **Открытие диалогового окна WINS Server Statistics**

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык WINS.
2. В дереве консоли щелкните требуемый сервер WINS.
3. В меню Action выберите команду Display Server Statistics (Отобразить статистику сервера).
4. Для обновления данных во время просмотра статистики WINS щелкните кнопку Refresh (Обновить).

Резюме

Для внедрения WINS необходимо специальным образом сконфигурировать и сервер, и клиенты. Статические привязки «имя-адрес» для клиентов без поддержки WINS позволяют WINS-клиентам удаленных сетей взаимодействовать с ними. Первое, что необходимо сделать при устранении неполадок WINS, — убедиться, что на клиентах и на сервере выполняются соответствующие службы.

Занятие 4. Конфигурирование репликации WINS

Все серверы WINS вашей сети можно настроить для полного тиражирования записей БД. Это гарантирует, что имя, зарегистрированное на одном сервере WINS, будет тиражировано на все остальные серверы WINS. Сейчас мы расскажем о репликации записей БД WINS между серверами WINS.

Изучив материал этого занятия, вы сможете:

- ✓ добавить партнер по репликации;
- ✓ провести репликацию БД WINS.

Продолжительность занятия — около 20 минут.

Основы репликации

При любых изменениях БД, включая освобождсние имени, происходит репликация БД. Репликация позволяет серверу WINS разрешать NetBIOS-имена узлов, зарегистрированные на других WINS-серверах. Например, компьютер подсети Subnet I зарегистрирован сервером WINS той же подсети и хочет связаться с компьютером подсети Subnet 2. В случае если два упомянутых сервера WINS не тиражировали между собой информацию, компьютерам не удастся установить соединение.

Для тиражирования записей БД каждому серверу WINS необходимо выбрать опрашивающего или извещающего партнера. И звещающий партнер передает опрашивающим партнерам сообщения, уведомляющие их об изменениях в БД извещающего сервера. После того как опрашивающий партнер ответит на уведомление запросом о репликации, извещающий сервер WINS передает своим партнерам копию новых записей БД (реплик).

Опрашивающий партнер — это WINS-сервер, который запрашивает репликацию обновленных записей базы данных WINS с других WINS-серверов (которые настроены как его извещающие партнеры) через указанный промежуток времени. Это делается запросом записей с большим номером версии, чем последняя запись, полученная от настроенного партнера.

Примечание Серверы WINS тиражируют только новые записи БД. Полное тиражирование БД WINS каждый раз не выполняется.

Настройка сервера WINS в; качестве опрашивающего или извещающего партнера

Выбор типа сервера WINS (опрашивающий или извещающий партнер) зависит от сетевого окружения (рис. 9-11).

- Компьютер рекомендуется настраивать в качестве извещающего партнера, если серверы соединены быстрым каналом, поскольку тиражирование реплик происходит по достижении определенного числа новых записей БД WINS.
- Узлы, в частности, соединенные медленными каналами, рекомендуется настраивать в качестве опрашивающих партнеров, поскольку извещающую репликацию можно сконфигурировать для выполнения через определенные интервалы времени.

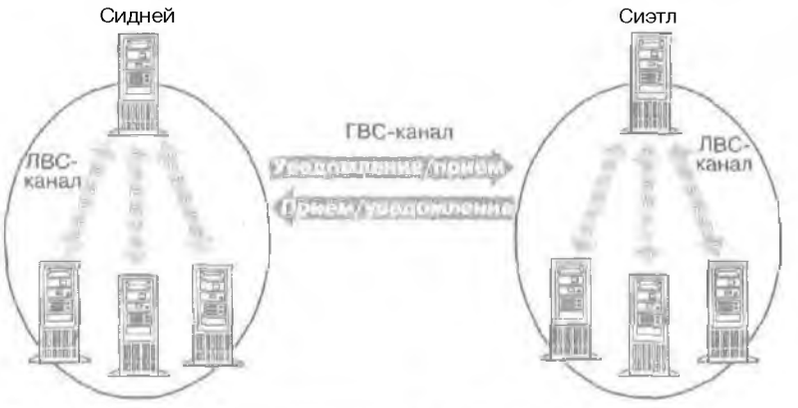


Рис. 9-11. **Настройка опрашивающих и извещающих партнеров**

- Для репликации записей БД между серверами последние рекомендуется настраивать одновременно в качестве извещающего и опрашивающего партнера.

Примечание Для настройки сервера WINS в качестве извещающего и опрашивающего партнера применяется административная утилита WINS.

- В Сиднее и Сиэтле все серверы WINS каждого узла передают новые элементы своих БД одному серверу.
- Серверы, получающие извещающую репликацию, сконфигурированы для взаимной опрашивающей репликации, поскольку скорость канала, соединяющего Сидней и Сиэтл, достаточно низка. Тиражирование должно осуществляться в периоды наименьшей загруженности сети, например поздно ночью.

Настройка репликации БД

Для тиражирования БД необходимо настроить минимум одного извещающего и одного опрашивающего партнера. Существует 4 способа тиражирования БД WINS.

1. При запуске системы. Если партнер репликации определен, служба WINS по умолчанию при запуске автоматически запрашивает новые записи БД. Сервер WINS можно также сконфигурировать для передачи новых записей при запуске системы.
2. В установленное время, например каждые 5 часов.
3. По достижении установленного числа регистраций и изменений в БД WINS сервер WINS уведомляет всех опрашивающих партнеров, которые затем запрашивают новые записи БД.
4. Принудительно, с помощью административной консоли WINS (рис. 9-12).

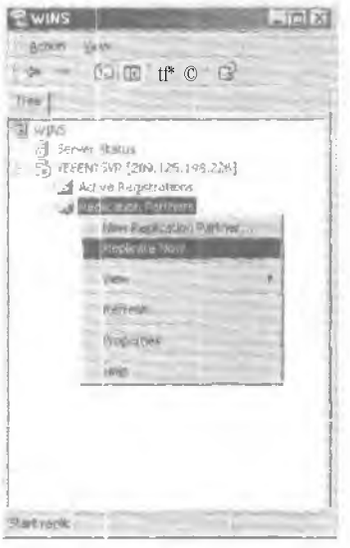


Рис. 9-12. Принудительная репликация БД WINS

Практикум: репликация БД WINS

Сконфигурируйте сервер WINS для тиражирования новых записей БД на другой сервер.

Примечание Для выполнения упражнения предварительно необходимо настроить в качестве сервера WINS второй компьютер (Server2).

Настройте второй компьютер (сервер WINS) в качестве партнера по тиражированию.

▶ **Задание 1: сконфигурируйте партнеров по репликации WINS**

1. Откройте оснастку WINS.
2. Раскройте узел вашего сервера WINS, щелкните правой кнопкой папку Replication Partners (Партнеры репликации) и выберите команду New Replication Partner (Создать партнера по репликации).

   Откроется диалоговое окно New Replication Partners (Новый партнер репликации).
3. В окне WINS Server введите IP-адрес сервера-партнера WINS и затем щелкните OK.

   В списке серверов WINS появится IP-адрес нового сервера (рис. 9-13).
4. В правой панели щелкните правой кнопкой значок только что добавленного сервера и выберите в контекстном меню команду Properties.

   Откроется диалоговое окно свойств сервера.
5. Перейдите на вкладку Advanced (Дополнительно).
6. В списке Replication Partner Type (Тип партнера репликации) выберите Pull (Опрашивающая).
7. Задайте интервал репликации равный 30 мин.
8. Шелкните OK.

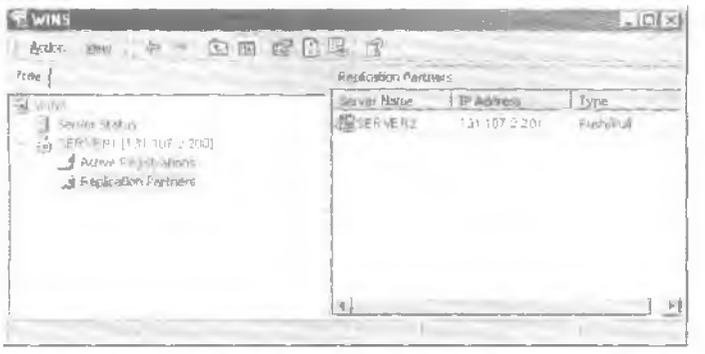


Рис. 9-13. Список партнеров по репликации в оснастке WINS

▶ **Задание 2: выполните принудительную репликацию**

1. Щелкните правой кнопкой папку Replication Partners.
2. В контекстном меню выберите команду Replicate Now (Запустить репликацию). Появится запрос, действительно ли вы уверены, что следует начать репликацию.
3. Щелкните кнопку Yes. Появится сообщение, что запрос на тиражирование был поставлен в очередь.
4. Щелкните OK.

Планирование необходимого числа серверов WINS

В небольшой сети один сервер WINS может обслуживать до 10 000 клиентов. Для обеспечения дополнительной отказоустойчивости системы стоит также сконфигурировать второй компьютер с Windows 2000 Server в качестве резервного сервера WINS. Если в вашей сети используется только два сервера, их можно легко настроить в качестве партнеров по тиражированию. Для осуществления простого тиражирования между двумя серверами достаточно настроить один из них в качестве извещающего, а другой — в качестве опрашивающего партнера. Тиражирование можно выполнять как автоматически, так и вручную. Для автоматической репликации на вкладке Advanced (Дополнительно) диалогового окна свойств папки Replication Partners (Партнеры репликации) пометьте флажок Enable Automatic Partner Configuration (Включить автоматическую настройку партнерства).

В крупных сетях необходимо большее число серверов WINS. Это вызвано несколькими причинами, наиболее важная из которых — количество клиентов, подключающихся к серверу. Количество клиентов, которое способен поддерживать сервер WINS, зависит от степени интенсивности его использования, а также от его возможностей по хранению и обработке данных. В некоторых сетевых средах для обработки WINS-запросов требуются надежные системы, и модернизация сервера может принести вам определенные преимущества. При планировании числа серверов помните, что каждый сервер WINS способен одновременно обрабатывать сотни регистрации и запросов в секунду. В целях обеспечения отказоустойчивости системы можно установить любое количество серверов. Тем не менее развертывать большое число серверов следует, только если это действительно необходимо. Ограничив количество серверов WINS в сети, вы снизите объем трафика репликации, повысите эффективность разрешения имен NetBIOS и сократите нагрузку по администрированию.

Автоматические партнеры по репликации WINS

Если ваша сеть поддерживает многоадресную рассылку, сервер WINS можно настроить для поиска других серверов WINS посредством многоадресной передачи сообщений на IP-адрес 224.0.1.24. По умолчанию эта рассылка осуществляется каждые 40 минут. При этом любые серверы WINS, обнаруженные в сети, автоматически конфигурируются в качестве извещающих и опрашивающих партнеров: интервал опрашивающей репликации равен 2 часам. Если сетевые маршрутизаторы не поддерживают многоадресную рассылку, сервер WINS сможет обнаружить серверы WINS только в своей подсети. Автоматическое партнерство серверов по умолчанию отключено. Чтобы отключить автоматическое партнерство серверон вручную, при помощи Registry Editor измените значение параметра UseSelfFndPnrs на 0, а значение MeastInt1 — на большее число.

Резервное копирование БД WINS

КонсольWINS включает средства резервного копирования, позволяющие архивировать и восстанавливать БД WINS. При резервном копировании БД сервера служба WINS создает в каталоге резервного копирования по умолчанию папку \Wins_bak\New. Здесь хранятся резервные копии БД WINS (WINS.MDB). По умолчанию каталог резервного копирования — это корневой каталог загрузочного раздела вашего компьютера, например C:. После того, как вы зададите папкудля архива БД, служба WINS каждые 3 часа булет помещать в нее резервную копию БД WINS. Кроме того, WINS можно настроить для автоматического резервного копирования БД при остановке службы или завершении работы сервера.

► Создание резервной копни БД WINS

1. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык WINS.
2. В дереве консоли выберите сервер WINS.
3. В меню Action выберите команду Backup Database (Резервное копирование).
4. Появится запрос на подтверждение. Щелкните кнопку Yes.
5. По завершении резервного копирования БД щелкните OK.

Внимание! Не указывайте в качестве папки резервного копирования БД WINS сетевой диск. Кроме того, если вы изменили в окне свойств сервера путь к папке резервного копирования или путь к БД WINS, выполните новое резервное копирование, чтобы гарантировать успешное восстановление БД WINS в будущем. Это единственный способ архивирования активной БД WINS, поскольку в процессе работы сервера WINS на БД накладывается блокировка.

Резюме

Все серверы WINS любой сети можно сконфигурировать для взаимодействия между собой, чтобы имя, зарегистрированное на одном сервере WINS, тиражировалось на все остальные серверы. Опрашивающий партнер запрашивает новые элементы БД WINS. Извещающий партнер уведомляет опрашивающих партнеров об изменениях в своей базе данных.

Закрепление материала

? Приведенные ниже вопросы помогут нам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные отпеты см. *к* приложении «Вопросы и ответы» в конце книги.

1. Назовите два преимущества использования службы WINS.

2. Назовите два способа активации службы WINS на клиентском компьютере.

3. Сколько серверов WINS необходимо в интрасети, включающей 12 подсетей?

4. Имена каких типов хранятся в БД WINS?

ГЛАВА 10

Внедрение DHCP

В этой главе

В этой главе рассказывается об использовании DHCP для автоматической настройки TCP/IP. Таким образом можно решить многие проблемы, связанные с его ручной настройкой. Вы установите и настроите DHCP-сервер, протестируете параметры DHCP и получите IP-адрес от DHCP-сервера.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить на своем компьютере Windows 2000 Server с TCP/IP.

Занятие 1 Знакомство с DHCP

DHCP автоматически назначает компьютерам IP-адреса. Это позволяет избежать трудностей, связанных с ручной настройки TCP/IP. На этом занятии мы расскажем основные принципы работы DHCP.

Изучив материал этого занятия, вы сможете:

- ✓ описать различия между автоматической и ручной настройкой TCP/IP;
- ✓ описать параметры настройки TCP/IP, которые могут быть назначены DHCP-сервером;
- ✓ описать запросы и предложения аренды IP;
- ✓ установить DHCP в Windows 2000.

Продолжительность занятия — около 20 минут.

Знакомство с DHCP

DHCP — расширение протокола начальной загрузки (BOOTP), который позволяет бездисковым клиентам загружаться и автоматически настраивать TCP/IP. DHCP служит для централизации и управления распределением параметров TCP/IP путем автоматического присвоения IP-адресов компьютерам-клиентам DHCP. Его использование также позволяет решить некоторые проблемы, связанные с ручной настройкой TCP/IP.

Как показано на рис. 10-1, каждый раз, когда DHCP-клиент загружается, он запрашивает у DHCP-сервера информацию — IP-адрес, маску подсети и некоторые другие, необязательные данные. К последним относятся адрес шлюза по умолчанию, адреса серверов DNS и WINS.

Рис. 10-1. Взаимодействие DHCP-клиента и DHCP-сервера

Когда сервер DHCP получает запрос на выделение IP-адреса, он выбирает информацию об IP-адресе из пула адресов, которые заданы в его БД, и предоставляет ее клиенту DHCP. Если клиент принимает эти данные. DHCP-сервер выделяет IP-адрес клиенту на определенный период времени. Если в пуле нет доступных адресок, то клиент не может инициализировать TCP/IP.

Сравнение ручной и автоматической настройки TCP/IP

Чтобы понять преимущества использования службы DHCP для настройки TCP/IP, полезно сравнить ручной и автоматический методы настройки TCP/IP.

Ручная настройка TCP/IP

Ручная настройка TCP/IP означает, что пользователи могут произвольно выбирать IP-адрес, а не получать его от администратора сети. Использование некорректных адресов приводит к некорректной работе сети, причем локализовать источник проблемы достаточно трудно.

К тому же необходимость ввода IP-адреса, маски подсети, адреса шлюза иногда вызывает многочисленные трудности: от проблем с подключением (неправильно заданы адрес шлюза или маска подсети) до проблем, связанных с дублированием IP-адресов.

Еще одно ограничение — возникновение административных издержек, если приходится часто перемещать компьютеры из одной подсети в другую. Например, необходимо менять IP-адрес и адрес шлюза по умолчанию, чтобы клиент мог успешно соединиться с нового места.

Настройка TCP/IP с использованием DHCP

Использование DHCP для автоматической настройки TCP/IP означает, что пользователям больше нет необходимости получать информацию о IP-адресах от администратора сети. Служба DHCP предоставляет всю необходимую информацию всем клиентам DHCP. Применение DHCP позволяет решить множество проблем, которые трудно выявить.

Информация о параметрах TCP/IP, которая может быть назначена DHCP-сервером, включает:

- IP-адрес для каждого сетевого адаптера клиентского компьютера;
- маски подсети, позволяющие отличать адрес сети от адреса узла в IP-адресе;
- шлюзы по умолчанию (маршрутизаторы), применяемые для полсоединения одного сегмента сети к другим;
- дополнительные параметры, которые могут быть переданы клиентам DHCP (такие, как IP-адреса DNS- или WINS-серверов, которыми может воспользоваться клиент).

Как работает DHCP

Настройка DHCP-клиента выполняется в четыре этапа (табл. 10-1). Если на компьютере установлено несколько сетевых адаптеров, настройку производят отдельно для каждого адаптера. Каждому адаптеру назначается уникальный IP-адрес. Все соединения DHCP реализованы через протокол UDP (порты 67 и 68).

Большинство сообщений DHCP — широковещательные. Если DHCP-клиенты соединяются с DHCP-сервером через удаленную сеть, то IP-маршрутизаторы должны поддерживать пересылку широковещательных сообщений DHCP. Фазы конфигурации DHCP показаны в табл. 10-1.

Табл. 10-1. Четыре фазы настройки DHCP-клиента

Фаза	Описание
Поиск сервера (IP lease discover)	Клиент инициализирует ограниченную версию и посылает широковещательный запрос о местонахождении DHCP-сервера и информацию об IP-адресах
Предложение аренды (IP lease offer)	Все DHCP-серверы, имеющие корректную конфигурацию клиента, посылают ему предложение

(см. след. стр.)

Табл. 10-1. Четыре фазы настройки DHCP-клиента *(окончание)*

Фаза	Описание
Запрос аренды (IP lease request)	Клиент берег информацию об IP-адресе из первого полученного предложения и отправляет широковещательное сообщение с запросом о выделении ему IP-адреса из предложения, которое он получи.
Подтверждение аренды (IP lease acknowledgment)	DHCP-сервер, сделавший предложение, отвечает Па сообщение, а все остальные серверы забирают спои предложения. Клиенту назначается IP-адрес и высылается подтверждение. Клиент заканчивает инициализацию и привязку TCP/IP. По окончании процесса автоматической настройки клиент может использовать все службы и утилиты TCP/IP для нормальной работы в сети и соединения с другими IP-узлами

В первых двух фазах клиент посылает широковещательное сообщение DHCP-серверу, а тот предлагает ему IP-адрес (рис. 10-2).

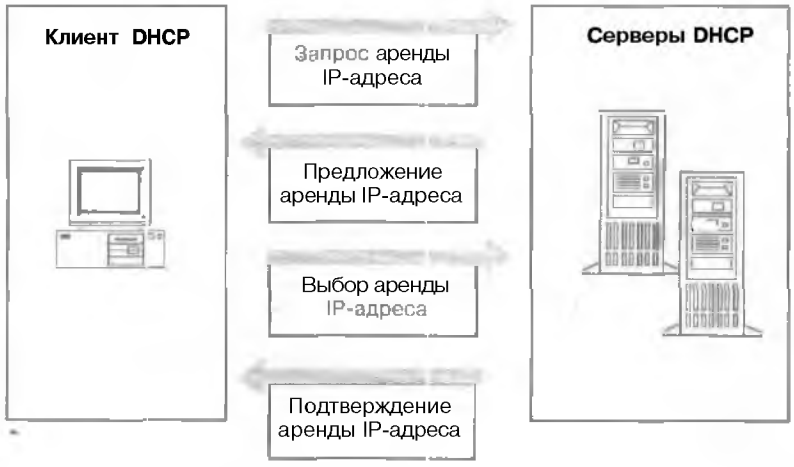


Рис. 10-2. Процесс аренды IP-адреса клиентом DHCP

Поиск сервера

Во время загрузки клиент запрашивает о выделении ему IP-адреса путем рассылки широковещательного запроса всем DHCP-серверам. Так как у клиента нет IP-адреса и он не знает IP-адреса DHCP-сервера, клиент использует 0.0.0.0 как адрес источника и 255.255.255.255 как адрес назначения.

Запрос посылается в виде сообщения **DHCPDISCOVER,** которое также содержит аппаратный адрес клиента и имя компьютера, чтобы DHCP-серверы знали, кто послал запрос.

Процесс выделения IP используется, если происходит одно из следующих событий:

- происходит первая инициализация TCP/IP на клиенте DHCP;
- клиент запросил определенный IP-адрес и получил отказ, вероятно, из-за того что DHCP-сервер прекратил для него аренду;
- клиент уже ранее арендовал IP-адрес, но освободил его и запрашивает новый.

Предложение аренды

Все DHCP-серверы, получившие запрос об аренде IP и имеющие корректную конфигурацию клиента, посылают широковещательное сообщение, и котором содержится следующая информация:

- аппаратный адрес клиента;
- предлагаемый IP-адрес;
- маска подсети;
- длительность аренды;
- идентификатор сервера (IP-адрес DHCP-сервера, пославшего сообщение).

DHCP-сервер посылает широковещательное сообщение, так как клиент еще не имеет собственного IP-адреса. Предложение об аренде посылается как сообщение DHCPOFFER (рис. 10-3). Клиент DHCP берет IP-адрес из первого полученного предложения. DHCP-сервер, предложивший IP-адрес, резервирует его, чтобы он не был предложен другому клиенту DHCP.

Рис. **10-3. Отправка *сообщения* DHCPOFFER**

Если нет работающих DHCP-серверов

Клиент ждет предложения 1 секунду. Если оно не приходит, клиент не сможет завершить инициализацию и пошлет запрос еще три раза (через 9, 13 и 16 секунд плюс некий интервал времени, который выбирается случайно в интервале между 0 и 1000 миллисекундами). Если ответа нет после четырех запросов, клиент будет возобновлять попытки каждые 5 минут.

Клиенты Windows 2000 могут автоматически настроить IP-адрес и маску подсети, если DHCP-сервер недоступен при загрузке. Эта новая возможность Windows 2000 называется Automatic Private IP Addressing (APIPA). Она полезна для клиентов в небольших частных сетях, таких, как домашний офис или клиент удаленного доступа. Служба DHCP-клиента Windows 2000 следующим образом автоконфигурирует клиент.

1. DHCP-клиент пытается найти DHCP-сервер и получить адрес и параметры.
2. Если DHCP-сервер не найден или не отвечает, DHCP-клиент автоматически настраивает свой IP-адрес и маску подсети, используя адрес, выбранный из сети класса B 169.254.0.0, зарезервированной за Microsoft, с маской подсети 255.255.0.0.

Клиент смотрит, есть ли конфликт адресов, чтобы убедиться, что выбранный IP-адрес уже не используется в сети. При обнаружении конфликта клиент выбирает другой IP-адрес. Клиент будет повторять попытки автоконфигурации, перебирая до 10 адресов.

3. Если автоконфигурация клиента прошла успешно, он настраивает сетевой интерфейс для использования данного IP-адреса. После этого клиент продолжает в фоновом режиме проверять наличие DHCP-сервера каждые 5 минут. Если позднее DHCP-сервер будет обнаружен, клиент откажется от прежней конфигурации и использует IP-адрес, предложенный DHCP-сервером, а также другую предоставленную информацию для обновления своих параметров TCP/IP.

Запрос аренды

В последних двух фазах клиент выбирает предложение, а DHCP-сервер подтверждает аренду.

После того как клиент получил по крайней мере одно предложение, он посылает всем DHCP-серверам широковещательное сообщение о том, что он сделал выбор и принял предложение.

Это сообщение посылается как сообщение DHCPREQUEST и содержит идентификатор сервера (IP-адрес), чье предложение принял клиент. Все другие DHCP-серверы отменяют свои предложения и оставляют IP-адреса для следующих запросов аренды.

Успешное подтверждение аренды

Последняя фаза в успешном процессе аренды DHCP наступает, когда DHCP-сервер, пославший принятое предложение, посылает широковещательное подтверждение клиенту в форме сообщения DHCPACK. Это сообщение содержит арендованный IP-адрес и, возможно, другую информацию о параметрах. Когда клиент DHCP получает подтверждение, TCP/IP полностью инициализируется, и клиент становится полноправным DHCP-клиентом. После этого клиент может использовать TCP/IP для соединения по сети.

Неуспешное подтверждение аренды

DHCP-сервер посылает широковещательное сообщение DHCPNACK, если клиент пытается арендовать предыдущий IP-адрес, который стал недоступным, или если IP-адрес некорректен, потому что клиент физически перемещен в другую подсеть. Если клиент получает такое сообщение, он начинает процесс аренды IP-адреса сначала.

Установка DHCP-сервера

Перед установкой DHCP-сервера необходимо знать:

- требования к оборудованию DHCP-сервера;
- какие компьютеры вы можете сразу настроить как DHCP-клиенты, а какие нужно настраивать вручную, со статическими параметрами TCP/IP, включая IP-адрес;
- типы и значения параметров DHCP, которые необходимо передать DHCP-клиентам. Перед установкой DHCP нужно ответить на несколько вопросов.
- Все ли компьютеры будут DHCP-клиентами? Если нет, учтите, что клиенты, не использующие DHCP, имеют статические IP-адреса, которые должны быть исключены из параметров DHCP-сервера. Если клиенту нужен конкретный адрес, то он должен быть зарезервирован.
- Будет ли DHCP-сервер предоставлять IP-адреса для нескольких подсетей? Если да, то учтите, что в этом случае все маршрутизаторы, соединяющие подсети, должны работать как агенты ретрансляции DHCP. Если ваши маршрутизаторы не могут работать как агенты ретрансляции DHCP, то необходимо иметь минимум один DHCP-сервер

на каждую подсеть, где есть DHCP-клиенты. DHCP-сервером может быть агент ретрансляции DHCP или маршрутизатор с включенным протоколом BOOTP.

- **Сколько потребуется DHCP-серверов? Учтите,** что DHCP-сервер не обменивается информацией с другими серверами. Поэтому необходимо указать каждому серверу уникальные IP-адреса для назначения клиентам.
- **Какие параметры IP-адресации будут получать от DHCP-сервера клиенты?** Эти параметры определяют, как надо сконфигурировать DHCP-сервер, а также надо ли создавать параметры для всех клиентов в сети, клиентов в конкретной подсети или индивидуально для каждого клиента. Параметры IP-адресации могут включать:
  - номер шлюза по умолчанию;
  - название DNS-сервера;
  - разрешение имен NetBIOS поверх TCP/IP;
  - названиеWINS-сервера;
  - код области NetBIOS.

▶ **Установка сервера DHCP**

1. Раскройте меню Start\Settings (Пуск\Настройка) и щелкните ярлык Control Panel (Панель управления).

   В панели управления дважды щелкните значок Add/Remove Programs (Установка и удаление программ), после чего щелкните кнопку Add/Remove Windows Components (Установка и удаление компонентов Windows).
2. В перечне компонентов выберите Networking Services (Сетевые службы).
3. Щелкните кнопку Details (Состав).
4. Выберите в списке Dynamic Host Configuration Protocol (DHCP), щелкните OK, а затем — Next.

   По запросу введите полный путь к дистрибутивным файлам Windows 2000 и шелкните кнопку Continue (Продолжить). Все необходимые файлы будут скопированы на диск.
5. Щелкните кнопку Finish (Готово), чтобы закрыть окно мастера Windows Components.

Примечание Рекомендуется вручную сконфигурировать компьютер DHCP-сервера для использования статического IP-адреса, так как DHCP-сервер не может быть DHCP-клиентом. Он должен иметь статический IP-адрес, маску подсети и шлюз по умолчанию.

Ipconfig

Ipconfig — утилита командной строки, которая выводит текущие параметры установленного стека IP на сетевом компьютере. Она может показать подробный отчет о параметрах для всех интерфейсов, включая IBC-минипорты, например, те, что используются для удаленного доступа или для подключений к VPN. Пример отчета приведен на рис. 10-4.

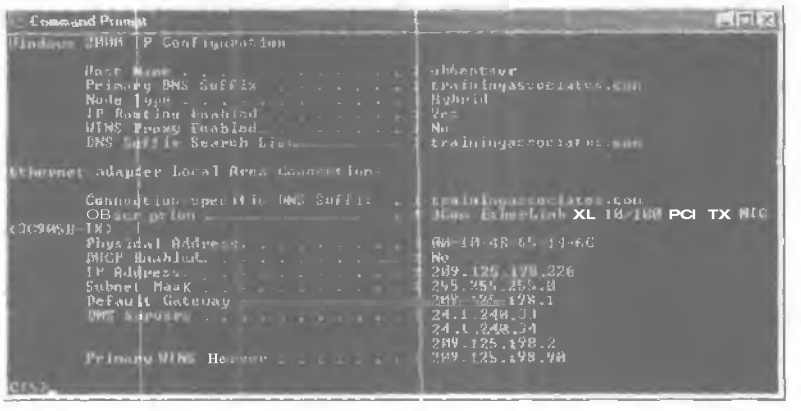


Рис. 10-4. Отчет, выдаваемый командой Ipconfig /All

Параметры Ipconfig

В системах, работающих с DHCP, часто используется команда Ipconfig, так как она позволяет определить, какие значения параметров TCP/IP были сконфигурированы DHCP. В табл. 10-2 приведены параметры командной строки Ipconfig.

Табл. 10-2. Параметры командной строки Ipconfig

Параметр	Описание
/all	Выводит подробный отчет о параметрах всех интерфейсов
/flushdns	Удаляет все записи из кэша имен DNS
/registerdns	Доменное имя DNS для разрешении клиента
/displaydns	Выводи" содержимое кэша DNS
/release <адаптер>	Освобождает IP-адрес заданного интерфейса
/renew <адаптер>	Обновляет аренду IP-адреса заданного интерфейса
/showclassid <адаптер>	Выводит все идентификаторы класса DHCP разрешенных для данного адаптера
/setclassid <адаптер>	Изменяет идентификатор класса DHCP для заданного <код_класса> адаптера
/?	Выводит пункты данной таблицы

Примечание Вывод можно перенаправить в файл и вставить в другие документы.

▶ **Проверка, прекращение или обновление аренды адреса**

1. На компьютере с Windows 2000, работающем как клиент DHCP, откройте окно командной строки.
2. Чтобы проверить, прекратить или обновить аренду адреса клиентом, используйте команду Ipconfig.

   Чтобы проверить текущие параметры DHCP и TCP/IP, наберите **ipconfig /all.**

   Чтобы прекратить аренду, наберите **ipconfig /release.**

   Чтобы обновить аренду, наберите **ipconfig** /renew.

Утилита Ipconfig также поставляется с Windows NT. Для клиентов с Windows 95 или Windows 98 для выполнения тех же задач можно использовать Winipcfg, программу настройки IP в Windows. Для запуска Winipcfg наберите **winipcfg** в командной строке либо в окне Run. Чтобы прекратить или обновить аренду, используя Winipcfg, щелкните соответственно Release или Renew.

Агент ретрансляции DHCP

Это небольшая программа, передающая сообщения DHCP/BOOTP между клиентами и серверами в разных подсетях. Компонент DHCP Relay Agent, поставляемый с маршрутизатором Windows 2000, — это агент ретрансляции BOOTP, который передает сообщения DHCP между DHCP-клиентами и DHCP-серверами в разных IP-сетях. Для каждого сегмента сети, в котором есть клиенты DHCP, необходимо наличие либо DHCP-сервера, либо компьютера, работающего как агент ретрансляции DHCP.

► **Добавление агента ретрансляции DHCP**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Routing And Remote Access.
2. В дереве консоли раскройте папку *имя_сервера*\IP Routing\General (*имя_сервера*\IP-маршрутизация \Общие).
3. Щелкните правой кнопкой папку General и выберите команду New Routing Protocol (Новый протокол маршрутизации).
4. Щелкните DHCP Relay Agent (Агент DHCP-ретрансляции), затем — OK.

Резюме

DHCP разработан для решения проблем с настройкой TCP/IP путем централизации конфигурационной информации TCP/IP. Аренда IP-адресов DHCP-клиентом выполняется в четыре этапа: поиск сервера, предложение адреса, запрос и подтверждение аренды. Кроме проверки параметров IP вы можете применять утилиту Ipconfig для обновления параметров времени аренды, а также для освобождения IP-адреса.

Занятие 2 Настройка DHCP

Вы узнаете, как настроить DHCP на сервере Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ описать преимущества использования DHCP;
- ✓ настроить DHCP-сервер и клиенты.

Продолжительность занятия - около 10 минут.

Использование DHCP в сети

Установка DHCP-серверов к сети обеспечивает следующие преимущества:

- администратор может назначать и задавать глобальные и частные параметры TCP/IP для подсети централизованно, чтобы использовать их во всей сети; .
- нет необходимости настраивать TCP/IP на клиентах вручную;

  Когда компьютер перемещают между подсетями, его старый IP-адрес освобождается для использования. Клиент автоматически переконфигурирует параметры TCP/IP при загрузке компьютера в новом месте;
- большинство маршрутизаторов способны пересылать запросы DHCP и BOOTP, так что нет необходимости устанавливать DHCP-сервер в каждой подсети.

Использование DHCP-сервера клиентами

Чтобы сделать компьютер с Windows 2000 DHCP-клиентом, нужно установить переключатель Obtain An IP Address (Получить IP-адрес автоматически) в окне свойств TCP/IP (рис. 10-5).

Если клиентский компьютер настроен для использования DHCP, он принимает предложение аренды и получает от сервера:

- корректный для данной сети IP-адрес для временного использования;
- дополнительные параметры конфигурации TCP/IP.

К тому же, если задано обнаружение конфликтов, то DHCP-сервер пытается проверить с помощью утилиты ping все доступные адреса в области, прежде чем предложить клиенту адрес для аренды. Тем самым гарантируется, что предлагаемые клиентам IP-адреса не используются компьютерами с ручной настройкой TCP/IP. Мы расскажем об этом подробно далее.

Предоставление DHCP-серверами необязательной информации

DHCP-сервер можно настроить так, чтобы он кроме IP-адреса предоставлял дополнительную информацию для полной настройки TCP/IP на клиентах. Наиболее часто настраиваются и распространяются во время процесса аренды следующие наборы параметров:

- шлюзы по умолчанию (маршрутизаторы), которые используются для соединения одного сегмента сети с другими сегментами;
- другие необязательные параметры, такие, как IP-адреса DNS-серверов или WINS-серверов, которые клиент может использовать для разрешения сетевых имен узлов.

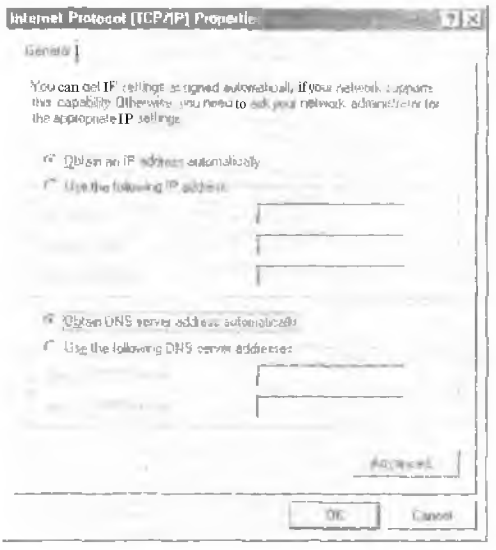


Рис. 10-5. Настройка клиента для получения IP-адреса от DHCP-сервера

Установка и настройка DHCP-сервера

Для соединения с DHCP-клиентами должна быть запущена служба DHCP-сервера. После того как DHCP-сервер был установлен и запущен, нужно настроить несколько параметров. Вот что надо сделать для установки и настройки DHCP:

- установить службу Microsoft DHCP Server;
- авторизовать DHCP-сервер;
- перед тем как DHCP-сервер сможет выделять IP-адреса DHCP-клиентам, необходимо настроить область или пул корректных IP-адресов;
- для конкретного клиента можно сконфигурировать параметры глобальной области и области клиента;
- настроить DHCP-сервер так, чтобы некоторым клиентам всегда выделялись одни и те же адреса.

Авторизация DHCP-сервера

Если DHCP-серверы корректно настроены и авторизованы для использования в сети, то они предоставляют полезную административную службу. Тем не менее, если в сети появляется некорректно настроенный или неавторизованный DHCP-сервер, это может вызвать проблемы. Например, после запуска неавторизованный DHCP-сервер может либо выделять некорректные IP-адреса, либо отрицательно отвечать DHCP-клиентам, пытающимся обновить аренду текущего адреса. Все это порождает дальнейшие проблемы с клиентами DHCP. Например, клиенты, получившие параметры от неавторизованного сервера, вполне вероятно, не смогут найти контроллер домена, а значит, не войдут в сеть.

В Windows 2000 для предотвращения этих проблем серверы проверяются, прежде чем они начинают обслуживать клиентов. Так предотвращаются случайные повреждения, вызываемые работой DHCP-серверов с некорректной конфигурацией или с корректной конфигурацией, но не в той сети.

Порядок авторизации DHCP-сервера

Авторизация DHCP-серверов полезна или необходима для DHCP-серверов, работающих под управлением Windows 2000 Server. Чтобы она выполнялась правильно, необходимо ввести сведения о первом DHCP-сервере вашей сети в Active Directory. Для этого установите сервер либо как контроллер домена, либо как рядовой сервер. При планировании или активном развертывании служб Active Directory, важно не устанавливать компьютер первого DHCP-сервера как изолированный сервер. Windows 2000 Server имеет встроенные средства поддержки безопасности для сетей, использующих Active Directory. Таким образом предотвращаются случайные повреждения, вызываемые работой DHCP-серверов с некорректной конфигурацией или с корректной конфигурацией, но не в той сети.

Порядок авторизации компьютера DHCP-сервера в Active Directory зависит от заданной роли сервера в вашей сети. В Windows 2000 Server (как и в более ранних версиях) каждому серверу можно задать одну из трех ролей (типов сервера).

1. Контроллер домена — компьютер хранит и обслуживает копию БД каталога Active Directory и обеспечивает безопасное управление учетными записями пользователей и компьютеров, включенных в домен.
2. **Рядовой сервер** — компьютер не работает как контроллер домена, но подсоединен к домену и имеет членскую учетную запись в БД Active Directory.
3. **Изолированный** сервер — компьютер, не являющийся ни контроллером домена, ни рядовым сервером домена. Вместо этого сервер известен в сети под заданным именем рабочей группы, которое может совместно использоваться другими компьютерами, но применяется только для просмотра и не предоставляет безопасного парольного доступа к общим ресурсам домена.

Если вы применяете Active Directory, все DHCP-серверы должны быть либо контроллерами домена, либо рядовыми серверами домена, прежде чем они будут авторизованы и смогут обеспечивать службы DHCP клиентам.

▶ Авторизация компьютера как DHCP-сервера службой Active Directory

1. Войдите в сеть, используя учетную запись, имеющую либо полные административные привилегии, либо делегированное право на авторизацию DHCP-сервера.

   В большинстве случаев проще всего войти в сеть с компьютера, на котором вы хотите авторизовать новый DHCP-сервер. Так вы удостоверитесь, что перед авторизацией другие параметры TCP/IP авторизуемого компьютера настроены правильно. Обычно можно использовать учетную запись, имеющую членство в группе Enterprise Administrators (Администраторы предприятия). Используемая учетная запись должна иметь права Full control (Полный доступ) в контейнере NetScrvices, хранящемся в корне Active Directory.
2. Если необходимо, установите службу DHCP на авторизуемом компьютере.
3. Раскройте меню Start\Programs\Administrative Tools и щелкните ярлык DHCP.
4. В меню Action выберите команду Manage Authorized Servers (Список авторизованных серверов) (рис. 10-6).
5. В открывшемся окне щелкните кнопку Authorize (Авторизовать).
6. По запросу введите имя или IP-адрес авторизуемого DHCP-сервера, после чего щелкните OK.

Защита от неавторизованных DHCP-серверов

Для хранения записей об авторизованных серверах применяется служба Active Directory. При появлении нового DHCP-сервера эта служба может быть использована для проверки его состояния. Если сервер не авторизован, он не будет отвечать на DHCP-запросы. Решать эту проблему должен сетевой администратор с соответствующими правами доступа. Ад-

министратор домена может назначить права доступа к папке DHCP, хранящей данные о параметрах, так, чтобы только уполномоченный персонал получил право добавлять DHCP-серверы к утвержденному списку.

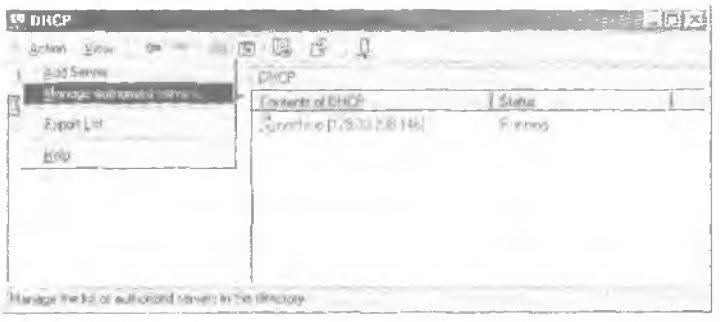


Рис. 10-6. Авторизация DHCP-сервера

Список авторизованных серверов создается в Active Directory с помощью оснастки DHCP. При первом запуске DHCP-сервер пытается выяснить, является ли он частью каталога домена. Если да, то он пытается соединиться с каталогом, чтобы найти себя в списке авторизованных серверов. Если это удается, он посылает сообщение DHCPINFORM, чтобы выяснить, есть ли другие службы каталогов и убедиться, что он также авторизован и в них. Если сервер не может соединиться с каталогом, то он считает себя неавторизованным и не отвечает на запросы клиентов. Аналогично, если он смог соединиться с каталогом, но не нашел себя в списке авторизованных серверов, то он также не отвечает на запросы. Если же сервер найдет себя в списке авторизованных, то начнет обслуживать клиентов.

Создание области DHCP

Прежде чем сервер DHCP сможет предоставить клиентам IP-адреса, надо определить *область DHCP* — пул действительных IP-адресов, которые могут быть выделены клиентам DHCP. Область создается после того, как служба DHCP установлена и запущена.

Создавая область DHCP, помните:

- для каждого сервера DHCP надо определить не менее одной области;
- из области следует исключить статические IP-адреса;
- для централизации администрирования и выделения IP-адресов, специфичных для конкретной сети, на сервере DCHP можно определить несколько областей; подсети разрешается присвоить лишь одну область;
- серверы DHCP не обмениваются информацией об областях; поэтому, создавая области на нескольких серверах DHCP, убедитесь, что в этих областях нет пересекающихся IP-адресов — это поможет избежать проблем с идентичными IP-адресами;
- перед созданием области надо определить ее начальный и конечный IP-адрес.

  В зависимости от них консоль DHCP предложит маску подсети по умолчанию, что имеет смысл для большинства сетей. Если вы знаете, что требуется другая маска подсети, измените это значение.

*

Создание области

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и выберите DHCP.
2. В дереве консоли щелкните название нужного DHCP-сервера.

3. В меню Action (Действие) выберите команду New Scope (Создать область).
4. "Следуйте инструкциям мастера создания области.

После того как вы закончите создание новой области, вы, возможно, захотите выполнить некоторую дополнительную настройку — активизацию области или назначение параметров области.

Дополнительная конфигурация после создания областей

После задания области вы можете дополнительно ее сконфигурировать.

- **Задание дополнительных интервалов для** исключения. Вы можете исключить любые другие IP-адреса, которые не надо выделять клиентам DHCP. Это необходимо проделать для всех устройств, которые должны быть настроены статически. Надо исключить все IP-адреса, которые вы назначили вручную другим DHCP-серверам, не-DHCP-клиентам, бездисковым рабочим станциям, а также PPP-клиентам, клиентам удаленного доступа и маршрутизируемым клиентам.
- Создание **резервирования**. Возможно, ны захотите зарезервировать некоторые IP-адреса для того, чтобы при аренде постоянно назначать их конкретным компьютерам или устройствам вашей сети. Резервирование необходимо только для устройств, работающих как DHCP-клиенты, и только для специфических целей (например, для выделения одного и того же адреса серверам печати).

  Если вы резервируете IP-адрес для нового клиента или адрес, отличающийся от текущего, то необходимо удостовериться, что этот адрес не выделен в данный момент кому-то другому. Резервирование IP-адреса в области не означает, что клиент, который использует его в данный момент, автоматически прервет аренду. Чтобы клиент, использующий IP-адрес, освободил его, необходимо чтобы он послал сообщение об окончании аренды. Если клиент работает под управлением Windows 2000, то для отправки такого сообщения надо набрать в командной строке **ipconfig** /release. Также резервирование IP-адреса на DHCP-сервсре не означает, что новый клиент, для которого был зарезервирован IP-адрес, немедленно начнет его использовать. Для этого надо, чтобы он послал запрос о выделении IP-адреса. В Windows 2000, чтобы это произошло, введите в командной строке **ipconfig** /renew.
- Изменение срока действия аренды. По умолчанию срок действия аренды — 8 дней. Для большинства локальных сетей значение по умолчанию вполне приемлемо, но его можно увеличить, если компьютеры редко перемещаются. Также разрешается установить бесконечный срок аренды, но такую возможность следует использовать осторожно.
- Настройка параметров и классов, **используемых** в области. Чтобы обеспечить полную конфигурацию клиентов, необходимо настроить и разрешить использование параметров DHCP для области. Для дискретного управления клиентами области можно добавить или разрешить применение пользовательских или уже существующих параметров.

В табл. 10-2 описаны некоторые из параметров, доступных в диалоговом окне настройки параметров области DHCP. В таблицу включены все параметры, поддерживаемые клиентами DHCP производства Microsoft.

Табл. 10-3. Параметры области DHCP

Параметр	Описание
003 Router (003 Маршрутизатор)	IP-адрес маршрутизатора, например адрес шлюза по умолчанию. Шлюз по умолчанию, локально определенный на клиенте, имеет преимущество перед соответствующим параметром DHCP
006 DNS Servers (DNS-серверы)	IP-адрес сервера DNS
015 DNS Domain Name (015 DNS-имя домена)	Доменное имя DNS для разрешения имен клиентов
044WINS/NBNS Servers (044WINS/NBNS-серверы)	IP-адрес WINS/NBNS-сервера, доступного клиентам. Адрес WINS-сервера, вручную явный на клиентской системе, переопределит соответствующие параметры, устанавливаемые DHCP
046WINS/NBT Node Type (046 Тип узла WINS/NBT)	Тип разрешения имен NetBIOS поверх TCP/IP, используемого клиентом. Возможные значения: 1 = B-node (широковещательный), 2=P-node (одноранговый), 4 = M-node (смешанный) и 8 = H-node (гибридный)
047 NetBIOS Scope ID (047 Кол области NetBIOS)	Локальный идентификатор области, используемый NetBIOS поверх TCP/IP. NetBIOS поверх TCP/IP устанавливает связь лишь с хостами NetBIOS, использующими идентичный идентификатор области

Использование нескольких DHCP-серверов

Если к нашей сети требуются нескольких DHCP-серверов, то необходимо создать уникальную область для каждой подсети. Чтобы гарантировать, что клиенты смогут получить IP-адрес в случае сбоя сервера, надо задать для каждой подсети несколько областей, распределенных по всем DHCP-серверам. Например:

- каждый DHCP-ссрвер должен иметь область, содержащую примерно 75% IP-адресов локальной подсети;
- каждый DHCP-сервер должен иметь область для каждой удаленной подсети, содержащую примерно 25% IP-адресов подсети.

Если DHCP-сервер клиента недоступен, он может подучить адрес от DHCP-сервера из другой сети, если, конечно, маршрутизатор является агентом ретрансляции DHCP.

Как покачано на рис. 10-7, сервер А имеет область для локальной подсети с интервалом IP-адресов от 131.107.4.20 до 131.107.4.150, а сервер В имеет область с интервалом IP-адресов от 131.107.3.20 до 131.107.3.150. Каждый сервер может выделять IP-адреса клиентам собственной подсети.

Кроме того, каждый сервер имеет область, содержащую небольшой интервал IP-адресов другой подсети. Например, сервер А имеет область для подсети 2 с интервалом IP-адресов от 131.107.3.151 до 131.107.3.200. Сервер В имеет область для подсети 1 с интервалом IP-адресов от 131.107.4.151 до 131.107.4.200. Если клиент из подсети 1 не сможет получить адрес от сервера А, он сможет подучить адрес в своей подсети от сервера В, и наоборот.

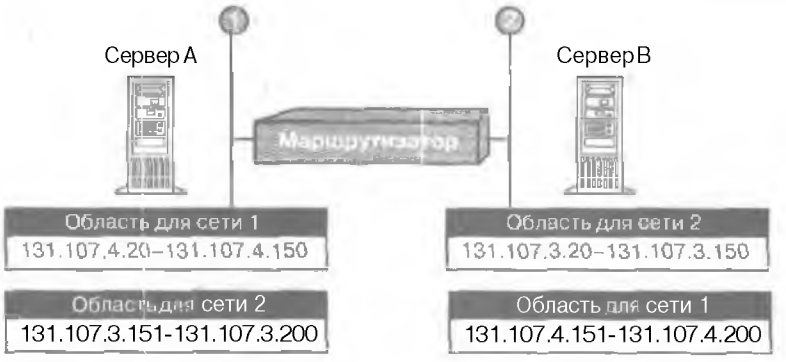


Рис. 10-7. Области и интервалы IP-адресов для серверов A и B

Резюме

Область — это интервал IP-адресов, доступных для аренды клиентам. Возможно создание нескольких областей и отдельных областей для каждой подсети, чтобы DHCP-клиенты могли получить корректный IP-адрес от любого DHCP-сервера. Для использования DHCP необходима установка программного обеспечения на клиенте и на сервере. Каждому DHCP-серверу нужна минимум одна область.

Занятие 3 Интеграция DHCP со службами разрешения имен

В Windows 2000 DHCP-сервер можно настроить для проведения динамических обновлений в пространстве имен DNS для любых клиентов, поддерживающих такие обновления. В этом случае клиенты области смогут применять протокол динамического обновления DNS для обновления информации о привязках «IP-адрес/имя» (они хранятся в зонах на DNS-сервере) при изменении их адресов, назначаемых DHCP. На этом занятии вы узнаете, как интегрировать DHCP с DNS.

Изучив материал этого занятия, вы сможете:

- ✓ провести интеграцию DHCP е DNS;
- ✓ описать, как работают обновления динамической DNS;
- ✓ описать, как обычно обрабатываются обновления DHCP-клиента.

Продолжительность занятия — около 25 минут,

DNS и DHCP

Хотя DHCP обеспечивает мощный механизм автоматической настройки IP-адреса клиента, до недавнего времени DHCP не извещал службу DNS для обновления DNS-записей клиента, а именно, для обновления привязок «IP-адрес/имя» и «имя/IP-адрес», хранящихся DNS-сервером. Если DHCP не сможет взаимодействовать с DNS, информация о DHCP-клиенте, поддерживаемая DNS, станет некорректной. Например, клиент получит IP-адрес у DHCP-сервсра, но записи DNS не будут отражать текущий IP-адрес, а также не удастся преобразовать новый IP-адрес в *полное доменное имя* (fully qualified domain name, FQDN).

Регистрация для обновлений Dynamic DNS

В Windows 2000 DHCP-серверы и клиенты могут взаимодействовать с DNS, если сервер поддерживает обновления *динамической системы доменных имен* (Dynamic DNS, DDNS). Служба DNS Windows 2000 поддерживает динамические обновления. DHCP-сервер Windows 2000 может зарегистрироваться на DNS-сервере и обновить записи ресурсов адреса узла (A) и записи ресурсов указателя (PTR) для своих DHCP-клиентов с помощью протокола обновлений DDNS. Возможность регистрировать и записи типа A, и записи типа PTR позволяет DHCP-серверу действовать как прокси-серверу для регистрации DNS для клиентов, использующих Windows 95 и Windows NT 4.0. DHCP-серверы могут различать Windows 2000 и другие клиенты. Дополнительный код настройки DHCP (Option Code 81) разрешает возврат FQDN клиента DHCP-серверу. Если такая возможность реализована, то DHCP-сервер способен динамически обновлять DNS для модификации записей ресурсов на DNS-сервере с помошью протокола динамических обновлений. Таким образом, для DHCP-клиентов, включающих Option Code 81 в запросы DHCP, посылаемые на сервер, DHCP-сервер обрабатывает DNS-информацию следующим образом:

- DHCP-сервер всегда регистрирует в DNS записи для прямого запроса (записи типа A) и для обратного запроса по имени (записи типа PTR) для DHCP-клиентов;
- DHCP-сервер никогда не регистрирует информацию о привязках «имя/IP-адрес» (записи типа A) для DHCP-клиентов;

- DHCP-сервер регистрирует и DNS записи для прямого запроса (записи типа A) и для обратного запроса по имени (записи типа PTR) для DHCP-клиентов только по требованию клиента.

DHCP и статическая служба DNS не способны синхронизировать информацию о привязках «имя/IP-адрес», что вызывает проблему при совместном использовании DHCP и DNS, если вы применяете более старые, статические DNS-серверы, которые не способны динамически реагировать на изменения конфигурации DHCP-клиентов.

▶ Как избежать появления неудавшихся запросов **DNS для DHCP-клиентов при** использовании статической **службы DNS**

1. Если в сети используются WINS-сервер, разрешите запросы WINS для DHCP-клиентов, применяющих NetBIOS.
2. Назначьте резервирование IP-адресов с бесконечным сроком аренды для DHCP-клиентов, не поддерживающих NetBIOS и использующих только DNS.
3. Как только станет возможным, обновите или замените старые статические DNS-серверы на DNS-серверы, поддерживающие обновления. Динамические обновления поддерживаются DNS фирмы Microsoft, включенным в Windows 2000.

Дополнительные рекомендации

При совместном использовании DNS и WINS рассмотрите некоторые возможности их взаимодействия.

- Если большое количество клиентов используют NetBIOS и вы применяете DNS, попробуйте запросы WINS на ваших DNS-ссрверах. Если в службе Microsoft DNS разрешены запросы WINS, то WINS используется для разрешения любых имен, не найденных при разрешении имен через DNS. Прямые запросы **WINS** и обратные запросы WINS-R поддерживаются только DNS. Если ваши серверы не поддерживают DNS, задействуйте диспетчер DNS, чтобы гарантировать, что записи WINS не будут переданы DNS-серверам, не поддерживающим запросы WINS'.
- Если в вашей сети много компьютеров с Windows 2000, рассмотрите вариант использования только DNS. Для этого необходимо разработать план обновления старых WINS-клиентов до Windows 2000. Вопросы поддержки, затрагивающие сетевую службу имен, упрощаются за счет использования единой службы именования и поиска ресурсов (WINS или **DNS).**

DHCP-клиенты Windows и протокол динамических обновлений DNS

В Windows 2000 Server служба DHCP-сервсра по умолчанию предоставляет поддержку регистрации и обновления в зонах DNS информации об устаревших DHCP-клиентах (компьютерах с Microsoft TCP/IP и старыми версиями Windows). Интеграция DNS и DHCP, обеспечиваемая в Windows 2000 Server, позволяет DHCP-серверу обновлять информацию в зонах прямого и обратного просмотра DNS тем DHCP-клиентам, которые не способны напрямую динамически обновить записи ресурсов DNS.

▶ Включение динамического **обновлении для DHCP-клиентов, не поддерживающих обновления DDNS**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните **ярлык DHCP,**
2. В дереве консоли щелкните нужную зону.
3. В меню Action (Действие) выберите команду Properties (Свойства).

4. На вкладке DNS пометьте флажок Enable Updates For DNS Clients That Do Not Support Dynamic Update (Разрешить обновление для DNS-клиентов, которые не поддерживают динамическое обновление).
5. Если требуемая зона интегрирована в Active Directory, включите безопасное обновление.

Процесс взаимодействия DHCP и DNS, описанный выше, происходит по-разному для клиентов Windows 2000 и клиентов с более ранними версиями Windows. Далее мы опишем эти различия.

Взаимодействие DHCP и DNS для DHCP-клиентов Windows 2000

DHCP-клиенты Windows 2000 взаимодействуют с протоколом динамических обновлений.

1. Клиент посылает сообщение DHCP с запросом (DHCPREQUEST) на сервер.
2. Сервер возвращает клиенту сообщение DHCP с подтверждением (DHCPACK) аренды IP-адреса.
3. По умолчанию клиент посылает запрос об обновлении записи для прямого просмотра (запись типа A) DNS-серверу.

   DHCP-сервер может выполнить это обновление от имени клиента при изменении его конфигурации.
4. Сервер посылает обновление записи обратного запроса (записи типа PTR), используя процесс, определенный в протоколе динамических обновлений DNS (рис. 10-8).

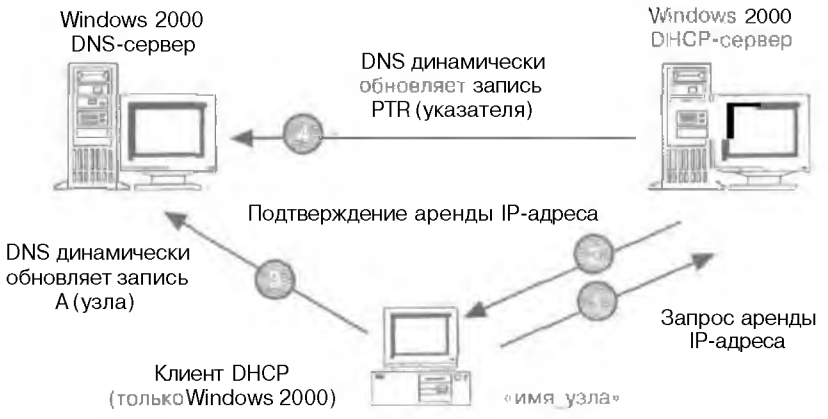


Рис. 10-8. Взаимодействие DHCP-клиента и протокола динамических обновлений DNS

Взаимодействие DHCP и DNS на устаревших DHCP-клиентах

Более ранние версии DHCP-клиентов Windows не поддерживают напрямую процесс динамического обновления DNS и, таким образом, не могут напрямую взаимодействовать с DNS-сервером. Вот как обычно выполняются обновления для таких DHCP-клиентов.

1. Клиент посылает сообщение DHCP с запросом (DHCPREQUEST) на сервер.
2. Сервер возвращает клиенту сообщение DHCP с подтверждением (DHCPACK) аренды IP-адреса.
3. После этого сервер посылает обновление записи прямого запроса (A) клиента на DNS-сервер.
4. Сервер также посылает обновление записи обратного запроса (PTR) клиента (рис. 10-9).

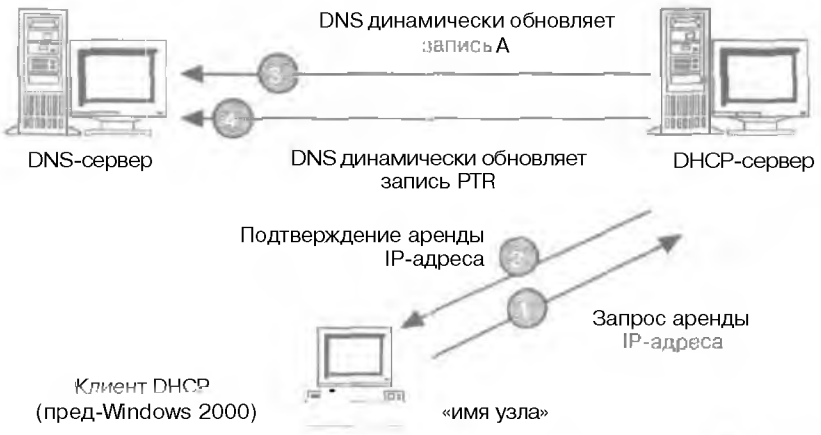


Рис. 10-9. Взаимодействие DHCP и DNS на устаревших клиентах Windows

Резюме

В Windows 2000 DHCP-сервер может разрешить динамические обновления пространства имен DNS для любых клиентов, поддерживающих такие обновления. При использовании динамических обновлений основной сервер зачастую настраивают для поддержки обновлений, инициированных другим компьютером или устройством, поддерживающим динамические обновления. Например, он может получать обновления от рабочих станций или от DHCP-серверов для регистрации записей ресурсов A и PTR.

Занятие 4 Использование DHCP с Active Directory

Microsoft DHCP обеспечивает интеграцию со службами Active Directory и DNS, а также улучшенные возможности по мониторингу и созданию статистических отчетов для DHCP-серверов, поддержку настроек производителей и пользовательских классов, групповое выделение адресов, а также обнаружение неавторизованных DHCP-ссрверов.

Изучив материал этого занятия, вы сможете:

- описать, как происходит управление IP-адресами и именами с помощью интеграции DHCP и Active Directory;
- описать, как происходит авторизация DHCP-ссрвера.

Продолжительность занятия — около 15 минут.

Интегрированное управление IP в Windows 2000

Службы имен и адресов в Windows 2000 Server упрощают гибкое управление сетями и взаимодействие с другими службами имен и адресов. Как и Windows NT Server 4.0, Windows 2000 Server предоставляет службы DHCP, DNS и WINS для упрощения процессов назначения адресов и разрешения имен. Новшества в Windows 2000 Server — поддержка DDNS, интеграция Active Directory для DHCP и DNS, а также агент ретрансляции DHCP.

Службы назначения адресов и службы имен

Управление IP-адресами и именами упрощается за счет интеграции с Active Directory. Пользователи могут применять Active Directory для репликации и синхронизации имен DNS в корпоративной сети. Таким образом, исчезает необходимость поддержки отдельной службы репликации для DNS. Интегрированные службы DHCP и DDNS используют информацию, хранящуюся в Active Directory, для обеспечения служб назначения адресов и служб имен. DNS и Active Directory динамически обновляются при выделении адресов службой DHCP. Таким образом, администраторы получают возможность менять IP-адреса конечных систем, при этом разрешение имен обновляется автоматически.

Поддержка устаревших серверов

Возможность взаимодействия с другими службами DHCP и DNS помогает сохранить капиталовложения в существующие службы. Пользователи могут применять уже существующие системы управления IP-адресами и именами при установке Windows 2000 Server DHCP, агента ретрансляции DHCP и/или службы DNS. Поддержка стандартной передачи зоны и *пересылок* (referrals) гарантирует, что служба DNS Windows 2000 Server сможет взаимодействовать с другими серверами DNS для разрешения корпоративных имен и имен Интернета. Таким образом, пользователи в своей сети получают интегрированные с Active Directory службы, сохраняя взаимодействие с Интернетом и другими корпоративными системами DNS. Например, компания может развертывать интегрированные с Active Directory DNS и DHCP в центральной части своей сети, работая также и с существующими DNS-серверами. Со временем инфраструктура управления IP, основанная на Active Directory, может быть расширена, причем возможность взаимодействия с внешними службами DNS сохранится.

DHCP в Windows 2000 также динамически интегрирована с DNS при помощи Active Directory. Более ранние версии DNS не поддерживают такую интеграцию.

Средства поиска неавторизованных серверов DHCP

Служба Windows 2000 DHCP предоставляет средства обнаружения неавторизованного DHCP-сервера. Таким образом предотвращается подсоединение неавторизованных DHCP-серверов к существующей сети DHCP, в которой используются Windows 2000 Server и Active Directory. В Active Directory создается объект DHCP-сервера, в котором перечислены IP-адреса авторизованных для предоставления услуг DHCP-серверов. Когда DHCP-сервер пытается начать работу в сети, запрашивается Active Directory с целью поиска IP-адреса компьютера *в* списке авторизованных DHCP-серверов. Если он будет найден, значит, сервер авторизован для предоставления услуг DHCP и может начать работу. Если нет. то сервер считается неавторизованным, и служба DHCP автоматически прекращает работу.

Резюме

Управление IP-адресами и именами упрощается за счет интеграции с Active Directory. DNS и Active Directory динамически обновляются при выделении адресов службой DHCP. Возможность взаимодействия с другими службами DHCP и DNS помогает сохранить капиталовложения в существующие службы, так как вы вправе использовать имеющиеся системы управления IP-адресами и именами с DHCP-серверами Windows 2000 Server. Процесс авторизации DHCP-сервера зависит от того, является ли сервер контроллером домена, рядовым сервером или изолированным сервером. Кроме того, для хранения записей об авторизованных DHCP-серверах применяется Active Directory, что позволяет обеспечить защиту от неавторизованных DHCP-серверов. Список авторизованных серверов создается в Active Directory с помощью оснастки DHCP.

Занятие 5. Устранение неполадок DHCP

Наиболее частая проблема с DHCP-клиентом такова: DO время загрузки ему не удается получить IP-адрес или другие параметры конфигурации с DHCP-сервера. Основные неполадки DHCP-сервера — не удается включить его и сетевую работу в домене Windows 2000 или Active Directory или клиенты не могут получить параметры настроек, хотя сервер работает. На этом занятии вы узнаете, как решать такие проблемы.

Изучив материал этого занятия, вы сможете:

- определить и устранить неполадку с DHCP-клиентом или DHCP-сервером.

Продолжительность занятия — около 35 минут.

Предотвращение проблем с DHCP

Проблемы с DHCP приводят к неверным параметрам настройки протокола TCP/IP на локальном компьютере или их полному отсутствию. Вот как предотвратить эти ошибки.

- Используйте правило разработки 75/25 для соблюдения баланса в распределении адресов области, если несколько DHCP-серверов обслуживают одну и ту же область. Использование нескольких DHCP-серверов в одной подсети уменьшает риск ошибок при обслуживании DHCP-клиентов. Так, если один из двух серверов занят, то второй включается в работу и продолжает выделять новые адреса или обновлять параметры существующих клиентов.
- Объединяйте области при наличии нескольких DHCP-серверов в каждой подсети. Они позволяют DHCP-серверу выделять адреса из нескольких областей клиентам в одной физической сети. При загрузке каждый DHCP-клиент распространяет по своей локальной подсети сообщение DHCPDISCOVER для поиска DHCP-сервера. При этом невозможно предсказать, какой из серверов (если их несколько) ответит на этот запрос клиента.
- **Деактивируйте** область только при полном ее удалении. Не стоит деактивировать область, пока она и ее подобласти не будут полностью выведены из использования в данной сети. Когда область деактивирована, DHCP-сервер перестает воспринимать ее адреса как действительные.
- Используйте систему определения конфликтов на DHCP-сервере только при необходимости. Эта система применяется и DHCP-серверами, и DHCP-клиентами для определения, не используется ли уже и сети IP-адрес, предполагаемый к выделению или использованию.
- Зарезервируйте адреса на всех DHCP-серверах, которые потенциально могут быть задействованы для обслуживания привилегированных клиентов. Резервирование клиентов применяется, если нужно, чтобы компьютеру с DHCP-клиентом при загрузке выделялся один и тот же IP-адрес. Следовательно, такие зарезервированные адреса должны иметься на каждом DHCP-сервере, который может быть задействован для обслуживания зарезервированного клиента.
- Для повышения производительности сервера комплектуйте его жесткими дисками с максимально высоким быстродействием, поскольку технология DHCP предполагает интенсивное использование дисков. Применение DHCP приводит к частым и интенсивным обращениям к жестким дискам сервера. Для улучшения производительности используйте дисковые массивы RAID 0 или RAID 5.

- **Ведите журнал аудита.** По умолчанию служба DHCP записывает в такой журнал связанные со своей работой события. В Windows 2000 Server журнал аудита служит долговременным средством контроля, не требуя значительных дисковых ресурсов сервера.
- **Комбинируйте DHCP с другими службами — например, WINS и DNS.** Обе эти службы регистрируют динамически устанавливаемые привязки «имя/адрес» в локальной сети. Для обеспечения работы систем разрешения имен следует заранее спланировать взаимодействие DHCP с этими службами. Многие администраторы сетей, используя DHCP, также планируют применение серверов WINS и DNS.
- **Используйте столько DHCP-серверов, сколько нужно для обслуживания DHCP-клиентов в локальной сети. В** небольшой сети (например, одной физической сети без маршрутизаторов) единственный DHCP-сервер способен обслужить всех своих клиентов. Для более сложной сети требуется больше серверов в зависимости от различных факторов — числа DHCP-клиентов, скорости передачи между сегментами сети, скорости сетевых соединений, класса IP-адресов в данной сети, а также от того, действует ли служба DHCP во всей корпоративной сети или только в отдельной физической подсети.

Устранение неполадок DHCP-клиентов

Большая часть неполадок, связанных с DHCP, такова: клиент не получает правильные IP-параметры. Сначала надо удостовериться, не произошла ли неполадка по вине клиента, а затем проверить журнал системных событий и журнал аудита DHCP-сервера. Если DHCP-сервер не запускается, эти журналы обычно содержат информацию об ошибке. Далее можно средствами утилиты командной строки Ipconfig попробовать получить информацию об установленных параметрах TCP/IP на локальном компьютере или компьютерах сети.

В следующих разделах мы опишем наиболее частые признаки неполадок с DHCP-клиентами. Используйте эту информацию для определения источника ошибок в ситуации, когда клиент не получил IP-параметры.

Неверный IP-адрес

Если на DHCP-клиенте совсем не установлен IP-адрес или он имеет вид 168.254.x.x — это означает, что этот клиент не смог связаться с DHCP-сервером и получить выделенный ему IP-адрес. Причина — либо в неполадках сетевого оборудования, либо в недоступности сервера. В этом случае надо проверить правильность сетевых подключений, в частности, кабелей и сетевого адаптера клиента.

Проблемы автоматического конфигурирования в данной сети

Если на DHCP-клиенте установлен автоматически сконфигурированный IP-адрес, который недействителен в данной локальной сети, это означает, что DHCP-клиент под управлением Windows 2000 или Windows 98 не смог найти DHCP-сервер и использовал режим API PA для задания своего IP-адреса. В больших сетях этот режим желательно отключить. APIPA генерирует IP-адрес в виде 169.254.x.y (где x.y — уникальный идентификатор для сети, генерируемый клиентом) и маску подсети 255.255.0.0. Microsoft зарезервировала IP-адреса с 169.254.0.1 до 169.254.255.254 и использует этот диапазон для работы API PA.

Исправление неверного для данной сети автоматически заданного IP-адреса

1. Сначала используйте команду PING для проверки соединения клиента с сервером. Затем проверьте или попробуйте вручную обновить выделяемый клиенту адрес. В зависимости от параметров локальной сети, возможно, потребуется отключить у клиента режим API PA.

2. Если сетевое оборудование клиента исправно, проверьте доступность DHCP-сервера с помощью тестового опроса командой PING с другого компьютера этой же сети. Далее следует попытаться обновить адрес или еще раз выделить его клиенту, а затем проверить параметры автоматической адресации TCP/IP.

Отсутствуют дополнительные параметры конфигурации

Если на DHCP-клиенте отсутствуют дополнительные параметры конфигурации, то, возможно, они не выделены ему сервером либо потому что на сервере не установлено выделение таких параметров, либо клиент не поддерживает параметры, предложенные сервером. Если это произошло на DHCP-клиенте Microsoft, удостоверьтесь, что были настроены основные параметры на уровне сервера, области, клиента или класса. Проверьте параметры DHCP.

Иногда у клиента установлен полный и правильный набор параметров DHCP, но его сетевая конфигурация тем не менее не работает. Если на DHCP-сервере задан неверный режим DHCP-маршрутизатора (код 3) для адреса шлюза по умолчанию (в случае клиента с Windows 98 или более ранней ОС), сделайте следующее.

1. Измените список IP-адресов маршрутизаторов (шлюзов по умолчанию) для используемого сервера или области.
2. Задайте правильное значение на вкладке Scope Options в диалоговом окне свойств области.

В особых случаях приходится настраивать DHCP-клиент на использование списка маршрутизаторов, отдельного от остальных клиентов данного диапазона адресок. Для этого можно создать зарезервированный адрес и настроить параметры списка маршрутизаторов специально для этого клиента.

Клиенты с Windows NT или Windows 2000 не будут применять неправильный адрес, так как они поддерживают функцию определения неработающих шлюзов. Эта функция протокола TCP/IP в Windows 2000 изменяет шлюз по умолчанию на указанный следующим в списке шлюзов, заданных по умолчанию, когда при определенном числе соединений посылаемые пакеты возвращаются.

DHCP-сервер не выделяет IP-адрес

Если DHCP-клиенту не удается получить IP-адрес с сервера, возможно несколько причин.

- **IP-адрес DHCP-сервера изменился.** DHCP-сервер может обслуживать запросы только для области, у которой идентификатор сети совпадает с идентификатором сети IP-адреса сервера. Удостоверьтесь, что IP-адрес DHCP-сервера удовлетворяет этому требованию. Например, сервер с IP-адресом из сети 192.168.0.0 не может выделять адреса из области 10.0.0.0 (если не используется объединение областей).
- **DHCP-клиенты, соединенные с подсетью, где находится DHCP-сервер, через маршрутизатор, не могут получить адрес с этого сервера.** DHCP-сервер выдает IP-адреса компьютерам клиентов в удаленные подсети, только если маршрутизатор работает как DHCP-передатчик. Проблему решают так.
  1. Создайте в подсети клиента (в одном фрагменте физической сети) агент ретрансляции BOOTP/DHCP. Его надо расположить либо на самом маршрутизаторе, либо на компьютере с Windows 2000 Server с включенной службой ретрансляции DHCP.
  2. На DHCP-сервере создайте диапазон адресов, подходящий к адресам подсети, в которой находятся клиенты с данной проблемой.
  3. Удостоверьтесь, что в этой области маска подсети подходит для удаленной полсети.
  4. Не включайте эту область (область для удаленной подсети) в объединение областей, предназначенное для локальной подсети или сегмента, где расположен DHCP-сервер.

- Несколько DHCP-серверов находятся в одной ЛВС. Удостоверьтесь, что при наличии в одной ЛВС нескольких DHCP-серверов их области не перекрываются. Возможно также, что проблемный DHCP-сервер — это компьютер под управлением Small Business Server (SBS). Служба DHCP спроектирована так, что она, работая под управлением SBS, автоматически останавливается, если обнаруживает другой DHCP-сервер в данной ЛВС.

Устранение неполадок DHCP-серверов

Когда серверу не удается выделить адреса своим клиентам, они обнаруживают это по следующим признакам:

1. клиент настроен на использование IP-адреса, который не был выделен сервером;
2. сервер выдал клиенту отрицательный ответ, и клиент видит аварийное сообщение, что DHCP-сервер не найден;
3. сервер выделяет клиенту адрес, но у клиента возникают проблемы с параметрами сети, такими, как невозможность регистрировать или разрешать имена DNS или NetBIOS, или различать компьютеры за пределами своей подсети.

Первое, что надо сделать для устранения таких неполадок, — удостовериться, что служба DHCP запущена. Для этого используют консоль службы DHCP или папку Services And Applications (Службы и приложения) в меню Computer Manager (Управление компьютером). Если служба не запущена, запустите ее. В редких случаях DHCP-сервер не запускается, и появляется сообщение об ошибке Stop. В этом случае надо перезапустить остановленный DHCP-сервер.

▶ **Перезапуск остановленного DHCP-сервера**

1. Запустите Windows 2000 Server и войдите в систему как администратор.
2. В командной строке наберите net start **dhcpserver** и нажмите Enter.

Примечание Для поиска источников проблем службы DHCP используйте программу Event Viewer (Просмотр событий) из группы Administrative Tools.

Служба DHCP Relay Agent установлена, но не работает

Видимо, служба DHCP Relay Agent запущена на том же компьютере, что и служба DHCP. Поскольку обе эти службы ждут сообщений BOOTP и DHCP и отвечают на них по портам UDP 67 и 68, они не могут работать на одном компьютере. Поэтому установите их на разных компьютерах.

Консоль DHCP неправильно сообщает об окончании действия адреса

Когда консоль DHCP показывает время окончания действия адреса для зарезервированного клиента в области, то возможны варианты:

- если время действия области не ограничено, то сообщается, что время действия зарезервированного адреса также бесконечно;
- если время действия области конечно (например 8 дней), то время действия зарезервированного адреса имеет такое же значение.

Условия выделения адреса зарезервированному клиенту DHCP определяются условиями, заданными для всей зарезервированной группы. Чтобы создать зарезервированных клиентов с неограниченным временем действия, создайте область с неограниченным временем и добавьте к нему зарезервированную группу адресов.

DHCP-сервер использует рассылку по сети для ответа на сообщения всех клиентов

DHCP-сервер использует широковещательную рассылку для ответа на запросы всех клиентов пне зависимости от того, какой флаг рассылки установлен дли каждого DHCP-клиента. DHCP-клиент может устанавливать этот флаг (первый бит в 16-разрядном поле флагов заголовка сообщения DHCP) при отправке сообщений DHCPDISCOVER, чтобы сообщить DHCP-серверу, что отправлять отклик DHCPOFFER для этого клиента надо по адресу ограниченного широковещания (255.255.255.255).

По умолчанию DHCP-сервер в Windows NT Server 3.51 и более ранних версиях игнорировал флаг рассылки в сообщениях DHCPDISCOVER и отправлял только отклики DHCPOFFER. Это было сделано, чтобы избежать проблем с клиентами, настроенными для TCP/IP, которые не могли получать или обрабатывать персонально адресованные отклики.

Начиная с Windows NT Server 4.0, служба DHCP также пытается посылать отклики DHCP как IP-рассылки по адресу 255.255.255.255, если только в реестре не разрешена поддержка персональных ответов — параметр IgnoreBroadcastFlag равен 1. Этот параметр находится в разделе реестра; HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ DHCPServer\Parameters\. Если это значение равно 1, то флаг рассылки в запросе клиента игнорируется, и псе отклики DHCPOFFER отправляются сервером по всем адресам. Если оно равно 0, то поведение сервера в отношении рассылки определяется значением флага рассылки в запросе клиента DHCPDISCOVER. Если этот флаг установлен, сервер рассылает свой отклик по ограниченному числу локальных адресов. Если он не установлен, сервер посылает отклик непосредственно клиенту.

DHCP-сервер не может выделить адрес для новой области

Для упорядочения адресов в существующей сети на DHCP-сервере была добавлена новая область, однако DHCP-клиенты не получают адресов из этой области. Такая ситуация часто возникает при попытке изменения нумерации существующей IP-сети. Например, вы получили зарегистрированный класс IP-адресов для вашей сети или изменить класс адресов, чтобы включить в сеть больше компьютеров, и теперь хотите, чтобы клиенты получали адреса из новой области. Затем вы намереваетесь удалить старую область

Вне зависимости оттого, используются или нет суперобласти, только одна область DHCP может быть активной в сети в данный момент. Активная область, применяемая для выделения адресов, должна содержать первый IP-адрес, назначенный сетевому адаптеру DHCP-сервера. Если на сервере устанавливаются дополнительные IP-адреса на вкладке дополнительных параметров TCP/IP, они не влияют на определение активной области и отклики на запросы DHCP-клиентов сети.

Проблему решают следующим образом.

- Создают на DHCP-сервсре объединенную область, включающую старые и новые диапазоны адресов.
- Изменяют основной IP-адрес сетевого адаптера DHCP-ссрвера (указанный и окне свойств TCP/IP) на адрес, входящий в новую область.

  В Windows NT Server 3.51 объединение областей не поддерживается. В этом случае измените первый IP-адрес сетевого адаптера сервера на адрес из новой области. Если необходимо продолжить использование сервером старого IP-адреса, переместите его в список дополнительных адресов на вкладке дополнительных параметров TCP/IP.

Наблюдение производительности сервера

Так как DHCP-серверы являются важным компонентом во многих сетях, мониторинг их производительности весьма важен. В Windows 2000 Server служба DHCP включает набор счетчиков для определения производительности при различных видах деятельности сервера. По умолчанию эти счетчики включаются при установке службы DHCP. Для просмотра их показаний предназначена оснастка System Monitor (ранее — Performance Monitor). Счетчики фиксируют;

- все типы сообщений DHCP, посылаемых и получаемых службой DHCP;
- среднее время обработки DHCP-сервером посылаемого и получаемого пакета сообщения;
- число пакетов, пропущенных из-за занятости DHCP-сервера.

Перемещение базы данных DHCP-сервера

Иногда требуется переместить БД DHCP на другой компьютер. Вот что для этого надо сделать.

▶ **Перемещение базы данных DHCP**

1. Остановите службу Microsoft DHCP на данном компьютере.
2. Скопируйте папку \System32\Dhcp на новый компьютер с DHCP-сервером.

   Удостоверьтесь, что новая папка находится на том же логическом диске и по тому же пути, что и на старом компьютере. Если нужно копировать файлы в иную папку, скопируйте DHCP.MDB, но не копируйте файлы с расширениями .log или .chk.
3. Запустите службу Microsoft DHCP на новом компьютере. Она будет автоматически использовать файлы со старого компьютера с расширениями .mdb и .log.

При проверке оснастка DHCP выдаст сообщение, что данная область все еще существует, так как реестр сохранил информацию о ней, включая информацию об уже используемых адресах. Необходимо устранить противоречия в БД путем добавления в нее записей для выделенных адресов. После того как клиенты обновят свои адреса, база данных будет готова.

▶ **Устранение противоречий в базе данных**

1. В оснастке DHCP щелкните область правой кнопкой и выберите команду Reconcile (Согласование).
2. В открывшемся окне щелкните кнопку Reconcile (Проверить).

Хотя это и не требуется, можно заставить DHCP-клиентов обновить выделенные им адреса, чтобы внести исправления в БД DHCP как можно быстрее. Для этого введите в командной строке **ipconfig /renew.**

Резюме

Наиболее частая проблема с DHCP-клиентом заключается в том, что во время загрузки ему не удается получить IP-адрес или другие параметры конфигурации с DHCP-сервера. Основные неполадки DHCP-сервера — невозможность зарегистрировать его в домене Windows 2000. Источник проблем DHCP, как правило, кроется в неверной IP-конфигурации клиента, поэтому начинать проверку надо именно с этого.

Закрепление материала

? Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Что такое DHCP?

2. Как взаимодействуют DHCP и DNS?

3. Что такое DHCP-клиент?

4. Опишите автоматическое конфигурирование IP в Windows 2000.

5. Почему важно планировать реализацию DHCP в сети?

6. Какое средство в Windows 2000 предназначено для управления DHCP-сервером?

7. Каковы признаки неполадок DHCP?

ГЛАВА 11

Маршрутизация и удаленный доступ

В этой главе

Вы научитесь внедрять *службу маршрутизации и удаленного доступа* (Routing and Remote Access Service, RRAS) для предоставления клиентам доступа к ресурсам сети, когда они находятся дома или в дороге, а также создавать *виртуальные частные сети* (virtual private network, VPN).

Прежде всего

Для изучения материалов этой главы потребуется:

- два сервера Windows 2000, соединенных по локальной сети.

Занятие 1. Знакомство с RRAS

Служба **RRAS** в Windows 2000 Server позволяет удаленным пользователям подключаться по телефонным линиям к корпоративной сети и обращаться к ее ресурсам, как если бы они были подключены к этой сети напрямую. RRAS также содержит службы VPN, позволяющие предоставлять доступ к корпоративным сетям через Интернет.

Изучив материал этого занятия, вы сможете:

- ✓ пояснить основные функции RRAS;
- ✓ установить RRAS;
- ✓ описать различия между RRAS и удаленным управлением;
- ✓ пояснить преимущества перехода на RRAS.

Продолжительность занятия - около 25 минут.

Общие сведения о RRAS

Служба RRAS в Windows 2000 Server обрабатывает подключения удаленных пользователей. В итоге они работают так, как если бы их компьютеры были физически соединены с сетью. Пользователи (или клиенты) запускают ПО удаленного доступа для подключения к серверу удаленного доступа — компьютеру с Windows 2000 Server и службой RRAS. Он идентифицирует пользователей и обслуживает подключения до их завершения. При удаленном подключении клиентам доступны те же службы, что и пользователям ЛВС, в том числе службы доступа к файлам и принтерам, доступ к Web-серверам и обмен сообщениями.

Клиенты удаленного доступа применяют стандартные средства для доступа к сетевым ресурсам. Например, на компьютере с Windows 2000 клиенты могут средствами Windows Explorer (Проводник) подключиться к сетевым дискам и принтерам. Подключения постоянны, так что пользователям не нужно возобновлять связь с сетевыми ресурсами во время удаленного сеанса. Поскольку RRAS полностью поддерживает буквы дисков и имена UNC, большинство приложений не требуют модификации для работы с удаленным доступом. Сервер Windows 2000 обслуживает два типа удаленных подключений.

- **Подключение по коммутируемой (телефонной) линии.** Клиент удаленного доступа может установить временное телефонное подключение с физическим портом на сервере удаленного доступа, пользуясь услугами поставщика телекоммуникаций, по аналоговой линии, линиям ISDN или X.25. Типичный пример такого подключения — клиент, набирающий телефонный номер одного из портов сервера удаленного доступа

  Удаленное подключение по аналоговой линии или **ISDN** — прямое физическое соединение клиента и сервера. Передаваемые по такому каналу данные можно шифровать, хотя это и не обязательно.
- **Виртуальная частная сеть (VPN).** Это реализация зашифрованных соединений типа «точка-точка» через частную или общедоступную сеть, например Интернет. Для вызова порта на сервере VPN клиент использует специальные протоколы, основанные на TCP/IP, называемые туннельными. Типичный пример VPN — подключение клиента по телефону через Интернет к серверу корпоративной сети. Сервер удаленного доступа отвечает на виртуальный вызов, идентифицирует вызывающего и передает данные между клиентом VPN и корпоративной сетью.

  В отличие от прямого подключения по телефону работа через VPN — это логическое (а не физическое) соединение между клиентом и сервером. Для гарантии безопасности рекомендуется шифровать данные, передаваемые по VPN-подключению.

Функции RRAS

Служба RRAS включает функции преобразования сетевых адресов (Network Adress Translation, NAT), мультипротокольной маршрутизации, протокол туннелирования канального уровня (Layer Two Tunneling Protocol, L2TP), службу проверки подлинности в Интернете (Internet Authentication Service, IAS) и политики удаленного доступа (Remote Access Policies, RAP). В конце этого занятия рассказано о фильтрах подключения по запросу, настройке времени подключения и свойств удаленного доступа для объекта пользователя, применении серверов имен и DHCP, протоколе BAP и мониторинге удаленного доступа.

Обнаружение маршрутизатора

Согласно RFC 1256, в Windows 2000 реализована новая функция, называемая *обнаружением маршрутизатора* (Router Discovery). Это модернизированный метод настройки и обнаружения шлюзов по умолчанию. При использовании DHCP или ручной настройке параметров стандартного шлюза невозможно приспособиться к изменениям сети. Обнаружение маршрутизатора позволяет клиентам динамически находить маршрутизаторы и при сбое в сети или необходимости переключаться на резервные маршрутизаторы. Поиск маршрутизатора выполняется пакетами двух видов.

1. **Запрос на определение маршрутизатора (Router solicitation).** Узел, поддерживающий RFC 1256, имеет шлюз по умолчанию путем передачи запроса в виде сообщения протокола ICMP. Этот запрос может быть послан на IP-адрес 224.0.0.2, локальный широковещательный IP-адрес или на адрес ограниченного широковещания (255.255.255.255). На практике узлы посылают запросы маршрутизатора на адрес 224.0.0.2. Маршрутизаторы в сети узла, поддерживающие RFC 1256, немедленно отвечают на этот запрос, после чего узел выбирает оптимальный маршрутизатор в качестве шлюза по умолчанию.
2. **Объявление маршрутизатора (Router Advertisment).** Это периодическое явное извещение узлов сети о доступности маршрутизатора с помощью сообщений по протоколу ICMP. Объявления маршрутизатора могут посылаться на локальный широковещательный IP-адрес или на адрес ограниченного широковещания. На практике, как и запросы на определение маршрутизатора, объявления маршрутизатора посылаются на адрес 224,0.0.2.

Примечание **Windows 2000 поддерживает поиск маршрутизатора и в качестве узла, и в качестве маршрутизатора.**

NAT

Это стандарт, определенный в RFC 1631. NAT — маршрутизатор, преобразующий IP-адреса интрасети или домашней ЛВС в действительные адреса Интернета. NAT позволяет подключаться к Интернету с любого компьютера частной сети через один IP-адрес. Windows 2000 Server включает полную реализацию NAT, называемую Connection Sharing (Общее подключение), и не конфигурируемую версию — Shared Access (Общий доступ).

Многоадресная маршрутизация

Windows 2000 Server реализует ограниченную форму многоадресной маршрутизации, используя многоадресный прокси-узел для расширения многоадресной поддержки до полноценного многоадресного маршрутизатора. Лучше всего использовать многоадресный прокси-узел для многоадресной рассылки среди удаленных пользователей или в одной ЛВС, подключенной к Интернету. На одном или нескольких интерфейсах Windows 2000 играет роль многоадресного маршрутизатора, обеспечивая многоадресную рассылку для локальных клиентов. На интер-

фейсе, который имеет прямой доступ к настоящему многоадресному маршрутизатору. Windows 2000 выполняет функции многоадресного клиента, перенаправляющего трафик со стороны локальных клиентов.

Протокол L2TP

Его считают следующей версией протокола PPTP. Работа L2TP напоминает PPTP, однако первый включает технологию перенаправления Layer 2 Forwarding (L2F), разработанную Cisco. Вскоре протокол L2TP будет принят в качестве индустриального стандарта и опубликован в RFC. Протокол L2TP соответствует канальному уровню модели OS1 и применяется для VPN.

Служба IAS

Это сервер Remote Authentication Dial-In User Service (RADIUS). Сетевой протокол RADIUS позволяет проводить удаленную аутентификацию, авторизацию и учет удаленных пользователей, которые подключаются к *серверу доступа к сети* (Network Access Server, NAS). NAS (например, сервер RRAS E Windows 2000) может быть клиентом или сервером RADIUS.

Примечание Сокращенная версия сервера RADIUS включена в Windows NT 4.0 Option pack. Сервер RADIUS (IAS) теперь доступен в Windows 2000.

Политики удаленного доступа

В Windows NT 3.5 и более поздних версиях удаленный доступ предоставлялся в зависимости от значения параметра Grant Dial-in Permission To User для объекта пользователя или средствами утилиты Remote Access Admin. Параметры обратного вызова также задавались индивидуально для каждого пользователя.

В Windows 2000 удаленный доступ предоставляется на основе свойств объекта пользователя и соответствующей политики — набора условий и параметров подключения, позволяющих сетевым администраторам более гибко настраивать разрешения удаленного доступа. Примеры таких условий — дата, принадлежность к группе или тип подключения (телефонное или VPN). Примеры параметров подключения: требования аутентификации и шифрования, использование многоканальных линий связи и длительность подключений. Одним из достоинств такого дополнительного контроля является требование шифрования при VPN-соединениях и отказ от шифрования при подключении по модему.

Политики удаленного доступа хранятся на локальном компьютере и совместно используются оснасткой Routing and Remote Access (Маршрутизация и удаленный доступ) и службой IAS. Политики удаленного доступа настраиваются из оснасток Internet Authentication Service (Служба проверки подлинности в Интернете) и Routing and Remote Access.

Включение службы RRAS

До включения RRAS оснастка управления этой службой выглядит, как на рис. 11-1.

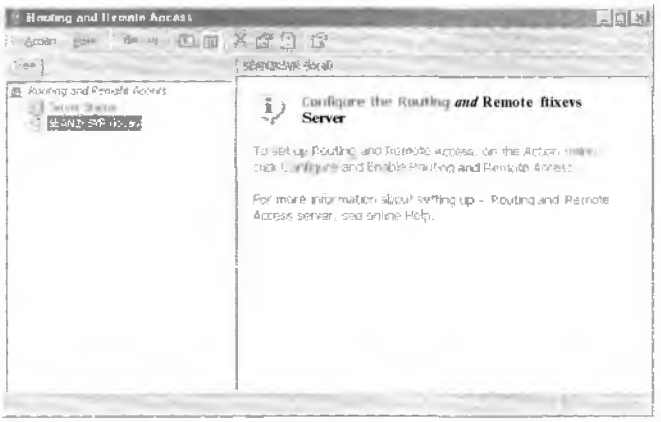


Рис. 11-1. Оснастка Routing and Remote Access (Маршрутизация и удаленный доступ) перед включением RRAS

Практикум: **установка** службы **RRAS**

Вы установите сервер RRAS, используя оснастку Routing and Remote Access.

▶ Задание 1: установите сервер RRAS

1. Запустите оснастку Routing and Remote Access.
2. Правой кнопкой щелкните имя вашего компьютера и выберите команду Configure And Enable Routing And Remote Access Server (Настроить и включить маршрутизацию и удаленный доступ).
3. В окне мастера установки сервера RRAS щелкните кнопку Next.
4. В окне Common Configurations (Общие параметры) щелкните переключатель Remote Access Server (Сервер удаленного доступа), затем — Next.
5. В окне Remote Client Protocols (Протоколы удаленных клиентов) убедитесь, что в списке протоколов перечислен TCP/IP. Удостоверьтесь, что выбран параметр Yes, All The Required Protocols Are On This List (Да, все требуемые протоколы присутствуют в списке), и щелкните Next.
6. В окне IP Address Assigment (Назначение IP-адреса) щелкните переключатель From A Of Specified Range Of Addresses (Из заданного диапазона адресов) и затем — Not.
7. В окне Address Range Assignment (Назначение диапазонов IP-адресов) щелкните кнопку New (Создать). В поле Starting Address (Начальный IP-адрес) введите **10.0.0.10** для компьютера 1 и **10.0.0.20** — для компьютера 2. В поле End Of IP Address (Конечный IP-адрес) введите **10.0.0.19** для компьютера I и **10.0.0.29** — для компьютера 2. Убедитесь, что в поле Number Of Addresses (Количество адресов) указано 10. Щелкните OK. Чтобы закрыть окно Edit Address Range, затем — Next.
8. Убедитесь, что в окне Managing Multiple Remote Access Servers (Управление несколькими серверами удаленного доступа) выбран параметр No, I Don't Want To Set This Server Up To Use RADIUS Now (Нет, не настраивать данный сервер для работы с RADIUS-сервером), затем щелкните Next.
9. Щелкните кнопку Finish (Готово).
10. Щелкните OK в ответ на любое сообщение.

Оснастка Routing and Remote Access Manager будет выглядеть, как на рис. 11-2.

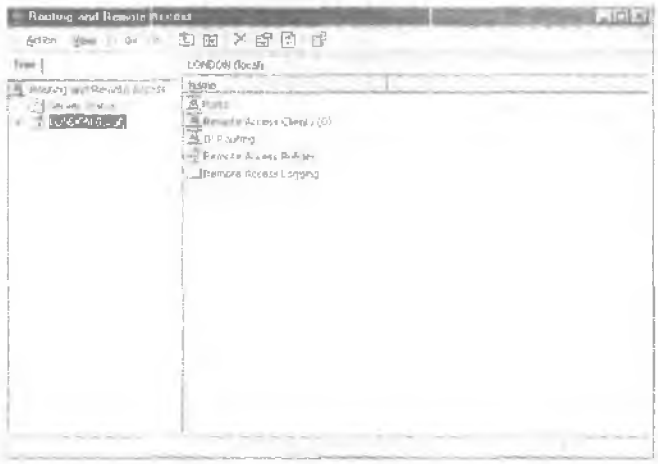


Рис. 11-2. Оснастка **Routing and Remote** Access **после включения RRAS**

▶ **Задание 2: предоставьте разрешение удаленного доступа учетной записи Administrator (Администратор)**

1. Откройте оснастку Active Directory Users And Computers (Active Directory — пользователи и компьютеры, если вы работаете на контроллере домена) или Computer Management (Управление компьютером, если вы работаете в составе рабочей группы).
2. Раскройте окно свойств учетной записи Administrator (Администратор), перейдите на вкладку Dial-In (Входящие звонки) и щелкните переключатель Allow Access (Разрешить доступ).

Удаленный доступ и удаленное управление

Различия между этими режимами таковы;

- сервер удаленного доступа — это программный многопротокольный маршрутизатор, а режим удаленного управления подразумевает совместное использование экрана, клавиатуры и мыши по линии связи. При удаленном доступе приложения запускаются на компьютере-клиенте;
- при удаленном управлении клиенты совместно используют один или несколько центральных процессоров сервера. В этом режиме приложения запускаются на сервере, и процессор сервера удаленного доступа обслуживает подключения клиентов к сетевым ресурсам, а не собственно приложения.

Преимущества использования RRAS

При обновлении Windows NT 4.0 до 2000 возникает одна проблема. Windows NT 4.0 применяет учетную запись LocalSystem. Когда какая-нибудь служба запускается под этой учетной записью, имя пользователя и пароль не предоставляются.

Active Directory по умолчанию отклоняет запросы атрибутов объектов через подобные подключения. Поэтому в смешанной среде необходимо предусмотреть, чтобы серверы RAS Windows NT 4.0 и **RRAS** Windows 2000 могли получать параметры удаленного доступа для подключающихся пользователей из Active Directory. Серверам такой доступ необходим для ответа на вопрос, уполномочен ли пользователь подключаться, и выяснения других параметров соединения, например номеров обратного вызова.

Примечание Если для учетной записи не заданы реквизиты (как в случае с LocalSystem), получить доступ к сетевым ресурсам на основе аутентификации NTLM не удастся. Для организации такого доступа на удаленном компьютере надо явно разрешить подобные подключения.

Условия обновления RAS

Чтобы сервер RAS Windows NT 4.0 мог получать сведения о пользователе из Active Directory, надо выполнить одно из условий:

- домен работает в смешанном режиме, и сервер **RRAS** одновременно играет роль резервного контроллера домена. В этой ситуации RRAS имеет доступ к локальной БД безопасности;
- домен работает в смешанном режиме, и сервер RRAS получает информацию о подключающемся пользователе от резервного контроллера домена. Это также позволяет получить доступ к локальной БД безопасности;
- домен работает в смешанном или естественном режиме, и защита Active Directory ослаблена после присвоения группе Everyone (Все) разрешений на чтение любого свойства любого объекта пользователя. Такая конфигурация задается мастером установки Active Directory (программой DCPROMO.EXE) при выборе параметра Permission Compatible With Pre-Windows 2000 Server.

Примечание Если не ослабить защиту Active Directory и не установить сервер RRAS на резервном контроллере домена, подключение будет нестабильным. Даже если ваш домен работает в смешанном режиме, не удастся настроить сервер RRAS, чтобы он соединялся с резервным контроллером домена только для аутентификации. Если проверку подлинности выполняет контроллер домена Windows 2000, подключение будет отклонено.

Параметр Permission Compatible With Pre-Windows 2000 Server включает группу Everyone в локальную группу Pre-Windows 2000 Compatible Access (Пред-Windows 2000 доступ). Вы можете ужесточить ограничения, удалив из последней группу Everyone, после обновления всех серверов удаленного доступа до Windows 2000.

Примечание Применяйте трюк с группой Everyone, только если хорошо представляете его воздействие на безопасность Active Directory. Если в вашей ситуации ослабление защиты неприемлемо, обновите сервер RRAS Windows NT 4.0 до Windows 2000 и включите его в домен Windows 2000 смешанного или естественного режима. Это поможет стабилизировать телефонный доступ во время работы домена в смешанном режиме.

Если вы хотите ослабить защиту, чтобы серверы RRAS Windows NT 4.0 могли работать и после установки Active Directory, добавьте группу Everyone в группу Pre-Windows 2000 Compatible Access, введя команду **net localgroup «Pre-Windows 2000 Compatible Access» Everyone** /add.

Резюме

Вы получили представление об основных функциях удаленного доступа, включая обнаружение маршрутизатора, NAT, многоадресную маршрутизацию, протокол L2TP, службу IAS и политику удаленного доступа. Также вы научились запускать службу RRAS.

Занятие 2. Настройка сервера RRAS

После включения RRAS вы можете настроить обслуживание входящих подключений, ограничить удаленный доступ средствами политики, добавить профили удаленных пользователей и контролировать доступ с помощью протокола BAP.

Изучив материал этого занятия, вы сможете:

- ✓ разрешить входящие подключения;
- ✓ создать политики удаленного доступа;
- ✓ настроить профиль удаленного доступа;
- ✓ настроить протокол BAP.

Продолжительность занятия - около 25 минут.

Включение входящих подключений

При первом запуске RRAS автоматически создаются 5 портов PPTP и 5 портов L2TP (рис. 11-3). Число доступных любому удаленному серверу VPN-портов не ограничено. Вы вправе настроить порты R папке Ports (Порты) в дереве консоли оснастки Routing and Remote Access (Маршрутизация и удаленный доступ).

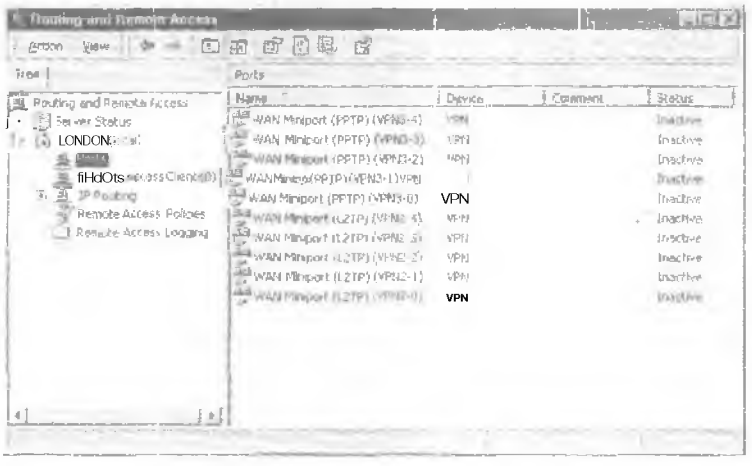


Рис. 11-3. Список портов

В папку Ports также можно добавить параллельный порт. Последовательные коммуникационные порты будут отображаться только после установки модема. Оба типа портов способны обрабатывать входящие и исходящие подключения.

Создание политики удаленного доступа

Политика удаленного доступа — это именованный набор условий (рис. 11-4), определяющий пользователей, которым разрешен удаленный доступ к сети, и характеристики этого подключения. Принятие или отклонение подключения зависит от разных параметров: даты и времени подключения, членства в группе, типа службы и т. п. Например, вы можете разрешить подключение по IDSN длительностью не более 30 минут без передачи пакетов HTTP.

Примечание Политики совместно используются службами RRAS и IAS. Политики разрешается настраивать средствами любой оснастки, управляющей этими службами.

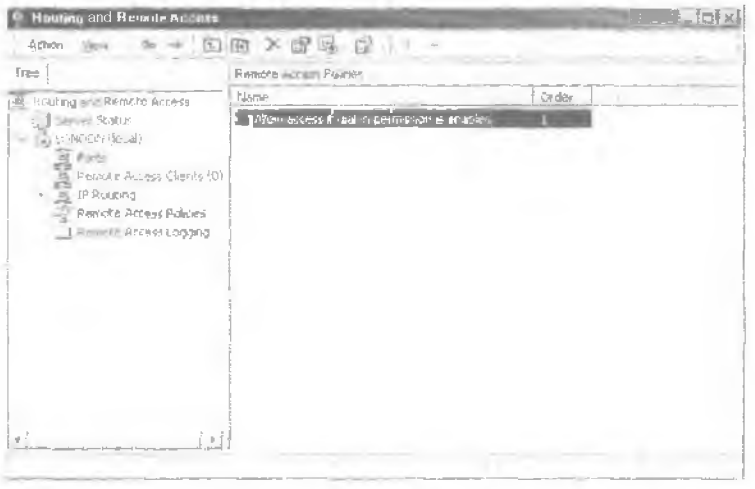


Рис. 11-4. Политики удаленного доступа

Средствами оснастки RRAS политики можно создавать, удалять, переименовывать и упорядочивать. Заметьте, что команда Save при этом недоступна, так что сохранить копию на дискету невозможно. Порядок политик важен, поскольку подключение отклоняется или принимается после прохождения первой подходящей политики.

Примечание Политики удаленного доступа не хранятся в Active Directory; они хранятся локально в файле IAS.MDB. Политики нужно создавать вручную на каждом сервере. Политики применяются к пользователям в домене смешанного, режима, хотя разрешение удаленного доступа для пользователя принимает только два значения: Allow Access (Разрешить доступ) или Deny Access (Запретить доступ) (рис. 11-5). Параметр Control Access Through Remote Access Policy (Управление на основе политики удаленного доступа) недоступен на контроллерах домена в смешанном режиме. Если для пользователя задано Allow Access, то перед установлением подключения оно все равно проверяется на соответствие политике.

Условия

Условия политики определяют ситуации, когда следует предоставлять или запрещать удаленный доступ. Условия учитываются вместе с разрешением удаленного доступа. Блок-схема на рис. 11-6 иллюстрирует логику обработки запроса подключения.

Примечание Если политики удаленного доступа не существуют (например удалена политика по умолчанию), пользователям не удастся подключиться к сети вне зависимости от их индивидуальных разрешений и параметров RRAS.

На основе этой блок-схемы можно предсказать результат запроса подключения в любой ситуации. Например, для объекта пользователя задан параметр Control Access Through Remote Access Policy, а в политике указано Allow Access If Dial-In Permission Is Enabled (Разрешить доступ, если разрешены входящие подключения). Согласно блок-схеме пользователю будет отказано в подключении.

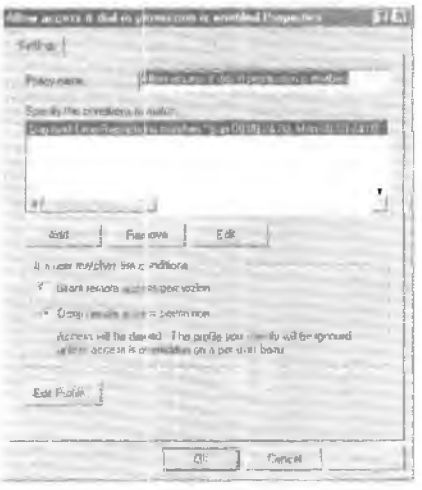


Рис. 11-5. Настройка политики удаленного доступа

Рис. 11-6. Схема применения политики удаленного доступа

Впрочем, если для объекта пользователя (рис. 11-8) задать параметр Allow Access, применение той же политики по умолчанию приведет к тому, что подключение будет принято.

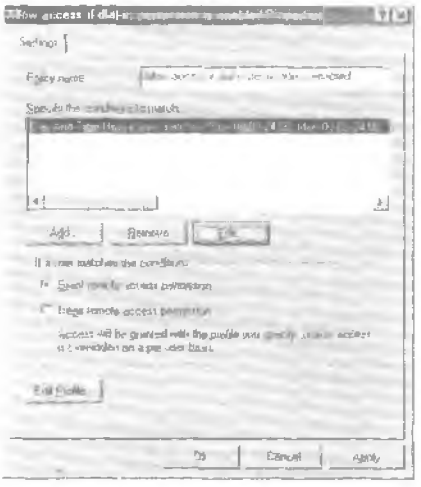


Рис. 11-7. Настройка параметров объекта пользователя для предоставления удаленного доступа

Идентификатор звонящего

Позволяет удостовериться, что пользователь подключается с указанного телефонного номера. Для применения этой функции требуется поддержка передачи телефонного номера от абонента к службе RRAS, иначе подключение будет отклонено.

Примечание Для совместимости с предыдущими версиями Windows NT в смешанном режиме не поддерживаются политики удаленного доступа, идентификатор звонящего, параметры Apply Static Routes и Assign Static IP Address.

Практикум: создание политики удаленного доступа

Сейчас вы создадите политику, разрешающую удаленный доступ в зависимости от членства в группе.

► **Задание: создайте политику удаленного доступа**

1. В оснастке Routing and Remote Access щелкните правой кнопкой Remote Access Policies (Политика удаленного доступа) и выберите команду New Remote Access Policy (Создать политику удаленного доступа).
2. Введите понятное имя политики **Allow Domain** Users, затем щелкните Next.
3. Щелкните кнопку Add (Добавить), чтобы добавить условие.
4. Выберите в списке Windows-groups и щелкните кнопку Add.
5. В открывшемся окне щелкните кнопку Add, выберите группу Domain Users (Пользователи домена), затем снова щелкните Add и OK.
6. Щелкните OK, чтобы закрыть окно Groups (Группы).
7. Щелкните Next, затем выберите Grant Remote Access Permition (Предоставить право удаленного доступа).
8. Щелкните Next, затем — Finish.

Настройка профиля удаленного доступа

Профиль определяет тип доступа, предоставляемого пользователю при соблюдении условий. Для настройки профиля предназначено шесть вкладок: Dial-In Constraints (Ограничения по входящим звонкам), IP, Multilink (Многоканальное подключение), Authentication (Проверка подлинности), Encryption (Шифрование) и Advanced.

Ограничения по входящим звонкам

Настраиваются из диалогового окна Edit Dial-in Profile (Изменение профиля коммутируемых подключений) на вкладке Dial-In Constrains (Ограничения по входящим звонкам) (рис. 11-8). Возможные параметры таковы: время простоя до отключения, максимальная продолжительность сеанса, допустимые дата и время подключения, номер телефона, с которого разрешается подключаться, и тип подключения (IDSN, туннель и т. п.).

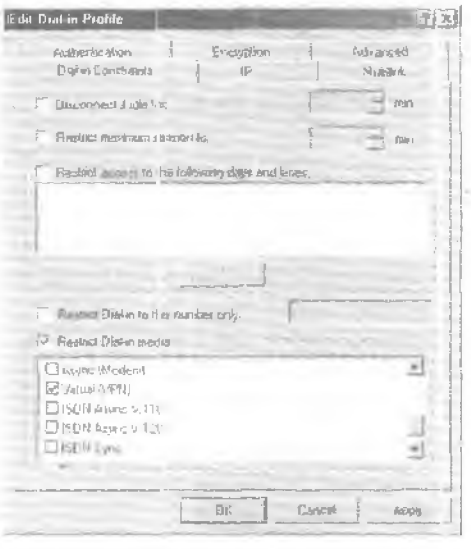


Рис. 11-8. Диалоговое окно Edit Dial-in Profile (Изменение профиля коммутируемых подключений)

Вкладка IP

Здесь настраиваются выделение IP-адрес клиенту и фильтрование IP-пакетов. Фильтры пакетов настраиваются для исходящих и входящих пакетов, также можно указать наблюдаемые протокол и порт.

Многоканальное подключение

Задает параметры многоканального подключения и протокола BAP. Часть линий можно отключить, если нагрузка будет ниже указанного уровня определенное время.

Проверка подлинности

Залает протоколы аутентификации, такие, как PAP, CHAP и EAP.

Шифрование

Здесь настраиваются уровни шифрования.

Дополнительно

На этой вкладке задаются дополнительные параметры сети, не относящиеся к серверам RRAS, например стандартные атрибуты RADIUS и Ascend, применяемые к NAS-оборудованию сторонних изготовителей.

Практикум: создание фильтра политики

Вы измените профиль политики Allow Access If Dial-In Permission Is Enabled, чтобы пользователям, получающим доступ через эту политику, не удалось проверить наличие связи с сетью сервера RRAS, в то время как пользователи, получающие доступ через политику Allow Domain Users, могли это сделать.

▶ **Задание: создайте эхо-фильтр TCMP в политике Allow Access If Dial-In Permission Is Enabled**

1. Щелкните правой кнопкой политику Allow Access If Dial-In Permission Is Enabled t Разрешить доступ, если разрешены входящие подключения) и выберите команду Properties (Свойства).
2. Щелкните кнопку Edit Profile (Изменить профиль).
3. Перейдите на вкладку IP.
4. Щелкните фильтр From Client (Or клиента).
5. Щелкните кнопку Add (Добавить).
6. Пометьте флажок Destination Network (Сеть назначения).
7. В поле IP-адреса введите адрес и м.аску подсети сервера RRAS.
8. Выберите в списке протокол ICMP.
9. В поле ICMP type (Тип ICMP) введите 8, а и поле ICMP code (Код ICMP) — 0. (Тип 8 в ICMP соответствует эхо-запросу).
10. Щелкните OK, чтобы закрыть окно Edit IP filter (Изменение IP-фильтра).
11. Щелкните OK, чтобы закрыть окно настройки фильтра входа.

Настройка протокола BAP

Протоколы Bandwidth Allocation Protocol (BAP) и Bandwidth Allocation Control Protocol (BACP) повышают эффективность многоканальных подключений путем динамического добавления и отключения линий связи. Оба протокола являются управляющими протоколами PPP и работают совместно для предоставления полосы пропускания по запросу.

Функции динамического перераспределения полосы пропускания реализуются посредством компонентов, описанных ниже.

- **Link Discriminator** — новая функция протокола управления связью (Link Control Protocol, LCP), используемая для уникальной идентификации каждой линии связи в многоканальном пучке.
- **Протокол BACP** — использует LCP-согласования для определения предпочтител ,ного узла, если узлы одновременно передают один и тот же запрос BACP.
- **Протокол BAP** — предоставляет механизм для управления каналом и полосой пропускания. Управление каналом позволяет добавлять и отключать дополнительные каналы связи при необходимости. Управление полосой пропускания решает, когда добавить или отключить канал, в зависимости от текущей нагрузки на каналы связи.

Данные протоколов BAP и BACP инкапсулируются *в* кадрах протокола PPP, включая поле протокола (в шестнадцатеричном виде). Эта информация полезна при чтении журналов протокола PPP. Вы можете включить управление полосой пропускания средствами BAP и BACP на вкладке PPP диалогового окна свойств сервера удаленного доступа (рис. 11-9).

Рис. 11-9. Настройка параметров PPP для политики удаленного доступа

▶ **Включение и отключение BAP/BACP** на сервере

1. В оснастке Routing and Remote Access щелкните правой кнопкой сервер, на котором вы хотите включить BAP/ BACP, и выберите команду Properties.
2. На вкладке PPP пометьте флажок Dynamic Bandwidth Protocol Using BAP Or BACP (Динамическое управление пропускной способностью (BAP/BACP)).

Политики BAP осуществляются посредством параметров профиля или политик удаленного доступа.

Дополнительные телефонные номера BAP

Сервер может предоставить клиенту дополнительный телефонный номер, если требуется дополнительная емкость полосы пропускания. Клиенту нужно знать только один телефонный номер, но в ходе сеанса при необходимости могут быть добавлены дополнительные линии связи (рис. 11-10).

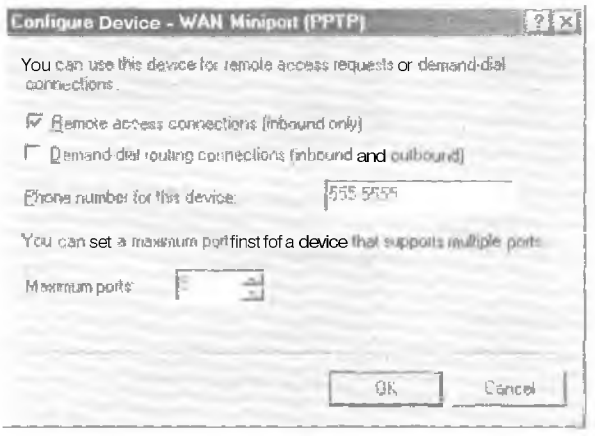


Рис. 11-10. Задание дополнительных телефонных номеров BAP

Резюме

Мы рассказали, как настроить службу Routing and Remote Access для обработки входящих и исходящих соединений, заблокировать ее средствами политики, добавить профили удаленного доступа для безопасности и контролировать ее через протокол BAP.

Занятие 3 Внедрение IP-маршрутизации на сервере RRAS

Сейчас вы узнаете, как сделать сервер удаленного доступа IP-маршрутизатором, дополнить его таблицы маршрутов и реализовать маршрутизацию по требованию.

Изучив материал этого занятия, вы сможете:

- ✓ внедрить IP-маршрутизацию (служба Routing and Remote Access);
- ✓ дополнять таблицы маршрутов;
- ✓ внедрить маршрутизацию по требованию.

Продолжительность занятия — около 30 минут.

Внедрение IP-маршрутизации

Процесс внедрения IP-маршрутизации в целом аналогичен установке сервера удаленного доступа. Как показано в следующем упражнении, для внедрения IP-маршрутизации используется тот же мастер, что и для установки службы удаленного доступа. Если эта служба уже имеется на вашем компьютере, установите службу IP Routing, как рассказано далее.

▶ **Установка службы IP-маршрутизации**

1. В оснастке Routing and Remote Access Manager откройте окно свойств сервера, на вкладке General (Общие) пометьте флажок Router (Маршрутизатор) и щелкните OK.
1. Появится сообщение, что изменения вступят в силу только после перезагрузки компьютера. Щелкните Yes.

Если сервер удаленного доступа не установлен на вашем компьютере, выполните следующий практикум.

Практикум: установка и настройка сервера RRAS

Сейчас вы установите сервер RRAS с помощью диспетчера Routing and Remote Access Manager (рис. 11-11).

▶ Задание: **установите сервер RRAS**

1. Откройте диспетчер Routing and Remote Access Manager.
2. Щелкните правой кнопкой мыши узел своего компьютера и выберите в контекстном меню команду Configure And Enable Routing And Remote Access.
3. В окне мастера Routing And Remote Access Server Setup Wizard щелкните Next.
4. На странице Common Configurations щелкните переключатель Network Router (Маршрутизатор сети). Затем щелкните Next.
5. Убедитесь, что в списке протоколов в окне Remote Client Protocols указан протокол TCP/IP. Убедитесь также, что помечен флажок Yes, All The Required Protocols Are On This List. Щелкните кнопку Next.
6. Убедитесь, что на странице Demand-Dial Connections в группе You Can Set Up Demand-Dial Routing Connections After This Wizard Finishes выбран переключатель No, и щелкните Next.
7. Щелкните кнопку Finish.

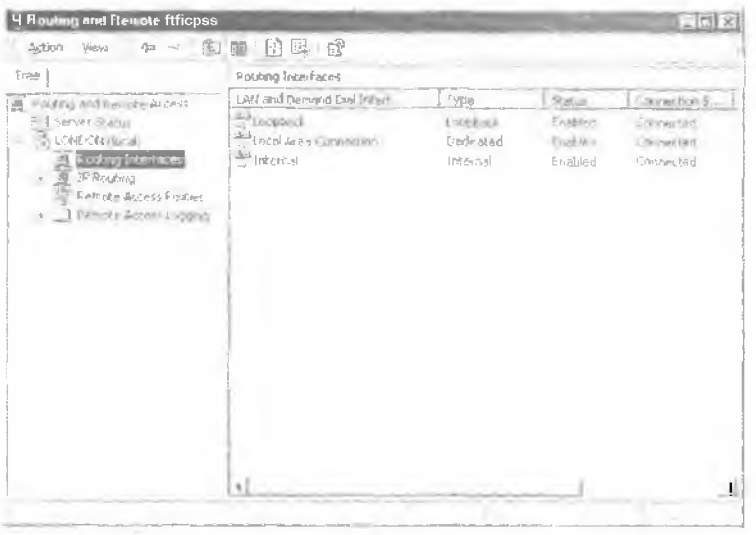


Рис. 11-11. Управление сервером маршрутизации и удаленного доступа

Обновление таблицы маршрутов

На выбор маршрута передачи пакетов влияет информация о доступных в интрасети сетевых адресах (или сетевых идентификаторах). Эта информация запрашивается из БД, которая называется таблицей маршрутов и представляет собой серии записей (маршрутов), содержащих сведения о расположении сетевых идентификаторов промежуточной сети. Таблица маршрутов имеется не только у маршрутизаторов, но также и у обычных компьютеров, использующих ее для выбора оптимального маршрута.

Типы записей таблицы маршрутов

Каждая запись в таблице маршрутов считается маршрутом и относится к одному из следующих типов:

- **сетевой** маршрут — маршрут к определенному сетевому идентификатору в промежуточной сети;
- маршрут компьютера — маршрут к адресу промежуточной сети (сетевой идентификатор и идентификатор узла). Маршруты этого типа используются для создания заказных маршрутов к определенным узлам в целях контроля и оптимизации сетевого трафика. Маршрут компьютера эквивалентен сетевому маршруту с маской сети 255.255.255.255;
- маршрут по умолчанию — применяется при отсутствии в таблице других маршрутов, например, если маршрутизатор или компьютер не может найти в таблице сетевой маршрут или маршрут компьютера к конечной точке. Маршрут по умолчанию упрощает настройку узлов. Вместо того чтобы вставать компьютерам маршруты для всех сетевых идентификаторов промежуточной сети, вы можете воспользоваться одним маршрутом по умолчанию для пересылки пакетов в конечную сеть или на адрес промежуточной сети, не найденный в таблице маршрутов. Маршрут по умолчанию эквивалентен сетевому маршруту с маской подсети 0.0.0.0.

Структура таблицы маршрутов

На рис. 11-12 изображена таблица маршрутов.

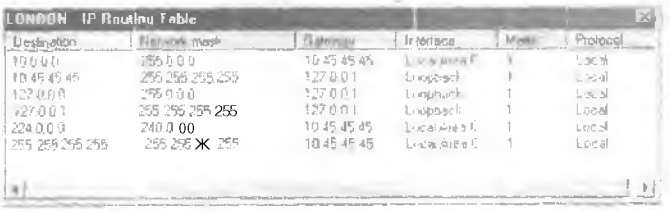


Рис. 11-12. Таблица маршрутов

Каждая запись таблицы маршрутов включает несколько полей. Четыре перечислены ниже:

- **Destination (Назначение)** — сетевой идентификатор или адрес промежуточной сети для маршрута компьютера. На IP-маршрутизаторах имеются дополнительные поля маски подсети, выделяющие идентификатор IP-сети из конечного IP-адреса;
- **Gateway (Шлюз)** — аппаратный адрес или адрес промежуточной сети, на который пересылается пакет. Для сетей, к которым напрямую подключен узел или маршрутизатор, поле Gateway может содержать адрес интерфейса, подсоединенного к сети;
- **Interface (Интерфейс)** — сетевой интерфейс, через который пакеты пересылаются сетевому идентификатору. Данное поле содержит номер порта или другой логический идентификатор;
- **Metric (Метрика)** — значение данного поля указывает степень предпочтительности маршрута. Обычно меньшим значением метрики соответствуют наиболее предпочтительные маршруты. Если к конечному адресу существует несколько маршрутов, используется маршрут с наименьшим значением метрики. Некоторые алгоритмы маршрутизации хранят в таблице маршрутов только простейший маршрут к любому сетевому идентификатору, даже если существует несколько маршрутов. В этом случае метрика позволяет маршрутизатору выбрать маршрут, который будет занесен в таблицу.

Примечание Это лишь примерный список полей таблицы маршрутизации. Реальный перечень полей зависит от используемого маршрутизируемого протокола.

Маршрутизация по требованию

Интерфейс доступа по требованию — это интерфейс маршрутизатора, вызываемый в случае необходимости; для выявления такой необходимости используется анализ сетевого трафика. Соединение по требованию устанавливается лишь в случае, если из таблицы маршрутов следует, что данный интерфейс необходим для достижения конечного IP-адреса. Маршрутная таблица не позволяет выбрать пользователя или протокол, который способен устанавливать соединение по запросу. Выбор осуществляется в зависимости от места назначения трафика.

Фильтры доступа по требованию определяют, для какого трафика может устанавливаться соединение по требованию. Фильтры разрешается настроить для допуска или блокирования конкретных/конечных IP-адресов, портов и протоколов. Кроме того, вы вправе задать ограничения по времени суток. Даже если соединение соответствует параметрам фильтра, при несоответствии ограничениям по времени суток попытка установить это соединение будет заблокирована.

Ниже описаны поля из заголовков IP, TCP, UDP, которые допустимо применять для создания фильтров доступа по требованию. Служба Routing and Remote Access позволяет выполнять фильтрование по нескольким полям: заголовок IP, заголовок TCP, заголовок UDP, заголовок ICMP.

Заголовок IP

IP-дейтаграмма включает заголовок IP длиной 20 байт со следующими полями:

- **IP-протокол** — идентификатор клиентского IP-протокола. Например, идентификатор для TCP — 6, для UDP — 17, для ICMP — 1. Поле Protocol применяется для пересылки IP-пакета протоколу более высокого уровня;
- **Исходный IP-адрес** — IP-адрес исходного узла;
- **Целевой IP-адрес** — IP-адрес конечного узла. В качестве конечного IP-адреса можно указать маску подсети, что позволяет охватить одним фильтром диапазон IP-адресов.

Заголовок TCP

В протоколе TCP данные, содержащиеся в сегменте TCP, считаются последовательностью байтов без границ записей или полей. Ниже описаны ключевые поля заголовка TCP:

- **Исходный TCP-порт** — данное поле позволяет определить исходный процесс, пославший сегмент TCP;
- **Целевой TCP-порт** — данное поле позволяет определить конечный процесс для данного сегмента TCP.

Заголовок UDP

Протокол UDP используется приложениями, не требующими подтверждения приема данных и обычно пересылающих небольшие объемы информации. Ниже описаны ключевые поля заголовка UDP:

- **Исходный UDP-порт** — данное поле позволяет определить исходный процесс, пославший сообщение UDP;
- **Целевой UDP-порт** — данное поле позволяет определить конечный процесс для данного сообщения UDP.

Примечание Список широко используемых портов вы можете найти в *systemroot*\system32\drivers\etc\services или в RFC 1700.

Заголовок ICMP

Сообщения ICMP инкапсулируются в IP-дейтаграммы, благодаря чему их удается маршрутизировать через промежуточную сеть. Ниже описаны ключевые поля пакета ICMP:

- **Тип ICMP** — указывает тип пакета ICMP (эхо-запрос, эхо-ответ и т. д.);
- **Код ICMP** — указывает одну из нескольких возможных функций в пределах данного типа.

Настройка фильтров доступа по требованию

В Windows 2000 разрешается настраивать фильтры доступа по требованию и определять время, когда подключение разрешено.

▶ **Настройка *фильтров* доступа по *требованию***

1. Откройте оснастку Routing and Remote Access.
2. Щелкните узел Routing Interfaces (Интерфейсы маршрутизации).
3. Щелкните правой кнопкой мыши значок интерфейса доступа по требованию.
4. Выберите в контекстном меню команду Set Demand-Dial Filters.
5. В диалоговом окне Set Demand-Dial Filters (рис. 11-13) щелкните кнопку Add.

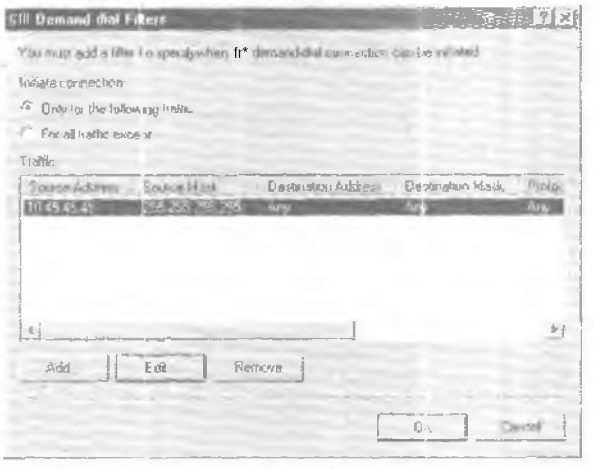


Рис. 11-13. Настройка фильтров доступа по требованию

Исходный и конечный IP-адреса

Указываются как маска подсети, что позволяет охватить одним фильтром диапазон IP-адресов (соответствующих сетевым идентификаторам). Например, фильтр 10.45.45.45 с маской 255.2:55.255.255 относится только к одному адресу, в то время как фильтр 10.0.0.0 с маской 255.0 0.0 распространяется на всю сеть класса А.

Протокол

Для каждого фильтра можно применять различные протоколы:

- для протоколов TCP и UDP указываются номера начального и конечного портов;
- для протокола ICMP указываются тип и код ICMP;
- ANY означает любой протокол.
- Other позволяет указать идентификатор (название или номер) IP-протокола. Преобразование имен протоколов в номера осуществляется с использованием файла PROTOCOL, хранящегося в каталоге *systemwinroot*\system32\drivers\etc.

Действие

Фильтрование соединений по требованию основано на исключениях. Например, вы вправе настроить службу RRAS, чтобы соединения устанавливались для любого трафика, соответствующего фильтрам, или любого трафика, кроме указанного в фильтрах.

Задание времени, когда разрешено подключение

Вы вправе указать время суток и дни недели, когда подключения по требованию запрещаются или разрешаются.

► **Настройка ограничений по времени суток**

1. Откройте оснастку Routing and Remote Access.
2. Щелкните узел Routing Interfaces.
3. Щелкните правой кнопкой мыши значок интерфейса доступа по требованию.
4. Выберите в контекстном меню команду Dial-Out Hours.
5. В диалоговом окне Dial-Out Hours (рис. 11-14) залайте часы, когда можно или нельзя устанавливать соединения.

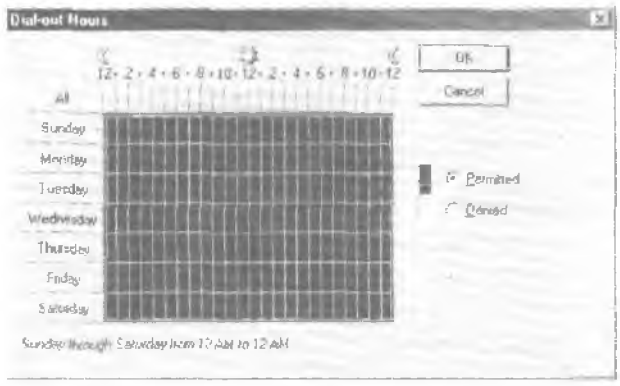


Рис. 11-14. Диалоговое окно Dial-Out Hours

Резюме

Вы узнали, как сделать сервер удаленного доступа IP-маршрутизатором, установить службу RRAS, обновить таблицы маршрутов IP-маршрутизатора и внедрить маршрутизацию по требованию.

Занятие 4. Поддержка VPN

VPN обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через *промежуточную сеть* (internetwork), например Интернет. Здесь рассказывается о VPN в маршрутизируемых средах и Интернете.

Изучив материал этого занятия, вы сможете:

- ✓ дать определение виртуальной частной сети;
- ✓ рассказать о VPN в маршрутизируемой среде;
- ✓ рассказать о сервере VPN в Интернете.

Продолжительность занятия - около 20 минут.

Внедрение виртуальных частных сетей

VPN обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть (рис. 11-15). Дома или в пути пользователи могут, применяя VPN-подключения, соединяться с сервером организации через инфраструктуру общедоступной сети (например Интернета). С точки зрения пользователя, VPN-подключение выглядит как прямое соединение «точка-точка» между его компьютером (клиентом VPN) и сервером организации (сервером VPN). Конкретная инфраструктура общедоступной сети значения не имеет, так как логически данные передаются через выделенное частное подключение.

Рис. 11-15. Схема виртуальной частной сети

Организации через VPN-подключения осуществляют соединения между географически уделенными подразделениями или подключаются к серверам других организаций через общедоступные сети (например Интернет) с поддержкой безопасной связи. VPN-подключения через Интернет логически выглядят как выделенные подключения через ГВС.

Интерфейс виртуальной сети предоставляет пользователю защищенное подключение к частной сети через общедоступную.

Основы туннелирования

Туннелирование (tunneling), или *инкапсуляция* (encapsulation), — это способ передачи полезной информации через промежуточную сеть (рис. 11-16). Такой информацией могут быть кадры (или пакеты) другого протокола. При инкапсуляции кадр не передается в сгенерированном узлом-отправителем виде, а снабжается дополнительным заголовком, содержащим информацию о маршруте, позволяющую инкапсулированным пакетам проходить через промежуточную сеть. На конце туннеля кадры деинкапсулируются и передаются получателю.

Рис. 11-16. Туннель VPN

Этот процесс (включающий инкапсуляцию и передачу пакетов) и есть туннелирование. Логический путь передвижения инкапсулированных пакетов в транзитной сети называется *туннелем* (tunnel).

Протоколы VPN

Для формирования VPN в Windows 2000 используются протоколы PPTP, L2TP, IPSEC и IP-IP.

- Протокол PPTP — позволяет инкапсулировать IP-, IPX- и NetBEUI-трафик в заголовки IP для передачи по IP-сети, например Интернету;
- Протокол **L2TP** — позволяет шифровать и передавать IP-трафик с использованием любых протоколов, поддерживающих режим «точка-точка» доставки дейтаграммам. Например, к ним относятся протокол IP, ретрансляция кадров и асинхронный режим передачи (ATM);
- Протокол **IPSec** — позволяет шифровать и инкапсулировать полезную информацию протокола IP в заголовки IP для передачи по IP-сетям, например Интернету;
- Протокол **IP-IP** — IP-дейтаграмма инкапсулируется с помощью дополнительного заголовка IP. Главное назначение IP-IP — туннелирование многоадресного трафика в частях сети, не поддерживающих многоадресную маршрутизацию.

Интеграция VPN в маршрутизируемую среду

В некоторых корпоративных промежуточных сетях (рис. 11-17) информация определенных отделов (отдел кадров и т. д.) может быть настолько важной, что ЛВС отдела физически отключается от других сегментов сети корпорации. Это позволяет защитить данные отдела, но создает проблемы с доступом к информации для пользователей, физически не соединенных с данной ЛВС.

Рис. 11-17. Корпоративная транзитная сеть

При использовании VPN ЛВС отдела может быть физически подключена к сети корпорации, но доступ к этой ЛВС будет осуществляться через VPN-сервер. Обратите внимание, что VPN-сервер не является маршрутизатором между сетью отдела и сетью корпорации. Пользователи корпоративной сети с соответствующими правами доступа могут установить собственное VPN-соединение с VPN-сервером для работы с защищенными ресурсами отдела. Кроме того, в целях обеспечения конфиденциальности все коммуникации по VPN-сетям разрешается шифровать. Пользователи без соответствующих прав доступа не видят ЛВС отдела в сетевом окружении.

Интеграция VPN-серверов с Интернетом

Удаленный пользователь вместо междугороднего или международного звонка для подключения к корпоративному или стороннему NAS подсоединяется к локальному *поставщику услуг Интернета* (Internet service provider, ISP). Через соединение с ISP, а значит и Интернетом, создается виртуальная частная сеть между пользователем, соединяющимся по телефону, и корпоративным сервером виртуальных частных сетей (рис. 11-18).

Рис. 11-18. Удаленный доступ через Интернет

Соединить сети через Интернет можно одним из двух способов (рис. 11-19).

- **Выделенная линия.** Вместо применения обычных методов соединения, таких, как ретрансляция кадров, дочерний офис и корпоративные маршрутизаторы соединяются с Интернетом, используя локальный выделенный канал и локального ISP. Локальные подключения к ISP позволяют создавать виртуальные частные сети между дочерним офисом и корпоративным маршрутизатором через Интернет.
- **Телефонная линия.** Маршрутизатор дочернего офиса вместо междугородного телефонного звонка на корпоративную сеть или шлюзовый сервер сетевого доступа соединяется со своим локальным провайдером. Через соединение с локальным провайдером виртуальные частные сети создаются между дочерним офисом и корпоративным маршрутизатором через Интернет.

Рис. 11-19. VPN через Интернет

Примечание В обоих случаях пользователи не платят за междугородный разговор, поскольку применяются только физические локальные линии связи.

Для обеспечения надежного соединения с VPN корпоративный маршрутизатор, являющийся сервером VPN, должен соединяться с локальным ISP через выделенную линию. Сервер VPN должен ждать входящих VPN-соединений круглосуточно. Хотя это возможно и при соединении по телефону, этот вариант менее надежен, так как динамические IP-адреса используются совместно и могут быть непостоянными.

Практикум: создание интерфейса VPN

Вы создадите интерфейсы VPN на каждом маршрутизаторе.

▶ **Задание 1: создайте интерфейс VPN**

1. Откройте Routing and Remote Access Manager, щелкните правой кнопкой Routing Interfaces, выберите команду New Demand-Dial Interface и щелкните Next.
2. Назовите интерфейс именем удаленного маршрутизатора, к которому вы будете подсоединяться.
3. В окне Connection Type щелкните переключатель Connect Using Virtual Private Network и затем — Next.
4. В окне VPN Type щелкните L2TP, затем — Next.
5. Введите IP-адрес удаленного маршрутизатора, к которому вы собираетесь подключаться, и щелкните кнопку Next.
6. В окне Protocols And Security пометьте флажки Route IP Packet On This Interface и Add User Account So A Remote Router Can Dial In. Затем щелкните Next.

   Откроется диалоговое окно Dial-In Credentials, где указано имя, с которым будет подключаться удаленный маршрутизатор. Оно выделено серым, поскольку это имя создаваемого нами интерфейса.
7. Щелкните кнопку Next.
8. Введите в диалоговом окне Dial-Out Credentials локальное имя маршрутизатора. Маршрутизатор будет использовать это имя при соединении с удаленным маршрутизатором. Имя будет соответствовать имени интерфейса доступа по требованию на удаленном маршрутизаторе. Не заполняя поля Domain и Password, щелкните Next.
9. Щелкните кнопку Finish.
10. Повторите пункты 1- 9 для другого маршрутизатора.

Примечание При создании туннеля между маршрутизаторами через общедоступную сеть для наружных интерфейсов маршрутизаторов необходимо определить фильтры, которые будут пропускать только трафик туннеля.

► **Задание 2: обменяйтесь таблицами маршрутов с помощью функции Auto Static update**

1. Откройте оснастку Routing and Remote Access и в дереве консоли раскройте узел IP Routing\General.
2. Щелкните правой кнопкой значок интерфейса доступа по требованию и выберите в контекстном меню команду Update Routes.
3. Повторите пункты 1 — 2 для другого маршрутизатора.

► **Задание 3; просмотрите новые маршруты**

1. Откройте оснастку Routing and Remote Access и в дереве консоли раскройте узел IP Routing\Static Routes.

► **Задание 4: проверьте туннель**

1. На первом маршрутизаторе выполните команду ping с IP-адресом второго.
   Будет установлен туннель по требованию, и команда ping успешно выполнится.

Резюме

VPN обладает свойствами выделенной частной сети и позволяет передавать данные между двумя компьютерами через промежуточную сеть, например Интернет. На этом занятии мы рассказали о VPN в маршрутизируемых средах и Интернете.

Занятие 5 Поддержка многоканальных подключений

Многоканальные подключения, впервые реализованные в службе RAS Windows NT 4.0, позволяют объединять несколько физических соединений в один логический канал. Обычно объединяют две и более ISDN-линий или модемных подключений для расширения полосы пропускания.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о многоканальных подключениях.

Продолжительность занятия — около 10 минут.

Протокол PPP

Протокол Point-to-Point Protocol (PPP) разработан для передачи данных по телефонным линиям и выделенным соединениям «точка-точка». PPP инкапсулирует пакеты IP, IPX и NetBIOS в кадры PPP и передает их по каналу «точка-точка». Протокол PPP может использоваться маршрутизаторами, соединенными выделенным каналом, или клиентом и сервером RAS, соединенными удаленным подключением. Ниже описаны основные компоненты PPP:

- **инкапсуляция** — обеспечивает мультиплексирование нескольких транспортных протоколов по одному каналу;
- **протокол LCP** — **PPP** задает гибкий LCP для установки, настройки и проверки канала связи. LCP обеспечивает согласование формата инкапсуляции, размер пакета, параметры установки и разрыва соединения, а также параметры аутентификации. В качестве протоколов аутентификации могут использоваться PAP, CHAP, EAP и др.;
- **протоколы управления сетью** — предоставляют специфические конфигурационные параметры для соответствующих транспортных протоколов. Например, IPCP — это протокол управления IP.

Примечание Подробности OPPP см. в документах RFC 1661 «The Point-to-Point Protocol» и RFC 1990 «PPP Multilink».

Многоканальный PPP

Многоканальные подключения, впертые реализованные в службе RAS Windows NT 4.0, позволяют объединять несколько физических соединений в один логический канал. Обычно объединяют две и более ISDN-линии или модемных подключения для расширения полосы пропускания. Поддержка многоканальности стала возможной благодаря:

- **новому параметру LCP** — во время фазы LCP протокола PPP определяется, можно ли создать многоканальное подключение;
- **новому протоколу PPP** — он называется MP (Multilink PPP) и для PPP выглядит как стандартная полезная информация. MP изменяет последовательность и содержимое пакетов перед тем, как передать их транспортному протоколу, например TCP/IP.

MP инкапсулируется в кадры канального уровня PPP; в поле протокола указывается шестнадцатеричное значение 003D. Эта информация может оказаться полезной при просмотре журналов протокола PPP.

Резюме

Многоканальные подключения, впервые реализованные в службе RAS Windows NT 4.0, позволяют объединять несколько физических соединений в один логический канал. Обычно объединяют две и более ISDN-линии или модемных подключения для расширения полосы пропускания.

Занятие 6. Совместное использование служб RRAS и DHCP

Если пул адресов службы RRAS сконфигурирован для использования DHCP, клиентам RRAS не передается ни одного пакета DHCP. Сейчас мы расскажем, как служба RRAS взаимодействует со службой DHCP.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о службах RRAS и DHCP;
- ✓ установить агент ретрансляции DHCP.

Продолжительность занятия — около 10 минут.

Службы RRAS и DHCP

Если пул адресов службы RRAS сконфигурирован для работы DHCP, клиентам RRAS не передается ни одного пакета DHCP. RRAS использует службу DHCP для выделения адресов в блоках по 10 штук и сохраняет назначенные адреса в реестре. Если на сервере установлено два и более сетевых информационных центров (NIC), применяемых для выделения DHCP-адресов, клиент может настраивать эти NIC-центры. В предыдущих версиях Windows сервер RAS продлевал аренду выделенных адресов на неограниченно долгий срок. В Windows 2000 при выключении службы RRAS все выделенные DHCP-адреса освобождаются.

Число адресов, которое служба RRAS может одновременно выделять, определяется параметром реестра: *\System\CurrentControlSet\Services\RemoteAccess\Parameters\Ip\InitialAddressPoolSize*. Значение данного параметра — число адресов, резервируемых службой RRAS при запуске. Адреса хранятся в реестре и предоставляются клиентам RRAS. Если все адреса из начального пула уже выданы, резервируется другой блок из аналогичного количества адресов.

Агент ретрансляции DCHP

Теперь его можно применять совместно со службой RRAS. Клиент RRAS получает IP-адрес от сервера RRAS; тем не менее для получения адресов WINS- и DNS-серверов, имени домена и других параметров DHCP клиент вправе использовать пакеты DHCPINFORM. Сообщения DHCPINFORM возвращают дополнительные сведения без IP-адреса.

Примечание Передача имени домена с помощью сообщений DHCPINFORM особенно важна, поскольку протокол PPP задает имя домена.

Адреса WINS- и DNS-сервера, полученные с сообщениями DHCPINFORM, переопределяют адреса, назначенные сервером RRAS.

Практикум: настройка агента ретрансляции DCHP, работающего совместно с RRAS

► **Задание: настройте агент ретрансляции DCHP**

1. Откройте оснастку Routing and Remote Access. Щелкните узел IP Routing\General правой кнопкой мыши и выберите в контекстном меню команду New Routing Protocol.
2. Щелкните DCHP Relay Agent. Затем — кнопку OK.

3. Откройте **окно свойств агента** ретрансляции **DCHP.**
   Здесь **можно задать IP-адрес любого сервера DCHP.**
4. **Щелкните OK. чтобы закрыть это** диалоговое **окно.**
5. Щелкните правой **кнопкой** DCHP **Relay** Agent и выберите в **контекстном меню** команду New Interface.
6. **Щелкните** Internal, затем — OK.
7. Щелкните **OK. чтобы** закрыть **диалоговое окно свойств** агента ретрансляции DCHP.

Резюме

Если пул адресов службы **RRAS** настроен для **использования DHCP,** клиентам **RRAS не** передается ни **один пакет DHCP. Вы** узнали **о том, как служба RRAS взаимодействует со** службой и агентом **ретрансляции DHCP.**

Занятие 7. Управление и мониторинг удаленного доступа

В Windows 2000 имеются средства управления и мониторинга удаленного доступа. Сейчас мы расскажем о протоколировании аутентификации, учете событий, утилитах Netsh, Network Monitor и т. д.

Изучив материал этого занятия, вы сможете:

- ✓ рассказать о протоколировании аутентификации;
- ✓ создать профили;
- ✓ рассказать об утилите Netsh;
- ✓ описать назначение утилиты Network Monitor в службе RRAS;
- ✓ перечислить утилиты мониторинга удаленного доступа.

Продолжительность занятия — около 30 минут.

Протоколирование аутентификации пользователей и учетных запросов

Получая от серверов NAS запросы, служба IAS создает файлы журналов, собирая эти пакеты в одном месте. Настройка и использование таких журналов для контроля аутентификационной информации, например сведений о допуске, упрощает администрирование службы RRAS. Вы можете создать и использовать файлы журналов для регистрации учетной информации, например, сведений о времени входа и выхода из сети для оценки стоимости подключения (рис. 11-20).

При настройке протоколирования вы вправе указать:

- регистрируемые запросы;
- формат файла журнала;
- частоту создания новых файлов журнала;
- место **хранения файлов** журнала.

Кроме того, можно определить, какие из получаемых сервером IAS запросов следует регистрировать:

- запросы на учет событий, в том числе:
  - запросы на включение учета — посылаются сервером NAS и указывают, что он включен и способен принимать входящие соединения;
  - запросы на отключение учета — посылаются сервером NAS и указывают, что он отключается от сети;
  - запросы на начало учета — посылаются сервером NAS (после того как пользователь будет принят сервером IAS) и сообщают о начале сеанса работы пользователя;
  - запросы на останов учета — посылаются сервером NAS и сообщают о завершении сеанса работы пользователя;

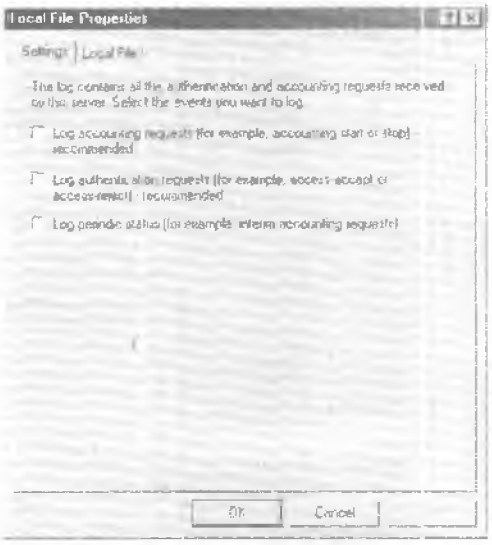


Рис. 11-20. Учет событий удаленного доступа

- запросы на аутентификацию, включая:
  - запросы на аутентификацию — посылаются сервером NAS от лица подключающегося пользователя. Соответствующие записи журнала содержат лишь входящие атрибуты;
  - сообщения о подтверждении и отказе в аутентификации — посылаются сервером IAS и указывают, следует ли принять или отклонить запрос подключения. Соответствующие записи журнала содержат лишь исходящие атрибуты;
  - сведения о состоянии, пересылаемые некоторыми NAS в течение сеанса работы;
  - периодические запросы на учет событий — пересылаются сервером NAS в течение сеанса работы пользователя (если атрибут acct-interim-interval профиля удаленного доступа сервера IAS настроен для поддержки периодических запросов).

  Мы рекомендуем регистрировать события обеих групп и, после того как вы определите, какие события вам требуются, исключить из групп ненужные элементы.

При настройке серверов можно указать периодичность создания нового файла журнала — ежедневно, еженедельно, ежемесячно или по достижении файлом определенного размера. Кроме того, можно настроить систему для ведения одного файла журнала независимо от его размера. Тем не менее это не рекомендуется. Соглашение об именовании файлов журнала зависит от периодичности их создания. Изменение параметров соглашения может привести к перезаписи старых файлов, и поэтому вам следует предварительно скопировать эти файлы в отдельный каталог. По умолчанию файлы журнала хранятся в папке %systemroot%\system32\LogFiles, однако вы можете выбрать и другую папку.

Записи файлов журнала

Атрибуты записываются в формате UTF-8 через запятые. Формат записей файлов журнала зависит от формата файла.

- в файлах формата IAS каждая запись содержит заголовок фиксированного формата, включающий IP-адрес сервера NAS, имя пользователя, время и дату записи, имя службы и имя компьютера, за которыми следуют пары значений-атрибутов;

- в файлах БД каждая запись содержит значения атрибутов в строгой последовательности, начиная с имени компьютера, имени службы, времени и даты записи. Некоторые серверы NAS могут использовать не все атрибуты, однако и в этом случае их расположение сохраняется путем разделения запятыми. Указываются даже места атрибутов, значения которых не определены.

Регистрация событий

Службу RRAS можно настроить для протоколирования информации в:

- локальных файлах журнала (при регистрации событий средствами Windows). Чтобы указать протоколируемые события и место хранения журналов, воспользуйтесь окном свойств папки Remote Access Logging в оснастке Routing and Remote Access;
- журналах сервера RADIUS (при регистрации событий средствами RADIUS). Если сервер RADIUS является также сервером IAS, файлы журнала хранятся на сервере IAS. Чтобы указать протоколируемые события и место хранения журналов, воспользуйтесь окном свойств папки Remote Access Logging в оснастке Internet Authentication Service.

Чтобы выбрать, как будет осуществляться регистрация событий службы RRAS, воспользуйтесь вкладкой Security диалогового окна свойств сервера удаленного доступа в оснастке Routing and Remote Access (рис. 11-21). Кроме того, можно применить утилиту командной строки Netsh.

Рис. 11-21. Служба учета удаленного доступа

Netsh

Служит для написания сценариев настройки и контроля сетевых компонентов Windows 2000. Netsh позволяет также сохранять сценарий конфигурации в текстовом файле для архивных целей или для конфигурирования других серверов.

Netsh поддерживает компоненты Windows 2000 при помощи вспомогательных DLL-файлов. Они расширяют функциональность Netsh, предоставляя дополнительные команды для просмотра или конфигурирования сетевого компонента Windows 2000. Каждый вспомогательный DLL-файл имеет свой контекст — набор команд для настройки сетевого

компонента. Внутри каждого контекста могут находиться подчиненные контексты. Например, внутри контекста маршрутизации находятся подчиненные контексты ip и ipx для группировки команд маршрутизаторов IP и IPX.

Для RRAS команда Netsh имеет контексты:

- ras — команды для конфигурирования удаленного доступа;
- aaaa — команды для конфигурирования компонента AAAA, используемого службами маршрутизации и удаленного доступа и проверки подлинности в Интернете; AAAA хранит параметры конфигурации сервера IAS;
- **routing** — команды для конфигурирования маршрутов IP и IPX;
- **interface** ~ команды для настройки интерфейса вызова по требованию.

Network Monitor

Позволяет выявлять и устранять проблемы ЛВС и ГВС. в том числе и RRAS-соединений. Средствами утилиты Network Monitor определяют модель трафика и выявляют проблемы в работе с сети. Например, вы можете обнаружить проблемы клиент-серверных соединений, найти компьютер, генерирующий слишком много рабочих запросов, перехватывать кадры (пакеты) непосредственно из сети, просматривать и фильтровать их, а также идентифицировать несанкционированных пользователей в сети. Подробнее об этом — в главе 4.

Утилиты из комплекта ресурсов

Ниже описываются утилиты, упрощающие управление и мониторинг службы RRAS.

Raslist.exe

Утилита RASLIST.EXE работает в режиме командной строки и отображает оповещения сервера RRAS, поступающие из сети. RASLIST.EXE прослушивает сеть на предмет оповещений, используя все активные сетевые интерфейсы компьютера, на котором она выполняется. Вывод утилиты показывает, какая именно плата получила оповещение. Raslist.exe — это утилита мониторинга. Появление данных иногда задерживается на несколько секунд; вывод информации будет осуществляться до завершения работы утилиты.

Rassrvmon.exe

Утилита RASSRVMON.EXE позволяет вести детальный мониторинг активности сервера удаленного доступа, включая:

- сведения о сервере — время первого обращения к серверу, время последнего обращения к серверу, число обращений, число байт, прошедших через сервер, общая продолжительность соединений, сведения о подключенных в настоящий момент пользователях и их соединениях;
- сведения о портах — время первого обращения к порту, время последнего обращения к порту, число обращений к порту с момента запуска сервера, число байт, прошедших через порт, число ошибок порта и сведения о текущем состоянии порта;
- общую информацию, например статистику для каждой пары «пользователь — компьютер», которая ведется с начала мониторинга — обшее время соединения, общее число переданных байт, число соединений, среднее время соединений, общее число ошибок;
- индивидуальную информацию, включая статистику по отдельным соединениям, — имя пользователя/имя компьютера, IP-адрес, время установления соединения, продолжительность соединения, число переданных байт, число ошибок, скорость передачи данных.

Для более гибкого мониторинга и контроля службы RRAS при срабатывании оповещений могут запускаться выбранные вами приложения. Это позволяет отсылать сообщения по электронной почте, на пейджер, по сети (net send) и предпринимать любые другие действия, которые можно реализовать средствами сценария или исполнимого файла.

Rasusers.exe

Позволяет получить список имен пользователей домена или сервера, имеющих разрешение на подключение к сети с использованием службы RRAS.

Traceenable.exe

Это утилита с графическим пользовательским интерфейсом, предназначенная для трассировки. Служба RRAS Windows 2000 обладает широкими возможностями трассировки, которые полезны для устранения сложных проблем в работе сети. При трассировке записываются внутренние переменные компонентов, вызовы функций и взаимодействия. Отдельные компоненты службы RRAS можно независимо сконфигурировать для записи результатов трассировки в файл (файловая трассировка). Для включения трассировки следует изменить параметры реестра Windows 2000 с помощью Traceenable.exe.

Использование Traceenable.exe

При выборе элемента трассировки для него отображаются значения. Внесите требуемые изменения и щелкните кнопку Set. Изменения будут записаны в реестр. Для регистрации работы компонента вам следует предварительно включить консольную трассировку и пометить флажок в верхней части окна Traceenable.exe. Например, чтобы создать файл журнала для протокола PPP:

1. выберите PPP из раскрывающегося списка;
2. щелкните Enable File Tracing;
3. **щелкните Set.**

Резюме

В Windows 2000 имеются средства управления и мониторинга удаленного доступа. Вы узнали о протоколировании аутентификации, учете событий, утилитах Netsh, Network Monitor и т. д.

Закрепление материала

9 | Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. *в* приложении «Вопросы и ответы» в конце книги.

1. Что такое виртуальная частная сеть?

2. На основе каких полей пакета фильтры доступа по требованию просматривают трафик?

3. Истина или ложь — при определении разрешений удаленного доступа (Allow Access. Deny Access) в окне свойств учетной записи пользователя политики удаленного доступа не используются.

4. Истина или ложь — пакеты DCHP никогда не пересылаются по каналам удаленного доступа.

5. Для чего предназначен протокол BAP?

ГЛАВА 12

Поддержка протокола NAT

В этой главе

Протокол трансляции сетевых адресов, Network Address Translation (NAT), позволяет сети с частными адресами обращаться к данным Интернета посредством трансляции протокола IP. В этой главе мы расскажем о настройке домашней сети или сети небольшого офиса для подключения к Интернету через единственное соединение с использованием NAT.

Прежде всего

Для изучения материалов этой главы необходимо:

- изучить материал главы 10.

Занятие 1. Знакомство с NAT

NAT позволяет преобразовывать для входящего и исходящего трафика Интернета частные IP-адреса в открытые JP-адреса Интернета. Это предотвращает передачу трафика непосредственно во внутреннюю сеть, одновременно снижая затраты времени и средств пользователя на получение и поддержку диапазона открытых адресов. На этом занятии вы познакомитесь с протоколом NAT.

Изучив материал этого занятия, вы сможете:

- ✓ описать назначение, компоненты и схему работы NAT.

Продолжительность занятия - около 45 минут.

Network Address Translation

Протокол Microsoft Windows 2000 NAT позволяет компьютерам небольшой сети совместно использовать одно соединение с Интернетом, имеющее только один IP-адрес. Компьютер, на котором установлен протокол NAT, может работать в качестве транслятора сетевых адресов, упрощенного сервера DHCP, прокси-сервера DNS и прокси-сервера WINS. Протокол NAT позволяет компьютерам разделять один или несколько зарегистрированных открытых IP-адресов, увеличивая пространство доступных для выделения открытых адресов.

Основы NAT

Протокол NAT в Windows 2000 позволит вам настроить домашнюю сеть или сеть небольшого офиса для совместного использования одного подключения к Интернету. Ниже перечислены составляющие NAT.

- **Компонент трансляции.** Маршрутизатор Windows 2000 с поддержкой NAT (далее — NAT-компьютер) выступает в качестве преобразователя сетевых адресов, транслирующего IP-адреса и номера портов пакетов TCP/UDP, передаваемых между частной сетью и Интернетом.
- **Компонент адресации.** NAT-компьютер передает другим компьютерам домашней сети сведения о конфигурации IP-адреса. Компонент адресации — это упрощенный сервер DHCP, выделяющий IP-адрес, маску подсети, шлюз по умолчанию и IP-адрес DNS-сервера. Для автоматического получения конфигурационных сведений IP-адреса компьютеры домашней сети следует настроить в качестве клиентов DHCP. По умолчанию компьютеры с Windows 2000, Windows NT, Windows 95 и Windows 98 являются клиентами DHCP.
- **Компонент разрешения имен.** NAT-компьютер становится для остальных компьютеров домашней сети DNS-сервером. При получении запросов на разрешение имен NAT-компьютер передает их находящемуся в Интернете DNS-серверу, для работы с которым он сконфигурирован, и возвращает ответ компьютеру домашней сети.

Маршрутизируемые и транслируемые соединения с Интернетом

Существует два вида подключения к Интернету: маршрутизируемое и транслируемое. При планировании маршрутизируемого соединения вам надо получить у своего поставщика услуг Интернета диапазон IP-адресов, который будет использоваться во внутренней части нашей сети; кроме того, поставщик даст вам IP-адрес DNS-сервера, который вы и будете

применять. Вы можете назначить компьютерам статические IP-адреса или воспользоваться DHCP-сервером.

Маршрутизатор Windows 2000 следует настроить на работу с сетевым адаптером внутренней сети (например, 10BaseT или 100BaseT Ethernet). Кроме того, для маршрутизатора необходимо создать подключение к Интернету, например, аналоговый или ISDN-модем, xDSL-модем, кабельный модем.

Транслируемый доступ (с использованием NAT) значительно безопаснее, поскольку адреса частной сети полностью скрываются от Интернета. NAT-компьютер, разделяемый соединением, преобразует все адреса Интернета в адреса частной сети и наоборот. Не забывайте, однако, что NAT-компьютер не способен транслировать всю полезную информацию. Это связано с тем, что некоторые приложения используют IP-адреса в других полях, помимо стандартных полей заголовка TCP/IP.

С NAT не работают следующие протоколы:

- Kerberos;
- IP Security Protocol (IPSec).

Поддержка протоколом NAT выделения адресов DHCP-сервером позволяет всем DHCP-клиентам в сети автоматически получить от NAT-компьютера IP-адрес, маску подсети, шлюз по умолчанию и адрес DNS-сервера. Если в сети имеются компьютеры без поддержки DHCP, настройте для них статические IP-адреса.

Для минимизации затрат на ресурсы в небольшой сети достаточно установить лишь один сервер с Windows 2000. В зависимости от типа соединения (транслируемое или маршрутизируемое) этот сервер может выполнять службы NAT, APIPA, Routing And Remote Access и DHCP.

Общие и частные адреса

Если ваша интрасеть не подключена к Интернету, вы вправе внедрить любую схему IP-адресации. Если вам требуется прямое (через маршрутизатор) или косвенное (через прокси-сервер или транслятор) соединение с Интернетом, стоит использовать общие и частные адреса.

Общие адреса

Общие адреса присваиваются центром InterNIC и состоят из сетевых идентификаторов, которые основаны на классах, или блоков адресов, которые основаны на протоколе Classless Inter-Domain Routing (CIDR-блоки) и гарантированно являются глобально уникальными в Интернете. Если назначаются общие адреса, в Интернет-маршрутизаторы заносятся маршруты, чтобы трафик к общим адресам достигал конечной точки. Интернет-трафик к конечным общим адресам достигает своего места назначения.

Частные адреса

Каждому IP-узлу требуется IP-адрес, являющийся в данной IP-сети уникальным. В случае с Интернетом каждому IP-узлу сети, подключенной к Интернету, необходим IP-адрес, являющийся в Интернете глобально уникальным. С развитием Интернета подключающимся к нему организациям требовалось все больше общих адресов — для каждого из узлов их интрасетей. Это привело к тому, что диапазон доступных общих адресов значительно сократился.

Анализируя потребности организаций в адресах, разработчики Интернета заметили, что во многих организациях большинство узлов интрасети не нуждалось в прямом соединении с узлами Интернета. Те узлы, которым действительно требовался определенный

набор служб Интернета, например, доступ к World Wide Web и электронной почте, обычно работали с этими службами через шлюзы прикладного уровня вроде прокси-серверов и серверов электронной почты. В результате оказалось, что большей части организаций необходимо лишь небольшое число общих адресов для узлов, непосредственно подключенных к Интернету (прокси-серверы, маршрутизаторы, брандмауэры, трансляторы и др.).

Компьютерам внутри организации, не нуждающимся в прямом доступе к Интернету, необходимы IP-адреса, отличные от уже присвоенных общих адресов. Для решения этой проблемы разработчики Интернета зарезервировали часть пространства IP-адресов и назвали это пространство пространством частных адресов. Частные IP-адреса никогда не присваиваются в качестве общих. Поскольку пространства частных и общих адресов не пересекаются, частные адреса никогда не дублируют общие адреса. RFC 1918 определяет следующие диапазоны IP-адресов:

- **10.0.0.0—10.255.255.255** — частная сеть с IP-адресом 10.0.0.0 — сетевой идентификатор класса A, допускающий использование действительных IP-адресов из диапазона 10.0.0.1—10.255.255.254. У частной сети 10.0.0.0 имеется 24 разряда для обозначения узла, которые можно использовать для внедрения в организации любой схемы подсетей;
- **172.16.0.0—172.31.255.255** — частная сеть с адресом 172.16.0.0 интерпретируется как блок из 16 сетевых идентификаторов класса B или как 20-разрядное присваиваемое пространство адресов (20 разрядов для обозначения узла), которое можно использовать для внедрения в организации любой схемы подсетей. Частная сеть 172.16.0.0 допускает использование действительных IP-адресов из диапазона 172.16.0.1—172.31.255.254;
- **192.168.0.0—192.168.255.255** - частная сеть 192.168.0.0/16 интерпретируется как блок из 256 сетевых идентификаторов класса C или как 16-разрядное присваиваемое пространство адресов (16 разрядов для обозначения узла), которое можно использовать для внедрения в организации любой схемы подсетей. Частная сеть 192.168.0.0 допускает использование действительных IP-адресов из диапазона 192.168.0.1—192.168.255.254.

Обращаться к частным адресам из Интернета нельзя. Следовательно, компьютер с частным адресом должен посылать свой Интернет-трафик шлюзу прикладного уровня (например, прокси-серверу), обладающему действительным общим адресом, или использовать транслятор, который будет перед пересылкой графика в Интернет преобразовывать частный адрес этого компьютера в действительный общий адрес.

Принципы работы NAT

Транслятор сетевых адресов — определенный в стандарте RFC 1631 IP-маршрутизатор, способный в процессе передачи пакетов транслировать их IP-адреса и номера портов TCP/UDP. Рассмотрим небольшую сеть из нескольких компьютеров, подключающихся к Интернету. В обычной ситуации компании потребовалось бы получить у поставщика услуг Интернета для каждого из этих компьютеров общий IP-адрес. Протокол NAT позволяет реализовать в сети компании схему частной адресации (см. RFC 1597) и привязать частные адреса компьютеров к одному или нескольким общим IP-адресам, полученным у поставщика услуг Интернета. Например, интрасеть небольшой компании реализована как частная сеть с адресом 10.0.0.0, и поставщик услуг Интернета выделил фирме общий IP-адрес 198.200.200.1. NAT привязывает (статически или динамически) все используемые в сети 10.0.0.0 частные IP-адреса к общему IP-адресу 198.200.200.1.

Статическая и динамическая привязка адресов

Протокол NAT использует статическую или динамическую привязку адресов. При статической привязке трафик всегда направляется в определенное место. Весь входящий и ис-

ходящий трафик определенного сегмента частной сети можно привязать к определенному месту в Интернете. Например, чтобы установить Web-сервер на одном из компьютеров частной сети, вы создаете статическую привязку общего IP-адреса (порт номер 80 протокола TCP) к частному IP-адресу (порт номер 80 протокола TCP).

Динамические привязки создаются, если пользователи частной сети обмениваются информацией с узлами Интернета. Служба NAT автоматически добавляет эти привязки в свою таблицу привязок и обновляет их при каждом обращении. Не применяемые динамические привязки по истечении определенного времени удаляются из таблицы привязок проекций NAT после заданного периода времени. Тайм-аут привязки для TCP-подключений по умолчанию составляет 24 часа. Для трафика UDP тайм-аут равняется 1 минуте.

Корректное преобразование полей заголовков

По умолчанию NAT преобразовывает IP-адреса и порты TCP/UDP. При этом в IP-дейтаграмму вносятся определенные изменения, которые требуют модификации и корректировки следующих полей заголовков IP, TCP и UDP:

- исходного IP-адреса;
- контрольной суммы TCP, UDP и IP;
- исходного порта.

Если информация об IP-адресах и портах содержится только в заголовках IP и TCP/UDP, как, например, в протоколе HTTP или трафике WWW, прикладной протокол может транслироваться прозрачно. Впрочем, некоторые приложения и протоколы записывают информацию об IP-адресах и портах в собственные заголовки. Например, протокол FTP хранит в заголовке FTP для команды порта FTP десятичную нотацию IP-адреса. При некорректном преобразовании адреса протоколом NAT иногда возникают проблемы связи. Кроме того, в случае с FTP IP-адрес хранится в десятичной нотации, и поэтому преобразованный IP-адрес в заголовке FTP может иметь иной размер. В связи с этим во избежание потери данных служба NAT должна также изменять порядковые номера TCP.

Редакторы NAT

Они необходимы, если компоненту NAT требуется дополнительно преобразовывать и распределять полезную информацию вне заголовков IP, TCP и UDP. Редактор NAT — устанавливаемый компонент, позволяющий корректно транслировать полезную информацию, которую нельзя преобразовать каким-либо другим образом, для пересылки через NAT. В Windows 2000 встроены редакторы NAT для следующих протоколов:

- FTP;
- ICMP;
- PPTP;
- NetBIOS поверх TCP/IP.

Кроме того, протокол маршрутизации NAT включает программное обеспечение прокси-сервера для следующих протоколов:

- H.323;
- Direct Play;
- LDAP (регистрация ILS на основе LDAP);
- RPC.

Примечание Преобразование трафика IPSec невозможно.

Пример использования NAT

Предположим, что небольшая фирма применяет для своей частной интрасети сетевой идентификатор 192.168.0.0 и получила от поставщика услуг Интернета общий адрес w1.x1.y1.z1. В этом случае служба NAT привяжет все частные адреса 192.168.0.0 к IP-адресу w1.x1.y1.z1. Если к одному общему адресу привязано несколько частных адресов, для различения узлов интрасети NAT использует динамически выбираемые порты TCP и UDP. На рис. 12-1 показано прозрачное подключение интрасети к Интернету с использованием NAT.

Примечание Адреса w1.x1.y1.z1 и w2.x2.y2.z2 в данном примере — действительные общие IP-адреса, назначенные центром InterNIC или поставщиком услуг Интернета.

NAT-процессы службы RRAS в Windows 2000

Чтобы активизировать компонент NAT для службы Windows 2000 Routing and Remote Access, воспользуйтесь одноименной оснасткой и добавьте NAT в качестве протокола маршрутизации.

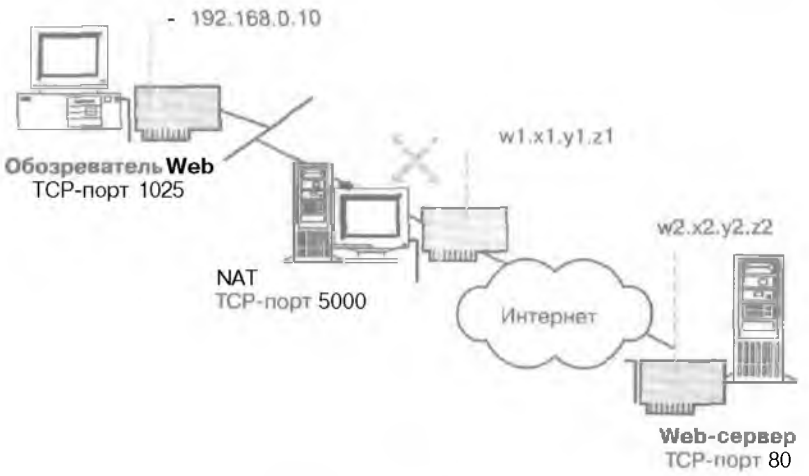


Рис. 12-1. Прозрачное подключение интрасети к Интернету с использованием NAT

Примечание Службы NAT также применяются при совместном использовании подключения к Интернету (см. занятие 2). Совместное использование подключений к Интернету работает аналогично протоколу маршрутизации NAT из оснастки Routing and Remote Access (Маршрутизация и удаленный доступ), но допускает очень маленькую гибкость конфигурации. Подробности о настройке совместного использования подключений к Интернету и применении NAT см. в справочной системе Windows 2000 Server.

Вместе с протоколом маршрутизации NAT устанавливаются несколько редакторов NAT. Если полезная информация преобразовываемого пакета соответствует спецификациям одного из установленных редакторов, NAT запускает его. Редактор модифицирует полезную информацию и возвращает результат компоненту NAT. NAT взаимодействует с протоколом TCP/IP двумя способами;

- для поддержки динамической привязки портов компонент NAT по мере необходимости запрашивает из стека протоколов TCP/IP уникальные номера портов TCP и UDP;

- через компонент TCP/IP; при этом пакеты, передаваемые между частной сетью и Интернетом, сначала передаются компоненту NAT для преобразования.

На рис. 12-2 показаны компоненты NAT и их связь с TCP/IP и прочими компонентами маршрутизатора.

Рис. 12-2. Компоненты NAT

Исходящий трафик Интернета

При выводе исходящего трафика частной сети через интерфейс Интернета NAT сначала определяет, существует ли для пакета статическая или динамическая привязка адреса/порта. Если таковая отсутствует, создается динамическая привязка. NAT создает проекцию в зависимости от числа доступных общих IP-адресов.

- Если доступен один общий IP-адрес, NAT запрашивает для него новый уникальный порт TCP или UDP и использует этот порт в качестве привязанного порта.
- При наличии нескольких общих IP-адресов NAT привязывает частный IP-адрес к общему IP-адресу. Для таких привязок номера портов не преобразовываются. Если из всех IP-адресов свободным останется только один адрес, NAT переключится на привязку портов и адресов, как в случае с единственным общим IP-адресом.

После привязки NAT обращается к редакторам и при необходимости запускает один из них. Завершив редактирование, NAT изменяет заголовки IP и TCP или UDP и передает пакет, используя интерфейс Интернета. Процесс обработки исходящего трафика Интернета компонентом NAT проиллюстрирован на рис. 12-3.

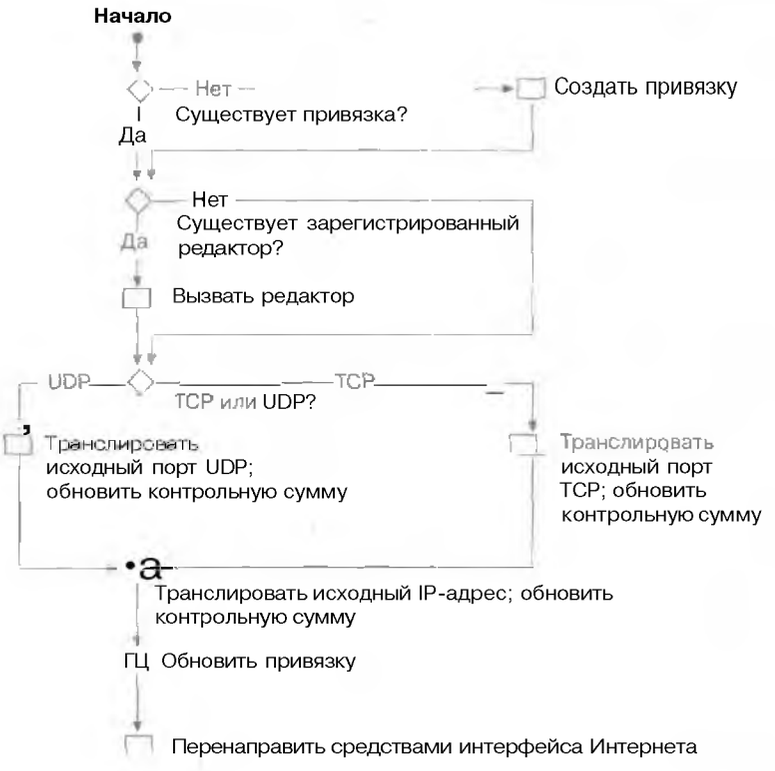


Рис. 12-3. Обработка исходящего трафика **Интернета компонентом NAT**

Входящий трафик Интернета

При поступлении входящего трафика частной сети через интерфейс Интернета NAT сначала определяет, существует ли для пакета статическая или динамическая проекция адреса/порта. При отсутствии проекции NAT отбрасывает пакет.

Это позволяет защитить частную сеть от злоумышленников из Интернета. Возможны только два случая передачи трафика Интернета в частную сеть — в ответ на трафик, который инициировал пользователь частной сети, создавший динамическую привязку, или при наличии статических привязок, позволяющих пользователям Интернета обращаться к определенным ресурсам частной сети.

После привязки NAT обращается к редакторам и при необходимости запускает один из них. Завершив редактирование, NAT изменяет заголовки IP и TCP или UDP и передает пакет, используя интерфейс Интернета. Процесс обработки входящего трафика Интернета компонентом NAT проиллюстрирован на рис. 12-4.

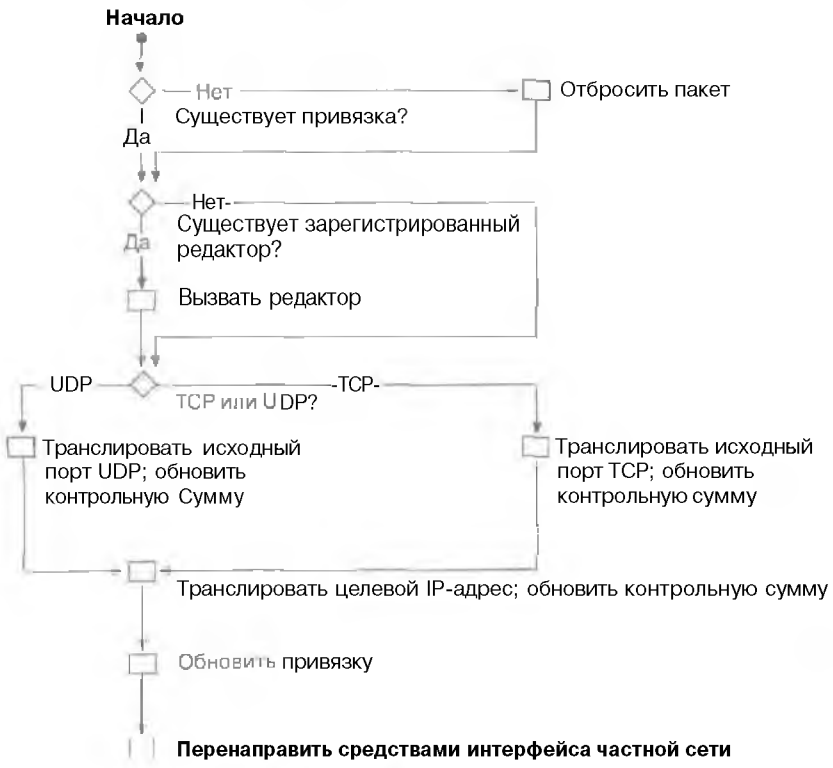


Рис. 12-4. Обработка входящего трафика Интернета компонентом NAT

Дополнительные компоненты протокола маршрутизации NAT

Для упрощения настройки небольших сетей, подключающихся к Интернету, протокол маршрутизации NAT в Windows 2000 также дополнен распределителем DHCP и прокси-сервером DNS.

Распределитель DHCP

Предоставляет информацию о конфигурации IP-адресов остальным компьютерам сети. Распределитель DHCP — это упрощенный DHCP-сервер, выделяющий IP-адрес, маску подсети, шлюз по умолчанию и IP-адрес DNS-сервера. Для автоматического получения конфигурационной информации IP-адреса компьютеры сети DHCP следует настроить в качестве DHCP-клиентов. Параметры TCP/IP по умолчанию TCP/IP компьютеров с управлением Windows 2000, Windows NT, Windows 95 и Windows 98 заданы таким образом, что система является клиентом DHCP.

В табл. 12-1 перечислены параметры DHCP, передаваемые распределителем DHCP в сообщениях DHCPOFFER и DHCPACK в процессе настройки аренды IP-адреса. Изменять эти или настраивать дополнительные параметры DHCP нельзя.

Табл. 12-1. Параметры настройки аренды IP-адреса

Номер параметра	Значение параметра	Описание
1	255.255.0.0	Маска подсети
3	IP-адрес частного интерфейса	Маршрутизатор (шлюз по умолчанию)
6	IP-адрес частного интерфейса	DNS-сервер (назначается только в случае, если активизирован прокси-сервер DNS)
58 (0x3A)	5 минут	Интервал обновления
59 (0x3B)	5 дней	Интервал повторной привязки
51	7 дней	Время аренды IP-адреса
15 (0x0F)	Основное доменное имя NAT-компьютера	DNS-домен

Распределитель DHCP поддерживает единственную область IP-адресов, определяемую в оснастке Routing And Remote Access в окне свойств протокола NAT на вкладке Address Assignment (Назначение адресов). Распределитель не поддерживает работу с несколькими областями, суперобластями и многоадресными областями. Если же вам необходимо работать с такими областями и нужна эта функция, установите DHCP-сервер и отключите компонент — распределитель DHCP протокола маршрутизации NAT.

Прокси-сервер DNS

Выступает для компьютеров сети в качестве DNS-сервера. DNS-запросы, посылаемые компьютером NAT-серверу, передаются DNS-серверу. DNS-сервер передает ответы на запросы NAT-серверу, и тот пересылает их компьютеру сети.

Резюме

NAT преобразует частные IP-адреса в общие IP-адреса для входящего и исходящего трафика Интернета. Это позволяет обезопасить внутреннюю сеть от атак из Интернета и снизить затраты на получение и поддержку диапазона общих адресов. В обычной ситуации компании потребовалось бы получить у поставщика услуг Интернета для каждого из этих компьютеров общий IP-адрес. Протокол NAT позволяет реализовать во внутренней сети схему частной адресации и привязать частные адреса компьютеров к одному или нескольким общим IP-адресам, полученным у поставщика услуг Интернета.

Занятие 2. Установка Internet Connection Sharing

Функция совместного использования подключения к Интернету — Internet Connection Sharing (ICS) доступна к папке Network and Dial-Up Connections и позволяет подключать вашу домашнюю сеть или небольшую офисную сеть к Интернету, например сеть, подсоединенную к Интернету через удаленное подключение. На этом занятии рассказывается об установке ICS и Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ включить функцию ICS в Windows 2000;
- ✓ настроить параметры Интернета для совместного использования подключений.

Продолжительность занятия — около 35 минут.

ICS

ICS включает службы DHCP, NAT и DNS. Средствами ICS легко и просто подключить сеть к Интернету. Поскольку ICS обеспечивает транслируемое соединение, все компьютеры сети могут работать с ресурсами Интернета, например, с электронной почтой, Web- и FTP-узлами. 1CS обеспечивает;

- простоту конфигурации;
- единственный общий **IP-адрес;**
- фиксированный диапазон адресов для компьютеров:
- прокси-сервер DNS для разрешения имен;
- автоматическую IP-адресацию.

ICS предоставляет гораздо больше возможностей, чем просто преобразование адресов, Microsoft добавила и Windows 2000 много возможностей, упрощающих настройку подключения к Интернету. Администрирование и настройка ICS осуществляются из оснастки Routing And Remote Access. Для настройки простой домашней сети можно также запустить мастер. Мастер не позволяет изменять какие-либо параметры, но поможет вам подключить домашнюю сеть к Интернету в считанные минуты. Автоматическая адресация и автоматическое разрешение имен средствами распределителя DHCP, прокси-сервера DNS и прокси-сервера WINS значительно облегчают настройку. Эти компоненты представляют собой упрошенные версии серверов DHCP, DNS и WINS.

Включив ICS на компьютере, использующем удаленное соединение, вы предоставляете всем компьютерам домашней сети службы адресации, разрешения имен и NAT. После того как вы включите ICS, пользователи сети, проверив свои параметры, смогут работать с Microsoft Internet Explorer, Microsoft Outlook Express и другими приложениями так, как если бы их компьютеры были напрямую подключены к поставщику услуг Интернета. ICS-компьютер дозванивается до поставщика услуг Интернета и устанавливает соединение, чтобы клиент мог обратиться к требуемому Web-адресу или ресурсу. Для совместного использования подключения к Интернету всем клиентам сети следует настроить свой компьютеры для автоматического получения IP-адресов.

Включение ICS

При включении ICS надо соблюдать несколько правил.

- ICS не рекомендуется использовать в сети, где имеются другие контроллеры домена Windows 2000 Server, серверы DNS, шлюзы, серверы DHCP и компьютеры со статичным IP-адресом.

- После включения **ICS** сетевому адаптеру, подсоединенному к сети, присваивается новый IP-адрес. Существующие TCP/IP-соединения компьютера с ICS разрываются, и их необходимо восстанавливать.
- Для совместного использования подключения к Интернету клиентам следует настроить свои компьютеры для автоматического получения IP-адресов.
- Если ICS-компьютер подключен к Интернету через ISDN или модем, пометьте флажок Enable On-Demand Dialing (Разрешить вызов по требованию).

▶ **Настройка ICS для сетевого подключения**

1. Раскройте меню Start\Settings\Network And Dial-Up Connections (Пуск\Настройка\Сеть и удаленный доступ к сети).
2. Правой кнопкой мыши щелкните значок удаленного подключения, подключения к VPN или входящего подключения, которое требуется совместно использовать, и в контекстном меню выберите команду Properties.
3. На вкладке Sharing (Общий доступ) пометьте флажок Enable Internet Connection Sharing For This Connection (Разрешить общий доступ для этого подключения).
4. Если требуется, чтобы при попытке любого из компьютеров сети обратиться к внешним ресурсам связь всегда устанавливалась с использованием этого соединения, пометьте флажок Enable On-Demand Dialing (Разрешить вызов по требованию).

Установка ICS

Для настройки функции ICS используется оснастка Routing And Remote Access.

▶ **Установки разделения соединения**

1. В оснастке Routing And Remote Access откройте папку IP Routing (IP-маршрутизация) и щелкните правой кнопкой значок General (Общие).
2. В контекстном меню выберите команду New Routing Protocol (Новый протокол маршрутизации) (рис. 12-5).
3. В открывшемся окне выберите протокол NAT.

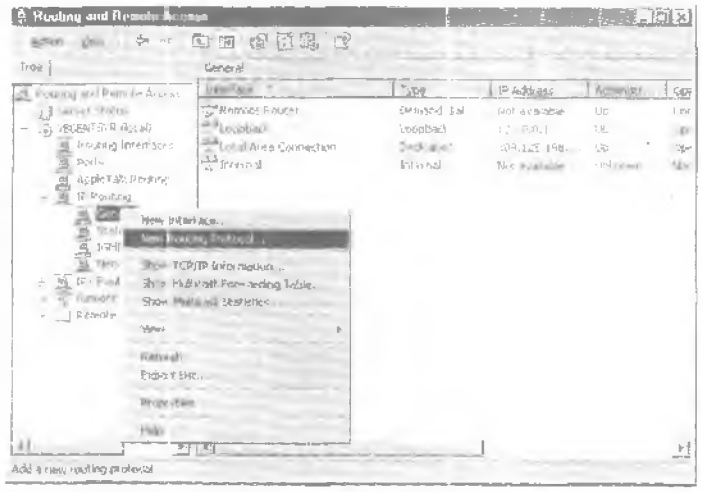


Рис. 12-5. Добавление протокола маршрутизации в оснастке Routing And Remote Access

Настройка параметров Интернета для ICS

Если вы ранее не подключались к Интернету, выполните следующие действия.

▶ **Установка соединения с Интернетом**

1. Запустите Internet Explorer.
2. В окне мастера подключения к Интернету щелкните переключатель I Want To Set Up My Internet Connection Manually Or ! Want To Connect Through A Local Area Network (Настроить соединение е Интернетом вручную или подключиться к Интернету через локальную сеть), затем щелкните Next.
3. Щелкните переключатель I Connect Through A Local Area Network (Я подключаюсь к Интернету через локальную сеть), затем — Next.
4. Сбросьте флажок Automatic Discovery Of Proxy Server (Автоматическое определение прокси-сервера) и щелкните Next.
5. Если вы хотите настроить учетную запись почты и знаете все требуемые сведения, щелкните переключатель Yes и введите запрашиваемую информацию. В противном случае щелкните No, а затем — кнопки Next и Finish (Готово).

Если вы уже настроили подключение к Интернету, вам будет предложено выполнить следующие действия.

▶ **Настройка параметров Интернета для ICS**

1. В меню Tools (Сервис) выберите команду Internet Options (Свойства обозревателя).
2. На вкладке Connections (Подключение) щелкните переключатель Never Dial A Connection (Не использовать), затем щелкните кнопку LAN Settings (Настройка сети).
3. В окне Automatic Configuration (Настройка локальной сети) сбросьте флажки Automatically Detect Settings (Автоматическое определение настроек) и Use Automatic Configuration Script (Использовать сценарий автоматической настройки).
4. Сбросьте флажок Use A Proxy Server (Использовать прокси-сервер).

ICS и NAT

Для подключения домашней сети или сети небольшого офиса к Интернету можно использовать маршрутизируемое или транслируемое соединение. При маршрутизируемом соединении компьютер с Windows 2000 Server выступает в качестве IP-маршрутизатора, передающего пакеты между внутренней сетью и Интернетом. Хотя маршрутизируемое соединение достаточно простое, его настройка требует знаний в области IP-адресации и маршрутизации. Однако маршрутизируемые соединения позволяют передавать между внутренними компьютерами сети и Интернетом любой трафик.

При транслируемом соединении компьютер с Windows 2000 Server выступает в качестве преобразователя сетевых адресов. Для транслируемых соединений, использующих компьютеры под управлением Windows 2000 Server, требуется меньше знаний в области IP-адресации и маршрутизации и проще настройка компьютеров и маршрутизатора Windows 2000. Тем не менее транслируемые соединения могут не пропускать определенный IP-трафик между узлами небольшой сети и узлами Интернета.

Для создания транслируемого соединения в Windows 2000 Server можно воспользоваться функцией ICS, доступной в папке Network And Dial-Up Connections, либо протоколом маршрутизации NAT, входящим в состав службы Routing And Remote Access. И ICS, и NAT предоставляют компьютерам сети службы преобразования, адресации и разрешения имен.

Как мы уже говорили ранее, цель ICS — упростить создание на компьютерах с Windows 2000 транслированного соединения с Интернетом для всех узлов сети. Тем не менее после включения ICS нельзя настраивать, за исключением приложений и сервисов. Например,

ICS может работать только с одним IP-адресом, получаемым у поставщика услуг Интернета, и не позволит вам изменять диапазон IP-адресов, выделенных компьютерам.

На занятии 1 вы узнали, что протокол маршрутизации NAT разработан с целью обеспечить максимальную гибкость в настройке компьютера с Windows 2000 Server для создания транслируемого соединения с Интернетом. NAT требует дополнительной конфигурации; тем не менее каждый из дополнительных этапов является настраиваемым. Протокол NAT работает с диапазоном IP-адресов, полученных у поставщика услуг Интернета, и допускает изменение диапазона IP-адресов, назначенных узлам.

В табл. 12-2 перечислены возможности и особенности ICS и NAT.

Табл. 12-2. Возможности ICS и NAT

ICS	NAT
Настройка одним флажком	Настройка вручную
Единственный общий IP-адрес	Несколько общих IP-адресов
Фиксированный диапазон адресов для внутренних узлов	Настраиваемый диапазон адресов для внутренних узлов
Единственный внутренний интерфейс	Несколько внутренних интерфейсов

Назначение служб ICS и NAT в Windows 2000 Server — подключение небольших сетей к Интернету. ICS и NAT не предназначены для:

- прямого соединения отдельных частных сетей;
- соединения сетей, составляющих интрасеть;
- прямого подключения сетей филиалов организации к корпоративной сети;
- подключения сетей филиалов организации к корпоративной сети через Интернет.

Предотвращение неполадок NAT

Для предотвращения неполадок при совместном использовании подключений (NAT) решите некоторые вопросы.

- **Все ли интерфейсы (общие и частные) добавлены к протоколу маршрутизации Connection Sharing (NAT)?**

  Для протокола маршрутизации NAT следует добавить как общие (Интернет), так и частные (небольшой офис или домашняя сеть) интерфейсы.

- Включена **ли поддержка преобразования на интерфейсе Интернета (внешнем интерфейсе)?**

  Убедитесь, что интерфейс маршрутизатора Windows, соединяющего сеть с Интернетом, настроен для поддержки преобразования. Для этого в окне свойств интерфейса Интернета на вкладке General (Общие) пометьте флажок Enable Translation Across This Interface.

- **Включена ли поддержка Connection Sharing на частном (внутреннем) интерфейсе?**

  Убедитесь, что интерфейс маршрутизатора Windows, соединяющего сеть с Интернетом, настроен для поддержки Connection Sharing. Для этого в окне свойств домашней сети на вкладке General (Общие) пометьте флажок Allow Clients On This Interface To Access Any Shared Networks.

- **Включено ли преобразование портов TCP/IP?**

  Если у вас имеется лишь один общий IP-адрес, убедитесь, что в окне свойств внешнего интерфейса на вкладке General (Общие) помечен флажок Translate TCP/UDP Headers (Преобразовать TCP/UDP-заголовки).

- **Верно ли задан диапазон общих адресов?**

  При наличии нескольких общих IP-адресов убедитесь, что они правильно указаны в окне свойств внутреннего интерфейса на вкладке Address Pool (Пул адресов). Если ваш диапазон адресов включает IP-адрес, который не был выделен вам вашим поставщиком услуг Интернета, привязанный к этому адресу входящий Интернет-трафик может пересылаться поставщиком в другое место.

- **Является ли используемый программой протокол транслируемым?**

  При наличии приложений, которые, по всей видимости, не поддерживают NAT, можно попробовать запустить их с NAT-компьютера. Если программы работают с NAT-компьютера и не работают при запуске с компьютера частной сети, преобразование полезной информации приложения невозможно. Стоит проверить, входит ли используемый приложением протокол в список протоколов, поддерживаемых редакторами NAT.

- **Включена ли адресация Connection Sharing в домашней сети?**

  Если в частной сети не заданы статические адреса, убедитесь, что на интерфейсах, соответствующих этой сети, включена адресация Connection Sharing. Для этого в окне свойств объекта совместного использования подключения на вкладке Addressing щелкните кнопку Interfaces.

Резюме

Internet Connection Sharing — это возможность, доступная в папке Network and Dial-Up Connections и позволяющая подключать вашу домашнюю сети или небольшую офисную сеть к Интернету. Администрирование и настройку ICS можно осуществлять из оснастки Routing And Remote Access Manager. Включив ICS на компьютере, использующем удаленное соединение, вы предоставляете всем компьютерам домашней сети службы адресации, разрешения имен и NAT.

Занятие 3. Установка и настройка NAT

Основное назначение NAT — сохранение уменьшающегося пространства IP-адресов. Преимущество NAT — возможность создать сетевые подключения без знаний в области IP-маршрутизации и протоколов IP-маршрутизации. NAT можно использовать без специальных знаний или без взаимодействия с поставщиком услуг Интернета. Обращаться к поставщику по каким-либо вопросам, за исключением добавления статических маршрутов, не надо. На этом занятии рассказывается об установке и настройке NAT.

Изучив материал этого занятия, вы сможете:

- ✓ описать некоторые особенности проектирования, которые необходимо учитывать при реализации NAT;
- ✓ включить адресацию NAT;
- ✓ настроить диапазон IP-адресов и специальные порты интерфейса;
- ✓ настроить сетевые приложения NAT.

Продолжительность занятия — около 20 минут.

Особенности **проектирования NAT**

NAT используется в основном для подключения небольших сетей к Интернету. Во избежание проблем при внедрении NAT следует учесть несколько особенностей. Например, при использовании NAT частные адреса используются во внутренней сети обычным порядком. Как уже говорилось на занятии 1, частные адреса предназначены для внутренних сетей, то есть для сетей, не подключенных к Интернету напрямую. Такие адреса рекомендуется использовать вместо произвольно выбираемых IP-адресов, чтобы предотвратить возможное дублирование последних. Кроме того, вместо NAT рекомендуется применять маршрутизацию, поскольку это быстрый и эффективный способ и протокол IP разрабатывался с поддержкой маршрутизации. Тем не менее для внедрения маршрутизации требуются специальные знания и действительные IP-адреса.

Проблемы IP-адресации

Рекомендуется использовать следующие IP-адреса из диапазона идентификаторов частных сетей, определенного центром InterNIC: 10.0.0.0 с маской подсети 255.0.0.0, 172.16.0.0 с маской подсети 255.240.0.0 и 192.168.0.0 с маской подсети 255.255.0.0. По умолчанию NAT применяет для частной сети идентификатор частной сети 192.168.0.0 с маской подсети 255.255.255.0.

Если вы работаете с общими IP-сетями, адреса которых не были выделены центром InterNIC или вашим поставщиком услуг Интернета, то, возможно, используете идентификатор IP-сети, выделенный другой организацией Интернета. Это называется нелегальной или перекрывающейся IP-адресацией. При применении перекрывающихся общих IP-адресов вы не сможете обратиться к ресурсам Интернета, адреса которых соответствуют адресам вашей сети. Например, если у вас действует адрес 1.0.0.0 с маской подсети 255.0.0.0, нам не удастся обратиться к Интернет-ресурсам организации, использующей сеть 1.0.0.0. Кроме того, из заданного диапазона можно исключить определенные IP-адреса; они не будут выделяться узлам частной сети.

▶ **Настройка сервера NAT**

1. Установите и активизируйте службу Routing and Remote Access.

В мастере установки сервера маршрутизации укажите, что нам требуются служба ICS и маршрутизатор с протоколом маршрутизации NAT. По окончании работы мастера процесс настройки NAT будет завершен. В этом случае пункты 2 — 8 выполнять не требуется. В случае если служба Routing and Remote Access уже запущена, вам придется выполнить пункты 2 — 8.

2. Настройте IP-адрес интерфейса домашней сети.
3. Для IP-адреса ЛВС-адаптера, подключенного к домашней сети, потребуется указать:
   - IP-адрес 192.168.0.1;
   - маску подсети 255.255.255.0;
   - отсутствие шлюза по умолчанию.

Примечание Приведенный выше IP-адрес интерфейса домашней сети основан на определенном для компонента адресации NAT диапазоне адресов по умолчанию 192.168.0.0 с маской подсети 255.255.255.0. Если вы измените назначенный диапазон адресов по умолчанию, вам потребуется изменить IP-адрес частного интерфейса для NAT-компьютера так, чтобы он стал первым адресом в заданном диапазоне. Это — наша рекомендация, а не обязательное требование компонентов NAT.

---

4. Настройте маршрутизацию на порте удаленного доступа.

   При наличии постоянного подключения к Интернету, которое отображается в Windows 2000 как ЛВС-интерфейс (например, DDS, T-Carrier, ретрансляция кадров, постоянный ISDN-, xDSL- или кабельный модем), или если ваш компьютер с Windows 2000 подключен к Интернету через дополнительный маршрутизатор, а для ЛВС-интерфейса статически или с помощью DHCP определены IP-адрес, маска подсети и шлюз по умолчанию, перейдите к пункту 6.
5. Создайте интерфейс подключения по запросу для соединения с вашим поставщиком услуг Интернета.

   Вам необходимо создать интерфейс подключения по запросу, поддерживающий IP-маршрутизацию и использующий установленное на вашем компьютере оборудование удаленного доступа, а также аутентификационные сведения, предоставленные вашим поставщиком услуг Интернета.
6. Создайте статический маршрут по умолчанию, использующий интерфейс Интернета.

   Для статического маршрута по умолчанию следует выбрать интерфейс подключения по запросу (для удаленных соединений) или ЛВС-интерфейс (для постоянных или промежуточных соединений с маршрутизатором, используемый для подключения к Интернету. Конечный адрес — 0.0.0.0, маска подсети — 0.0.0.0. Для интерфейса подключения по запросу IP-адрес шлюза не указывается.
7. Добавьте протокол маршрутизации NAT.

   Инструкции по установке протокола маршрутизации NAT приведены в следующем разделе.
8. Добавьте к протоколу маршрутизации NAT интерфейсы Интернета и домашней сети.
9. Включите адресацию и разрешение имен NAT.

▶ Добавление NAT в качестве протокола маршрутизации

1. Раскройте меню Start\Programs\Administrative Tools\Routing and Remote Access.
2. В дереве консоли раскройте узел Routing And Remote Access*имя_сервера*\IP Routing и щелкните правой кнопкой значок General.
3. В контекстном меню выберите команду New Routing Protocol.

4. В окне Select Routing Protocol щелкните Network Address Translation, затем — OK.

▶ **Включение адресации NAT**

1. Раскройте меню Start\Programs\Administrative Tools\Routing and Remote Access.
2. В дереве консоли щелкните узел NAT правой кнопкой мыши.
3. В контекстном меню выберите команду Properties.
4. На вкладке Address Assignment пометьте флажок Automatically Assign IP Addresses By Using DHCP (Автоматически назначать IP-адреса с использованием DHCP).
5. При возможности задайте в окне IP-адрес маску подсети, которые будут назначаться DHCP-клиентам частной сети.
6. При необходимости щелкните кнопку Exclude (Исключить) и укажите адреса, которые следует исключить из числа адресов, выделяемых DHCP-клиентам частной сети. Затем щелкните OK.

Один или несколько общих адресов

Если вы используете один общий IP-адрес, выделенный поставщиком услуг Интернета, дополнительной настройки IP-адресов не требуется. При использовании нескольких IP-адресов вам следует настроить интерфейс NAT для работы с диапазоном общих IP-адресов. Определите, можно ли выразить диапазон общих IP-адресов, используя IP-адрес и маску.

Если количество выделенных вам IP-адресов кратно двум (2, 4, 8, 16 и т.д.), весь диапазон назначенных адресов можно выразить с помощью единственного IP-адреса и маски. Например, поставщик услуг Интернета выделил вам 4 общих IP-адреса 200.100.100.212, 200.100.100.213, 200.100.100.214 и 200.100.100.215. Эти 4 адреса можно выразить как 200.100.100.212 с маской подсети 2.55.255,255.252. Если используемые вами IP-адреса нельзя выразить, применяя IP-адрес и маску подсети, их можно вводить какдиапазон или набор диапазонов, указывая начальный и конечный IP-адреса.

▶ **Настройка диапазонов IP-адресов интерфейса**

1. Раскройте меню Start\Programs\Administrative Tools\Routing and Remote Access.
2. В дереве консоли щелкните узел NAT.
3. В правой панели щелкните правой кнопкой значок интерфейса, который требуется настроить, и выберите в контекстном меню команду Properties.
4. На вкладке Address Pool (Пул адресов) шелкните кнопку Add (Добавить).
5. Укажите в полях Start Address и End Address начальный и конечный IP-адреса диапазона соответственно.

Разрешение входящих подключений

При обычном использовании NAT к небольшой сети допускаются исходящие соединения компьютеров частной сети с общей сетью. Выполняющиеся из частной сети программы, например Web-браузеры, создают соединения с ресурсами Интернета. Обратный трафик из Интернета будет передаваться через NAT, поскольку соединение было инициировано компьютером частной сети. Чтобы предоставить пользователям Интернета доступ к ресурсам вашей частной сети, выполните следующие действия:

- настройте на сервере ресурсов статическую IP-конфигурацию, включая IP-адрес (из диапазона IP-адресов, выделенных NAT-компьютеру), маску подсети (из диапазона IP-адресов, выделенных NAT-компьютеру), шлюз по умолчанию (частный IP-адрес NAT-компьютера) и DNS-сервер (частный IP-адрес NAT-компьютера);

- исключите IP-адрес, используемый сервером ресурсов, из диапазона IP-адресов, выделяемых NAT-компьютером;
- настройте специальный порт — статическую привязку общего адреса и номера порта к частному адресу и номеру порта. Специальный порт привязывает входящее подключение пользователя Интернета к определенному адресу вашей частной сети. Используя специальный порт, вы можете создать в частной сети доступный из Интернета Web-сервер.

▶ **Настройка специальных портов интерфейса**

1. Раскройте меню Start\Programs\Administrative Tools\Routing and Remote Access.
2. В правой панели щелкните правой кнопкой значок интерфейса, который требуется настроить, и выберите в контекстном меню команду Properties.
3. На вкладке Special Ports щелкните TCP или UDP, затем — кнопку Add.
4. В поле Incoming Port введите номер порта входящего общего трафика.
5. Если задан диапазон общих IP-адресов, щелкните кнопку On This Address Pool Entry и затем введите общий IP-адрес входящего общего трафика.
6. В поле Outgoing Port введите номер порта ресурса частной сети.
7. В поле Private Address введите частный адрес ресурса частной сети.

Настройка приложений и служб

Вам может потребоваться настроить приложения и службы для корректной работы и Интернете. Например, если пользователи небольшой сети хотят сыграть в «Diablo» с пользователями Интернета, NAT следует настроить для работы с приложением «Diablo».

▶ **Настройка сетевых приложений NAT**

1. Раскройте меню Start\Programs\Administrative Tools\Routing and Remote Access.
2. В дереве консоли щелкните значок NAT правой кнопкой мыши.
3. Выберите в контекстном меню команду Properties.
4. На вкладке Translation (Преобразование) щелкните кнопку Applications (Приложения).
5. Чтобы добавить сетевое приложение, щелкните кнопку Add (Добавить).
6. В открывшемся окне введите параметры сетевого приложения и щелкните OK.

Примечание Для редактирования параметров или удаления сетевого приложения NAT из списка в окне Applications щелкните кнопку Edit (Изменить) или Remove (Удалить) соответственно.

VPN-соединения из транслируемой сети

Для доступа к частной интрасети по VPN-соединению из транслируемой сети можно воспользоваться протоколом PPTP и установить с компьютера интрасети VPN-соединение с VPN-сервером, находящимся в другой частной интрасети. Протокол маршрутизации NAT включает редактор NAT для трафика **PPTP.** Соединения, использующие протокол L2TP поверх IPSec, не транслируются через сервер NAT.

Виртуальные частные сети и протоколы NAT

NAT способна преобразовывать далеко не весь трафик. Некоторые приложения имеют встроенные IP-адреса (отсутствующие в заголовке IP) или просто зашифрованы. Для работы таких приложений пользователь может создать туннельное соединение через NAT, применив протокол PPTP, которому не требуется редактор, имеющийся в NAT. Редактируются

и преобразовываются лишь заголовки IP и Generic Routing Encapsulation (GRE). Исходная IP-дейтаграмма не затрагивается. Это позволяет шифрованию или другим не поддерживаемым приложениям работать через NAT.

Исходный адрес PPTP-пакетов транслируется в адрес NAT. Инкапсулированному IP-пакету исходный адрес назначается сервером PPTP. Если пакет находится вне сервера PPTP, инкапсуляция удаляется, и исходным адресом пакета становится адрес, назначенный сервером PPTP. Если сервер PPTP применяет пул действительных адресов Интернета, клиент получает действительный адрес и возможность обращаться к любым ресурсам Интернета. При этом будет работать любое приложение, поскольку исходная IP-дейтаграмма не преобразовывалась. Протокол NAT транслирует только инкапсуляцию (оболочку).

Примечание Протоколу L2TP не требуется редактор NAT. Тем не менее NAT не может транслировать протокол L2TP поверх IPSec. Редактор NAT для IPSec не существует.

Данный метод обхода NAT полезен лишь при наличии PPTP-сервера, с которым можно установить туннельное соединение. Это удобно для филиалов компании или пользователей, создающих туннельное соединение с корпоративной сетью (рис. 12-6).

Рис. 12-6. Реализация VPN через сервер NAT

Резюме

При применении NAT частные адреса используются во внутренней сети обычным порядком. Такие адреса рекомендуются вместо произвольного выбора IP-адресов, это позволяет предотвратить возможное дублирование IP-адресов, недействительных в Интернете. Во избежание проблем при внедрении NAT следует учесть несколько моментов. При обычном использовании NAT в небольшой сети допускаются исходящие соединения компьютеров частной сети с общей сетью. Помните также, что NAT способен преобразовывать далеко не весь трафик, поскольку некоторые приложения используют встроенные IP-адреса или зашифрованы. Для работы таких приложений следует установить через NAT туннельное соединение, применив протокол PPTP.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Опишите назначение протокола NAT.

2. Перечислите компоненты, составляющие протокол NAT.

3. Небольшая фирма использует для своей частной интрассти сетевой идентификатор 10.0.0.0 и получила от поставщика услуг Интернета общий IP-адрес 198.200.200.1. К какому общему IP-адресу протокол NAT привяжет все частные IP-адреса в сети 10.0.0.0?

4. Как предоставить пользователям Интернета доступ к ресурсам вашей частной сети?

ГЛАВА 13

Внедрение служб сертификации

В этой главе

Сертификаты являются фундаментальными элементами инфраструктуры открытых ключей Microsoft (Public Key Infrastructure, PKI). Они позволяют пользователям применять смарт-карты для входа в систему, рассылать зашифрованную электронную почту и подписывать электронные документы. Сертификаты выпускаются, управляются, продлеваются и отзываются при помощи сертификационных центров. В этой главе рассказано, как установить и настроить сертификаты.

Прежде всего

Для изучения материалов этой главы необходимо:

- установить Windows 2000 Server;
- установить службу Active Directory;
- установить службу Domain Name System (DNS).

Занятие 1 Знакомство с сертификатами

На этом занятии вы узнаете о цифровых сертификатах и службах сертификации Windows 2000, а также о центре сертификации (ЦС) — Certification Authority (CA), — поддерживаемом Windows 2000.

Изучив материал этого занятия, вы сможете:

- ✓ определять сертификаты;
- ✓ объяснять назначение компонентов сертификата;
- ✓ создать отказоустойчивый корень DFS;
- ✓ объяснить порядок использования сертификатов;
- ✓ различать корпоративные и отдельные центры сертификации.

Продолжительность занятия — около 25 минут.

Общие сведения о сертификатах

Сертификат (цифровой сертификат, сертификат открытого ключа) представляет собой цифровой документ, подтверждающий соответствие открытого ключа объекту. Основное назначение сертификатов — гарантировать, что открытый ключ, содержащийся в сертификате, действительно принадлежит объекту, указанному в сертификате. Сертификаты играют главную роль в инфраструктуре открытого ключа (рис. 13-1).

Рис. 13-1. Служба сертификации, интегрированная с Active Directory и распределенной службой безопасности

Сертификат может состоять из открытого ключа, подписанного доверенным объектом. Наиболее широко используемые структура и синтаксис цифровых сертификатов определены в документе ITU-T Recommendation X.509. На рис. 13-2 показан сертификат, используемый для проверки подлинности отправителя сообщения электронной почты.

Сертификат X.509 содержит информацию, определяющую пользователя, организацию, выпустившую сертификат, серийный номер сертификата, срок его действия, имя и подпись запрашивающей стороны и имя субъекта (или пользователя). В качестве субъекта могут выступать физическое лицо, школа, коммерческая или другая организация, в той числе ЦС.

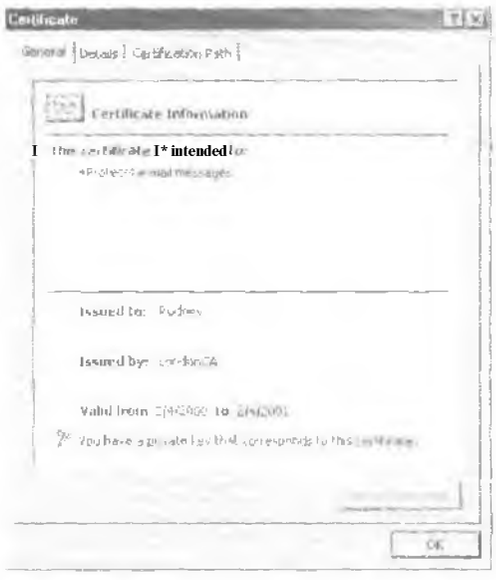


Рис. 13-2. Пример сертификата

Создание сертификата

Сертификаты подписываются центром сертификации, который может быть любой доверяемой службой или объектом, желающим проверить подлинность того, для кого сертификат выпущен, и его связь с конкретным ключом. Компании вправе выпускать сертификаты для своих работников, школы — для своих учащихся, и т. п. Необходимо, чтобы достоверность открытого ключа центра сертификации была полностью определена, иначе не будет доверия к выпускаемым им сертификатам. Так как UC может создать кто угодно, степень доверия к нему определяется степенью доверия к организации, выдавшей ему ключ. Ниже описаны шесть этапов процесса запроса и выпуска сертификата.

1. **Генерация** пары ключей. Претендент генерирует пару из открытого и закрытого ключа или назначает автора пары ключей из своей организации.
2. Сбор требуемой информации. Претендент собирает всю информацию, необходимую ЦС для выдачи сертификата. Она может включать адрес электронной почты претендента, свидетельство о рождении, отпечатки пальцев или другие нотариально заверенные документы, подтверждающие подлинность претендента. ЦС со строгими идентификационными требованиями выпускают сертификаты с высокой степенью доверия. О самих ЦС говорят, что они имеют высокую, среднюю или низкую степень доверия.
3. Запрос **сертификата**. Претендент посылает в ЦС запрос на сертификат, состоящий из своего открытого ключа и необходимой дополнительной информации. Запрос на сертификат может быть зашифрован с использованием открытого ключа ЦС. Запросы разрешается посылать по электронной почте, посредством обычной почты или курьерской службы, например при необходимости нотариального заверения самого запроса.
4. Проверка информации. Чтобы удостовериться в том, что претендент получит сертификат, ЦС применяет любые необходимые правила политик. В соответствии с идентификационными требованиями политика и процедуры верификации ЦС влияют на степень доверия выпускаемых им сертификатов.

5. Создание сертификата. ЦС создает и подписывает цифровой документ, содержащий открытый ключ претендента и другую необходимую информацию. Подпись ЦС подтверждает привязку имени субъекта к его открытому ключу. Подписанный документ и является сертификатом.
6. **Отправка или рассылка сертификата**. ЦС отправляет претенденту сертификат или помещает его в каталог.

Использование сертификата

Сертификат гарантирует законность конкретного открытого ключа. Сертификат должен подписываться закрытым ключом изготовителя, иначе он не будет считаться сертификатом. Поэтому подпись изготовителя проверяется с использованием его открытого ключа. Если объект доверяет изготовителю, он также уверен и в том, что открытый ключ, содержащийся в сертификате, принадлежит субъекту, упомянутому в нем.

Корпоративный и изолированный центр сертификации

Службы сертификации предусматривают два варианта политик, разрешающих использование двух классов ЦС: корпоративного и изолированного. В каждый класс входят два типа ЦС: корневой и подчиненный. Модули политики определяют изменяемый при необходимости порядок действий, предпринимаемый ЦС при получении запроса на сертификат.

ЦС организованы иерархически: наиболее доверенный ЦС находится ближе к вершине. Windows 2000 PKI поддерживает иерархическую модель ЦС. В ней может быть множество не связанных между собой иерархий. Совместное использование всеми ЦС общего родителя верхнего уровня не требуется.

Корпоративный ЦС

На предприятии корневые ЦС обладают самой высокой степенью доверия. В домене Windows 2000 может быть несколько корпоративных корневых ЦС, но только одному из них разрешено основать иерархию. Остальные являются корпоративными подчиненными ЦС.

Организация устанавливает корпоративный ЦС для выдачи сертификатов своим пользователям или компьютерам. Нет необходимости устанавливать ЦС в каждом домене организации. Например, пользователи дочернего домена могут обратиться к ЦС в родительском домене. Модуль политики корпоративного ЦС предписывает порядок обработки и выпуска сертификатов. Необходимая этим модулям информация о политике хранится централизованно в Windows 2000 Active Directory.

Примечание Перед установкой корпоративного ЦС необходимо запустить службы Active Directory и DNS-сервер.

Изолированный ЦС

Организация, которая предполагает выпускать сертификаты для пользователей или компьютеров, расположенных за ее пределами, должна установить изолированный ЦС. Их может быть несколько, но в каждой иерархии допустимо существование только одного изолированного ЦС. Остальные ЦС в иерархии считаются изолированными или корпоративными подчиненными ЦС.

Автономный ЦС имеет относительно простой заданный по умолчанию модуль политики и не хранит информацию удаленно. Поэтому изолированному ЦС не нужна служба Active Directory.

Типы центров сертификации

В этом разделе описаны требования для установки каждого из четырех типов ЦС службы Certificate Services.

Корпоративный корневой ЦС

Считается корнем иерархии ЦС в организации. Его устанавливают, если ЦС предполагает выпускать сертификаты для пользователей и компьютеров своей организации. В больших организациях корпоративный корневой ЦС применяется только для выпуска сертификатов подчиненным ЦС, которые генерируют сертификаты для остальных пользователей и компьютеров.

Для работы корпоративного корневого ЦС необходимы:

- служба DNS Windows 2000;
- служба Active Directory Windows 2000;
- администраторские полномочия на всех серверах.

Корпоративный подчиненный ЦС

Выпускает сертификаты, действующие в пределах организации. Не является самым доверенным ЦС в организации и подчинен другому ЦС в иерархии.

Для работы корпоративного подчиненного ЦС необходимы:

- связь с ЦС, выполняющим запросы сертификатов подчиненного ЦС. Он может быть внешним коммерческим или автономным ЦС;
- служба DNS Windows 2000;
- служба Active Directory Windows 2000;
- администраторские полномочия на всех серверах.

Изолированный корневой ЦС

Является корнем доверительной иерархии ЦС. Для него требуются административные полномочия на локальном сервере. Организации необходимо установить изолированный корневой ЦС, если он будет выпускать сертификаты за пределы корпоративной сети организации, и необходимо, чтобы он был корневым. Корневой ЦС, как правило, выпускает сертификаты только для подчиненных ЦС.

Изолированный подчиненный ЦС

Функционирует как отдельный сертификационный сервер или в составе доверительной иерархии ЦС. Устанавливается для выдачи сертификатов объектам за пределами организации.

Для работы изолированного подчиненного ЦС необходимы:

- связь с ЦС, выполняющим запросы сертификатов подчиненного ЦС. Он может быть внешним коммерческим ЦС;
- полномочия администратора на локальном сервере;
- регистрация сертификата — процесс получения цифрового сертификата.

Резюме

Сертификаты являются фундаментальными элементами инфраструктуры открытых ключей Microsoft (Public Key Infrastructure, PKI). Они позволяют пользователям применять смарт-карты для входа в систему, рассылать зашифрованную электронную почту, подписывать электронные документы и т. п. Сертификаты выпускаются, управляются, продлеваются и аннулируются сертификационными центрами. На следующем занятии вы научитесь устанавливать и настраивать сертификаты.

Занятие 2, Установка и настройка центров сертификации

Для установки и зашиты ЦС рассмотрим сертификаты более детально и познакомимся со способами их регистрации.

Изучив материал этого занятия, вы сможете:

- ✓ объяснить порядок использования Certificate Authority Manager (Диспетчер авторизации сертификата);
- ✓ объяснить порядок установки и зашиты ЦС;
- ✓ описать процесс регистрации сертификата.

Продолжительность занятия — около 35 минут.

Развертывание центра сертификации

В следующем практикуме на этом занятии вы установите ЦС. Мастер установки служб сертификации поможет администратору шаг за шагом выполнить процесс установки. А сейчас мы расскажем о ключевых элементах, которые необходимо изучить перед началом установки.

- **Установка домена Windows 2000.** Если требуется развернуть корпоративный ЦС, до установки служб сертификации необходимо установить домен.
- **Интеграция службы Active Directory.** Во время установки информация о корпоративных ЦС записывается в виде соответствующих объектов в Active Directory. Эти данные используются клиентами домена для определения доступных ЦС и типов сертификатов, выпускаемых ими.
- **Выбор несущего сервера.** Корневой ЦС мржет работать на любой платформеWindows 2000 Server, включая контроллер домена. При выборе необходимо руководствоваться требованиями физической безопасности, ожидаемой нагрузки и характеристиками связи.
- **Назначение имен.** Имена ЦС встраиваются в выпускаемые ими сертификаты, и, следовательно, менять их нельзя. Переименование компьютера, на котором установлены службы сертификации невозможно. При выборе имен ЦС необходимо учитывать соглашения об именах, принятые в организации, и будущие требования. Имя ЦС (или вообще имя) важно, т. к. о'но используется для идентификации объектов ЦС. созданных в Active Directory для корпоративных ЦС.
- **Генерация ключей.** Пара открытых ключей ЦС генерируется при установке и является уникальной для конкретного ЦС.
- **Сертификация ЦС.** Для корневого ЦС в процессе установки автоматически генерируется сертификат ЦС, который подписывается своей же парой из открытого и закрытого ключа. Для дочернего ЦС администратор имеет возможность сгенерировать запрос на сертификат к промежуточному или корневому ЦС.
- **Политика выпуска.** Программа установки корпоративною ЦС автоматически устанавливает и настраивает модуль корпоративной политики ЦС по умолчанию. Программа установки изолированного ЦС автоматически устанавливает и настраивает модуль политики ЦС по умолчанию. При необходимости специальные модули политики можно заменить.

После установки корневого ЦС разрешается установить промежуточный или подчиненный ЦС. Единственное существенное различие в политике установки заключается в

генерации запроса к корневому или к промежуточному ЦС. Данный запрос может маршрутизироваться к работающему ЦС автоматически средствами Active Directory или вручную в автономном сценарии. В любом случае перед началом работы ЦС необходимо установить полученный сертификат.

Доверительная модель корпоративного ЦС может как соответстаовать, так и не соответствовать модели доверия домена Windows 2000. Полного совпадения этих моделей не требуется. Ничто не мешает автономному ЦС обслуживать объекты в нескольких доменах или объекты за пределами домена. Аналогичным образом данный домен может иметь несколько корпоративных ЦС.

Защита центра сертификации

ЦС очень важны, и поэтому необходимо обеспечивать их защитой высокого уровня. Для этого используют следующие методы.

- Физическая зашита. ЦС на предприятии являются объектами с высоким доверием, поэтому их необходимо защищать от вмешательства извне. Это требование зависит от значимости сертификатов, выдаваемых ЦС. Физическая изоляция сервера ЦС в месте, доступном только администраторам безопасности, может значительно уменьшить возможность таких физических атак.
- Управление ключами. Закрытый ключ ЦС является основой для доверия в процессе сертификации. Его необходимо защищать от внешних вторжений. Криптографические аппаратные модули (доступ к службам сертификации при помощи CryptoAPI CSP) обеспечивают надежное хранение ключей и отделение выполнения криптографических операций от работы остального ПО сервера. Это существенно уменьшает вероятность компрометации ключа ЦС.
- Восстановление. Выход из строя ЦС (например, из-за отказа оборудования) создает ряд административных и оперативных проблем и предотвращает аннулирование существующих сертификатов. Службы сертификации поддерживают резервное копирование экземпляра IJC в целях его восстановления. Это важная часть всего процесса управления ЦС.

Регистрация сертификата

Процесс получения цифрового сертификата называют его регистрацией. Инфраструктура открытых ключей (PKI) Windows 2000 поддерживает регистрацию сертификатов в корпоративных, автономных и сторонних ЦС. Регистрация не зависит от транспорта и основана на использовании промышленных стандартов шифрования с открытым ключом PKCS #10 (Сообщения с запросом сертификата) и PKCS #7 (Ответы. содержащие выданный сертификат или последовательность сертификатов). На момент написан'ия данной главы сертификаты поддерживали RSA- и DSA-ключи и подписи, а также ключи Diffie-Hellman.

Методы регистрации

PKI поддерживает множество методов регистрации, в том числе сетевую регистрацию. мастер регистрации и управляемую политикой авторегистрацию, которая происходит как часть процесса входа пользователя в систему. В будущем Microsoft планирует усовершенствовать процесс регистрации сертификатов, способом совместимым с синтаксисом запроса сертификата (Certificate Request Syntax, CRS), проект которого разрабатывается в Internet Engineering Task Force (IETF) рабочей группой PKIX.

Сетевая регистрация

Процесс сетевой регистрации начинается с запроса сертификата клиентом и заканчивается установкой сертификата в клиентское приложение. Управление регистрацией и ее формами выполняется на Web-странице администрирования служб сертификации *http://<имя_сервера>/certsrv/default.asp* (рис. 13-3). Вы можете настроить Web-страницы служб сертификации, изменив параметры пользователей или дав ссылки на интерактивную службу или инструкции пользователям.

Регистрация клиентских сертификатов

Службы сертификации поддерживают регистрацию сертификатов клиентов, применяющих обозреватель Internet Explorer версии 3.0 и выше. Для получения клиентских сертификатов при помощи данных обозревателей пользователю необходимо открыть страницу аутентификации клиента и ввести идентификационную информацию. Созданный клиентский сертификат возвращается в обозреватель, который затем устанавливает его на клиент.

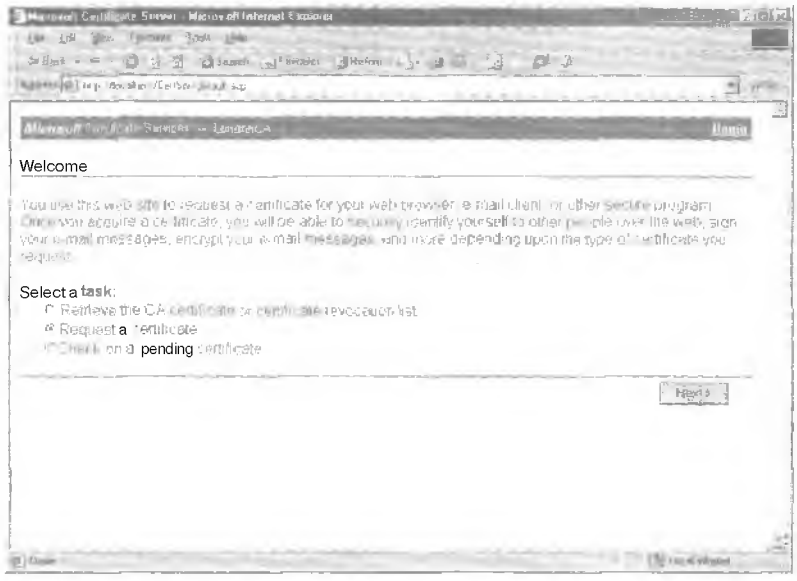


Рис. 13-3. Запрос сертификатов

Автоматическая регистрация

Процесс автоматической регистрации управляется двумя ключевыми элементами: типами сертификата и объектами авторегистрации. Они интегрированы в объекты Group Policy (Групповой политики) и определяются на основе узла, домена, организационной единицы, компьютера или пользователя.

Типы сертификатов предоставляют шаблон для сертификата и связывают его с обычным именем для простоты администрирования. В шаблоне определяются такие элементы, как требования к именам, срок действия, допустимые CSP для генерации закрытых ключей, алгоритмы и добавления, которые необходимо включить в сертификат. Типы сертификатов логически разделяются на типы компьютеров и пользователей и применяются соответственно к объектам политики. Определенные однажды, типы сертификатов используют в объектах авторегистрации и мастере получения сертификатов.

Данный механизм интегрирован в политику выпуска корпоративного ЦС, а не подменяет се. Служба ЦС получает набор типов сертификатов в качестве части их объектов по-

литики. Для определения типов сертификатов, выпускаемых ЦС, они используют модуль Enterprise Policy (Корпоративной политики). ЦС отвергает запросы сертификатов, не соответствующих этим критериям.

Объект авторегистрации определяет политику сертификатов, которые представляют собой объекты в домене. Их применяют на основе компьютеров или пользователей. Типы сертификатов соответствуют типам сертифицируемых объектов, разрешается применять любой определенный тип. Объект авторегистрации предоставляет достаточную информацию для определения необходимого объекту сертификата и регистрирует на корпоративном ЦС отсутствующие сертификаты. Объекты авторегистрации также определяют политику обновления сертификатов, так что администратор может самостоятельно задать срок службы сертификата, без вмешательства пользователя. Обработка объектов авторегистрации и вступление в силу сделанных изменений происходит после любого обновления политики (вход в систему, обновление объектов групповой политики и т. д.).

Практикум: установка изолированного подчиненного центра сертификации

Задание 1: установите изолированный подчиненный ЦС

1. В панели управления щелкните значок Add/Remove Programs (Установка/Удаление программ).
2. Перейдите на вкладку Add/Remove Windows Components (Установка/Удаление компонентов Windows).
3. Пометьте флажок напротив Certificate Services (Службы сертификации), затем щелкните Next.
4. Щелкните переключатель Stand-Alone Root ЦС (Изолированный корневой ЦС), затем — Next.
5. Заполните идентификационную информацию ЦС.
   В поле ЦС name (Имя ЦС) наберите *Имя_компьютера* **ЦС** и щелкните Next.
6. Используйте хранилище данных по умолчанию и щелкните Next.
7. Во время процесса установки ЦС иногда требуется остановить службу IIS. Для этого щелкните кнопку OK и задайте местоположение установочных файлов Windows 2000 (конкретно Certsrv*).
8. Щелкните кнопку Finish (Готово).
9. Закройте окно Add/Remove Programs.

Задание 2: запросите и установите сертификат с локального ЦС

1. Запустите оснастку Certification Authority (Центр сертификации).
   Удостоверьтесь, что служба работает (рис. 13-4).
2. Запустите Internet Explorer и подключитесь к *http://<ваш_сервер>/certsrv/default.asp*.
3. Запросите сертификат обозревателя Web. Запрос будет поставлен в очередь.
4. Закройте Internet Explorer.
5. Откройте оснастку Certificate Authority (Авторизация сертификата) и выберите папку Pending Requests (Запросы в ожидании). Щелкните правой кнопкой мыши ваш запрос, выберите All Tasks (Все задания) и щелкните команду Issue (Выдать).
6. В дереве консоли щелкните папку Issued Certificates (Выданные сертификаты) и удостоверьтесь, что ваш запрос был выполнен.
7. Откройте Internet Explorer, подключитесь к *http://<ваш_сервер>/certsrv/default.asp*, проверьте папку Pending Certificate Request, затем установите сертификат.

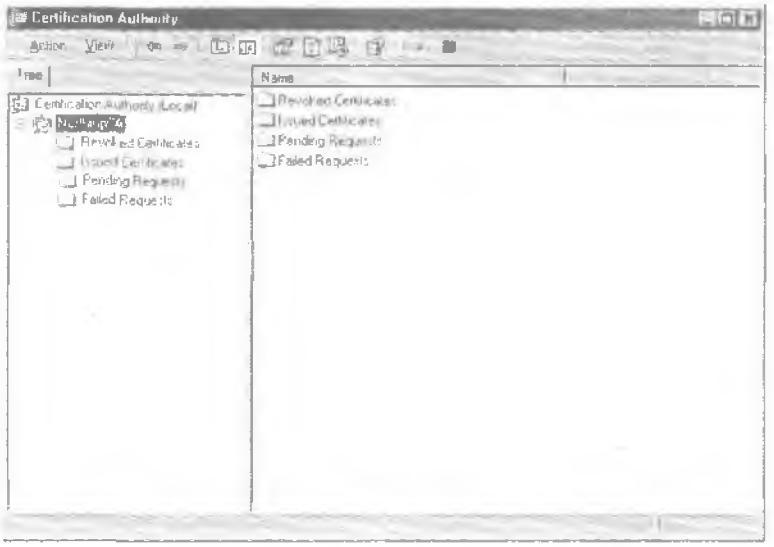


Рис. 13-4. Оснастка Certification Authority (Центр сертификации)

8. В меню Tools (Сервис) выберите команду Internet Options (Свойства обозревателя), затем перейдите на вкладку Content (Содержание) и щелкните кнопку Certificates (Сертификаты).
9. В окне Certificates выберите ваш сертификат и щелкните кнопку View (Просмотр). Заметьте, что сертификат был выпущен вашим компьютером. Закройте все окна.

Хранение криптографических ключей

В Microsoft PKI криптографические ключи и связанные с ними сертификаты хранятся и управляются подсистемой CryptoAPI. Ключи обслуживаются при помощи CSP, а сертификаты — при помощи CryptoAPI хранилищ сертификатов. Хранилища являются архивами сертификатов вместе со связанными с ними свойствами. Обычно PKI определяет пять стандартных хранилищ сертификатов (табл. 13-1).

Табл. 13-1. Стандартные хранилища сертификатов PKI

Хранилища	Описание
MY	Применяется для хранения сертификатов компьютеров пользователей, для которых имеются связанные с ними закрытые ключи
CA	Используется для хранения выпущенных или промежуточных сертификатов ЦС, применяемых при построении цепочек проверок сертификатов
TRUST	Используется для хранения списков доверия сертификатов. Это альтернативный механизм для задания администратором набора доверяемых ЦС. Их преимущество состоит в том, что они подписаны электронной подписью и могут передаваться по открытым каналам
ROOT	Используется для хранения только сертификатов доверяемых корневых ЦС, им же и подписанных
UserDS	Используется для логичного представления архива сертификатов, хранящихся в Active Directory (например, в свойствах userCertificate объекта User). Он предназначен для облегчения доступа к этим внешним архивам

Они являются логическими хранилищами, предоставляющими полное представление доступных сертификатов в масштабе системы, которые могут находиться на различных физических носителях (жестком диске, смарт-карте и т. п.). Эти службы позволяют приложениям применять сертификаты совместно и гарантируют правильность работы административной политики. Функции управления сертификатами поддерживают расшифровку сертификатов X.509 v3 и предоставляют функции нумерации для облегчения поиска конкретного сертификата.

Для облегчения разработки приложений MY-хранилища поддерживают свойства сертификатов, которые указаны CSP, и набор ключевых имен для связывания с закрытыми ключами. После выбора приложением сертификата оно использует эту информацию при получении CSP-контекста для правильности закрытого ключа.

Обновление сертификата

Концепция обновления сертификатов похожа на регистрацию и использует преимущество доверительных отношений, которым отличаются существующие сертификаты. Обновление предполагает, что запрашивающему объекту нужен новый сертификате теми же атрибутами, что и у существующего, но с продленным сроком действия. При обновлении используется существующий или новый открытый ключ.

Обновление идет в основном на ПС. Запрос на обновление обрабатывается более эффективно, потому что нет необходимости проверять уже существующий сертификат. В настоящий момент обновление поддерживается в Windows 2000 PKI для автоматически зарегистрированных сертификатов. В других системах обновление рассматривается как новый запрос на регистрацию.

Промышленный стандарт протоколов сообщений на обновление сертификатов еще не определен, но уже включен в предварительный вариант IETF PKIX CRS. После принятия этих стандартов Microsoft планирует разработать связанные с сообщениями форматы.

Восстановление сертификата и ключа

Пары открытых ключей и сертификаты имеют большое значение. При утрате в результате сбоя системы их замена отнимает много времени и денег. Для решения данной проблемы в Windows 2000 PKI встроена возможность архивирования и восстановления сертификатов и связанных с ними пар ключей, используя административные инструменты управления сертификатами.

При экспорте сертификата средствами диспетчера пользователь вправе также экспортировать и связанную с ним пару ключей. При этом информация экспортируется в зашифрованном (на основе пароля пользователя) сообщении PKCS #12. Затем его можно импортировать в свою или другую систему или восстановить сертификат и ключи.

Пару ключей можно экспортировать средствами CSP, например, на базе Microsoft, если «о время генерации набора ключей пометить флажок экспорта. CSP сторонних фирм могут поддерживать или не поддерживать экспорт закрытого ключа. Например, CSP смарт-карт вообще не поддерживает данную операцию. Для программных CSP с неэкспортируемыми ключами альтернативой служит полное резервное копирование образа системы, включая всю информацию реестра.

Роуминг

В контексте данного обсуждения роуминг означает возможность использовать одни и те же приложения на основе открытых ключей на разных компьютерах в пределах Windows 2000 окружения предприятия. Принципиальным требованием является предоставление досту-

па пользователям к криптографическим ключам и сертификатам независимо от места входа пользователя в систему. PKI Windows 2000 выполняет данное требование двумя способами.

Сначала, в случае применения CSP на базе Microsoft, ключи и сертификаты роуминга поддерживаются механизмом профиля роуминга. Если профили роуминга разрешены, для пользователя данный механизм является прозрачным. Маловероятно, что данный метод будет поддерживаться CSP других фирм, которые чаще всего реализуют различные методы зашиты ключевых данных, основанные на аппаратных устройствах.

Аппаратные эстафетные устройства, например смарт-карты, поддерживают роуминг, если они включают физическое хранилище сертификата. CSP смарт-карт, поставляемый с платформой Windows 2000, поддерживает эти функциональные возможности. Поддержка роуминга выполняется перемещением аппаратного маркера вместе с пользователем.

Отзыв сертификатов

Сертификаты являются долгосрочными верительными грамотами. В силу ряда причин они иногда становятся ненадежными до истечения их срока:

- при компрометации или подозрении в компрометации целостности закрытого ключа;
- при мошенничестве при получении сертификата;
- при изменении статуса.

Функциональные возможности на базе открытого ключа позволяют реализовать распределенную проверку, причем без прямого соединения с центральным доверенным центром, который ручается за их реквизиты. При этом требуется аннулировать информацию, которая может стать известной тем, кто пытается проверить сертификаты.

Потребность в аннулировании информации и ее своевременности зависит от приложения. PKI Windows 2000 включает поддержку промышленного стандарта списков аннулирования сертификатов (CRL). Корпоративные ЦС поддерживают аннулирование сертификата и публикацию CRL в Active Directory при административном управлении. Клиенты домена могут отбирать данную информацию, кэшировать локально и использовать ее при проверке сертификатов. Этот же механизм поддерживает CRL, выпускаемые коммерческими ЦС или сертификационными серверами других фирм, обеспечивающих доступ клиентам сети к опубликованным CRL.

Доверие

Проверка сертификатов главными образом выполняется клиентами, использующими приложения на основе PK. Если выданный конечный сертификат может быть показан в «цепочке» к известному доверенному корневому ЦС и если предписанное использование сертификата совместимо с контекстом приложения, то это допустимо. Если хотя бы одно из условий не выполняется, то подобная степень доверия недопустима.

В PKI пользователям можно создать доверительные решения, затрагивающие только их самих. Это делается путем установки или удаления доверенных корневых ЦС и настройки связанных ограничений использования с применением административных средств.

Ожидается, что данные доверительные отношения будут устанавливаться как часть политики предприятия. Устанавливаемые политикой доверительные отношения автоматически распространяются на клиентские компьютеры с Windows 2000.

Доверенные корни ЦС

Для установления доверительных отношений, используемых клиентами домена при проверке PK сертификатов, доверие в корневых ЦС устанавливается при помощи политики.

Набор доверенных ЦС настраивается средствами редактора политики групп. Он настраивается на основе каждого компьютера и может быть распространен на всех пользователей компьютера.

Кроме доверяемого корневого ЦС администратор задает применение связанных с ЦС свойств. Они ограничивают допустимые цели, для которых ЦС выпускает сертификаты. В приложении к предварительной редакции IETF PKIX (часть I расширения Extended-KeyUsage) определены ограничения, основанные на идентификаторах объекта. В настоящее время используются следующие комбинации ограничений:

- аутентификация сервера;
- аутентификация клиента;
- подпись кода;
- электронная подпись;
- протокол безопасности IP (IPSec);
- туннель IPSec;
- пользователь IPSec;
- временные отметки;
- шифрованная файловая система Microsoft.

Резюме

Это занятие посвящено тому, как установить и защитить ЦС. ЦС являются очень важными ресурсами, которые необходимо защищать. Вы узнали, как зарегистрировать сертификат и несколько методов выполнения этой операции. Для получения клиентского сертификата пользователю необходимо открыть страницу аутентификации клиента и ввести идентификационную информацию. После создания службами сертификации клиентский сертификат возвращается обозревателю и устанавливается на компьютер клиента.

Занятие 3, Управление сертификатами

Управление сертификатами — важная задача. На этом занятии вы узнаете, как управлять сертификатами, отзывать их и пользоваться политикой восстановления шифрованной файловой системы — Encrypting File System (EFS).

Изучив материал этого занятия, вы сможете:

- ✓ описать последовательность действий для отзыва сертификата;
- ✓ описать порядок выполнения политики восстановления EFS.

Продолжительность занятия — около 30 минут.

Отозванные сертификаты

Перемешаются в папку Revoked Certificates (Отозванные сертификаты); появляются и CRL после повторного опубликования. Сертификаты, отозванные с кодом Certificate Hold, могут быть восстановлены, оставлены в хранилище до истечения срока их действии или изменения кода причины отзыва. Только код отзыва позволяет скорректировать статус сертификата.

Выданные сертификаты и очередь запросов

На припой панели просмотрите запросы на сертификаты и обратите внимание на имя запрашивающего, его адрес электронной почты и остальные поля, которые, на ваш В1гляд, являются важными для выпуска сертификата.

Неудачные запросы

Запросы на сертификаты вправе отклонять члены групп Cert Publishers (Издатели сертификатов) или Administrators (Администраторы).

Процедура выдачи сертификата

После представления объекту сертификата как средства его (субъекта сертификата) идентификации объект должен выразить доверие выдавшему сертификат ЦС. Выпуск сертификатов происходит в несколько этапов.

- **Генерация** ключа. Претендент, запрашивающий сертификат, генерирует пару из открытого и закрытого ключей. Исключением является создание персональных цифровых сертификатов, для которых ЦС сам генерирует открытый и закрытый ключи и рассылает их конечным пользователям.
- **Проверка соответствия политике.** Претендент предоставляет дополнительные сведения, необходимые для выдачи сертификата (например, удостоверение личности, номер налогоплательщика, адрес электронной почты и т. п.). Требуемые для выдачи сертификата данные определяются ЦС.
- **Рассылка открытых ключей и информации.** Претендент высылает в адрес ЦС открытые ключи и необходимую информацию (часто зашифрованную открытым ключом ЦС).
- **Проверка информации.** Для проверки возможности приема претендентом сертификата ЦС применяет любые требуемые правила политики.
- **Создание сертификата.** ЦС создает цифровой документ со всей необходимой информацией (открытые ключи, дата истечения срока действия и другие данные) и подписывает его своим закрытым ключом.

- **Рассылка сертификата.** ЦС посылает сертификат претенденту или публикует его в хранилище. Сертификат загружается в систему пользователя.

Отзыв сертификата

ЦС публикует CRL, содержащие отозванные им сертификаты. Закрытый ключ владельца сертификата может быть скомпрометирован, либо для запроса на сертификат использовалась неверная информация. CRL позволяет удалить сертификат после его выпуска. CRL доступны для загрузки и интерактивного просмотра клиентскими приложениями.

Для проверки сертификата необходимы открытый ключ ЦС и доступ к списку отзыва, опубликованного этим ЦС. Сертификаты и ЦС устраняют проблемы распространения открытых ключей и использования нескольких открытых ключей одним субъектом. Если открытый ключ ЦС не вызывает подозрений, на него можно полагаться для проверки других сертификатов.

Практикум: отзыв сертификата

Задание: отзовите сертификат, выданный на занятии 2

1. Откройте оснастку Certification Authority (Центр сертификации).
2. Щелкните правой кнопкой ваш запрос в папке Issued Certificates (Выданные сертификаты), выберите All Tasks (Все задания), а затем — команду Revoke Certificate (Отзыв сертификата).
3. Выберите причину отзыва — Cease Of Operation. Щелкните Yes.
4. В дереве консоли щелкните Revoked Certificates (Отозванные сертификаты). Убедитесь, что ваш запрос аннулирован (рис. 13-5).

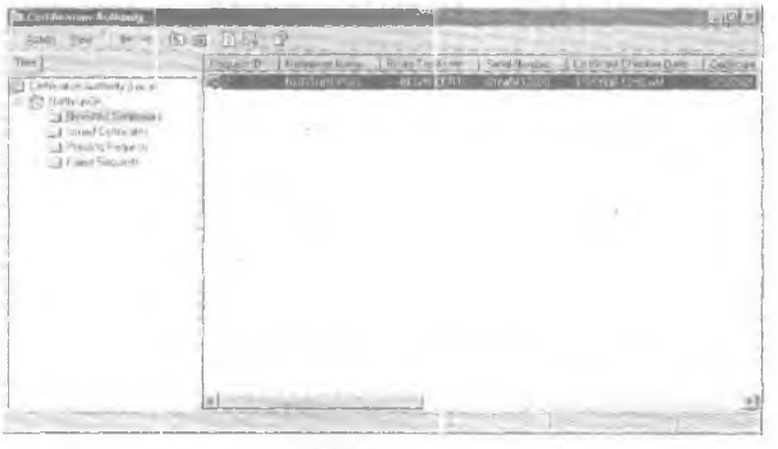


Рис. 13-5. Отозванные сертификаты

Политика восстановления EFS

Восстановление данных EFS является частью всей политики безопасности системы. Например, даже если вы потеряете сертификат для шифрования файлов и связанный с ним закрытый ключ (из-за отказа диска или по другой причине), агент восстановления сможет восстановить информацию. В случае увольнения сотрудника из организации зашифрованные им данные также удастся восстановить.

Политика восстановления **EFS** определяет информацию учетных записей агентов восстановления, применяемую и пределах политики. EFS требует присутствия шифрованных данных политики агента восстановления перед его использованием и, если не определены учетные записи агентов, применяет учетную запись по умолчанию (Администратор). В домене только члены группы Domain Admins (Администраторы домена) имеют право определять учетные записи агентов восстановления. На малых предприятиях и дома при отсутствии домена учетная запись администратора локального компьютера является *по* умолчанию учетной записью агента восстановления. Только администратор вправе изменить политику восстановления на компьютере.

Учетная запись агента восстановления используется для восстановления информации всех компьютеров, на которые распространяется заданная политика. При утере закрытого ключа закрытый им файл можно скопировать и переслать администратору агента восстановления средствами защищенной электронной почты. Администратор восстанавливает резервную копию, открывает ее для чтения, копирует файл в простой текст и возвращает текстовый файл пользователю по защищенной электронной почте.

Есть и альтернативный способ: администратор импортирует свой сертификат агента восстановления и восстанавливает информацию непосредственно на компьютере с зашифрованным файлом. Однако это небезопасно из соображений секретности ключа восстановления: администратору ни в коем случае не рекомендуется оставлять ключ восстановления на другом компьютере.

Практикум: изменение политики восстановления

На этом занятии вы измените политику восстановления локального компьютера. Перед этим необходимо сначала скопировать ключи восстановления на дискету. В домене политика восстановления по умолчанию применяется при установке первого контроллера домена. Администратор домена выпускает подписанный им же сертификат, которым администратор домена назначается агентом восстановления. Для изменения политики восстановления по умолчанию в домене пойдите в качестве администратора в систему первого контроллера домена.

Примечание Для выполнения этого этапа необходимо иметь соответствующие разрешения на запрос сертификата, и ЦС должен быть настроен на выпуск сертификатов данного типа.

▶ Задание: **измените политику восстановления на локальном компьютере**

1. В меню Start (Пуск) выберите команду Run (Выполнить), в открывшемся окне наберите mmc /a и щелкните **OK.**
2. В меню консоли выберите команду Add/Remove Snap-In (Добавить/удалить оснастку) и щелкните кнопку Add (Добавить).
3. Выберите оснастку Group Policy (Групповая политика) и щелкните кнопку Add (Добавить).
4. Убедитесь, что объектом групповой политики является Local Computer (Локальный компьютер) и щелкните последовательно кнопки Finish (Готово), Close (Закрыть) и OK.
5. Раскройте узел Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Public Key Policies (Политика «Локальный компьютер»\ Конфигурация компьютера\Конфигурация Windows\Параметры безопасности\ Политики открытого ключа), щелкните правой кнопкой Encrypted Data Recovery Agents (Агенты восстановления шифрованных данных), а затем выберите одну из следующих команд:

- команда Add (Добавить) позволяет с помощью мастера назначить пользователя дополнительным агентом восстановления;
- команда Delete Policy (Уладить политику) удаляет данную EFS-политику и всех агентов восстановления. В результате пользователи не смогут расшифровать файлы на данном компьютере. Компьютер выпускает подписанный им же сертификат, назначающий локального администратора агентов восстановления по, умолчанию. Если вы удалите этот сертификат при отсутствии другой политики, политика восстановления компьютера не будет задана. Это означает, что агентов восстановления нет. При этом отключается EFS, поэтому ни один пользователь не сможет зашифровывать файлы на данном компьютере.

6. Для изменения сертификата восстановления файлов щелкните в дереве консоли Encrypted Data Recovery Agents (рис. 13-6). В правой панели щелкните правой кнопкой сертификат и выберите команду Properties (Свойства). Например, дайте сертификату понятное имя и введите текстовое описание.

Рис. 13-6. Групповая политика для восстановления EFS

Резюме

Сертификатами управляют при помощи оснастки Certificationion Authority (Центр сертификации). Сергификаты, отозванные с кодом причины Certificate Hold, можно восстановить. Их также разрешается оставить в хранилище сертификатов до истечения срока их действия или изменения кода причины отзыва. Восстановление данных доступно в EFS как часть всей политики безопасности системы.

Закрепление материала

Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Что такое сертификат и каково его назначение?
2. Что такое центр сертификации (ЦС) и чем он занимается?
3. Назовите четыре типа авторизации сертификатов Microsoft.
4. Назовите одну из причин для отзыва сертификата.
5. Назовите пять стандартных хранилищ сертификатов **PKI.**

ГЛАВА 14

Безопасность сети предприятия

В этой главе

В этой главе мы расскажем о внедрении и планировании сетевой безопасности, а также об установке и обеспечении безопасного удаленного доступа к сети. Также мы обсудим устранение неполадок и отслеживание использования сетевых ресурсов и удаленного доступа.

Прежде **всего**

Для изучения материалов этой главы необходимо:

- установить Microsoft Windows 2000 Server;
- выполнить упражнения глав 2 — 10.

Занятие 1. Внедрение сетевой безопасности

При планировании сети необходимо внедрить технологии безопасности. Причем это следует сделать на стадии планирования установки Windows 2000; таким образом вы обеспечите безопасную работу в сети. Сейчас мы расскажем, как внедрить сетевую безопасность.

Изучив материал этого занятия, вы сможете:

- ✓ описать разделы плана сетевой безопасности;
- ✓ определить ситуации, когда есть риск снижения сетевой безопасности;
- ✓ описать функции безопасности Windows 2000;
- ✓ защитить соединение сети с Интернетом.

Продолжительность занятия - около 35 минут.

Планирование сетевой безопасности

Даже если вы уверены, что наладили безопасную работу в сети, вам следует пересмотреть политику безопасности с учетом возможностей Windows 2000, Некоторые новые технологии сетевой зашиты Windows 2000, возможно, заставят вас переделать план безопасности. По мере разработки плана сетевой безопасности вам следует:

- выявить ситуации, когда возможен риск снижения сетевой безопасности;
- определить размер сервера и требования размещения;
- подготовить персонал;
- создать и опубликовать политики и процедуры безопасности;
- использовать формальную методологию для создания плана безопасности;
- определить группы пользователей, их нужды и риски снижения безопасности.

Выявление ситуации, когда возможен риск снижения сетевой безопасности

Совместное использование и получение безопасности — очень удобная возможность, однако при этом надо учесть и риск снижения безопасности (табл.14-1).

Табл. 14-1. Риски снижения сетевой безопасности

Риск снижения безопасности	Описание
Перехват реквизитов пользователя	Нарушитель получает имя и пароль действительного пользователя. Это можно осуществить как при общении с пользователями, так и техническими способами
Маскировка	Нарушитель маскируется под действительного пользователя. Например, пользователь присваивает IP-адрес надежной системы и с его помощью получает права доступа, предназначенные соответствующему устройству или системе
Атака повтора	Нарушитель записывает сетевой обмен между пользователем и сервером и затем воспроизводит его, чтобы выдать себя за пользователя
Перехват данных	Если данные перемешаются по сети в виде открытого текста, нарушители могут отследить и перехватить их

Табл. 14-1. Риски снижения сетевой безопасности *(окончание)*

Риск снижения безопасности	Описание
Манипулирование	Нарушитель изменяет или повреждает сетевые данные. Незашифрованные сетевые финансовые транзакции доступны для манипулирования. Вирусы могут повредить сетевые данные
Отказ	Основанные на работе в сети деловые или финансовые транзакции подвергаются риску, если получатель транзакции не способен идентифицировать автора сообщения
Макровирусы	Вирусы приложений, использующие макроязык сложных документов
Отказ в обслуживании	Нарушитель бомбардирует сервер запросами, потребляющими системные ресурсы, и либо выводит сервер из строя, либо не позволяет выполнять нужную работу. Вывод сервера из строя иногда позволяет проникать в систему
Злонамеренный изменяющийся код	Изменяющийся код автоматически выполняемых ActiveX-элементов или Java-программ, которые загружаются из Интернета
Неверное использование прав	Системный администратор сознательно или ошибочно использует полные права работы с ОС для получения частных данных
Троянский конь	Это общий термин для наносящей вред программы, маскирующейся под полезную утилиту
Социальная атака	Иногда доступ в сеть удается получить, просто сообщив новым работникам, что вы из отдела автоматизации, и попросив их подтвердить свои пароли

Иногда конкуренты пытаются получить доступ к информации о запатентованных продуктах или несанкционированные пользователи портят Web-страницы или перегружают компьютеры так, что они выходят из строя. Кроме того, служащие могут получить доступ к конфиденциальной информации. Важнейшая задача — предотвращение этих рисков.

Сетевая аутентификация

Аутентификация — это процесс определения пользователей, пытающихся подключиться к сети. Пользователи, *аутентифицированные* в сети, могут использовать *сетевые ресурсы* на основе своих прав доступа. Для проверки подлинности сетевых пользователей создаются учетные записи. Это важнейшая часть управления безопасностью. Без аутентификации ресурсы, например файлы, доступны любым *пользователям*.

План сетевой безопасности

Для обеспечения доступа к ресурсам и данным только санкционированных пользователей необходимо тщательно спланировать стратегию сетевой безопасности. Это также позволяет вести учет использования сетевых ресурсов. Основные этапы планирования стратегий сетевой безопасности изображены на рис. 14-1.

Подготовка персонала

Технологиями безопасности должны управлять надежные и опытные работники. Их задача _ объединять всю сеть и инфраструктуру сетевой безопасности так, чтобы исключить

слабые места в безопасности сети или сократить их количество. Они постоянно поддерживают целостность инфраструктуры сетевой безопасности, особенно при изменении среды и требований.

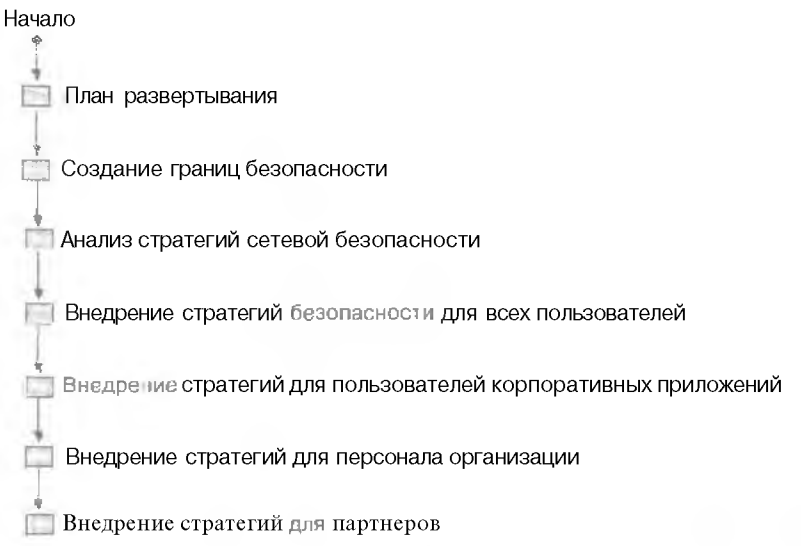


Рис. 14-1. Основные этапы планирования стратегий сетевой безопасности

Решающим фактором успешной работы вашего персонала по обеспечению безопасности работы в сети является постоянное совершенствование сотрудниками их навыков и знаний. Персонал должен изучить Windows 2000, в особенности технологии сетевой безопасности. Теоретические знания необходимо подкреплять практикой. Функции безопасности Windows 2000 описаны в табл. 14-2.

Табл. 14-2. Функции безопасности Windows 2000

Функция	Описание
Шаблоны безопасности	Позволяет администраторам настраивать глобальные и локальные параметры безопасности, включая важные для безопасности значения реестра, управление доступом к файлам и реестру и безопасность системных служб
Аутентификация Kerberos	Основной протокол безопасности для доступа внутри или через домены Windows 2000. Обеспечивает взаимную аутентификацию клиентов и серверов и поддерживает делегирование и авторизацию посредством прокси-механизмов
Инфраструктура открытого ключа (PKI)	Инфраструктура PKI применяется для надежной защиты служб Интернета и предприятий, включая основанные на экстрасетях коммуникации
Инфраструктурасмарт-карты	Windows 2000 имеет встроенную стандартную модель подключения устройств чтения смарт-карт и самих карт к компьютеру, а также не зависящие от устройств интерфейсы программирования приложений, работающих со смарт-картами

Табл. 14-2. Функции безопасности Windows 2000 *(окончание)*

Функция	Описание
Управление протоколом IPSec	Протокол IPSec поддерживает аутентификацию на уровне сети, целостность данных и шифрование для обеспечения надежности соединений интрасети, экстрасети и Интернета
Шифрование в файловой системе	Основанная на открытых ключах файловая система NTFS может быть активизирована на уровне файлов или подкаталогов основе

Хотя технологии безопасности могут быть очень эффективными, сама безопасность сочетает эти технологии с профессиональными навыками ведения бизнеса. Качество технологий безопасности зависит от применяемых методов.

Планирование распределенной сетевой безопасности

Распределенная сетевая безопасность подразумевает координирование многих функций безопасности в сети для создания полной политики безопасности. Распределенная безопасность позволяет пользователям регистрироваться в компьютерных системах, находить и применять нужную информацию. Большая часть информации в сетях доступна всем клиентам для чтения, но только небольшой группе людей позволено изменять ее. Если данные важные или частные, только санкционированным пользователям или группам разрешено считывать файлы. Защита и обеспечение конфиденциальности информации, передаваемой по телефонным сетям, Интернету и даже участкам внутренних сетей компании, также весьма сложны. Этот вопрос обсуждается далее на этом занятии и на занятии 2.

Типичный план безопасности включает разделы, показанные в табл. 14-3. Впрочем, план сетевой безопасности может содержать и дополнительные разделы.

Табл. 14-3. Разделы плана сетевой безопасности

Раздел плана	Содержание
Риски снижения безопасности	Типы рисков снижения безопасности предприятия
Стратегии безопасности	Основные стратегии безопасности, необходимые для защиты от рисков
Политики PKI	Планы развертывания сертификационных центров для внутренних и внешних функций безопасности
Описания групп безопасности	Описания групп безопасности и их отношения между собой. Этот раздел связывает политики групп и группы безопасности
Групповая политика	Описание параметров безопасности групповой политики, например политик сетевого пароля
Стратегии регистрации в сети и аутентификации	Политики аутентификации для регистрации в сети и для использования удаленного доступа и смарт-карты для входа. Подробнее об этом — на занятии 2
Стратегии безопасности информации	Описание обеспечения безопасности информации, например, безопасности электронной почты и Web-соединений
Политики администрирования	Политики делегирования административных заданий и отслеживание журналов аудита для определения подозрительныхдействий

Кроме того, вашей организации иногда требуется более одного плана безопасности. Количество планов зависит от размера организации. Например, международной организации нужен отдельный план для каждого подразделения, а локальной — один план всего. Компаниям с разграниченными политиками для различных групп пользователей может потребоваться отдельный план для каждой группы.

Тестирование плана безопасности

Необходимо всегда проверять планы безопасности в лабораторных условиях, имитирующих вашу организацию. Кроме того, стоит выполнить пилотные программы для совершенствования плана безопасности.

Параметры подключения к Интернету

Сейчас большинство организаций стремится подключиться к Интернету. Этот уникальный информационный канал позволит сотрудникам общаться с людьми из разных стран мира посредством электронной почты и получать информацию и файлы из многих источников. Кроме того, клиенты вашей организации смогут в любое время получать предоставляемую вашей фирмой информацию и услуги, персонал — использовать ресурсы компании дома, в отеле и т. д., а партнеры — более эффективно сотрудничать с вашей компанией. Между тем, доступные через Интернет службы иногда применяются не по назначению, что заставляет реализовать стратегии сетевой безопасности.

Установка брандмауэра

Для обеспечения безопасной работы вашей организации в Интернете необходимо установить брандмауэр (рис. 14-2). Он уменьшает риск подключения к Интернету, а также препятствует получению доступа к нашему компьютеру из Интернета, за исключением компьютеров, имеющих право такого доступа.

Рис. 14-2. Брандмауэр

Брандмауэр использует фильтрование пакетов для разрешения или запрещения потока определенных видов сетевого трафика. Фильтрование пакетов IP позволяет вам точно определить, какой IP-трафик может пересекать брандмауэр. Эта функция важна при подключении частных сетей к общедоступным сетям, например к Интернету. Многие брандмауэры способны распознавать и отражать сложные атаки.

Брандмауэры часто выступают в роли прокси-серверов или маршрутизаторов, потому что они передают трафик между частной и общей сетями. Программное обеспечение брандмауэра или прокси-сервера проверяет все сетевые пакеты каждого интерфейса и определяет адрес их места назначения. Если они соответствуют определенному заданному критерию, то пакеты передаются получателю другого сетевого интерфейса. Брандмауэр может просто маршрутизировать пакеты или действовать как прокси-сервер и переводить IP-адреса частной сети.

Microsoft Proxy Server

Обеспечивает как функции прокси-сервера, так и некоторые функции брандмауэра. Proxy Server выполняется на компьютерах с Windows 2000, и оба они должны быть настроены так, чтобы обеспечивать полную сетевую безопасность. Если у вас установлена более ранняя, чем 2.0, версия Proxy Server и Service Pack 1, необходимо обновить ее для совместимости с Windows 2000 — это делается в момент обновления сервера ло Windows 2000

Зачастую один прокси-сервер не способен справиться с объемом трафика между сетью организации и Интернетом. В этих случаях применяются несколько прокси-серверов. Трафик распределяется между ними автоматически. Пользователям Интернета и интрасети кажется, что существует единственный прокси-сервер.

Примечание За дополнительной информацией **о Proxy** Server **и технологиях безопасности** обращайтесь по адресу *http://windows.microsoft.com/windows2000/reskit/webresources.*

После установки прокси-сервера, настройки параметров контроля и подготовки персонала пришло время подключать сеть к внешней сети. Вы должны убедиться, что доступны только службы, которые вы санкционировали, и риск злоупотреблений практически отсутствует. Эта среда требует тщательного контроля и поддержки, но вы также будете готовы к предоставлению других служб сетевой безопасности.

Резюме

Необходимо планировать стратегии безопасности, чтобы только санкционированные пользователи получали доступ к ресурсам и данным сети. Следует внедрять технологии безопасности, подходящие для вашей организации, и всегда тестировать планы сетевой безопасности в лабораторных условиях, имитирующих условия вашей организации. Чтобы обезопасить доступ сети вашей организации в Интернет, можно использовать брандмауэр. Proxy Server на компьютере с Windows 2000 Server выполняет функции прокси-сервера и брандмауэра.

Занятие 2. Настройка безопасности RAS

Удаленный доступ позволяет клиентам подключаться к сети с удаленного компьютера с помощью различных аппаратных устройств, включая карты сетевого интерфейса и модемы. Получив соединение удаленного доступа, клиенты могут использовать сетевые ресурсы, например, файлы, так же как они использовали бы клиентский компьютер, напрямую подключенный к ЛВС. Здесь рассказывается о конфигурировании безопасности для удаленного доступа к сети.

Изучив материал этого занятия, вы сможете:

- ✓ создать политику удаленного доступа;
- ✓ сконфигурировать безопасность удаленного доступа, протоколы шифрования и аутентификации;
- ✓ настроить безопасность сетевого протокола и устранить неполадки.

Продолжительность занятия - около 60 минут.

Знакомство с удаленным доступом

Routing and Remote Access (RRAS) — это служба, позволяющая удаленным пользователям подключиться к локальной сети по телефону. Удаленный доступ позволяет несанкционированным пользователям проникнуть в сеть, поэтому Windows 2000 предлагает ряд мер безопасности для обеспечения защиты сети. При установке удаленного соединения с сервером клиент получает доступ к сети, если:

- запрос соответствует одной из политик удаленного доступа, заданных для сервера;
- учетная запись пользователя активизирована для удаленного доступа;
- аутентификация клиент/сервер завершена успешно.

Доступ клиента к сети может быть ограничен для определенных серверов, подсетей и типов протоколов в зависимости от клиентского профиля удаленного доступа. В противном случае все службы, обычно доступные для подключенного к ЛВС пользователя (включая совместное использование файлов и принтеров, доступ к Web-серверу и доставке сообщений), активизированы посредством соединения удаленного доступа.

Настройка протоколов безопасности

Предположим, некто может перехватить имя пользователя и пароль в момент подключения к серверу RRAS, используя технологии, аналогичные перехвату телефонных разговоров. Для предотвращения этой ситуации в RRAS предусмотрен безопасный метод аутентификации пользователя.

- **Challenge Handshake Authentication Protocol (CHAP).** Протокол CHAP разработан для управления передачей паролей в открытом тексте, CHAP — это наиболее популярный протокол аутентификации. Поскольку алгоритм вычисления откликов протокола CHAP хорошо известен, необходимо тщательно подбирать и задавать достаточно длинные пароли. CHAP-пароли, являющиеся обычными словами или именами, легко вычисляются с помощью словаря путем сравнения откликов CHAP с каждым словом в словаре. Недостаточно длинные пароли выявляются сравнением CHAP-откликов с откликами пользователя (эта операция выполняется до тех пор, пока не найдено совпадение).
- **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).** Протокол MS-CHAP представляет собой разновидность протокола CHAP, которой не требуется пароль в виде

открытого текста на сервере аутентификации. MS-CHAP-пароли хранятся на сервере в большей безопасности, но доступны вычислению так же, как и CHAP-пароли. В протоколе MS-CHAP ответ на запрос вычисляется с помощью Message Digest 4 (MD4)-хешируемой версии пароля и ответа *сервера доступа к сети* (Network access server, NAS). Это активизирует аутентификацию по Интернету на контроллер домена Windows 2000 (или на контроллер домена Windows NT 4.0, на котором не было выполнено обновление).

- **Password Authentication Protocol (PAP).** Протокол PAP передает пароль в виде строки от пользовательского компьютера устройству NAS. Когда NAS передает пароль, он шифрует его с применением секретного ключа протокола RADIUS в качестве ключа шифрования. PAP — это наиболее гибкий протокол, потому что передача пароля в виде открытого текста серверу аутентификации позволяет серверу сравнить пароль практически с любым форматом хранения. Например, пароли ОС UNIX хранятся в виде зашифрованных строк, которые не могут быть расшифрованы. PAP-пароли можно сравнить с этими строками путем воспроизведения метода шифрования. Поскольку протокол PAP использует пароль в виде открытого текста, его безопасность уязвима. Хотя протокол RADIUS шифрует пароль, он передается через удаленное соединение в виде открытого текста.
- **Shiva Password Authentication Protocol (SPAP).** SPAP — это механизм двустороннего шифрования, применяемый серверами удаленного доступа Shiva. Клиент удаленного доступа может использовать SPAP для собственной аутентификации на удаленном сервере Shiva. Клиент удаленного доступа с 32-разрядной ОС Windows 2000 может применять SPAP для собственной аутентификации на удаленном сервере Windows 2000. SPAP более надежен, чем PAP, но менее надежен, чем CHAP или MS-CHAP. SPAP не имеет защиты против олицетворения удаленного сервера.

Как и PAP, SPAP — это простой обмен сообщениями. Сначала клиент удаленного доступа посылает сообщение Authenticate-Request (Запрос аутентификации) серверу удаленного доступа, содержащему клиентское имя пользователя и зашифрованный пароль. Затем сервер удаленного доступа расшифровывает пароль, проверяет имя пользователя и пароль и возвращает либо сообщение Authenticate-Ack (Аутентификация прошла), когда информация пользователя верна, либо сообщение Authenticate-Nak (Аутентификация не прошла) с объяснением причины, почему информация пользователя неверна.

- **Extensible Authentication Protocol (EAP).** Это расширение протокола PPP, позволяющее применять произвольные механизмы аутентификации для подтверждения соединения PPP. При использовании таких протоколов аутентификации PPP, как MS-CHAP и SPAP, на этапе установки соединения выбирается определенный механизм аутентификации. Затем на этапе аутентификации соединения используется согласованный протокол аутентификации для подтверждения соединения. Протокол аутентификации — это фиксированные наборы сообщений, посылаемых в определенном порядке. EAP разработан для аутентификации подключаемых модулей как клиента, так и сервера. Путем установки библиотечного EAP-файла на клиенте удаленного доступа и сервере удаленного доступа может поддерживаться новый тип EAP. Это позволяет продавцам в любое время поставлять новую схему аутентификации. EAP обеспечивает наибольшую гибкость аутентификации уникальности и изменений.

Практикум: использование протоколов безопасности для VPN

► **Задание: активизируйте сервер VPN для использования аутентификации CHAP**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Routing and Remote Access.
2. Щелкните правой кнопкой мыши имя сервера, для которого хотите активизировать протоколы аутентификации, и в контекстном меню выберите пункт Properties (Свойства). Откроется диалоговое окно свойств сервера.
3. На вкладке Security (Безопасность) щелкните кнопку Authentication Methods (Методы проверки подлинности).
   Откроется одноименное окно.
4. Пометьте флажок Encrypted Authentication (Шифрованная проверка подлинности) и щелкните OK (рис. 14-3).
5. Чтобы закрыть диалоговое окно свойств сервера, щелкните OK.

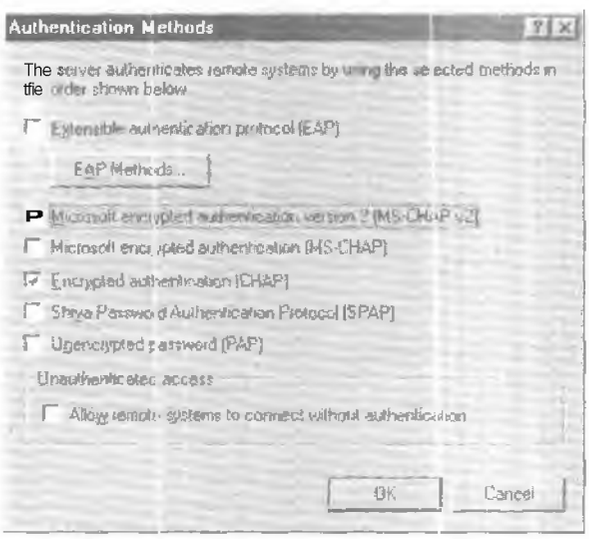


Рис. 14-3. Использование метода аутентификации CHAP

Создание политик удаленного доступа

Службы RRAS и Internet Authentication Service (IAS) используют политики удаленного доступа для разрешения или запрещения подключения. В обоих случаях политики удаленного доступа хранятся локально и определяют правила на уровне отдельных подключений.

При использовании политик удаленного доступа вы можете предоставить или запретить авторизацию в зависимости от времени суток или дня недели, от группы, к которой принадлежит удаленный пользователь, и типа запрашиваемого соединения (удаленная сеть или VPN) и т. д.

Локальное и централизованное управление политиками

Поскольку политики удаленного доступа хранятся локально на сервере удаленного доступа или IAS-сервере, для централизованного управления одним набором политик для не-

скольких серверов удаленного доступа или VPN-серверов выполните действия, описанные ниже.

1. Установите на компьютер IAS в качестве RADIUS-сервера.
2. Сконфигурируйте IAS для RADIUS-клиентов для каждого сервера удаленного доступа или VPN-сервера.
3. На IAS-сервере создайте основной набор политик, используемых всеми серверами удаленного доступа.
4. Сконфигурируйте каждый сервер удаленного доступа в качестве RADIUS-клиента для IAS-сервера.

После этого локальные политики удаленного доступа, хранящиеся на сервере удаленного доступа, не будут использоваться. Централизованное управление политиками удаленного доступа применяется так же, когда серверы удаленного доступа работают пол управлением Windows NT 4.0 и имеют службу RRAS. Вы вправе сконфигурировать Windows NT 4.0-сервер, имеюший службу RRAS, в качестве RADIUS-клиента для IAS-сервера. Вы не можете сконфигурировать сервер удаленного доступа под управлением Windows NT 4.0, не имеюший службы RRAS, для использования централизованных политик удаленного доступа.

Использование протоколов шифрования

Шифрование применяется для защиты данных, пересылаемых между клиентом и сервером удаленного доступа. Шифрование данных важно для финансовых институтов, правительственных и других организаций, требуюших безопасной передачи данных. Если требуется сохранение конфиденциальности данных, сетевой администратор может настроить сервер удаленного доступа, что бы он требовал зашифрованных соединений. Пользователям, подключающимся к такому серверу, придется шифровать их данные, иначе доступ будет запрещен.

Для VPN-соединений вы защищаете данные, шифруя их между конечными точками сети VPN. Для VPN-соединений всегда следует *шифровать* данные при передаче их по общедоступной сети, например по Интернету, так как присутствует риск несанкционированного доступа.

Для удаленных сетевых соединений можно защитить данные, шифруя их при передаче по линии связи между клиентом и сервером удаленного доступа. Шифрование следует использовать, если существует риск *перехвата* данных. Для удаленных соединений существуют два вида шифрования: MPPE и IPSec.

- **MPPE.** Все PPP-соединения, включая PPTP, кроме L2TP могут использовать MPPE. MPPE применяет шифр потока RSA RC4 и действует только совместно с методами аутентификации TLS или MS-CHAP (версии 1 или 2). MPPE может использовать 40-, 56- или 128-разрядные ключи шифрования: 40-разрядный ключ предназначен для обратной совместимости и международного использования; 56-разрядный ключ — для международного использования и подчиняется американским законам экспорта шифрования; 128-разрядный ключ действует в Северной Америке. По умолчанию в процессе установки соединения выбирается наибольшая длина ключа, поддерживаемая вызывающим и отвечающим маршрутизаторами. Если отвечающий маршрутизатор требует ключ большей длины, чем поддерживаемый вызывающим маршрутизатором, доступ запрещается.

Примечание Для удаленных сетевых подключений Windows 2000 использует MPPE.

- **IPSec.** Для соединений по требованию, применяющих L2TP поверх IPSec, шифрование определяется путем генерации *сопоставления безопасности* (security association, SA). Доступные алгоритмы шифрования включают DES с 56-разрядным ключом и 3DES, использующий 56-разрядный ключ и предназначенный для высоконадежных сред. Начальные ключи шифрования поступают от процесса аутентификации IPSec.

Для VPN-соединений Windows 2000 применяет MPPE с протоколом PPTP и шифрование IPSec с протоколом L2TP.

▶ **Настройка шифрования для удаленного подключения**

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните Routing and Remote Access (Маршрутизация и удаленный доступ).
2. В списке имен сервера щелкните Remote Access Policies (Политики удаленного доступа).
3. На правой панели щелкните правой кнопкой политику удаленного доступа, которую хотите конфигурировать, и выберите в контекстном меню команду Properties (Свойства).
4. Щелкните кнопку Edit Profile (Изменить профиль).
5. На вкладке Encryption (Шифрование) задайте нужные параметры (рис. 14-4) и щелкните OK.
6. Щелкните OK, чтобы закрыть диалоговое окно свойств.

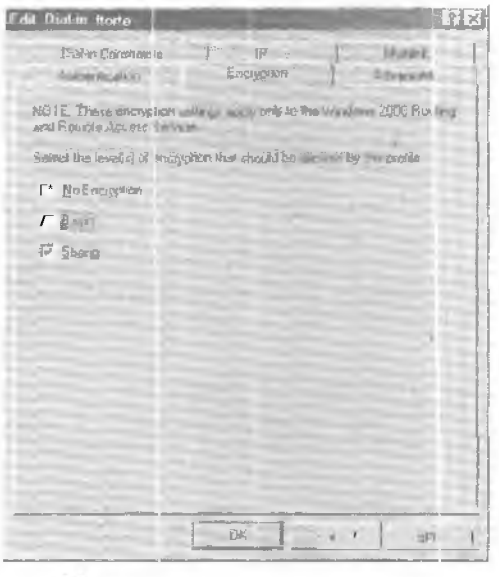


Рис. 14-4. Настройка уровня шифрования

Резюме

Удаленный доступ позволяет клиентам подключиться к сети с удаленного компьютера посредством аппаратных устройств, в том числе карт сетевых интерфейсов и модемов. После установки удаленного соединения клиент может использовать сетевые ресурсы, например, файлы, так, будто клиентский компьютер напрямую подключен к ЛВС. В Windows 2000 создаются политики удаленного доступа, которые затем конфигурируются для обеспечения безопасности. Для удаленного доступа разрешается задать уровень шифрования и разрешения.

Занятие 3. Наблюдение событий безопасности

Политики администрирования для плана безопасности включают политики делегирования административных заданий и проверку журналов аудита для обнаружения подозрительных действий. Здесь рассказывается о том, как отслеживать события безопасности, чтобы предотвратить проникновение в сеть извне.

Изучив материал этого занятия, вы сможете:

- ✓ управлять и отслеживать сетевой трафик;
- ✓ управлять и отслеживать удаленный доступ.

Продолжительность занятия — около 45 минут.

Наблюдение за сетевой безопасностью

Технологии сетевой безопасности обеспечат надежную зашиту сети только в случае их тщательного планирования и конфигурирования. Тем не менее предвидеть все риски сложно, так как:

- возникают новые риски;
- системы могут выходить из строя, и среда, в которой они функционируют, меняется.

Для контроля сетевой безопасности вам необходимы средства для получения информации о действиях и анализа данных. Например, Microsoft Proxy Server поддерживает протоколирование на двух уровнях: обычное и подробное. Windows 2000 включает также протоколирование событий, которое можно дополнить активизацией аудита безопасности. IAS, обсуждаемый далее в этой главе, имеет дополнительные опции отчетов о деятельности. Существуют также продукты других фирм, помогающие наблюдать за серверами и приложениями, включая серверы и приложения безопасности.

Примечание При использовании серверов и приложений безопасности изучите документацию по применяемым системам и выберите параметры протоколирования, лучше всего соответствующие вашим требованиям.

Использование оснастки Event Viewer для наблюдения за безопасностью

Оснастка Event Viewer (Просмотр событий) позволяет отслеживать события в системе. Она поддерживает на компьютере журналы с информацией о событиях программ, безопасности и системных событиях. Event Viewer применяется для просмотра и управления журналами событий, сбора информации и аппаратных и программных сбоях и отслеживания событий безопасности. Служба Event Log запускается автоматически при запуске Windows 2000. Все пользователи могут просматривать журналы приложений и системы. Вы вправе также настроить ОС Windows для аудита доступа к определенным ресурсам и для записи их в журнал безопасности. В табл. 14-4 приведен список доступных для аудита событий, а также перечислены ситуации, когда возникает угроза безопасности, которые отслеживают события аудита.

Табл. 14-4. Угрозы безопасности, обнаруженные посредством аудита

Событие	Возможная угроза
Неудачный вход-выход	Произвольный подбор пароля
Успешный вход-выход	Вход по украденному паролю
Изменение прав пользователей, управление пользователем и группой, изменение политики безопасности, перезагрузка, завершение работы	Неверное использование привилегий
Доступ к файлам и объектам, чтение-запись важных файлов подозрительными пользователями или группами	Неверный доступ к важным файлам
Доступ к принтерам и объектам подозрительных пользователей или групп в диспетчере печати	**Неверный** доступ к принтерам
Запись в программные файлы (с расширениями .exe и .dll) и наблюдение за процессами. Запуск подозрительных программ. (Проверьте журнал безопасности на предмет неожиданных попыток изменения программных файлов или создания неожиданных процессов.)	Результат действия вируса

Практикум: запись неудачных попыток входа

По умолчанию аудит безопасности отключен. Вы должны активизировать нужные типы аудита, воспользовавшись оснасткой Group Policy (Групповая политика). Стоит также включить аудит для общих областей или определенных событий, которые вы хотите отслеживать.

▶ **Задание: активизируйте аудит неудачных попыток** входа

1. В меню Start (Пуск) выберите команду Run (Выполнить), введите команду **mmc** и щелкните OK.
2. В меню Console (Консоль) щелкните Add/Remove Snap-In (Добавить/Удалить оснастку), затем — кнопку Add (Добавить).
   Откроется одноименное окно.
3. Щелкните кнопку Add.
   Откроется диалоговое окно Add Standalone Snap-In (Добавить изолированную оснастку).
4. Выберите Group Policy (Политика группы) и щелкните кнопку Add.
   Откроется диалоговое окно Select Group Policy (Выбор объекта групповой политики).
5. Чтобы добавить локальный компьютер, щелкните кнопку Finish (Закончить).
   Вы можете также щелкнуть кнопку Browse (Просмотреть) и выбрать другой компьютер сети.
6. В диалоговом окне Add Standalone Snap-In щелкните кнопку Close (Закрыть).
7. В диалоговом окне Add/Remove Snap-In щелкните OK.
8. Раскройте узел Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies (Политика «Локальный компьютер»\Конфигурация компьюте-

ра\Конфигурация Windows\ Параметры безопасности\Локальные политики) и щелкните Audit Policy (Политика аудита) (рис. 14-5).

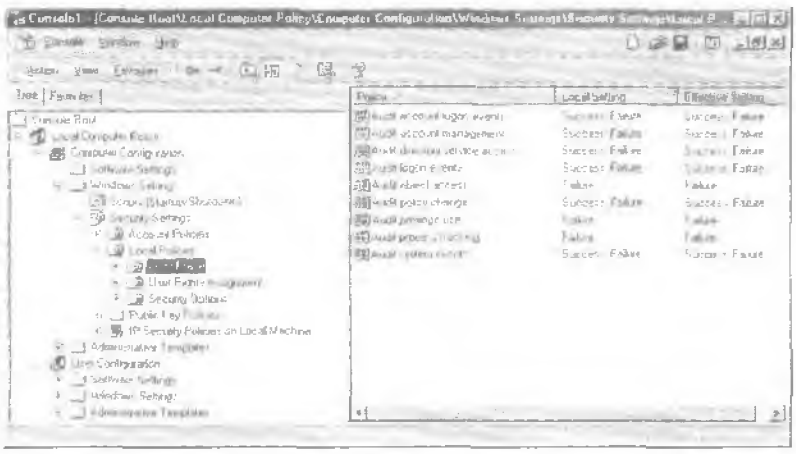


Рис. 14-5. Выбор политики аудита для политики локального компьютера

9. На правой панели дважды щелкните Audit Logon Events (Аудит событий входа в систему). Откроется диалоговое окно Local Security Policy Setting (Параметр локальной политики безопасности).
10. В области Audit These Attempts (Вести аудит следующих попыток доступа) выберите Failure (Отказ) и щелкните OK.

Просмотр журнала событий безопасности

Вы можете задать запись событий в журнал событий безопасности в момент выполнения определенных действий или доступа к файлам. Запись аудита показывает выполняемое действие, его дату и время, имя выполнившего его пользователя. Вы можете выявлять кик успешные, так и неудачные попытки, так что аудит покажет, кто пытался выполнить несанкционированные действия. Журнал безопасности просматривают средствами Event Viewer.

Запись событий безопасности — это форма обнаружения вмешательства посредством аудита. Аудит и протоколирование сетевой деятельности являются важными мерами предосторожности. Windows 2000 позволяет наблюдать за множеством событий, которые можно использовать для выявления несанкционированных действий в сети.

Журнал безопасности записывает такие события безопасности, как успешные и неудачные попытки входа, а также события, связанные с использованием ресурсов, например, созданием, открытием или удалением файлов и других объектов. Журнал безопасности помогает выявлять изменения в системе безопасности. Например, в журнале безопасности записаны попытки входа в систему, если включен аудит входа и выхода. Регулярный просмотр журнала безопасности позволяет обнаружить некоторые типы атак до того, как они станут успешными. После проникновения в систему журнал безопасности позволит определить, как нарушитель проник в систему и что он сделал. Записи журнала служат доказательством вины нарушителя.

Примечание Для обеспечения безопасности регулярно просматривайте журналы.

Практикум: просмотр журнала безопасности

Журналы событий состоят из заголовка, описания события (основанного на типе события) и необязательных дополнительных данных. Большинство записей журналов безопасности состоит из заголовка и описания. Event Viewer отображает события каждого журнала отдельно. Каждая строка показывает информацию об одном событии, включая дату, время, источник, тип события, категорию, идентификатор события, учетную запись пользователя и имя компьютера. Просмотрите журнал событий безопасности для определения попыток несанкционированного доступа к сети. Для выполнения этого задания вы должны выполнить предыдущее.

▶ **Задание: просмотрите журнал событий безопасности**

1. Попытайтесь войти в компьютер, на котором установлен аудит неудачных попыток входа, воспользовавшись недействительным именем и паролем.
2. После неудачной попытки войдите в компьютер с действительным именем и паролем.
3. Раскройте меню Start\Programs\Administrative Tools и щелкните Event Viewer.
4. В дереве консоли щелкните Security Log (Журнал безопасности).

   Заметьте; неудачные попытки входа показаны в правой панели окна Event Viewer (рис.14-6).
5. Дважды щелкните значок события, чтобы открыть окно его свойств.

   Заметьте: раздел описания отображает причину неудачи и введенное имя пользователя, но не отображает введенный пароль.
6. Щелкните OK, чтобы закрыть окно свойств события.

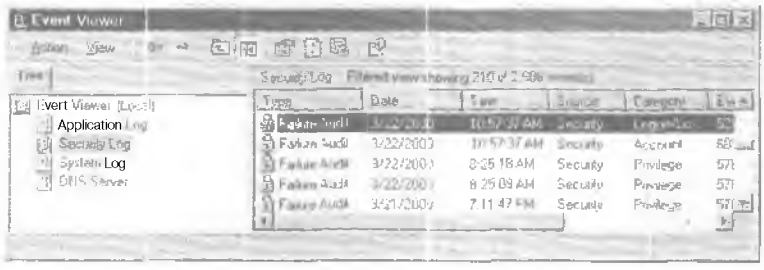


Рис. 14-6. Запись попытки неудачного входа в журнале безопасности

Утилита System Monitor

System Monitor (Системный монитор) — это инструмент, позволяющий контролировать использование системных ресурсов как приложением, так и клиентом (памяти, центрального процессора, сети и диска). Дополнительные счетчики, не связанные с производительностью, сообщают важную информацию о безопасности сервера, в том числе:

- Server\Errors Access Permissions (Сервер\Ошибок отсутствия права доступа);
- Server\Errors Granted Access (Сервер\Ошибок предоставленного доступа);
- Server\Errors **Logon (Сервер\Ошибок** входа);
- IIS Security.

▶ **Просмотр событий безопасности средствами** System **Monitor**

f. Раскройте меню Start\Programs\Adminstrative Tools (Пуск\Программы\Администрирование) и щелкните Performance (Системный монитор).

2. На панели оснастки щелкните кнопку Add (Добавить).
   Откроется диалоговое окно Add Counters (Добавить счетчики) (рис. 14-7).
3. В списке Performance Object (Объект) выберите Server (Сервер).
4. Щелкните Select Counters From List (Выбрать счетчики из списка).
5. Выберите счетчик и щелкните кнопку Add.
6. Щелкните кнопку Close (Закрыть), чтобы закрыть диалоговое окно Add Counters

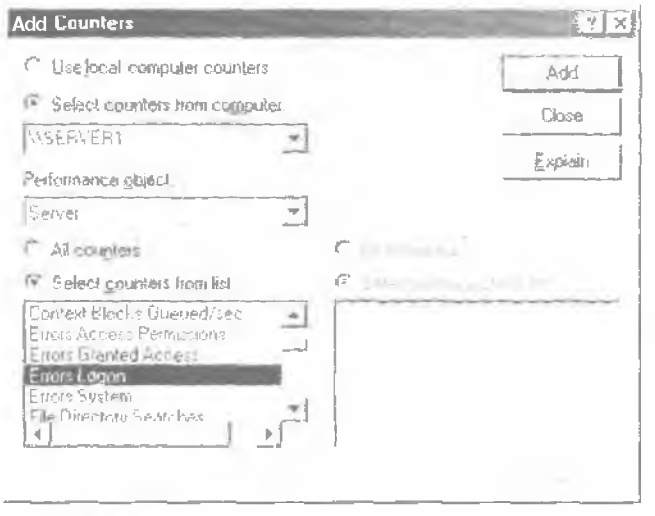


Рис. 14-7. Добавление счетчика Error Logon (Ошибок входа)

Утилита IPSec Monitor

Утилита IPSec Monitor (Монитор безопасности IP) подтверждает надежность защиты сети посредством отображения активных SA на локальных или удаленных компьютерах. Например, IPSec Monitor используется, чтобы определить, имел ли место отказ аутентификации или SA, указывая на несовместимость локальных политик безопасности. IPSec Monitor выполняется на локальном или удаленном компьютере.

Работа с IPSec Monitor

1. Щелкните кнопку Start (Пуск) и в меню выберите команду Run (Выполнить).
2. Введите **ipsecmon** *<имя_компьютера>* и щелкните OK.
   Откроется диалоговое окно Security Monitor (Монитор безопасности) (рис.14-8). Запись отображается для каждого активного SA. Каждая запись включает имя активной политики IPSec, имя фильтра IP и конечную точку туннеля (если она была задана).
3. Щелкните кнопку Options (Параметры), чтобы задать частоту обновления.

IPSec Monitor также полезен в настройке производительности и устранении неполадок, предлагая такие сведения, как:

- количество и тип активных SA;
- общее количество основных и сеансовых ключей. Успешные SA первоначально создают один главный ключ и один сеансовый ключ. Последующие регенерации ключей отображаются как дополнительные сеансовые ключи;
- общее количество полученных-отправленных конфиденциальных или аутентифицированных байт.

Рис. 14-8. Интерфейс **IP Security Monitor (Монитор безопасности IP)**

Накладные расходы при внедрении безопасности

Безопасность достигается путем неизбежного снижения производительности системы. Вычисление накладных расходов стратегии безопасности — не только вопрос выявления определенного процесса или риска. Функции модели безопасности Windows 2000 и другие службы безопасности встроены в некоторые другие службы ОС. Нельзя изменять параметры безопасности отдельно от других параметров служб. Вместо этого чаше определяются накладные расходы безопасности посредством выполнения тестов, сравнивающих производительность сервера с применением функций безопасности и без него. Необходимо выполнять тесты с одной и той же нагрузкой и конфигурацией сервера, меняя только параметры безопасности.

Во время тестон нужно определить:

- работу и очередь процессора;
- используемое ОЗУ;
- сетевой трафик:
- задержки.

Резюме

Необходимо выявлять события сетевой безопасности для определения слабых мест в защите сети. пока ими не воспользовался злоумышленник. Для этого применяется оснастка Event Viewer. Запись в журнале показывает выполненное действие, его дату и время. имя выполнившего его пользователя. Утилиты System Monitor и Network Monitor предоставляют необходимые сведения о безопасности сервера. Утилита IPSec Monitor показывает. надежно ди защищена сеть. Можно также использовать службу Routing and Remote Access лдя выявления удаленного трафика и активизации протоколирования для просмотра этих данных.

Закрепление материала

? Приведенные ниже вопросы помогут вам лучше усвоить основные темы данной главы. Если вы не сумеете ответить на вопрос, повторите материал соответствующего занятия. Правильные ответы см. в приложении «Вопросы и ответы» в конце книги.

1. Какие потенциальные ситуации, при которых возникает риск снижения безопасности, следует предусмотреть в плане защиты?

2. Что такое аутентификация и как ее внедрить?

3. Назовите некоторые функции безопасности Windows 2000.

4. Как обезопасить подключение сети к Интернету?

5. Назовите некоторые протоколы удаленного доступа для обеспечения безопасности.

6. Назовите две формы шифрования для соединений по требованию.

7. Каким образом утилиты System Monitor и Network Monitor позволяют контролировать безопасность сети?

8. Как Event Viewer используется для соблюдения мер безопасности?

9. Каким образом активизировать протоколирование удаленного доступа?

Приложение

Вопросы и ответы

Глава 1 Проектирование сети Windows 2000

Закрепление материала

стр. 17

1. Предположим, вы вручную настраиваете TCP/IP для новых компьютеров и компьютеров, перемещенных из одном полсети в другую. Вы хотите упростить управление TCP/IP адресами и и назначать их автоматически. Какая сетевая служба Windows 2000 для этого применяется?

   Для автоматизации выделения и централизованного управления адресами TCP/IP применяется служба **DHCP.**

2. У вас имеется сервер с процессором Alpha. ОЗУ объемом Я Гб и восемью процессорами. Вы хотите предоставить службу доступа к файлам 400 членам вашего предприятия. Какую ОС Windows 2000 лучше выбрать для этого и почему?

   Лучше использовать ОС Windows 2000 Advanced Server, **поддерживающую балансировку** сетевой **нагрузки и корпоративную** архитектуру **памяти. Windows** 2000 **Server поддерживает только** 2 **Гб** оперативной **памяти, поэтому не удовлетворяет требованиям.**

3. Вы хотите подключить сервер Windows 2000 к сети Macintosh, использующей протокол AppteTalk, и обеспечить ее маршрутизацию. Какой протокол следует установить?

   AppleTalk. Windows 2000 поддерживает весь стек протоколов AppleTalk н программные средства маршрутизации, то есть сервер Windows 2000 теперь может подключаться к сетям Macintosh и обеспечивать для них маршрутизаиню.

Глава 2 Внедрение TCP/IP

Закрепление материала

стр. 44

1. Опишите пакет протоколов TCP/IP.

   TCP/IP — это набор протоколов, обеспечивающих маршрутизацию в ГВС и подключение к различным узлам в Интернете.

2. Назовите утилиты TCP/IP, используемые для проверки и тестирования конфигурации протокола TCP/IP.

Утилиты ping и Ipconfig.

3. Опишите назначение маски подсети.

   Маска подсети скрывает часть IP-адреса, позволяя выделить из него идентификаторы сети и узла.

4. Назовите минимальное число областей в промежуточной сети OSPF.

   Промежуточная сеть OSPF состоит минимум из одной области, называемой магистралью.

5. Что такое внутренний маршрутизатор?

   Это маршрутизатор, все интерфейсы которого подсоединены к одной области.

6. Что такое граничный маршрутизатор?

   Интерфейсы граничного маршрутизатора подсоединены к разным областям.

7. Назовите административную утилитуWindows 2000, позволяющую управлять внутренними и граничными маршрутизаторами.

   Оснастка Routing and Remote Access.

Глава 3. Внедрение NWLink

Закрепление материала

стр. 65

1. Что такое NWLink и какое отношение он имеет к Windows 2000?

   NWLink представляет собой реализацию протокола IPX/SPX фирмой Microsoft. Этот протокол используется службой шлюза и клиента для NetWare для соединения с сервером NetWare.

2. Что такое SPX?

   SPX — это транспортный протокол, предоставляющий службы, ориентированные на соединение, через IPX. Он используется утилитами, требующими непрерывного соединения. SPX обеспечивает надежную доставку данных за счет соблюдения последовательности передачи пакетов и запроса уведомлений о приеме каждого пакета. Кроме того, SPX поддерживает механизм передачи сгруппированных пакетов, при котором нет необходимости передавать все пакеты в определенной последовательности и получать подтверждение о приеме каждого пакета.

3. Что такое Gateway Service for NetWare?

   Служба Gateway Service for NetWare позволяет создать шлюз, через который компьютеры без клиентского ПО Novell NetWare способны получить доступ к файлам и принтерам в сетях NetWare.

4. Что надо принять во внимание при выборе между использованием Gateway Service for NetWare и Client Service for NetWare?

   Если вы собираетесь создать и какое-то время поддерживать неоднородную среду, включающую серверы Windows 2000 и NetWare, лучше выбрать службу клиента. Если вы планируете постепенно перейти с NetWare на Windows 2000 или желаете упростить администрирование, лучше выбрать службу шлюза.

5. Для чего предназначена функция автоопределения в NWLink?

   Она определяет тип кадров и номер сети в параметрах серверов NetWare локальной сети. Ее рекомендуют применять для настройки этих параметров на клиентских системах. Если некоторые из параметров для адаптера невозможно определить автоматически, их следует задать вручную.

Глава 4 Мониторинг сетевой активности

Закрепление материала

стр. 83

1. Какова цель анализа кадров с помощью Network Monitor?

   Анализ сетевых кадров позволяет выявить проблемы клиент-серверных соединений, найти компьютер, выполняющий несоразмерное число запросов, и устранить неполадки сети на прикладном уровне.

2. Какие данные содержат кадры?

   Каждый кадр содержит адреса отправителя и приемника, заголовки используемых протоколов и полезную информацию.

3. Что такое фильтр записи и для чего он используется?

   Фильтр записи работает как запрос к базе данных и используется для мониторинга сетевых данных. Например, для записи кадров, содержащих определённые адреса или заголовки определенных протоколов, необходимо создать БД адресов, добавить их к фильтру и сохранить фильтр в файле. Фильтры записи экономят пространство буфера и сокращают время анализа. Файл, в котором хранится фильтр записи, можно использовать в дальнейшем.

Глава 5 Внедрение IPSec

Занятие 3

Практикум: создание пользовательской политики IPSec

стр. 108

На данный момент вы еще не создали собственное правило, а лишь настроили свойства правила ответа, используемого по умолчанию.

Опишите назначение правила ответа по умолчанию.

Стандартное правило ответа разрешает согласование с компьютерами, запрашивающими IPSec. Оно добавляется к каждой созданной политике, но не активизируется автоматически. Стандартное правило отклика используется на незащищенных компьютерах, которые должны правильно реагировать, когда другой компьютер запрашивает безопасное соединение. Оно также может применяться как шаблон для создания пользовательских правил.

Закрепление материала

стр. 116

1. Какая организация стандартизовала протокол IPSec?

   Рабочая группа IETF IP Security.

2. Опишите отличия криптографии с секретным и открытым ключом.

   В криптографии на основе секретного ключа используется один общий ключ, а в криптографии на основе открытого ключа — пара ключей: одна — для шифрования данных и проверки цифровых подписей, а вторая — для расшифровки данных и создания цифровых подписей.

3. Назовите функции службы ISAKMP/Oakley.

   ISAKMP/Oakley формирует защищенный канал связи между двумя компьютерами и генерирует сопоставление безопасности.

4. Что включает в себя правило?

   Правило состоит из IP-фильтров, политик согласования, **методов** аутентификации, **атрибутов** IP-туннелирования **и типов** адаптера.

5. Когда надо использовать сертификат открытого ключа?

   Сертификат позволяет недоверенному компьютеру домена использовать IPSec для соединения с **доверенным компьютером домена.**

6. Для чего применяется IP-фильтр?

   IP-фильтры проверяют дейтаграммы на соответствие условиям, что позволяет отбирать **записи в зависимости от** адреса **отправителя и получателя, DNS-имени, протокола или** портов протокола.

Глава 6 Разрешение имен узлов в сети

Занятие 3

Практикум: работа с файлом HOSTS и DNS

▶ Задание 2: проверьте локальное имя узла с помощью ping

стр. **125**

1. Наберите ping **Server1** (где Server1 — имя вашего компьютера) и нажмите Enter. Каков отклик?

   Четыре сообщения «Reply from IP address».

▶ Задание 3: проверьте локальное имя компьютера с помощью ping

стр. 125

1. Введите **"ping computertwo** и нажмите клавишу Enter.

   Каков отклик?

   Сообщение «Bad IP address computertwo».

▶ Задание 5: используйте файл HOSTS для разрешения имени

стр. 125

1. Введите **'ping computertwo** и нажмите клавишу Enter.

   Каков отклик?

   Четыре сообщения «Reply from IP address».

Закрепление материала

стр. **126**

1. Что такое имя узла?

   Псевдоним, назначаемый узлу TCP/IP.

2. Каково назначение имени узла?

   Упрощает обращение к узлу. Имена узлов используются утилитой **ping и другими TCP/IP-приложениями.**

3. Из чего состоит запись файла HOSTS?

   Одно **или несколько имен узлов и соответствующий ему IP-адрес.**

4. Что происходит прежде всего в процессе разрешения имени: разрешение ARP или разрешение имени узла?

   Разрешение имени узла.

Глава 7. Внедрение DNS

Занятие 3

Сценарий 1. Проектирование DNS для небольшой сети

стр. 139

1. Сколько потребуется доменов DNS?

   Один (или ни одного, если поставщик услуг Интернета управляет сервером имен).

2. Сколько потребуется поддоменов?

   Ни одного.

3. Сколько потребуется зон?

   Одна (или ни одной, если поставщик услуг Интернета управляет сервером имен).

4. Сколько потребуется основных серверов?

   Один (или ни одного, если поставщик услуг Интернета управляет сервером имен).

5. Сколько потребуется дополнительных серверов?

   Один (или ни одного, если поставщик услуг Интернета управляет сервером имен).

6. Сколько потребуется серверов **кэширования?**

   Ни одного.

Сценарий 2. Проектирование DNS для сети среднего размера

стр. 140

1. Сколько потребуется доменов DNS?

   Необходимо выделить минимум один домен, который может содержать узлы (компьютеры или службы) и поддомены.

2. Сколько потребуется поддоменов?

   Три. Ваш домен DNS обслуживает несколько отделов, поэтому необходимо создать три поддомена, отражающих их группировку.

3. Сколько потребуется зон?

   Четыре. Выделив четыре зоны, можно распределить административные задачи между различными группами основных отделов. Это также улучшит распространение данных.

4. Сколько потребуется основных серверов?

   Четыре. Основные сайты осуществляют поддержку своего собственного оборудования и оборудования подключенных к ним подразделений. Следовательно, необходимо выделить четыре основных сервера имен.

5. Сколько потребуется дополнительных серверов?

   В филиалах — от 25 до 250 сотрудников, которым необходим доступ ко всем четырем основным сайтам. Дополнительный сервер позволяет разрешать имена в данной зоне при отказе основного сервера. Следовательно, необходимо выделить четыре дополнительных сервера.

6. Сколько потребуется серверов кэширования?

   Необходимо выделить 10 серверов только для кэширования (по одному на филиал). Это ускорит разрешение DNS-имен, сократит трафик, связанный с запросами DNS, и повысит надежность.

7. По данным таблицы расстояний спроектируйте размещение филиалов по зонам. Филиал должен быть в той же зоне, где ближайший головной офис.

Портленд	Бостон	Чикаго	Атланта
Лос-Анджелес	Монреаль	Денвер	Даллас
Солт-Лейк-Сити	Вашингтон	Канзас-Сити	Майами
Сан-Франциско			Новый Орлеан

Расстояние, миль	Атланта	Бостон	Чикаго	**Портленд**
Даллас	807	1817	934	2110
Денвер	1400	1987	1014	1300
Канзас-Сити	809	1454	497	1800
Лос-Анджелес	2195	3050	2093	1143
Майами	665	1540	1358	3300
Монреаль	1232	322	846	2695
Новый Орлеан	494	1534	927	2508
Солт-Лейк-Сити	1902	2403	1429	800
Сан-Франциско	2525	3162	2187	700
Вашингтон	632	435	685	2700

Сценарий 3. Проект DNS для большой сети

стр. 142

1. Сколько потребуется доменов DNS?

   Ни одного (домен этой компании находится в Женеве, в Швейцарии).

2. Сколько потребуется поддоменов?

   Одиннадцать. Помните, что необходимо предоставить контроль за оборудованием каждому филиалу и в каждом из них создать ресурсный домен.

3. Сколько потребуется зон?

   Филиалы каждого регионального управления осуществляют полный контроль пользователей в своем регионе. Следовательно, необходимо выделить 11 зон.

4. Сколько потребуется основных серверов?

   Одно из условий сценария в том, чтобы бизнес-приложения, выполняющиеся на вашнх компьютерах, были настроены как серверы внутри доменов. Следовательно, необходимо выделить 11 основных серверов.

5. Сколько потребуется дополнительных серверов?

   Вы можете настроить серверы для обслуживания стольких основных или дополнительных зон, сколько практически необходимо. В нашем случае бизнес-приложения должны быть доступны всем сайтам данного региона и другим региональным управлениям. Следовательно, для дублирования необходимо выделить 11 дополнительных серверов, которые позволят разрешать имена в данной зоне при отказе основного сервера.

6. Сколько потребуется серверов кэширования?

   Три или более, минимум по одному для каждого регионального управления.

Закрепление материала

стр. 154

1. Назовите три компонента DNS.

   Интерпретатор, сервер имен и доменное пространство имен.

2. Опишите разницу между основным, дополнительным и главным серверами.

   Основной сервер имен получает информацию о своей зоне из локальных файлов зон. Дополнительные серверы загружают информацию зоны. Главным называется сервер, с которого дополнительный сервер имен получает информацию о зоне (может являться основным или дополнительным сервером имен).

3. Перечислите три причины, по которым может потребоваться дополнительный сервер имен.

   Они таковы:

   - дополнительный сервер играет роль дублирующего сервера (дублирующие серверы следует иметь для каждой зоны);
   - при наличии удаленных клиентов дополнительный сервер помогает избежать использования медленных линий связи;
   - дополнительный сервер снижает нагрузку на основной сервер.

4. В чем разница между доменом и зоной?

   Домен — это ветвь в пространстве имен DNS. Зона — это часть домена, существующая как отдельный файл на диске, в котором хранятся записи ресурсов.

5. Чем отличаются итеративные и рекурсивные запросы?

   В ответ на рекурсивный запрос DNS-сервер возвращает либо требуемые данные, либо сообщение об ошибке, если данные не найдены. При итеративном запросе возвращается наилучший ответ: как правило, это ссылка на другой DNS-сервер, который поможет разрешить запрос.

6. Перечислите файлы, необходимые для работы версии DNS для Windows 2000.

   Файл базы данных, кэша и обратного просмотра.

7. Опишите назначение загрузочного файла сервера DNS.

   Загрузочный файл используется в версии Berkeley Internet Name Daemon для запуска и настройки DNS-сервера.

Глава 8. Использование DNS

Закрепление материала

стр. 165

1. Сколько зон способен обслуживать один DNS-сервер?

   DNS-сервер может не обслуживать зоны совсем либо обслуживать одну или сразу несколько зон.

2. Какие преимущества получают DNS-клиенты от динамического обновления в Windows 2000?

   Динамическое обновление позволяет DNS-клиентам регистрировать и динамически обновлять записи ресурсов при возникновении изменений. Это уменьшает необходимость администрирования записей зоны вручную, особенно для клиентов, которые часто меняют свое местоположение и используют для получения IP-адресов службу DHCP.

3. Назовите достоинства и недостатки DNS-сервера кэширования.

   Преимущество сервера кэширования в том, что он не создает зонального трафика, поскольку не содержит зон. Впрочем, серверы кэширования имеют один недостаток: при за-

иуске сервер не содержит кэшированной информации, и ее приходится заново воссоздавать по ходу обработки запросов.

4. Назовите три счетчика производительности DNS.
   Они таковы:
   - счетчики динамического обновления и безопасного динамического обновления для подсчета количества регистрации и обновлений, вызванных динамическими клиентами;
   - счетчики использования памяти для определения количества используемой памяти и ее распределения сервером Windows 2000 DNS;
   - счетчики обратного просмотра для подсчета количества запросов и ответов, при которых использовался обратный просмотр и DNS-имена были полностью разрешены.

Глава 9. Внедрение WINS

Закрепление материала

стр. 191

1. Назовите два преимущества использования службы WINS.
   Они таковы:
   - автомагическая регистрация и разрешение имен NetBIOS;
   - отпадает необходимость использования файла LMHOSTS.
2. Назовите два способа активации службы WINS на клиентском компьютере.
   Вручную или автоматически с помощью DHCP.
3. Сколько серверов WINS необходимо в интрасети, включающей 12 подсетей?
   Требуется только один, но для дублирования рекомендуется использовать несколько серверов.
4. Имена каких типов хранятся в БД WINS?
   Имена групп и уникальные имена NetBIOS.

Глава 10. Внедрение DHCP

Закрепление материала

стр. 221

1. Что такое DHCP?
   Протокол DHCP упрощает управление IP-адресами и предназначен для их автоматического выделения.
2. Как взаимодействуют DHCP и DNS?
   DHCP-сервер динамически обновляет пространство имен DNS для клиентов, которые поддерживают такие обновления. Всякий раз, когда происходят изменения адреса, назначенного DHCP, клиенты могут использовать динамическую DNS для изменения информации о привязке имени к IP-адресу.
3. Что такое DHCP-клиент?
   Термин «клиент» применяется к сетевым компьютерам, которые запрашивают и используют службы, предоставляемые DHCP-сервером.
4. Опишите автоматическое конфигурирование IP в Windows 2000.
   Если при запуске системы DHCP-сервер недоступен, клиенты Windows 2000 автоматически настраивают IP-адреса и маску подсети.
5. Почему важно планировать реализацию DHCP в сети?

Службы WINS или DNS используются для динамической регистрации привязок адресов к именам в вашей сети. Чтобы предоставить возможность разрешения имен, необходимо обеспечить взаимодействие DHCP с этими службами. Большинство администраторов, использующих DHCP, планируют стратегию применения серверов DNS и WINS.

6. • Какое средство в Windows 2000 предназначено для управления DHCP-сервером?

   Консоль DHCP. Ярлык для запуска этой консоли добавляется в меню Administrative Tools в ходе установки службы DHCP.

7. Каковы признаки неполадок DHCP?

   Большинство проблем, связанных с DHCP, относятся к ошибкам конфигурации TCP/IP на клиенте. Такие ошибки появляются при следующих обстоятельствах:

   - в настройках клиента указан неправильный IP-адрес;
   - сервер посылает отрицательный ответ обратно клиенту, а клиент выдает сообщение, что не может найти DHCP-сервер;
   - сервер выделяет клиенту IP-адрес, но клиент обнаруживает ошибки, связанные с настройкой сети, например, неспособность регистрировать или разрешить ичена DNS и NetBIOS или взаимодействовать с компьютерами вне данной подсети.

Глава 11 Маршрутизация и удаленный доступ

Закрепление материала

стр. 258

1. Что такое виртуальная частная сеть?

   Это имитация соединения «точка-точка» с использованием инкапсуляции. Такое соединение может пролегать через любую промежуточную сеть, включая Интернет. При передаче данных по VPN обычно применяется шифрование.

2. На основе каких полей пакета фильтры доступа по требованию просматривают трафик?

   IP-адреса отправителя и приемника, идентификатора протокола IP, портов отправителя и приемника, типа и кода ICMP.

3. Истина или ложь — при определении разрешении удаленного доступа (Allow Access, Deny Access) в окне свойств учетной записи пользователя политики удаленного доступа не используются.

   Ложь. Кажется, что в графическом интерфейсе политики удаленного доступа не применяются, но на самом деле параметры входящего подключения настраиваются с их помощью.

4. Истина или ложь — пакеты DHCP никогда не пересылаются по каналам удаленного доступа.

   Ложь. Клиенты службы Routing and Remote Access не используют DHCP для получения адресов, но могут использовать пакеты DHCPINFORM для получения других конфигурационных параметров. Для этого должен быть установлен агент ретрансляции DHCP и использован «внутренний» интерфейс.

5. Для чего предназначен протокол BAP?

   Задействовать или сбросить каналы связи для оперативного изменения емкости полосы пропускания.

Глава 12. Поддержка протокола NAT

Закрепление материала

стр. 279

1. Опишите назначение протокола NAT.

   NAT позволяет компьютерам небольшой сети, например, домашней или офисной, совместно использовать одно подключение к Интернету.

2. Перечислите компоненты, составляющие протокол NAT

   Компонент трансляции представляет собой маршрутизатор, на котором установлен NAT. Компонент адресации позволяет получить IP-адреса других компьютеров домашней сети. Компонент разрешения имен становится DNS-сервером для других компьютеров домашней сети. Запросы на разрешение имен компьютер NAT передает внешнему DNS-серверу, а результат возвращает компьютеру домашней сети.

3. Небольшая фирма использует для своей частной интрасети сетевой идентификатор 10.0.0.0 и получила от поставщика услуг Интернета общий IP-адрес 198.200.200.1. К какому общему IP-адресу протокол NAT привяжет все частные IP-адреса *в* сети 10.0.0.0?

   NAT привязывает (статически или динамически) все частные IP-адреса в сети 10.0.0.0 к внешнему IP-адресу 198.200.200.1.

4. Как предоставить пользователям Интернета доступ к ресурсам вашей частной сети?

   Для сервера ресурсов необходимо использовать статическую конфигурацию, которая включает IP-адрес, маску подсети, шлюз по умолчанию и DNS-сервер. IP-адрес сервера ресурсов необходимо исключить из диапазона IP-адресов, которые распределяются компьютером NAT. Кроме того, необходимо настроить специальный порт, статически связывающий внешние и частные адреса и номера портов.

Глава 13. Внедрение служб сертификации

Закрепление материала

стр. 299

1. Что такое сертификат и каково его назначение?

   Сертификат (цифровой сертификат, сертификат открытого ключа) — цифровой документ, удостоверяющий связь открытого ключа с его владельцем. Основная цель сертификата в том, чтобы подтвердить принадлежность открытого ключа лицу, указанному в сертификате.

2. Что такое центр сертификации и чем он занимается?

   Центр сертификации — организация, выпускающая сертификаты. Это может быть доверенная служба, гарантирующая подлинность лица, которому выдается сертификат с указанным ключом.

3. Назовите четыре типа авторизации сертификатов Microsoft.

   Корневой корпоративный, подчиненный корпоративный, корневой изолированный и подчиненный изолированный.

4. Назовите одну из причин для отзыва сертификата.

   Они таковы:

   - компрометация ключа;
   - обман при получении сертификата;
   - изменение состояния.

5. Назовите пять стандартных хранилищ сертификатов PKI.
   MY, CA, TRUST, ROOT и UserDS.

Глава 14 Безопасность сети предприятия

Закрепление материала

стр. 319

1. Какие потенциальные ситуации, при которых возникает риск снижения безопасности, следует предусмотреть в плане защиты?
   Конкуренты могут получить доступ к секретной информации. Пользователи, не обладающие правом доступа, могут попытаться изменить Web-е границы или перезагрузить ко пьютер, чтобы привести его в нерабочее состояние,
2. Что такое аутентификация и как ее внедрить?
   Под аутентификацией подразумевается процесс идентификации пользователей, подключающихся через сеть. Пользователи, прошедшие аутентификацию, получают доступ к общим ресурсам, ограниченный предоставленными разрешениями. Чтобы пользователи сети могли пройти аутентификацию, необходимо создать для них учетные записи.
3. Назовите некоторые функции безопасности Windows 2000.
   Они таковы:
   - шаблоны безопасности;
   - **протокол аутентификации Kerberos;**
   - инфраструктура открытого ключа (PKI);
   - протокол IPSec;
   - шифрование NTFS.
4. Как обезопасить подключение сети к Интернету?
   Чтобы обезопасить сеть вашей организации от несанкционированного доступа через Интернет, можно установить брандмауэр. Он позволяет пользователям получить доступ к Интернету, но препятствует проникновению в сеть из Интернета, кроме случаев, когда такой доступ предусмотрен.
5. Назовите некоторые протоколы удаленного доступа для обеспечения безопасности.
   Служба Routing and Remote Access использует методы безопасной аутентификации пользователей с помощью следующих протоколов:
   - Challenge Handshake Authentication Protocol (CHAP);
   - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP);
   - Password Authentication Protocol (PAP);
   - Shiva Password Authentication Protocol (SPAP);
   - Extensible Authentication Protocol (EAP).
6. Назовите два способа шифрования для подключений по требованию.
   Microsoft Point-to-Point Encryption (MPPE) и Internet Protocol Security (IPSec),
7. Каким образом утилиты System Monitor и Network Monitor позволяют контролировать безопасность сети?
   Утилита System Monitor используется для наблюдения различных параметров работы системы, а также мониторинга событий, связанных с безопасностью. Утилита Network Monitor позволяет наблюдать сетевую активность, анализировать сетевой трафик и работу сетевых компонентов. Полная версия Systems Management Server позволяет записывать и просматривать каждый сетевой пакет.

8. Как Event Viewer используется для соблюдения мер безопасности?
   Кроме сбора информации о программных и аппаратных ошибках, Event Viewer можно использовать для мониторинга событий, связанных с безопасностью, например попыток подбора пароля для входа в систему. Журнал безопасности содержит также сведения о событиях, связанных с использованием ресурсов, например создание, открытие и удаление файлов или других объектов.
9. Каким образом активировать протоколирование удаленного доступа?
   Регистрация событий включается на вкладке Event bogging в окне свойств сервера удаленного доступа службы Routing and Remote Access.

Словарь терминов

100BaseX Ethernet — *см.* «быстрый Ethernet».

100VG (Voice Grade) AnyLAN (100VGAnyLAN) - новая сетевая технология, объединяющая свойства Ethernet и Token Ring.

10Base2 — топология Ethernet с немодулированной передачей данных на скорости 10 Мбит/с и длиной сегмента до 185 метров. *См. также* «тонкий Ethernet».

10Base5 — *см.* «толстый (стандартный) Ethernet».

10BaseFL — сеть Ethernet на оптоволоконном кабеле.

10BaseT — топология Ethernet, использующая в основном кабель UTP, с передачей данных на скорости 10 Мбит/с и длиной сегмента до 100 метров. *См. также* «тонкий Ethernet».

A

Active **Directory** - *см.* служба каталогов Active Directory.

Active Directory Service Interfaces **(ADSI)** — основанная на COM модель службы каталогов, позволяющая ADSI-совместимым клиентским приложениям обращаться к каталогам с использованием разных протоколов доступа, включая LDAP, через простой стандартный набор интерфейсов. ADSI абстрагирует клиентское приложение от реализации и подробностей работы хранилища данных или протокола.

Address Resolution Protocol **(ARP)** — протокол разрешения адреса, позволяющий определить Ethernet-адрес узла (MAC-адрес) по его Интернет-адресу.

ADSI — *см.* Active Directory Service Interfaces (ADSI).

ADSL — *см.* асимметричный цифровой канал подписчика.

Advanced Program-to-Program Communication (APPC) — разработанная IBM спецификация, являющаяся частью модели Systems Network Architecture (SNA). Определяет способы прямого взаимодействия приложений, выполняющихся на разных компьютерах. *См. также* Systems Network Architecture.

AFP — *см.* файловый протокол AppleTalk (AFP).

ANSI - *см.* Американский национальный институт стандартов.

APPC — *см.* Advanced Program-to-Program Communication (APPC).

AppleShare — сетевая операционная система от Apple. Поддерживает совместное использование файлов. Клиентское программное обеспечение входит в состав операционной системы Apple. В AppleShare также реализован *сервер печати (серверный* спулер *печати)*.

AppleTalk — стек протоколов от Apple, входящий в операционную систему компьютеров Macintosh. Представляет собой набор сетевых протоколов, соответствующий модели OSI. Таким образом, сетевые функции встроены в операционную систему Macintosh. AppleTalk поддерживает протоколы LocalTalk, Ethernet (EtherTalk) и Token Ring (TokenTalk).

ArcNet (Attached Resource Computer **Network)** — немодулированная сеть архитектуры «шина» с передачей маркера и скоростью передачи данных 2,5 Мбит/с. Разработана DataPoint Corporation в 1977 г. Преемник первоначальной ArcNet — ArcNet Plus — обеспечивает *передачу данных* со скоростью до *20 Мбит/* сек. ArcNet — простая недорогая гибкая сетевая архитектура, предназначенная для ЛВС небольших рабочих групп. Строится по топологии «шина» или «звезда» на коаксиальном кабеле, витой паре или оптоволокне и поддерживает до 255 узлов. Технология ArcNet появилась раньше стандартов IEEE. F.F. Project 802. по имеет много общего со стандартом 802.4. *См. также* Project 802.

ARP — *см-* Address Resolution Protocol (ARP).

ARPANET (Advanced **Research Project Agency** Network) — аббревиатура названия Depart-ment of Defense Advanced Research Projects Agency. Одна из первых ГВС, предназначавшаяся для обмена информацией между университетами и другими исследовательскими организациями. Была введена в эксплуатацию в 60-е гг. и явилась прообразом сети Интернет.

ATM — *см.* асинхронный режим передачи.

AUI — *см.* интерфейс подключаемого модуля.

AWG (American Wire **Gauge)** — стандарт на диаметры проводов. Диаметр изменяется обратно пропорционально калибру.

B

Bandwidth Allocation **Protocol (BAP)** — управляющий протокол PPP. Обеспечивает выделение пауосы пропускания по запросу. Динамически управляет *многоканальными линиями, эффективно используя их* полосу пропускания.

BAP — *см.* Bandwidth Allocation Protocol (HAP).

BBS — cw. электронная доска объявлений.

BDC — *см.* резервный контроллер домена.

BIOS — *см.* базовая система ввода-вывода.

BISDN — *см.* модулированная ISDN.

bisync (binary **synchronous communications protocol)** протокол **двоичной синхронной связи** — разработан IBM; двоичная синхронная передача кодируется в ASCII или EBCDIC. Сообщение может быть любой длины, с необязательным предшествующим заголовком. Оно посылается блоками, или кадрами. Поскольку протокол bisync использует синхронную передачу, при которой биты разделяются заданным временным интервалом, каждый кадр проверяется и завершается специальными символами, которые позволяют принимающей и передающей машине синхронизировать свои таймеры.

BNC-компоненты - BNC components — семейство компонентов, включающих разъем BNC для кабеля, BNC-тройник, цилиндрический разъем BNC и BNC-терминатор. Происхождение **аббревиатуры BNC** неясно: есть несколько вариантов ее расшифровки, начиная от «British Naval Connector» (британский морской разъем) и кончая «Bayonet Neill-Concelman» (байонетный разъем Нейла-Консельмана).

bps - бит/с — единица измерения скорости передачи данных. *См. также* бит; скорость двоичной передачи в бодах.

C

CCEP — *см.* Commercial COMSEC Endorsement Program **(CCEP).**

Cellular Digital Packet Data (CDPD) — высокоскоростная сотовая связь, позволяющая компьютерам передавать данные в интервалах между **обычными** голосовыми звонками, когда сотовая сеть свободна.

Certificate Authority (CA) — *см.* центр сертификации.

Comite Consultatif Internationale ile Telegraphie et Telephonie (CCITT) — организация, расположенная в Женеве. — часть United Nations International **Telecommunications** Union (ITU). Рекомендует использованию единые для всего мира коммуникационные стандарты. Протоколы CCITT относятся к модемам, сетям и **факсимильной** связи.

Commercial COMSEC Endorsement Program (CCEP) — стандарт шифрования данных, внедренный National Security Agency. Поставщики (при соответствии требуемому уровню благонадежности) могут присоединиться к **CCEP,** а затем включать алгоритмы секретности в свои системы связи. Ог. *тж* шифрование.

CPU — *см.* центральный процессор.

CRC — *см.* цикличный **избыточный** код.

CSMA/CD — *см.* множественный доступ с контролем несущей и обнаружением коллизий.

D

Data Encryption Standard (DES) — повсеместно используемый алгоритм высокой надежности, разработанный U.S. National Bureau of Standards для шифрования и расшифровки данных. *См. также* шифрование.

DBMS — *см.* система управления базами данных.

DB-разъем - DB connector — разъем для параллельного ввода-вывода. DB — аббревиатура от Data Bus (шина данных). Число, следующее за буквами DB, означает количество проводников разъема. Например, у разъема DB-15 — 15 контактов, а у DB-25 — 25.

DCE — *см.* телекоммуникационное оборудование.

DECnet — программно-аппаратные средства фирмы Digital Equipment Corporation, реализующие Digital Network Architecture (DNA). Сеть на основе ЛВС Ethernet. **FDDf** MAN (Fiber Distributed Data Interface Metropolitan Area Network) и ГВС, использующих средства конфиденциальной и открытой передачи данных. Допускает применение как TCP/IP- и OSI-протоколов, так и DECnet-протоколов фирмы Digital.

DES — *см.* Data Encryption Standard (DES).

DFS (distributed file system) — *см.* распределенная файловая система.

DHCP — *см.* протокол динамической конфигурации узла.

DIP-переключатель ~ DIP (dual inline package) switch — один или несколько кулисных переключателей или полупроводников, которые можно установить в одну из двух позиций (открыто/закрыто) для переключения режимов работы электронного устройства.

DIX-разъем ~ DIX (Digital, Intel, Xerox) connector — разъем для подключения интерфейсного кабеля к сетевому адаптеру или внешнему трансиверу. Известен также как AUI-коннектор. *См. также* **интерфейс** подключаемого модуля.

DMA — *см.* прямой доступ к памяти.

DMA channel — *см.* канал прямого доступа к памяти.

DNS — *см.* система доменных имен.

DTE — *см.* терминальное оборудование.

DVD - *см.* цифровой видеодиск.

E

EAP — *см.* Extensible Authentication Protocol (EAP).

EBCDIC — *см.* расширенный двоично-десятичный код обмена информацией.

EFS (encrypting file system) — *см.* шифрованная файловая система.

EISA — *см.* Enhanced Industry Standard Architecture (EISA).

Enhanced Industry Standard Architecture (EISA) — 32-разрядная архитектура системной шины для компьютеров на базе процессоров Intel x86. Обнародована в 1988 г. консорциумом из девяти компаний — производителей компьютеров (AST Research, Compaq, Epson, Hewlett-Packard, NEC, Olivelli, Tandy, Wyse и Zenith). В слотах EISA могут функционировать платы ISA. *См. также* Industry Standard Architecture.

Enhanced Small Device Interface (ESDI) — стандарт, используемый жесткими дисками большой емкости и накопителями на магнитной ленте для обеспечения высокоскоростной связи с компьютером. ESDI-устройства обычно работают на скорости 10 Мбит/с.

ESDI — *см.* Enhanced Small Device Interface **(ESDI).**

Ethernet — ЛВС, разработанная фирмой Xerox в 1976 г. Нашел широкое применение после введения стандарта IEEE 802.3 для сетей с состязанием. Использует топологию «шина» и CSMA/CD для управления трафиком в линии связи.

EtherTalk — интерфейс, организующий работу протоколов AppleTalk в сети Ethernet. Плата EtherTalk позволяет компьютеру Apple Macintosh подключаться к сети Ethernet стандарта 802.3. ***См. также*** AppleTalk.

Extensible Authentication Protocol (EAP) — расширение протокола PPP. Работает с удаленными клиентами, а также с клиентами **PPTP** и L2TP. Позволяет проверить подлинность удаленного клиента с помощью произвольного механизма аутентификации —

он выбирается в ходе обмена данными между клиентом и сервером удаленного доступа.

F

FAT (file allocation table) — *см.* таблица размещения файлов.

Fiber Distributed Data Interface (FDDI) — стандарт для высокоскоростных оптоволоконных ЛВС, разработанный ANSI. Предусматривает спецификации для скорости передачи 100 Мбит/с в сетях топологии «кольцо».

FQDN (fully qualified domain name) — *см.* полное доменное имя.

FRS (file replication service) — *см.* служба репликации файлов.

FTP — *см.* протокол передачи файлов.

H

HCL — (MI. список совместимого оборудования.

High-Level Data Link Control (HDLC) — широко распространенный международный протокол управления передачей данных. Разработан International Standards Organization (ISO). HDLC — бит-ориентированный синхронный протокол, работающий на канальном уровне модели OSI. По протоколу HDLC данные пересылаются блоками (кадрами) произвольной длины, но стандартного формата.

HTML — *см.* Hypertext Markup Language.

Hypertext Markup Language (HTML) — язык, используемый для создания страниц World Wide Web. Позволяет задавать в тексте коды (теги), которые определяют шрифты, дизайн страницы, включаемую графику и гипертекстовые связи. Гипертекст представляет собой метод презентации текста, изображений, звука и видео, ассоциативно связанных друг с другом. Гипертекстовый формат позволяет просматривать разделы документа в любой последовательности. Существуют специальные инструменты и протоколы для путешествия по Интернету, поиска и печати информации и ее просмотра.

Hypertext Transport Protocol (HTTP) — протокол передачи Web-страниц по сети.

I

IAB — *см.* Internet Architecture Board (IAB)

ICMP — *см.* Internet Control Message Protocol (ICMP).

IDE — *CM.* Integrated Device Electronic (IDE).

IEEE — *CM.* Institute of Electrical and Electronic Engineers (IEEE).

IEEE Project 802 — сетевая модель, представленная в IEEE 802. Названа в честь даты своего появления (февраль 1980 г.). Определяет стандарты для физического и канального уровней модели OSI. Проект 802 подразделяет *канальный уровень* на два подуровня: управления доступом к среде (MAC) и управления логической связью (LLC).

IIS — *см.* Internet Information Services (IIS).

Image Color Management (ICM) 1 — API-интерфейс операционной системы, обеспечивающий соответствие цветов, отображаемых монитором, цветам, выдаваемым сканерами и принтерами.

Industry Standard Architecture (ISA) — название системной шины IBM PC/AT, позволяющей подключать к системе различные адаптеры, установив дополнительную плату в гнезде расширения. В общем случае под ISA понимают собственно гнезда расширения. Си. *также* Enhanced Industry Standard Architecture (EISA), Micro Channel Architecture.

Institute of Electrical and Electronics Engineers (IEEE) — организация, объединяющая специалистов в области инженерных разработок и электроники; известна благодаря выпуску стандартов IEEE 802 для физического и канального уровней ЛВС.

Integrated Device Electronics (IDE) — интерфейс жестких дисков, разработанный в 1988 г. как недорогая альтернатива интерфейсам ESDI и SCSI. Часть контроллера жесткого диска встроена в сам жесткий диск, что упрощает часть контроллера, устанавливаемую в компьютер. В настоящее время IBM PC-совместимый компьютер содержит до двух KOI троллеров IDE, причем к каждому можно подключать до двух жестких дисков.

International Organization for Standardization (ISO) — *организация*, объединяющая группы *стандартизации* разных стран. Например, США представлены Американским National Standards Institute (ANSI). ISO работает над созданием стандартов в области связи и обмена *информацией*. Одно из **главных** *достижений* — общепринятая семиуровневая эталонная модель взаимодействия открытых систем *ISO/OSI*. ISO иногда неверно расшифровывают как International Standards **Organization.** *Возможно, это связано* с *аббревиатурой* ISO. Однако ISO — не сокращение, слово образовано от греч. isos — равный.

International Telecommunications Union (ITU) - организация, отвечающая за разработку стандартов в области международных телекоммуникаций.

International Telecommunications Union-Telecommunication (ITU-T) — *отделение* ITU-T, ответственное за телекоммуникационные стандарты, заменяет CCITT. Стандартизирует архитектуру и работу модемов, а также сетевые протоколы и протоколы факсимильной передачи. *Это межправительственная* организация, отвечающая за регулирование и стандартизацию *телекоммуникационных систем* общего и *частного* пользования.

Internet Architecture Board (IAB) — структура, разрабатывающая и поддерживающая стандарты, касающиеся архитектуры Интернета. Также проводит диспуты по вопросам стандартов.

Internet Control Message Protocol (ICMP) — использует протокол IP вместе с более высокоуровневыми протоколами для обмена сообщениями о статусе пересылаемой информации.

Internet Information Services (IIS) — программные *службы, поддерживающие создание*, настройку и управление Web-узлами, а также другие средства Интернета. Включают NNTP, FTP и SMTP.

Internet Protocol (IP) — протокол сетевого уровня, составная часть стека протоколов TCP/IP. См. *также* Transport Control Protocol/Internet Proiocol (TCP/IP).

Internet Protocol Security (IPSec) — набор открытых стандартов для защиты частных соединений по IP-сетям с применением служб криптозащиты.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) — стек протоколов, используемый в сетях Novell NetWare. IPX — протокол сетевого уровня модели OSI. Сравнительно небольшой и быстрый протокол для ЛВС, наследник Xerox Network System (XNS). Поддерживает маршрут вещи. Ориентированный на соединение транспортный протокол SPX используется для гарантированной доставки данных. Реализация протокола IPX/SPX фирмой Microsoft носит название NWLink.

IP — *см.* Internet Proiocol (IP). *См. также* Transport Control Protocol/Internet Protocol (TCP/IP).

IP-адрес – IP address — 32-разрядный адрес, идентифицирующий узел в сети IP. Каждый учел сети IP должен иметь уникальный IP-адрес, состоящий из идентификаторов сети и обслуживающего компьютера. Этот адрес обычно записывается в точечно-десятичной нотации, в которой десятичное значение каждого октета отделяется точкой, например 192.168.7.27. В Windows 2000 можно выбрать статическую или динамическую настройку IP-адресов посредством службы DHCP.

IPSec — *см.* Internet Protocol Security (IPSec).

ipconfig — диагностическая команда, отображающая текущие параметры TCP/IP. Позволяет просматривать значения параметров TCP/IP, заданные сервером DHCP. *См. также* winipcfg.

IPX/SPX — *см.* Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

IRQ — *см.* вдрос прерывания.

ISA — *СМ.* Industry Standard Architecture (ISA).

ISDN — *см.* цифровая сеть комплексных услуг.

ISO — *см.* International Organization for Standardization (ISO).

ITU — *СМ.* International Telecommunications Union (ITU).

ITU-T — *СМ.* International Telecommunications Union-Telecommunication (ITU-T).

K

Kerberos — стандартный протокол безопасности Интернета для управления проверкой подлинности пользователей или систем. Согласно Kerberos пароли пересылаются по сетевым линиям в зашифрованном виде. Кроме того, в Kerberos входит и другие средства обеспечения безопасности.

L

L2TP — *см.* Layer-Two Tunneling Proiocol (L2TP).

LAN — *см.* локальная вычислительная сеть (ЛВС).

LAT — *см.* local area transport (LAT).

Layer-Two Tunneling Protocol (L2TP) — протокол для создания шифрованного туннеля через незащищенную сеть. Для создания шифрованного туннеля применяет технологии шифрования, например IPSec. Совместно с IPSec позволяет создать защищенную виртуальную частную сеть.

local area transport (LAT) — немаршрутизируемый протокол, разработанный Digital Equipment Corporation.

LocalTalk — кабельная система сети Applelalk. Включает кабели, соединительные модули и удлинители. Такие компоненты обычно характерны для топологии «шина» или «дерево». Сегмент LocalTalk поддерживает до 32 устройств включительно. В связи с ограничениями LocalTalk клиенты вместо него используют для сетей AppleTalk компоненты сторонних поставщиков, например PhoneNet компании Farallon поддерживает до 254 устройств.

M

MAC (Message Authentication Code) — *см.* код аутентификации сообщения.

MAN (metropolitan area network) — *см.* общегородская сеть.

MALI — *см.* модуль множественного доступа.

Micro Channel Architecture (MCA) — 32-разрядная системная шина в компьютерах IBM PS/2 (кроме моделей 25 и 30). Электрически и механически несовместима с шиной ISA. Имеет 32 разряда, высокую скорость передачи сигналов (до 160 Мб/с), может независимо управляться несколькими шинными контроллерами. Отличительная особенность — возможность выбора различных режимов работы, к которым в первую очередь относятся: перемещение и реконфигурация ресурсов; назначение прерываний; использование векторов арбитража для прямого доступа в память. *См. также* Enhanced Industry Standard Architecture (EISA), Industry Standard Architecture (ISA).

Microcom Network Protocol (MNP) — разработанный Microcom Systems, Inc. серия стандартов, предназначенных для сжатия данных и исправления ошибок при асинхронной передаче по телефонным линиям. Протокол настолько удачен, что многие компании приняли не только его первую Персию, но и более поздние. Сегодня большинство производителей модемов встраивает в свои устройства аппаратную поддержку MNP классов 2–5.

Microsoft Technical Information Network (TechNet) — источник информационной поддержки по продуктам Microsoft.

MMC (Microsoft Management Console) -*см.* консоль управления.

MNP - *см.* Microcom Network Protocol (MNP).

MO (magneto-optical) disk — *СМ.* магнитооптический диск (MO).

MSAU — *см.* модуль множественного доступа.

тих — *см.* мультиплексор.

N

NAS (network access server) — *см.* сервер доступа к сети.

NBP — *см.* протокол связи имен.

nbtstat — команда, отображающая статистику и текущие соединения протокола NBT (NetBIOS поверх TCP/IP). Доступна только после установки TCP/IP. *См. также* netstat.

NDIS — *см.* спецификация интерфейса сетевых устройств.

NetBEUI (NetBIOS Extended User Interface) — протокол, поддерживаемый всеми сетевыми ОС фирмы Microsoft. Преимущества: небольшой размер стека (что важно для компьютеров под управлением MS-DOS), высокая скорость передачи информации по сети, совместимость со всеми сетями Microsoft. Главный недостаток: не поддерживает маршрутизацию. Применяется только в сетях Microsoft.

NetBIOS (network basic input/output system) — интерфейс прикладного программирования (API), который может использоваться в ЛВС, состоящих из IBM-совместимых микрокомпьютеров под управлением MS-DOS, OS/2, Windows и некоторых версий UNIX. NetBIOS поставляет прикладным программам стандартный набор команд для запроса низкоуровневых сетевых услуг, необходимых для проведения сеансов связи между узлами сети и передачи данных между ними.

netslat — команда, отображающая статистику и текущие соединения протокола TCP/IP. Доступна только после установки TCP/IP. *См. также* nbtstat.

NetWare **Core Protocol (NCP)** — протокол транспортного и сеансового уровня, обеспечивающий взаимодействие между серверами и клиентами. Определяет управление соединением и кодирование запросов-ответов. Также реализует систему безопасности сети NetWare.

network adapter card — *см.* сетевая плата.

Network News Transfer Protocol **(NNTP)** — протокол, определенный в RFC 977. Стал стандартом де-факто, предназначен для обмена новостями Usenet.

NIC — *см.* сетевая плата.

NNTP — *см.* Network News Transfer Protocol (NNTP).

Novell **Netware** — одна из распространенных сетевых архитектур.

nslookup — служебная команда с интерфейсом командной строки, позволяющая создавать запросы DNS для проверки и устранения неполадок конфигурации DNS.

NTFS — *см.* файловая система NTFS.

O

ODI — *см.* Open Data-Link *Interface* (ODI).

Open Data-Link Interface **(ODI)** — спецификация, внедренная фирмами Novell и Apple. Упрощает разработку драйверов, обеспечивает поддержку нескольких протоколов сетевого уровня одной платы сетевого адаптера. По своему назначению похожа на NDIS. Ог. *также* спецификация интерфейса сетевых устройств.

Open Shortest Path First **(OSPF)** — алгоритм маршрутизации, использующий состояния каналов (link states). Разработан на основе протокола внутридоменной маршрутизации OSI. Требует более длительных вычислений и сравнении с дистанционно-векторной маршрутичацией (distance-vector routing), но предоставляет широкие возможности для управления маршрутизацией и быстрее реагирует на изменения. Для вычисления маршрута на основе числа транзитов (количества маршрутизаторов, через которые пройдет пакет на пути к получателю), пропускной способности линии, трафика и стоимост и использует алгоритм Дейкстры.

OS1 — *см.* эталонная модель взаимодействия открытых систем.

OSPF - *см.* Open Shortest Path First (OSPF).

P

Packet Internet **Groper** (ping) — простая утилита для *проверки соединения* между *компьютерами* с ест TCP/IP. Посылает сообщение в адрес удаленного узла, получив которое юг отправляет ответ, еодержащий его IP-адрес, число полученных бит, время, затраченное на отправку ответного сообщения (в миллисекундах) и TTL (в *секундах*). *Работает* на уровне IP и функционирует, даже если выше лежащие службы TCP/IP отказали.

PAD — *см.* сборщик/разборщик пакетов.

PBX Private **Branch Exchange** (PABX Private **Automated** Branch Exchange) — коммутируемая сеть для линий передачи речи или данных между абонентами внутренней телефонной сети предприятия.

PDA — *см.* персональный цифровой помощник.

PDC - *см.* главный контроллер домена.

PDL — *см.* язык описания страниц.

PDN — *см.* общедоступная сеть данных.

Performance monitor — утилита мониторинга производительности системы. Собирает и отображает статистику об активности компьютера, например, число отправленных и полученных пакетов, загрузку процессора, объем данных, отправленных сервером.

Peripherial Component Interconnect (PCI) — одна из системных шин компьютера. Во взаимодействии компонентов через эту шину центральный процессор не участвует. 32-разрядная шина с возможностью расширения до 64 разрядов. Мультиплексная шина с пиковой пропускной способностью 132 Мб/с при 32 разрядах и 300 Мб/с при 64 разрядах. Работает на частоте 33 МГц, под напряжением 5 или 3.3 В. Поддерживает технологию Plug-and-Play. *См. также* Enhanced Industry Standard Architecture (EISA); Industry Standard Architecture (ISA); Micro Channe Architecture (MCA).

Per-Seat Licensing — вид лицензирования, при котором для каждого клиентского компьютера, обращающегося к Windows 2000 Server, нужна отдельная

клиентская лицензия доступа (Client Access License, CAL). Число клиентов, одновременно обращающихся к серверу, ничем не ограничено.

Per-Server Licensing — вид лицензирования, при котором для каждого параллельного соединения с сервером нужна отдельная клиентская лицензия доступа независимо от наличия и сети других клиентских компьютеров, не подключающихся к серверу в данный момент.

phase change rewritable (PCR) — технология перезаписи оптических дисков. Устройства производятся только одной фирмой — Matsushita/Panasonic, а диски двумя — Panasonic и Plasmon.

ping — см. Packet Internet Groper (ping).

PKI (public key infrastructure) — *см.* инфраструктура открытых ключей.

Plug and Play (PnP) — 1) Возможность компьютерной системы автоматически сконфигурировать добавленное в нее устройство. Поддерживается компьютерами Macintosh на основе шины NuBus и, начиная с Windows 95, PC-совместимыми компьютерами. 2) Разработанный Intel и Microsoft стандарт автоматической настройки работы компьютера с периферийными устройствами: модемами, мониторами, принтерами и др.

Point-to-Point Protocol (PPP) — протокол канального уровня для передачи TCP/IP-пакетов по коммутируемым телефонным линиям, например между компьютером и Интернетом. **Разработан** Internet Engineering Task Force в 1991 г.

Point-to-Point Tunneling Protocol (PPTP) — расширенный протокол PPP, предназначенный для связи по Интернету. Разработан Microsoft как средство построения виртуальных частных сетей (VPN). Позволяет использовать Интернет в качестве выделенного канала связи. Помещает зашифрованные пакеты и защищенные капсулы, передаваемые по TCP/IP-соединению. *См. также* виртуальная частная сеть.

Project 802 — система стандартов для протоколов 1–3 уровней, принятых IEEE. Наибольшее распространение получили стандарты IEEE 802.2–802.5. Стандарт 802.2 считается общим — он определяет функциональное описание подуровня управления логической связью (LLC), **а стандарты** N02.3, 802.4 и 802.5 описывают различные варианты реализации подуровня управления доступом к среде (MAC) и физического уровня. **IEEE** 802.3 определяет стандарты для сетей топологии «шина» типа Ethernet, которые используют механизм множественного доступа с контролем несущей и обнаружением коллизий (CSMA/CD). IEEE 802.4 определяет стандарты для сетей топологии «шина» с передачей маркера. Право использования «шины» для передачи определяется логическим механизмом передачи маркера. IEEE 802.5 определяет стандарты для сетей топологии «кольцо» с передачей маркера. «Кольцо» организовано логически внутри концентратора, к которому станции подключаются радиально. Скорость передачи данных в сетях Token Ring фирмы IBM, построенных по этому стандарту, составляет 4 Мбит/с или 16 Мбит/с.

PVC (permanent virtual circuit) — *см.* постоянный виртуальный канал.

Q

QoS (Quality of Service) — *см.* качество обслуживания.

R

RADIUS — *см.* Remote Authentication Dial-In User Service (RADIUS).

RAID — *см.* избыточный массив независимых дисков.

Remote Access Server (RAS) — любой компьютер с Windows 2000, настроенный для обслуживания подключений удаленного доступа.

Remote Authentication Dial-In User Service (RADIUS) — протокол проверки подлинности, использующий клиент и сервер, широко применяемый поставщиками услуг Интернета на удаленных серверах третьих фирм (не Microsoft). Самое популярное средство проверки подлинности и предоставления доступа для удаленных пользователей и пользователей туннелей. RG-58 /U — коаксиальный кабель со сплошным центральным проводом.

Request for Comments (RFC) — официальные документы консорциума IETF, определяющие характеристики протоколов, включенных в семейство TCP/IP.

RC-58 A/U — коаксиальный кабель с многожильным центральным проводом. Военное наименование в США как RG-58 C/U.

RIP — *см.* Routing Information Protocol (RIP).

RISC — *см.* компьютер с сокращенным набором команд.

RJ-11 — 4-контактный модульный разъем для подключения телефонной розетки или оборудования связи (например модема — к телефонной линии).

RJ-45 — 8-контактный модульный разъем для подключения **телефонной** розетки или другого оборудования к телефонной линии. По размерам несколько больше RJ-11.

ROM — *см.* постоянное запоминающее устройство (ПЗУ).

Routing Information Protocol (RIP) — протокол, использующий дистанционно-векторные алгоритмы для выбора маршрутов. С помощью RIP маршрутизаторы обмениваются информацией и обновляют свои таблицы маршрутизации. Протоколы TCP/IP и IPX поддерживают RIP.

S

SAP (service access point) — *см.* точка доступа к услугам.

SAP — *см.* Service Advertising Protocol **(SAP).**

SCSI — *см.* интерфейс малых компьютерных систем.

SDLC — *см.* Synchronous Data Link Control (SDLC).

Sequenced Packet Exchange (SPX) — часть стека протоколов IPX/SPX для последовательной передачи

данных. *См. также* Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

Serial Line Internet Protocol (SLIP) — протокол передачи пакетов TCP/IP по последовательным линиям связи, например через модем, подключенный к последовательному порту компьютера. Определен в RFC 1055.

Server Message Block (SMB) — протокол, определяющий последовательность команд, используемых для передачи информации между компьютерами в сети. Разработан Microsoft, Intel и **IBM. Редиректор** помещает запросы SMB в блок управления сетью (network control block, NCB) — структуру, которая по сети может быть отправлена удаленному устройству. Сетевой поставщик услуг принимает предназначенные ему SMB-сообщения и извлекает из них данные, относящиеся к SMB-запросу. Эти данные обрабатываются локальным устройством.

Service Advertising Protocol (SAP) — протокол, позволяющий сетевым узлам — поставщикам услуг (серверам файлов, печати, приложений и шлюзов) — заявлять о своих службах и адресах.

SID (security indentifier *или* **security ID)** — *см.* идентификатор защиты.

SLIP — *см.* Serial Line Internet Protocol (SLIP).

SMB - *СМ.* Server Message Block (SMB).

SMDS — *см.* служба коммутируемых мультимегабитных данных.

SMP — *см.* симметричная многопроцессорная обработка.

SMTP — *см.* простой протокол передачи почты.

SNMP — *см.* простой протокол управления сетью.

SONET — *см.* синхронная оптическая сеть.

Spanning Tree Algorithm (STA) — алгоритм управления **маршрутизацией** в сложных сетях. Реализован Комитетом IEEE 802.1 для исключения избыточных маршрутов (несколько ЛВС могут быть связаны не одним маршрутом). Согласно STA, маршрутизаторы обмениваются определенной управляющей информацией, пытаясь найти избыточные маршруты. *Вычислив* самый *эффективный маршрут*, они используют его, блокируя остальные. Любой из заблокированных маршрутов можно активизировать, если основной стал недоступен.

SPX - *см.* Sequenced Packet Exchange (SPX).

SQL — *см.* язык структурированных запросов.

STA — *см.* Spanning Tree Algorithm (STA).

STP — от. экранированная витая пара.

SVC — *см.* коммутируемый виртуальный канал.

Synchronous Data Link Control (SDLC) — протокол синхронной пересылки данных, широко используемый в сетях IBM SNA. Определяет формат передаваемой информации. Бит-ориентированный протокол, организует информацию в структурированные блоки — кадры.

Systems Network Architecture (SNA) — широко используемая архитектура систем связи, разработанная IBM. Определяет стандарты, которые позволяют компьютерам различных типов обмениваться Данными и совместно их обрабатывать. Представляет собой эталонную модель, по которой соединения в сети разделяются на пять уровней. Каждый из этих уровней, как и и модели ISO/OSI, выполняет конкретные функции на пути от физического соединения к прикладному ПО.

SYSVOL — общий каталог, к котором хранятся серверные копии общих файлов домена, тиражируемые среди контроллеров этого домена.

T

TCO — *см.* совокупная стоимость владения.

TCP — см. Transmission Control Protocol **(TCP).**

TCP/IP — *см.* Transport Control Protocol/Internet Protocol (TCP/IP).

TDI — *см.* интерфейс драйвера транспорта.

TDR — *см.* рефлектометр.

Technet — *см.* Microsoft Technical Information Network (TechNet).

Telnet — программа эмуляции терминала (и соответствующий протокол), используемая для подключения к удаленному узлу в сетях TCP/IP (например в Интернете).

Token Ring — сетевая архитектура, при которой компьютеры организованы в виде кольца. В этом "кольце» от станции к станции передается маркер. Компьютеры подключаются радиально к концентратору, который называют модулем множественного доступа (MAU). Механически сеть представляет собой «звезду», а электрически — «кольцо». Такую топологию называют «звезда» — «кольцо». *См. также* маркер, **топология** «кольцо».

TokenTalk — плата расширения для подключении компьютеров Apple Macintosh II к сети Token Ring 802.5.

tracert — утилита, отображающая список всех маршрутизаторов, лежащих на пути TCP/IP-пакета от отправителя до получателя.

Transmission Control Protocol (TCP) — протокол транспортного и сеансовою уровней модели OSI, входящий в стек протоколов TCP/IP для последовательных данных. *См. также* Transport Control Protocol/Internet Protocol (TCP/IP).

Transport Control Protocol/Internet Protocol (TCP/IP) — стандартный стек протоколов, обеспечивающий связь в гетерогенной среде. Маршрутизируемый протокол широко используется и в ЛВС масштаба предприятия, и в ГВС, таких, как Интернет. Кроме протоколов TCP и IP включает множество других протоколов, охватывающих уровни от транспортного до прикладного. Практически для всех сетевых ОС существуют реализации TCP/IP.

TTL — *см.* время жизни.

T-разъем ~ T-connector — Т-образный разъем для соединения коаксиального кабеля Ethernet 10base2. Имеет дополнительный разъем для подключения сетевой платы.

U

UART — *см.* универсальный асинхронный приемник-передатчик.

UDP — *см.* User Datagram Protocol (UDP).

UNC (Universal Naming Convention) — см. универсальные правила именования.

UPS — *см.* источник **бесперебойного** питания (ИБП).

URI — *см.* универсальный указатель ресурса.

USB — *см.* универсальная последовательная шина.

User Datagram Protocol (UDP) — не ориентированный на соединение протокол передачи данных между оконечными узлами.

UTP — *см.* неэкранированная витая пара.

V

VPN — *см.* виртуальная частная сеть.

W

Web-сервер - Web server — компьютер, обслуживаемый системным администратором или поставщиком услуг Интернета и предназначенный для обработки запросов клиентских обозревателей.

Windows Internet Name Service (WINS) — программная служба, динамически сопоставляющая IP-адреса именам компьютеров (именам NetBIOS). Это позволяет пользователям обращаться к ресурсам по именам, а не по IP-адресам, которые трудно запоминать. Серверы WINS поддерживают клиенты Windows NT 4.0 и более ранние ОС производства Microsoft.

winipcfg — утилита Microsoft Windows 9x. Эквивалент команды ipconfig, но с графическим интерфейсом пользователя. *См. также* ipconfig.

World Wide Web (WWW) — гипертекстовая мультимедийная служба в Интернете. Содержит информацию в виде адресуемых страниц, написанных на **HTML**. *См. также* Hypertext Markup Language (HTML).

Write-Once Read-Many (WORM) — носитель информации, на который можно записать данные лишь однажды, но считывать их любое число раз. Обычно это оптический диск со специальным слоем, выжигаемым лазером для записи информации.

X

X.25 — рекомендации CCITT. Определяет **соединение** между терминалом и сетью с коммутацией пакетов. Содержит три определения: электрического соединения между терминалом и сетью, протоколы передачи и реализации виртуальных каналов между сетевыми пользователями. Вместе взятые, эти определения описывают синхронное полнодуплексное соединение терминал — сеть. Передаваемые по такой сети пакеты могут содержать либо данные, либо управляющие команды. Формат пакета, контроль ошибок и другие средства эквивалентны протоколу HDLC, определенному ISO. Стандарты X.25 соответствуют трем нижним уровням модели OSI.

X.400 — протокол CCITT для международной передачи электронной почты.

X.500 — протокол CCITT для поддержки единой логической структуры файлов и каталогов, размещенных на нескольких физических системах.

XNS (Xerox Network System) — протокол, разработанный фирмой Xerox для ЛВС Ethernet.

А

авторизация ~ authorization — процесс проверки прав и разрешений пользователя при обращении к ресурсу.

агент - agent — программа, выполняющая задачу в фоновом режиме и сообщающая пользователю о завершении выполнения этой задачи или о наступлении определенного события.

Американский национальный институт стандартов - American National Standards Institute (ANSI) — объединение американских промышленных и деловых групп, занимающееся разработкой торговых и коммуникационных стандартов. ANSI представляет **Америку** в Международной организации по стандартизации (ISO). *См. также* International Organization for Standardization (ISO).

американский стандартный набор символов для обмена информацией ~ American Standard *Code* **for** Information **Interchange (ASCII)** — система кодирования, которая приписывает числовые значения буквам, цифрам, знакам препинания и некоторым другим символам. Стандартизация набора этих числовых значений позволила компьютерам и программам обмениваться информацией.

анализатор протокола ~ protocol analyzer — см. сетевой анализатор.

аналоговая линия - analog line — линия связи, например телефонная линия, передающая информацию в аналоговой форме. Для выделения полезного сигнала на фоне искажений и шумов вдоль аналоговой линии периодически устанавливаются усилители.

аналоговый... - analog — описываемый непрерывной функцией, например напряжение или давление. Аналоговое устройство может выдавать бесконечное число значений в рамках своего рабочего диапазона. *См. также* цифровой.

аппаратное обеспечение ~ hardware — физические компоненты компьютерной системы (например, процессор, память, принтеры, модемы, мышь и т. п.).

асимметричный цифровой канал подписчика - Asymmetric Digital Subscriber Line (ADSL) — используемая в модемах новейшая технология, превращающая телефонные линии в витой парой в линии высокоскоростного доступа. Технология ADSL позволяет передавать информацию к абоненту со скоростью до 8 Мбит/с и до 1 Мбит/с в обратном направлении. ADSL рассматривается как протокол передачи физического уровня для неэкранированной витой пары.

асинхронная передача ~ asynchronous transmission — способ передачи данных, при котором информация посылается последовательно с произвольными времен-

ными интервалами. Общий для передающей и принимающей стороны таймер, который давал бы им возможность разделять данные на отдельные символы, основываясь на отсчетах времени, при этом не используется. Поэтому каждый передаваемый символ содержит некоторое число бит данных (обычно 8), которые предваряются стартовым битом и завершаются необязательным битом четности и одним, полутора или двумя стоповыми битами.

асинхронный режим передачи ~ Asynchronous Transfer Mode (ATM) — новейшая технология построения сетей с коммутацией кадров. Обеспечивает высокоскоростную передачу ланныч, посылая ячейки ланныч (кадры фиксированного размера) по модулированным ЛВС и ГВС. Размер ячеек 53 байта: 48 байт данных + 5 дополнительных байт адреса. Позволяет передавать разные виды ланныч: речь, двоичные данные, факсимильные сообщения, видео в реальном времени, звук с качеством компакт-диска, изображения — на скоростях в десятки, сотни и тысячи Мбит/с. В качестве мультиплексоров используют коммутаторы для обеспечения одновременной передачи ланныч по сети несколькими компьютерами. Большинство коммерческих плат ATM обеспечивают передачу ланныч со скоростью около 155 Мбит/сек, хотя теоретически достижима скорость 2.4 Гбит/с.

аудит ~ auditing — процесс, отслеживающий сетевые операции пользователей; стандартный элемент защиты сети. Позволяет создавать списки пользователей, обращающихся (или пытающихся обратиться) к определенным ресурсам, помогает администраторам выявлять несанкционированные действия. Также позволяет отслеживать такие операции, как попытки регистрации в системе, подключение и отключение от указанных ресурсов, изменения в файлах и каталогах, события и изменения на сервере, модификацию паролей и параметров регистрации в системе.

аутентификация - authentication — проверка, основанная на имени пользователя, пароле, а также ограничениях учетной записи и ограничениях по времени.

Б

базовая система ввода-вывода - Basic Input Output System (BIOS) — на PC-совместимых компьютерах — набор обязательных программных процедур, тестирующих систему при загрузке, запускающих ОС, а также обеспечивающих передачу данных между аппаратными устройствами. **BIOS** хранится в ПЗУ, что позволяет вызывать ее функции при включении компьютера. Хотя BIOS критична для производительности, обычно она не видна пользователям.

базовый адрес памяти ~ base memory address — определяет адрес в оперативной памяти компьютера, с которого начинается фрагмент памяти, используемый каким-либо устройством компьютера, например платой сетевого адаптера; иногда называется начальным адресом памяти.

базовый порт ввода-вывода - base I/O port — определяет канал, по которому идет обмен данными между центральным процессором и каким-либо другим устройством компьютера, например сетевой платой.

байт - byte — единица информации, равная 8 битам. В компьютерной обработке или хранении данных 1 байт эквивалентен одному символу, например, букве, цифре или знаку пунктуации. Так как байт представляет небольшое количество информации, размер памяти компьютеры и измеряют в килобайтах (1 кб=1024 байт=2^{10} байт), мегабайтах (1 Мб=1 048 576=2^{20} байт), гигабайтах (1Гб=1<)24 мегабайта=2^{30} байта К петабайтах (1024 терабайта=2^{50} байт) или экзабайтах (1024 петабайта=2^{60} байт).

балансировка нагрузки - load balancing — прием, используемый компонентом работы с кластерами Windows для изменения производительности серверных программ (например Web-серверы) посредством распределения клиентских запросов по нескольким серверам кластера. Для каждого узла можно задать процент нагрузки, и она будет равномерно распределена между всеми узлами. Если узел выйдет из строя, его нагрузка перераспределяется между оставшимися узлами.

бездисковый компьютер - diskless computer — компьютер без жестких и гибких дисководов. Использует специальное ПЗУ, программа которого выполняет загрузку компьютера по сети.

безопасный режим - safe mode — способ запуска Windows 2000 с применением основных файлов и драйверов и без поддержки сети. Доступен при нажатии клавиши F8 при загрузке Windows 2000. Позволяет загрузить компьютер при наличии неполадок, мешающих его запуску в обычном режиме.

беспроводная сеть ~ wireless network — сеть, не использующая кабель для связи компонентов.

беспроводной концентратор ~ wireless concentrator - компонент беспроводной сети, принимающий сигнал от беспроводных сетевых плат или передающий им сигналы.

беспроводной мост - wireless bridge — устройство для организации беспроводной связи между ЛВС.

билет - tickel — набор идентификационных данных для системы безопасности, выданных контроллером домена с целью проверки подлинности пользователя. В Windows 2000 применяются билеты двух видов: билет на выдачу билета (Ticket Gram Ticket, TGT) и билет службы.

бит - bit — разряд двоичного числа, 1 или 0 в двоичной системе счисления. Представляет собой минимальную порцию информации, которую обрабатывает и сохраняет компьютер. Физически — это единичный импульс, посланный по линии связи, или точка на магнитном диске, способная хранить только значение 1 или 0. Восемь бит составляют один байт.

бит-тайм ~ bit time — время, затрачиваемое каждой станцией на получение и запоминание бита.

блокировка учетной записи ~ account lockout — средство защиты Windows 2000, которое блокирует учетную запись пользователя, если за указанный промежуток времени он произведет определенное количество неудачных попыток регистрации в системе. Основан на параметрах блокировки, заданных в по-

литике защиты. Регистрация в системе под заблокированной учетной записью невозможна.

бод ~ **baud** — единица измерения скорости передачи данных, названная в честь французского инженера и телеграфиста Жана-Мориса Эмиля Бодо. Характеризует кол «честно осцилляции (изменений характеристик несущего сигнала) и единицу времени. Каждая осцилляция кодирует 1 бит данных, передаваемых по телефонной линии. Сначала в бодах измерялась скорость передачи данных к телеграфии, затем — скорость передачи данных модемом. Современные модемы одной осцилляцией кодируют несколько бит данных, поэтому в настоящее время скорость работы модемов измеряется в бит/с (bps).

брандмауэр - firewall — совокупность программных и аппаратных средств защиты сети от атак извне. Брандмауэр блокирует прямое взаимодействие компьютеров корпоративной сети с компьютерами внешней сети и наоборот. Вместо этого осуществляется маршрутизация всех входящих и исходящих потоков через прокси-сервер, расположенный вне сети организации. Брандмауэры также осуществляют аудит сетевой активности, фиксируя объем трафика и сведения о попытках несанкционированного доступа. См. *также* прокси-сервер.

буфер ~ **buffer** — резервный участок ОЗУ для временного хранения данных при их передаче или приеме.

«быстрый Ethernet» ~ **fast Ethernet** — расширение существующего стандарта Ethernet. Другое название — 100BaseX Ethernet. Использует кабель UTP категории 5, метод доступа CSMA/CD и топологию «звезда» — «шина». Передает данные со скоростью 100 Мбит/с.

В

виртуальная частная сеть ~ **Virtual Private Network (VPN)** — группа компьютеров в общедоступной сети, например в Интернете, соединенных друг с другом защищенными каналами связи. Работает так, как если бы компьютеры были соединены частными линиями связи.

виртуальный канал - virtual circuit — последовательность логических соединений между посылающим и принимающим компьютерами. Соединение считается установленным, если оба компьютера обменялись служебной информацией и подтвердили параметры связи, включая максимальный размер сообщения и маршрут. К параметрам виртуальных каналов, обеспечивающим надежность передачи, относится подтверждение приема, управление потоком данных и контроль ошибок. Виртуальные каналы могут быть временными (существуют только во время сеанса связи) или постоянными (существуют в течение всего времени, пока пользователи оставляют каналы связи открытыми). Си. *также* коммутируемый виртуальный канал; постоянный виртуальный канал,

вирус ~ **virus** — программа или фрагмент кода, скрытая внутри другой программы или в загрузочном секторе диска. Основное назначение вируса — размножение, дополнительное применение — разрушение данных или вывод из строя оборудования.

вирус-компаньон ~ **companion virus** — вирус, исполняемый файл которого имеет такое же имя, что и прикладная программа, но другое расширение: вместо .EXE используется .COM. В этом случае, если ввести имя программы, будет загружен и запущен вирус, так как файлы с расширением .COM имеют приоритет.

вирус-невидимка (стеле) - stealth virus — разновидность файлового вируса. Назван так из-за своей способности оставаться невидимым для антивирусных программ. При проверке системы он пытается перехватить запросы и выдать сфальсифицированный ответ, сигнализирующий, что все в порядке.

витая пара - twisted-pair cable — два скрученных изолированных провода, используемых для передачи электрических сигналов. Скручивание проводов уменьшает влияние внешних электромагнитных помех. Несколько витых пар часто помещают в защитную оболочку. Витая пара бывает экранированной и неэкранированной. Последняя распространена в телефонных сетях. Си. *также* неэкранированная витая пара; экранированная витая пара,

волновое сопротивление ~ **impedance** — полное электрическое сопротивление переменному току, включающее активную и реактивную составляющие; измеряется в омах (Ом).

вольтметр ~ **voltmeter** — *см.* цифровой вольтметр.

время жизни ~ **Time-to-Live (TTL)** — значение, которое включается в пакеты, пересылаемые по сетям TCP/IP. Задает срок хранения или использования пакета или любых его данных получателем. Значения TTL применяются в кэшах ресурсов и зоне для определения срока, в течение которого запрашивающие клиенты должны кэшировать и использовать данные, если они содержатся в ответе на запрос, присланном сервером DNS зоны.

время простоя ~ **downtime** — период времени, в течение которого компьютерная система или связанное с ней оборудование не работают. Иногда возникает из-за поломок оборудования, а иногда является и запланированной акцией (например, при выполнении профилактических работ, замене оборудования или архивировании файлов).

встроенная группа - built-in group — группа, предопределенная в Windows NT и Windows 2000. Обладает готовым набором прав и привилегий. В большинстве случаев нетроенные группы реализуют все необходимые для отдельного пользователя возможности. Например, если учетная запись пользователя домена принадлежит нетроенной группе Administrators (Администраторы), он получает права администратора контроллеров домена или сервера. См. *также* учетная запись пользователя.

встроенная программа ~ **firmware** — подпрограмма, находящаяся в ПЗУ, которое в отличие от ОЗУ сохраняет данные даже при отсутствии питающего напряжения. Встраиваются обычно процедуры низкого

НОИ загрузки и низкоуровневые процедуры ввода-вывода.

вторичный хозяин - secondary master — полномочный сервер DNS для зоны, используется в качестве источника для репликации зоны на другие серверы. Обновляет данные своей зоны только путем переноса данных зоны с других серверов DNS; не способен самостоятельно обновлять зону.

выделенный сервер - dedicated server — компьютер в сети, который выступает только в роли сервера и не используется при этом в качестве клиента. *См. также* сервер; сеть; ПО основе сервера.

вытесняющая многозадачность ~ preemptive multitasking — особенность ОС заключается в том, что она в любой момент может «отобрать» управление процессором у выполняемой задачи. *См. также* многозадачность; невытесняющая многозадачность.

Г

гермафродитный разъем - hermafroditic connector — разъем, не являющийся ни гнездовым, ни штыревым, например разъем для кабелей IBM. В отличие от BNC-разъемов, у которых соединяются лишь гнездовой и штыревой разъемы, у разъемов для кабелей IBM можно соединять любые два разъема.

герц (Гц) ~ hertz (Hz) — единица измерения частоты колебаний. Показывает, с какой регулярностью происходит *периодическое событие, например* изменение напряжения электрического тока. 1 Гц эквивалентен одному циклу в секунду. Частота нерелко измеряется в килогерцах (1 кГц=1000 Гц), мегагерцах (1 МГц=1000 кГц), гигагерцах (1 ГГц=1000 МГц) или терагерцах (1 ТГц=1000 ГГц).

гибридная сеть ~ hybrid network — сеть, объединяющая компоненты от разных поставщиков.

гибридный концентратор ~ hybrid hub — концентратор, к которому можно подключить кабели различных типов.

гигабайт ~ gigabyte (GB) — в большинстве случаев — тысяча мегабайт. Тем не менее точное значение зачастую изменяется и зависимости от контекста. 1 Гб = 1 млрд. байт. В контексте значений байты исчисляются в степенях двойки, следовательно, гигабайт может быть равен 1000 или 1024 мегабайтам, где 1 Мб = 1 048 576 байт (2^{20}).

гигабит ~ gigabit (Gb) — ранен 1 073 741 824 бит.

главный контроллер домена ~ primary domain controller (PDC) — самый первый в домене компьютер, на который устанавливается Windows NT Server. Хранит главную копию БД учетных записей домена, аутентифицирует пользователей; может работать как сервер файлов, сервер печати и сервер приложений. В каждом домене допустим только один PDC. *См. также* домен; контроллер домена.

глобальная вычислительная сеть (ГВС) - wide area network (WAN) — компьютерная сеть, использующая средства связи дальнего действия. Состоит из компьютеров, разделенных большими расстояниями.

глобальная группа ~ global group — в Windows NT Server это инструмент администрирования, помогающий управлять сетевыми пользователями. Глобальные группы создаются на главном контроллере домена и могут использоваться как в своем домене, так и в доверяющих доменах. При этом их наделяют правами и привилегиями, и они становятся членами локальных групп. Содержат учетные записи пользователей только своего домена. *См. также* главный контроллер домена; группа.

глобальный каталог ~ global calalog — служба и физическое хранилище, содержащее реплики определенных атрибутов всех объектов Active Directory.

«горячее» исправление - hot fixing — *см.* замена сектора.

группа ~ group — учетная запись, содержащая другие учетные записи, называемые членами группы. Права и привилегии, предоставляемые группе, распространяются и на ее членов. Создание группы — удобный способ предоставить общие права сразу нескольким пользователям. В Windows NT управление группами осуществляется через User Manager. В Windows NT Server для этого служит User Manger for Domains. *См. также* встроенная группа; глобальная группа.

Д

двухвариантная загрузка - dual boot — конфигурация компьютера, в которой по своему выбору можно загружать одну из двух установленных на нем ОС.

дейзи-цепочка ~ daisy chain — ряд последовательно соединенных устройств. Первое устройство дейзи-цепочки подключается к компьютеру, следующее подключается к первому устройству и т. д. Сигналы по цепочке перелаются от одного устройства к другому.

дерево ~ tree — группа доменов Windows 2000 с общим связанным пространством имен.

добавочное архивирование • incremental backup — копирование файлов, созданных или изменен ных со времени последнего обычного или добавочного архивирования.

доверительные отношения - trust relationships - односторонние логические связи между доменами. Позволяют осуществлять сквозную **аутентификацию**, при которой пользователь, имея только одну учетную запись в одном домене, получает доступ ко всей сети. Учетные записи пользователей и глобальные группы, определенные в доверяемом домене, могут быть наделены привилегиями и правами доступа к ресурсам в доверяющем домене, даже если этих учетных записей и **БД** доверяющего **домена** нет. При этом доверяющий домен возлагает аутентификацию на доверяемый домен.

домен ~ domain — в сетях Microsoft — совокупность компьютеров и пользователей, информация о которых хранится в базе данных на контроллере домена и в отношении которых проводится единая политика безопасности. Каждый домен имеет уникальное имя. *См. также* рабочая группа.

драйвер ~ driver — программный компонент, позволяющий компьютерной системе взаимодействовать с устройством. Драйвер принтера, например, преобразует поступающие от компьютера данные в форму, понятную конкретному принтеру. В большинстве случаев драйвер, кроме того, управляет аппаратурой.

драйвер принтера ~ printer driver — файлы(ы), позволяющий Windows 2000 преобразовать команды печати и команды вывода конкретного принтера, например PostScript. У каждого устройства печати свои драйвер.

драйвер протокола ~ protocol driver — отвечает за предоставление четырех или пяти базовых услуг остальным уровням сети и «скрывает» подробности фактической реализации этих услуг, включающих управление сеансом, службу дейтаграмм, сегментацию данных и контроль порядка пакетов, уведомление и иногда маршрутизацию к ГВС.

драйвер управления доступом к среде ~ Media Access Control (MAC) driver — драйвер устройства, работающий на полуровне управления доступом к среде модели OSI. Известен также как драйвер платы сетевого адаптера и и NIC-драйвер. Обеспечивает низкоуровневый доступ к сетевым адаптерам, предоставляя поддержку функции передачи данных и некоторым основным функциям управления адаптером. Кроме того, передает данные от физического уровня к транспортным протоколам сетевого и транспортного уровней.

дрожание ~ jitter — нестабильность формы волны сигнала. Часто вызывается взаимными помехами **или** неустойчивой работой «кольца» в сетях FDDI или Token Ring.

дублирование дисков ~ disk duplicating — см. зеркальные диски; отказоустойчивость.

дуплексная передача ~ duplex transmission — одновременная двунаправленная передача данных между двумя станциями. Известна также как полнодуплексная передача. Другие способы передачи: симплексная (передача в одном направлении) и полудуплексная (двунаправленная передача данных в каждом из направлений поочередно).

Ж

жесткий диск ~ hard disk — накопитель данных к вычислительных системах. Имеет одну или несколько жестких пластин с магнитным покрытием, которое позволяет записывать на него компьютерные данные. Обычно жесткий диск вращается со скоростью 3600–10 000 об/мин. Головки чтения/записи «парят» над ею поверхностью на воздушной подушке толщиной от 20 до 50 миллионных долей сантиметра. Герметичный корпус предотвращает попадание пыли в зазор между носителем и головками. Жесткие диски обеспечивают более быстрый доступ к данным, чем дискеты, и способны хранить больше информации. Так как пластины жесткие, в один корпус можно поместить сборкой сразу несколько пластин, обычно от 2 до 8.

З

заголовок ~ header — один из трех компонентов сетевого пакета. Состоит из сигнала, оповещающего о начале пакета, адреса отправителя и получателя и синхронизирующей последовательности битов.

заголовок кадра ~ frame preamble — служебная информация канального уровня модели OSI, добавляемая в начало кадра.

загрузочный вирус ~ boot-sector virus — вирус, записывающийся в первый сектор гибкого или жесткого диска и выполняющийся при загрузке компьютера. В таких вирусах используется один из наиболее распространенных способов заражения гибких дисков — при обращении к новому диску вирус копирует себя в загрузочную область.

загрузочный раздел ~ boot partition — раздел, содержащий ОС Microsoft Windows 2000 и необходимые ей файлы. Может, но не обязательно, одновременно быть и системным разделом.

загрузочный сектор раздела ~ partition boot sector — часть раздела жесткого диска, содержащая информацию о файловой системе диска и небольшую программу на машинном языке, загружающую ОС.

закрытый ключ ~ private key — закрытая (секретная) часть пары криптографических ключей, сгенерированных с применением алгоритма шифрования с открытым ключом. Обычно служит для расшифровки симметричного сеансового ключа, наложения цифровых подписей или для расшифровки сообщений, зашифрованных соответствующим открытым ключом.

замена сектора ~ sector sparing — система исправления ошибок. Известна также как «горячее» исправление. Автоматически добавляет в файловую систему механизм восстановления секторов. Если во время дисковой операции ввода/вывода встречается поврежденный сектор, драйвер исправления ошибок пытается переместить находящиеся в нем данные в исправный сектор и пометить поврежденный. Если это удалось, предупреждение файловой системе не пытается. Замена секторов для SCSI-устройств выполняется аппаратно, а для AT-устройств (ESDI и IDE) — программно.

запись ресурса ~ resource record — стандартные типы записей базы данных, используемые в зонах для связывания доменных имен DNS с данными, характерными для каждого сетевого ресурса, например с IP-адресом. Большинство основных типов ресурсов определяется спецификацией RFC 1035, однако существуют дополнительные типы записей, определенные другими RFC и утвержденные для применения в DNS.

запись ресурса PTR ~ pointer (PTR) resource record — запись ресурса, используемая в зоне локального просмотра, созданной в домене in-addr.arpa для задания обратного сопоставления IP-адреса с доменным именем DNS.

запись ресурса SOA ~ start-of-authority (SOA) resource record — запись, указывающая начальную (исходную) точку полномочий на данные зоны. Является

мерной записью, создаваемой при добавлении зоны. Содержит несколько параметров, предназначенных для других компьютеров, применяющих DNS с целью определения срока использования данных зоны и частоту необходимых обновлений. Также называется начальной записью зоны.

запись ресурса SRV - service (SRV) resource record — запись ресурса, используемая в зоне для регистрации и поиска известных служб TCP/IP. Описана в RFC 2052 и используется в Windows 2000 или более поздней версии с целью поиска контроллеров доменов для Active Directory.

запрос прерывания - interrupt request (IRQ) — сигнал, посылаемый центральному процессору от периферийного устройства. Сообщает о событии, обработка которого требует участия процессора.

допросчик ~ requester (LAN **requester**) — программа, установленная на компьютере-клиенте. Перенаправляет запросы на сетевые услуги со стороны работающих на этом же компьютере приложений на соответствующий сервер. Си. *также* редиректор.

затухание - attenuation — ослабление или искажение сигнала по мере удаления от источника. Относится к цифровому сигналу в кабеле или к уменьшению амплитуды электрического (аналогового) сигнала, если не происходит заметного изменения формы волны. Обычно измеряется в децибелах. Затухание *сигнала, передаваемого по витому кабелю*, компенсируется повторителем, который усиливает и восстанавливает форму приходящего сигнала перед его передачей к следующим сегментам кабеля.

защищенный паролем ресурс ~ password-protected share — доступ к общему ресурсу предоставляется при вводе соответствующего пароля.

зеркальные диски ~ disk mirroring — технология, при которой часть жесткого диска (или весь жесткий диск) дублируется на другом жестком диске, подключенном — что желательно — к отдельному дисковому контроллеру. Любые изменения на исходном диске сразу отражаются на зеркальном. Эта технология позволяет создавать резервную копию данных одновременно с их поступлением. И (иногда также как дублирование дисков. Си. *также* отказоустойчивость; чередование дисков.

зона ~ zone - 1) В сети Macintosh логическое объединение компонентов сети, упрощающее поиск ресурсов сети, таких, как серверы и принтеры, аналог домена в сети Windows 2000 Server. 2) Представляет часть базы данных DNS, которая управляется как отдельная единица сервером имен [>NS. Такая единица может состоять из одного домена или домена, содержащего подчиненные домены. Администратор зоны DNS задает для зоны имена одного или нескольких серверов имен.

зонная передача - zone transfer — процесс взаимодействия серверов DNS и целях обслуживания и синхронизации записей ресурсов. Сервер DNS, настроенный в качестве вторичного хозяина (дополнительный сервер зоны К *периодически опрашивает* другой сервер DNS, являющийся источником данных для зоны (основным сервером «ты»). Если версия данных на сервере-источнике изменилась, вторичный хозяин загружает и синхронизирует записи ресурсов с источника.

«зуб вампира» ~ vampire tap *или* **piercing tap transceiver** — соединитель, на котором размещен трансивер Ethernet. Снабжен острыми зубами, которые «прокалывают» изоляцию кабеля, «толстый Ethernet» и вступают в контакт с проводящей медной жилой. Разъем DIX (DB 15) трансивера обеспечивает подключение AUI-кабеля, соединяющего трансивер с компьютером, концентратором или повторителем.

И

идентификатор защиты - security indentifier *или* **security ID (SID)** — уникальный номер, идентифицирующий пользователя, группу и учетные записи компьютеров. Присваивается учетной записи при ее создании. **Внутренние** процессы Windows 2000 обращаются к учетным записям по идентификатору защиты, а не по имени пользователя или группы. Если удалить, а затем снова создать учетную запись с тем же *именем*, у нее не будет *первоначальных привилегий* и разрешений, поскольку у старой и новой записей разные SID.

избыточная система ~ redundancy system — отказоустойчивая система, защищенная от сбоев за счет дублирования *ответственных компонентов оборудования*. Это позволяет **сохранять работоспособность** в случае аппаратного сбоя. Си. *также* отказоустойчивость.

избыточный массив недорогих дисков ~ redundant array of inexpensive disks (RAID) - *см.* избыточный массив независимых дисков.

избыточный массив независимых дисков - redundant array of independent disks (RAID) — пятиуровневая спецификация, стандартизирующая работу отказоустойчивых накопителей. Пять уровней различаются по производительности, надежности и цене. Ранее данная спецификация называлась «избыточный массив недорогих дисков».

изолированная среда ~ stand-alone environment — рабочая среда, в которой каждого пользователя имеется отдельный компьютер. Однако все пользователи работают не вместе и не могут совместно использовать данные и другую важную информацию, которая в сетевой среде была бы доступна через сервер.

изолированный компьютер ~ stand-alone computer — компьютер, не подключенный к другим компьютерам и не являющийся частью сети.

изолированный сервер - stand-alone server — компьютер с Windows 2000 Server, не участвующий в домене. Содержит только собственную базу данных пользователей и самостоятельно обрабатывает запросы на вход в систему. Не использует учетные данные совместно с другими компьютерами и не может предоставлять доступ к учетным записям домена.

имя пользователя ~ user name — уникальное имя, идентифицирующее учетную запись пользователя в Windows 2000. Имя пользователя, определенное и

учетной записи. Не может совпадать с каким-либо другим именем группы или именем пользователя в том же домене или рабочей группе.

имя узла - host **name** — имя устройства в сети. В сетях Windows 2000/NT это имя может совпадать или не совпадать с именем компьютера.

интерфейс - interface — граница, разделяющая уровни. Например, в модели OSI каждый уровень предоставляет **некоторую службу** или операцию, готовящую данные для передачи по сети на другой компьютер.

интерфейс драйвера транспорта ~ transport driver interface (TDI) — интерфейс между драйверами файловой системы и драйверами транспортных протоколов. Позволяет любому совместимому TDI-протоколу взаимодействовать с драйверами файловой системы.

интерфейс малых компьютерных систем - Small Computer System **Interface (SCSI)** — стандарт высокоскоростного параллельного интерфейса. Разработан ANSI. Используется для подключения к микрокомпьютеру периферийных устроств, таких, как жесткие диски, CD- ROM-дисководы, принтеры, а также другие компьютеры или ЛВС. SCSI произносится как «скази».

интерфейс подключаемого модуля - Attachment Unit Interface (AUI) — разъем для подключения внешнего трансивера, установленного на магистральном коаксиальном кабеле, к сетевой плате; также называется DIX-разъемом.

интерфейс прикладного программирования - application programming interface (API) — набор процедур, которые вызывает приложение для выполнения операций нижнего уровня, возложенных на ОС.

интерфейсная часть - front end — 11 клиент-серверных приложениях — часть программы, выполняемая на компьютере-клиенте. Си. *также* прикладная часть.

инфракрасная передача ~ infrared transmission — электромагнитное излучение, частота которого в электромагнитном спектре располагается чуть ниже видимого красного света. В сетевых коммуникациях инфракрасные технологии обеспечивают очень высокую скорость передачи данных и большую полосу пропускания в сравнении с прочими способами связи.

инфраструктура открытых ключей ~ public key infrastructure (PKI) - термин, обычно используемый для описания законов, правил, стандартов и МО, относящихся к регулированию или работе с сертификатами, открытыми и закрытыми ключами. На практике PKI является системой цифровых сертификатов и центров сертификации, отвечающих за верификацию и аутентификацию каждого из участников **электронной** транзакции. Стандарты PKI находятся в процессе разработки, хотя они уже широко реализованы в качестве обязательного элемента электронной коммерции.

испускание маяка ~ beaconing — метод извещения компьютеров в топологии «кольцо» о перерыве в передаче маркера и связи с серьезной ошибкой. В сетях FDDI и Token Ring в передаче маркера участвуют все компьютеры. Для включения серьезных ошибок в кольце обнаруживший неисправность компьютер посылает по сети сигнал, называемый маяком. Затем этот компьютер будет продолжать посылать маяк, пока не примет ею от своего предшествующего соседа по кольцу. Этот процесс заканчивается, только когда в кольце останется единственный испускающий маяк компьютер. Когда и этот компьютер получит отправленный им маяк, он «поймет», что проблема устранена, и возобновит передачу маркера.

источник бесперебойного питания (ИБП) - uninterruptible power suply (UPS) — устройство, обеспечить полное электропитание оборудования при отключении основного электроснабжения. Устанавливается между источником электроэнергии, например электрической розеткой, и компьютером или другим электронным оборудованием. **Дополнительная** функция — защита оборудования от повышенного или пониженного напряжения в сети, колебаний напряжения, электромагнитных «шумов». Большинство высококлассных моделей имеет порт для взаимодействия с ОС защищаемого компьютера (например Windows NT), что позволяет автоматически завершить работу системы.

K

кабель с двойным экранированием ~ dual shielded cable — кабель со слоем фольги и плетения и слоем экранирующей металлической оплетки.

кабельная система компании IBM ~ IBM cabling system — стандарт, разработанный IBM в 1984 г., определяет разъемы кабелей, планшайбы, коммутационные панели и виды кабелей в сетях Token Ring. Многие параметры данного стандарта аналогичны спецификациям стандартов других компаний. Разъем для кабелей IBM имеет уникальную форму и является гермафродитным. Си. *также* гермафродитный разъем.

кадр ~ frame — пакет информации, передаваемый по сети в виде отдельного блока. Термин «кадр» наиболее часто используется в отношении сетей Ethernet. Кадр аналогичен используемым в других сетях пакетам. *См. также* кадр данных; пакет.

кадр данных ~ data frame — логический контейнер для транспортировки данных. При передаче данные разбиваются на небольшие фрагменты, к которым добавляются управляющая информация, например индикаторы начала и конца сообщения. Такой фрагмент называется кадром и передается как одно целое. Канальный уровень отвечает за «упаковку» в кадры потока бит, поступающих от физического уровня. Формат кадра зависит от применяемой сетевой топологии. *См. также* кадр.

канал - link — система связи, соединяющая две ЛВС посредством мостов, маршрутизаторов и шлюзов.

канал прямого доступа к памяти ~ direct memory access **(DMA) channel** — канал для прямого доступа к памяти, в котором не участвует микропроцессор. Обеспечивает прямую передачу данных между памятью и периферийным устройством.

канальный уровень ~ data link layer — второй уровень модели OSI. Здесь из последовательности бит, поступающих от физического уровня, формируются кадры. *См. также* эталонная модель взаимодействия открытых систем.

категории кабеля ~ cable categories — три основные группы кабелей: коаксиальный, витая пара (экранированная или неэкранированная) и оптоволоконный.

качество обслуживания - Quality of Service (QoS) — ряд новых и Windows 2000 набор стандартов контроля качества и механизмов для передачи данных.

кевлар - kevlar — фирменное название нитей в усиливающем пластиковом слое, окружающем каждое стекловолокно в оптоволоконном разъеме; стало нарицательным. Марка принадлежит корпорации DuPont.

кило... (к) ~ kilo (K) — 1) в метрической системе единиц означает 1000. В компьютерной терминологии, поскольку система вычислений построена на степенях двойки, зачастую означает 1 024 (2^{10}). Чтобы отличать эти значения в литературе на английском языке число 1000 зачастую обозначается миленькой буквой к, а число 1024 — большой буквой К. 1 килобайт равен 1024 байтам.

килобайт (кб) - kilobyte (KB) — 1024 байта. *См. также* бит; кило.

килобит (кбит) ~ kilobit (Kbit) — 1024 бита. *См. также* бит; кило.

клиент ~ client — компьютер (или программа), использующий сетевые ресурсы, которые предоставляет другой компьютер (или программа), называемый сервером. *См. также* сервер.

клиент DHCP ~ DHCP client — любое сетевое устройство, способное взаимодействовать с сервером **DHCP** для динамического получения IP-адреса и связанных дополнительных параметров.

клиент/сервер - client/server — сетевая архитектура, основанная на концепции распределенных вычислений. Приложение состоит из прикладной части, или сервера, которая хранит и обрабатывает данные, и интерфейсной части, или клиента, которая создает **комфортную** среду для работы пользователя и запрашивает необходимые данные с сервера. См. *также* **центральный** сервер фанлов.

ключ ~ key — 1) *В* БД идентификатор записи или группы записей в файле данных. Обычно и качестве ключа выступает содержимое специального поля, называемого ключевым или полем индекса (в зависимости от программы управления БД). Чтобы ускорить поиск записей, ключи объединяют в индексированные специальным образом таблицы. 2) Код для расшифровки данных.

коаксиальный кабель ~ coaxial cable (coax) — электрический кабель, имеющий соосное (коаксиальное) расположение центрального проводника, окруженного изолятором, и внешнею проводника, выполненного в виде проволочной оплетки. Снаружи коаксиальный кабель покрыт еще одним защитным слоем изолятора. Коаксиальный кабель менее подвержен помехам и ослаблению сигнала по сравнению с другими типами кабеля (например неэкранированной витой парой).

код аутентификации сообщения - Message Authentication Code (MAC) — алгоритм, гарантирующий подлинность блока данных.

кодек ~ codec (compression/decompression) — технология компрессии/декомпрессии для видеоданных и звука.

коммутация - switching — см. коммутация пакетов.

коммутация пакетов - packet switching — технология доставки сообщений, при которой пакеты ретранслируются станциями, расположенными в компьютерной сети вдоль наиболее удобного маршрута между источником и приемником. Данные перед отправкой разбиваются на небольшие пакеты, при получении восстанавливаются — процесс сборки пакетов (PAD). Маршруты (и время) прохождения пакетов из одного потока данных (виртуальному каналу) иногда различаются, однако принимающий PAD собирает пакеты в исходной последовательности. Сети с коммутацией пакетов быстры и эффективны. Из стандартов для сетей с коммутацией пакетов наиболее известен CCITT X.25. *См. также* сборщик/разборщик пакетов.

коммутируемый виртуальный канал ~ switched virtual circuit (SVC) — соединение между оконечными компьютерами, осуществляемое по определенному маршруту в сети. Известен также как соединение «один со многими». Сетевые ресурсы, выделенные каналу, и маршрут сохраняются до конца сеанса связи. *См. также* виртуальный канал.

компьютер с сокращенным набором команд - reduced instruction set computing (RISC) — тип архитектуры микропроцессора, ориентированный на быстрое и эффективное выполнение относительно небольшого набора команд. RISC-архитектура основана на предпосылке: большинство декодируемых и исполняемых компьютером команд являются простыми. Поэтому при RISC-архитектуре количество встроенных в микропроцессор команд ограничено. Зато они обеспечивают максимальную скорость выполнения, причем обычно за один такт. RISC-кристаллы выполняют простые команды быстрее, чем микропроцессоры, оперирующие обширным набором команд (CISC). Но чем сложнее операция, тем больше машинных команд ей требуется.

консоль управления - Microsoft Management Console (MMC) — «каркас» для встраивания административных утилит — консолей. Может включать утилиты, папки или другие контейнеры, Web-страницы и прочие административные средства. Все они отображаются на левой панели консоли — в дереве консоли. В главном окне MMC предусмотрены средства индивидуальной настройки консолей. При запуске консоли в пользовательском режиме средства настройки и дерево консоли могут быть скрыты.

контроллер домена ~ domain controller — в сетях Microsoft — компьютер Windows NT Server, аутентифицирующий регистрацию пользователей в домене, а

также хранящий политику защиты и главную базу данных домена. *См. также* главный контроллер домена; резервный контроллер домена.

концентратор 1) concentrator — сетевое устройство физического уровня, позволяющее объединять другие сетевые устройства. **1)** hub — связующий компонент, к которому подключаются все компьютеры и сети топологии «звезда». Активные концентраторы должны быть подключены к источнику электропитания; они могут восстанавливать и ретранслировать сигналы. Пассивные концентраторы просто выполняют коммутацию.

короткое замыкание ~ short ~ разрыв электрической цепи в результате контакта двух проводов под напряжением или провода под напряжением и земли.

криптография ~ cryptography — наука о защите данных и сообщений. Криптографические методы применяются для обеспечения конфиденциальности, целостности данных, аутентификации сущностей и данным и для предотвращения неавторизованной модификации передаваемой информации.

кэш - cache — специальный вид памяти или часть ОЗУ, где содержатся копии часто используемых данных. Обеспечивает к ним быстрый доступ. Кэш памяти хранит содержимое и адрес участка ОЗУ, к которому часто обращается процессор. При обращении процессора к адресу памяти кэш проверяет наличие у себя этого адреса. Если он его находит, обмен данными выполняется между процессором и кэшем; если не находит — между процессором и ОЗУ. Кэш полезен, когда скорость работы памяти меньше скорости работы процессора.

Л

лазерная передача - laser transmission — беспроводная сеть для передачи данных между устройствами посредством лазерного луча.

ЛВС-запросчик ~ LAN requester — *см.* запросчик.

линия T1 ~ T1 line — высокоскоростной коммуникационный канал, обеспечивающий цифровую передачу данных и доступ в Интернет со скоростью 1,544 Мбит/сек.

локальная вычислительная сеть (ЛВС) - local area network (LAN) — компьютеры, соединенные в сеть на ограниченной территории (например, в одной комнате, одном здании, группе близлежащих зданий).

локальная группа ~ local group — в Windows NT Server это учетная запись группы, определенная на отдельном компьютере. Группы могут включать учетные записи пользователей данного компьютера, учетные записи пользователей и глобальные группы своего домена, а также глобальные группы доверяемых доменов. Локальная группа, определенная для первичного контроллер домена, дублируется на всех резервных контроллерах лого домена. *См. также* группа.

локальный пользователь ~ local user — пользователь, непосредственно работающий на компьютере.

М

магистраль ~ backbone — основная линия связи, соединяющая все сегменты ЛВС, подключаемые к ней через концентраторы, коммутаторы, мосты и маршрутизаторы.

магистраль ~ trunk — отдельный кабель, также называемый главным, или сегментом.

магнитооптический диск (МО) ~ magneto-optical disk (MO) — пластиковый или стеклянный диск, покрытый составом с особыми свойствами. Чтение данных осуществляется с помощью отраженного маломощного луча лазера.

макровирус ~ macro virus — файловый вирус, названный так потому, что создается как макрос для определенного приложения. Обнаружение макровирусов затруднено, и они получают все большее распространение, поражая файлы популярных приложений, например текстовых процессоров. При открытии зараженного файла вирус прикрепляет себя к приложению и затем заражает все файлы, к которым обращается программа. *См. также* файловый вирус.

маркер ~ token — предопределенная комбинация бит, служебный кадр, который разрешает сетевой станции передать кадр данных. После передачи информационного кадра (а также при его отсутствии) станция передает маркер следующей в логическом «кольце» станции. В сетях Token Ring логическое «кольцо» совпадает с физическим. *См. также* ARC-Net; Token Ring; передача маркера.

маршрутизатор - router — устройство для соединения сетей различного типа, использующих разные архитектуры. Маршрутизаторы работают на сетевом уровне модели OSI; могут направлять пакеты через несколько сетей. Обмениваясь **служебной** информацией, маршрутизаторы определяют лучший путь для передачи данных. Кроме того, осуществляют фильтрование широковещательных сообщений.

маршрутизируемый протокол ~ mutable **protocol** — протокол, поддерживающий несколько маршрутов от одной ЛВС к другой. *См. также* протокол.

маска подсети - subnet mask — 32-разрядное число, состоящее из последовательной группы единичных битов для выделения поля IP-адреса кода сети и последовательной группы нулевых битов для выделения кода узла.

Мбит/с ~ Mbps — *см.* миллион бит в секунду (Мбит/с).

мегабайт (Мб) ~ megabyte (MB) — 1 048 576 байт (2 ^{20}). *См. также* байт.

мегабит (Мбит) ~ megabit (Mb) — 1 048 576 бит. *См. также* бит.

межсетевое взаимодействие ~ internetworking — обмен данными в сети, состоящей из нескольких небольших сетей.

миллион битов в секунду (Мбит/с) ~ millions of bits per second — единица измерения скорости передачи данных по коаксиальному кабелю, витой паре и оптоволокну. *См. также* бит.

многозадачность ~ multitasking — *организация* вычислительных процессов и ОС, при которой компьютер выполняет одновременно (или псевдоодновременно) несколько задач. **Существует дня** основных **типа** многозадачности: вытесняющая и невытесняющая. «Истинно» многозадачная ОС способна запускать столько задач, сколько имеется процессоров. Если же задач больше, чем процессоров, используется механизм разделения процессорного времени, когда каждая выполняемая задача занимает процессор на ограниченное время, после чего он переключается на выполнение другой запущенной задачи и т. д. *См. также* вытесняющая многозадачность; невытесняющая многозадачность.

множественный доступ с контролем несущей и избежанием коллизий - carrier-sense multiple access with collision avoidance (CSMA/CA) — способ доступа, при котором каждый компьютер, прежде чем передавать данные, сигнализирует об этом в сеть, тем самым предотвращая возможные коллизии. *См. также* способ доступа.

множественный доступ с контролем несущей и обнаружением коллизий ~ Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) — способ доступа, используемый в сетях топологий «шина» и «звезда». Станция «прослушивает» канал передачи данных, чтобы определить, не осуществляет ли уже другая станция передачу кадра данных. Если нет, «слушающая» станция посылает свои данные. Суть «прослушивания» — проверить наличие несущего определенного уровня напряжения или сигнал. Множественный доступ — несколько станций пытаются получить доступ к кабелю в одно и то же время. Обнаружение коллизий — станции определяют возникновение коллизии. Если две станции начинают передачу одновременно, происходит коллизия. Перед повторной попыткой передачи они должны выждать случайный промежуток времени. *См. также* способ доступа.

мобильные вычисления ~ mobile computing — интеграция мобильных компьютеров в существующие кабельные сети по беспроводным адаптерам, использующим технологию сотовой связи.

модель домена ~ domain model — группировка одного или нескольких доменов с установленными административными и коммуникационными связями для управления пользователями и ресурсами.

модем ~ modem — сокращение от МОдулятор-ДЕМодулятор. Устройство связи, позволяющее компьютеру передавать данные по обычной телефонной линии. Выполняет модуляцию звукового сигнала, передаваемого по **телефонной** линии, в соответствии с поступающими от компьютера цифровыми данными. При передаче преобразует цифровые сигналы в аналоговые. При приеме преобразует аналоговые сигналы в цифровые.

модулированная ISDN ~ Broadband ISDN (BISDN) — модулированная цифровая сеть комплексных услуг. Рекомендация CCITT по передаче речи, двоичных данных и видео в диапазоне скоростей порядка мегабит и гигабит. **BISDN**, кроме того, представляет собой отдельную ISDN-сеть, способную оперировать речью, двоичными данными и видео. Работает с транспортной сетью на оптическом кабеле, называемой синхронной оптической сетью (SONET), и с сетью на основе асинхронного режима передачи (ATM). Коммутируемые мультимегабитные служебы данных (SMDS) также являются службой **BISDN**, обеспечивающей высокую пропускную способность в ГВС. *См. также* асинхронный режим передачи; синхронная оптическая сеть; служба коммутируемых мультимегабитных данных.

модулированная сеть - broadband network — ЛВС, в которой передача данных осуществляется с помощью модуляции аналоговых сигналов. Вся полоса пропускания среды передачи разбивается на несколько интервалов (полос), каждый из которых служит каналом связи. Устройства в **такой** сети соединяются коаксиальным или оптоволоконным кабелем. Эти сети по одной физической среде могут одновременно передавать телепрограммы, речь, двоичные данные и т. п.

модуль множественного доступа ~ Multistation Access Unit (MAU *или* **MSAU**) — концентратор в сети **MX** Token Ring. Организует внутри себя кольцо из станций, подключаемых к MAU радиально.

монитор сети ~ network monitor — программно-аппаратное устройство, которое отслеживает весь сетевой трафик или его часть. Проверяет пакеты на уровне кадров, собирает информацию о типах пакетов, ошибках и трафике от каждого компьютера к каждому компьютеру.

монтажный блок - punch down block — приспособление или серия приспособлений, в которые можно вставить кабель для коммутации. Для сред, требующих централизованного расположения всей кабельной системы (упрощает модификацию), монтажный блок — оптимальный вариант.

мост ~ bridge — устройство для связи ЛВС. Позволяет станциям любой из сетей обращаться к ресурсам другой сети. Также используется для увеличения длины или количества узлов сети. Выполняет соединение на канальном уровне модели OSI.

мост-маршрутизатор - bridge-router, brouter — устройство для связи сетей, сочетающее свойства моста и маршрутизатора. Выполняет маршрутизацию для маршрутизируемых протоколов и функции моста — для немаршрутизируемых протоколов, представляя, таким образом, более экономичное и более гибкое в управлении средство для взаимодействия сетей по сравнению с отдельным мостом и маршрутизатором. Считается наилучшим вариантом для сред, в которых несколько однородных сегментов ЛВС объединены с двумя разнородными.

мультиплексор - multiplexer (mux) — устройство, позволяющее разделить канал передачи на несколько подканалов. Может быть реализован программно. Используется также для подключения нескольких линий связи к компьютеру.

Н

набор томов ~ volume set — совокупность разделов на жестких дисках, которые трактуются как единый раздел. Увеличивают, таким образом, дисковое про-

странство, ассоциированное с одним именем устройства. Объединяют от 2 до 32 областей неформатированного свободного дискового пространства на одном или нескольких физических устройствах. Эти области формируют один большой логический диск.

невытесняющая многозадачность - nonpreemptive multitasking — особенность ОС, при которой она не может «отобрать» управление процессором у выполняемой задачи. Задача сама решает, когда освободить процессор. Программы, написанные для систем с невытесняющей многозадачностью, должны иметь специальные средства для освобождения процессора. Никакая другая программа не начнет работу, пока исполняющаяся в данный момент задача не передаст ей управление процессором. *См. также* вытесняющая многозадачность; многозадачность.

немодулированная передача ~ baseband — способ передачи данных по кабелю, при котором каждый бит данных кодируется отдельным электрическим или световым импульсом. При немодулированной передаче вся ширина полосы пропускания кабеля используется как один канал связи.

неэкранированная витая пара ~ unshielded twisted-pair cable (UTP) — витая пара, не имеющая металлического экрана, что упрощает конструкцию кабеля и снижает его стоимость. *См. также* витая пара.

O

область DHCP ~ DHCP scope — диапазон IP-адресов, доступных в службе DHCP для назначения клиентам **DHCP.**

оболочка - shell — **ПО.** реализующее взаимодействие пользователя с ОС (пользовательский интерфейс). В Windows 2000 в качестве оболочки выступает Explorer (Проводник).

обратный вызов - callback — функция Windows 2000, позволяющая удаленному серверу вызывать клиента по телефонной линии. Снижает затраты клиента на телефонные переговоры, поскольку оплата производится за счет удаленного сервера, а также повышает защищенность данных — клиент вызывается по номеру, указанному администратором.

обратный просмотр ~ reverse lookup — запрос, в процессе которого осуществляется поиск IP-адреса компьютера с целью определения его понятного доменного имени DNS.

общегородская сеть - metropolitan area **network (MAN)** — компьютерная сеть масштаба города. По территориальному признаку выходит за рамки ЛВС, но не дотягивает до размеров ГВС. Характеризуется наличием высокоскоростных оптоволоконных магистралей.

общедоступная сеть данных - public data network (PDN) — коммерческая служба ГВС, реализованная телефонными компаниями.

объект ~ object — именованный набор атрибутов, представляющий сетевой ресурс в Active Directory. Например, к числу атрибутов учетной записи относятся имя и фамилия пользователя, отдел, где он работает, и адрес электронной почты.

одноранговая сеть ~ peer-|o-peer network — сеть, в которой нет выделенных серверов и иерархии компьютеров. Все компьютеры считаются равноправными. Обычно каждый компьютер выступает в роли и сервера, и клиента. *См. также* рабочая группа; сеть на основе сервера.

Ом ~ ohm — единица измерения электрического сопротивления. Сопротивление в 1 Ом пропускает ток силой 1 А при напряжении в 1 В. Электролампа мощностью 100 Вт имеет сопротивление приблизительно 130 Ом.

оперативная память (ОЗУ) ~ random access memory (RAM) — полупроводниковая энергозависимая память, доступная для чтения и записи со стороны микропроцессора или других аппаратных устройств. Доступ может осуществляться по произвольному адресу. Заметьте: различные виды постоянных запоминающих устройств (ПЗУ) также обеспечивают произвольный доступ. *См. также* постоянное запоминающее устройство (ПЗУ).

оптоволоконный кабель - fiber-optic cable — кабель, по которому цифровые данные передаются в виде модулированных световых импульсов. Состоит из чрезвычайно тонкого стеклянного цилиндра (ядро), окруженного слоем стекла (покрытие) с другим коэффициентом преломления.

оснастка - snap-in — тип инструмента, который можно добавить в консоль, производную от MMC. Изолированную оснастку можно использовать независимо от других оснасток, в то время как оснастку расширения можно задействовать только в качестве дополнения другой оснастки.

основной раздел - primary partition — том, создаваемый из невыделенного пространства базового диска. Windows 2000 и другие ОС загружаются с основного раздела. На базовом диске можно создавать до четырех основных разделов или три основных и один дополнительный раздел. Основные разделы разрешается создавать лишь на базовых дисках; они не могут содержать подразделов.

осциллограф - oscilloscope — устройство для отображении формы электрических сигналов на экране монитора. Современные осциллографы позволяют также измерять параметры электрических сигналов.

отказоустойчивость ~ fault tolerance — свойство компьютера или ОС сохранять работоспособность и данные при сбое питания или поломке оборудования.

открытый ключ - public key — открытая (несекретная) часть пары криптографических ключей, сгенерированных с применением алгоритма шифрования с открытым ключом. Обычно служит для верификации цифровых подписей или для расшифровки сообщений, зашифрованных соответствующим закрытым ключом.

отражение сигнала - signal bounce — явление, наблюдаемое в кабеле при несогласованной нагрузке. Электромагнитная волна распространяется по кабелю и, достигая его конца, отражается. Отраженная волна создает помехи, препятствующие нормальной работе станций в сети. Чтобы предотвратить отраже-

ния, к каждому концу кабеля подключаются терминаторы: они поглощают приходящий сигнал. Сопротивление терминатора должно быть согласовано с волновым сопротивлением кабеля (50 Ом — для сетей Ethernet и 93 Ом — для сетей ARCNet). Си. *также* герминатор.

очередь печати ~ **print queue** — буфер, в котором задание на печать хранится ло тех пор, пока принтер не будет готов принять его.

П

пакет ~ packet — блок информации сетевого уровня модели OSI, передаваемый между станциями сети. Содержит данные и.) протоколов более высокого уровня, а также заголовок с идентификатором, адресами источника и приемника, иногда — поля данных контроля ошибок. Си. *также* кадр.

передача маркера - token passing — способ управления доступом к среде в сетях Token Ring. Кадр данных (маркер) передается по кольцу от одной станции к другой. Си. *также* Token Ring; маркер.

перезаписываемый оптический диск - rewritable optical disk — оптический диск, допускающий многократную запись.

перекрестные помехи ~ **crosstalk** — наводки, производимые соседним проводом (проводами). Например, если вы, разговаривая по телефону, слышите, хотя и отдаленно, чью-то беседу, это значит, что ваша телефонная линия находится под влиянием перекрёстных помех.

перемычка ~ **jumper** — небольшой пластиковый переключатель (или пронесенные штырьки с контактной пластиной): соединяет две точки электронной схемы. Перемычки используются для выбора определенной цепи или параметра из нескольких возможных вариантов. Например, с помощью перемычек на плате сетевого адаптера выбирают тип соединения с линией. DIX или BNC.

периферийное устройство - peripheral — устройство, которое подключается к компьютеру и которым управляет его микропроцессор (жесткие диски, принтеры, мыши, джойстики и т. п.).

персональный **цифровой помощник** - Personal Digital Assistant (PDA) — карманный компьютер, выполняющий ряд специальных функций. Обычно это функции календаря, записной книжки, калькулятора, а также управление базами данных и услуги связи. Современные PDA в качестве устройства ввода вместо клавиатуры или мыши снабжены специальной ручкой. Все программное обеспечение PDA является встроенным, поэтому любые дополнительные программы устанавливаются через подключение платы PC (PC Card) или с управляемым ими устройством. Для хранения данных вместо дисковых накопителей PDA использует флэш-память. PDA осуществляет связь по сотовой или беспроводной технологии, часто встроенной в систему, но эти возможности также удается расширить, подключив плату PC.

петабайт - petabyte — *см.* байт.

ПЗУ удаленной **загрузки** ~ **remote-boot** PROM — специальная микросхема, устанавливаемая на сетевой плате. Содержит микропрограмму для загрузки компьютера по сети. Используется на бездисковых компьютерах. См. *также* бездисковый компьютер.

плакировка - cladding — концентрический слой стекла, окружающий сверхтонкий цилиндрический стеклянный сердечник оптоволоконного кабеля.

пленум - plenum — небольшое пространство между подвесным потолком и перекрытием, используемое во многих зданиях для вентиляции и прокладки кабеля. Правила противопожарной безопасности налагают жесткие требования к типу проложенного здесь кабеля.

повторитель - repeater — устройство регенерации сигналов, позволяющее передавать их по дополнительному сегменту кабеля (увеличивая тем самым общую длину линии связи) или подключать большее число компьютеров к существующему сегменту. Работают на физическом уровне модели OSI, объединяют однотипные сети (например Ethernet с Ethernet), но не выполняют преобразование или фильтрование данных. Чтобы повторитель работал, оба соединяемых им сегмента должны использовать одинаковую схему доступа к среде и архитектуру. *См. также* усилитель.

поддомен ~ **subdomain** — домен DNS, расположенный в дереве пространства имен на один уровень ниже другого (родительского) домена. Например, example.microsoft.com мог бы быть поддоменом домена microsoft.com.

подсеть ~ subnet — часть сети, которая может быть физически *независимым* сегментом сети, *совместно* использующая классовый сетевой адрес с другими частями той же сети и идентифицируемая по номеру подсети.

подуровень управления доступом к среде ~ Media Access Control (MAC) sublayer — согласно стандарту IEEE 802, канальный уровень модели OSI разбивается на два подуровня. Подуровень управления доступом к среде непосредственно взаимодействует с платой сетевого адаптера и отвечает за безошибочную передачу данных между двумя компьютерами в сети. См. *также* подуровень управления логической связью.

подуровень управления логической связью - Logical Link Control (LLC) sublayer — стандарт IEEE 802 подразделяет канальный уровень модели OSI на два подуровня: подуровень управления логической связью (верхний) и подуровень управления доступом к среде (нижний). Верхний из них управляет передачей данных и определяет использование логических точек интерфейса (называемых точками доступа *к* услугам (SAP)). Через эти точки информация передается от подуровня LLC к вышестоящим уровням модели OSI. См. *также* подуровень управления доступом к среде; точка доступа к услугам.

поливинилхлорид - PVC (polyvinyl chloride) — пластмасса, часто используемая в кабелях как изоляционный материал.

полиморфный вирус ~ polymorphic virus — вирус, написанный так, что при каждом заражении он изменяет свой код. Заражая очередной файл. Его обнаружение затруднено, потому что все копии вируса разные. *См. также* файловый вирус.

полнодуплексная передача • full-duplex transmission — одновременная двунаправленная передача данных между двумя станциями. Известна также как полнодуплексная передача. Другие способы передачи: симплексная (передача только в одном направлении) и полудуплексная (двунаправленная передача данных в каждом из направлений поочередно). *См. также* дуплексная передача.

полное доменное имя ~ fully qualified domain name (FQDN) — доменное имя узла согласно спецификации системы доменных имен, точно указывающее расположение узла в дереве пространства имен домена. Полные доменные имена отличаются от относительных тем, что для указания расположения относительно корня пространства имен части полных доменных имен обычно разделяются точками (т.е. например host.example.microsoft.com.

полоса пропускания ~ bandwidth — в системах связи — разность между максимальной и минимальной частотой в заданном диапазоне. Например, телефон имеет полосу пропускания 3000 Гц, равную разности между максимальной (3300 Гц) и минимальной (300 Гц) частотой, с которой он способен передавать данные. В компьютерных сетях полоса пропускания шире, что позволяет быстрее передавать данные.

полудуплексная передача ~ half-duplex transmission — двусторонняя связь, осуществляемая одновременно в одном направлении.

порт принтера ~ printer port — программный интерфейс, обеспечивающий взаимодействие компьютера с устройством печати через локально подключенный интерфейс. К числу поддерживаемых интерфейсов относятся LPT, COM, USB и такие сетевые устройства, как HP JetDirect и Intel NetPort.

последовательная передача ~ serial transmission — передача данных бит за битом.

постоянное запоминающее устройство (ПЗУ) ~ read-only memory (ROM) — полупроводниковая энергонезависимая память, содержащая команды или данные, которые можно считать, но нельзя изменить. *См. также* оперативная память (ОЗУ).

постоянный виртуальный канал - permanent virtual circuit (PVC) – соединение, похожее на арендуемую линию. Представляет собой постоянный и фактически существующий канал. В отличие от аренды линии вы платите только за то время, в течение которого его используете. Важность данного типа услуг связи возрастает, так как PVC используется при ретрансляции кадров и ATM. Ог. *также* виртуальный канал; коммутация пакетов.

потеря маркера ~ lost token — сбой в сети Token Ring. Владеющая маркером станция выходит из строя и не может его передать. В результате маркер в кольце пропадает.

поток данных ~ data stream — непрерывный поток байт данных.

правило -5-4-3» ~ 5-4-3 rule — гласит, что в сети на «тонком Ethernet» может быть до 5 сегментов, соединенных 4 повторителями, но лишь к 3 сегментам разрешается подключать компьютеры.

представительский уровень ~ presentation layer — шестой уровень модели OSI. Определяет формат, применяемый для обмена данными между компьютерами сети. На посылающем компьютере этот уровень преобразует данные из формата, в котором они поступают от прикладного уровня, в общий промежуточный формат. На принимающем компьютере этот уровень преобразует промежуточный формат в первоначальный, используемый прикладным уровнем. Кроме того, управляет сетевой системой безопасности, предоставляя такие услуги, как шифрование данных. Задает правила передачи данных, осуществляет сжатие данных для уменьшения числа передаваемых битов. *См. также* эталонная модель взаимодействия открытых систем.

привилегии - right — набор действий, которые пользователям разрешено выполнять в системе. В отличие от прав доступа, применяемых к отдельным объектам, применяются ко всей системе в целом. Примером может служить привилегия создавать резервные копии, включая файлы, к которым у пользователя нет прав доступа. *См. также* разрешение доступа.

привязать - bind — ассоциировать одну часть информации с другой.

привязка - binding — создание канала связи между сетевой службой, драйвером протокола и драйвером сетевой платы.

прикладная часть - back end — название части клиент-серверного приложения, выполняющейся на сервере.

прикладной уровень ~ application layer — верхний (седьмой) уровень модели OSI. Представляет службы, напрямую поддерживающие пользовательские приложения (например, передачу файлов, доступ к базам данных, электронную почту), то есть служит окном, через которое прикладные процессы получают доступ к сетевым службам.

принтер - printer — программный интерфейс между ОС и устройством печати. Определяет, куда и когда передать документ, чтобы он попал на устройство печати (локальный или сетевой порт или файл), а также обрабатывает процесс печати.

программное обеспечение (ПО) - software — компьютерная программа или набор инструкций, обеспечивающих работу оборудования. **ПО** можно разделить на четыре группы:

- операционные системы (ОС) — управляют работой компьютера;
- прикладное ПО — текстовые процессоры, электронные таблицы, базы данных и прочие программы, выполняющие задачи, ради которых люди используют компьютеры;

- сетевое ПО — обеспечивает взаимодействие групп компьютеров;
- языки программирования — средства, необходимые программистам для создания программ.

прокси-сервер ~ proxy server — компонент брандмауэра, управляющий входящим и исходящим трафиком Интернета в ЛВС. Определяет безопасность передачи сообщений или файлов в сеть организации, управляет доступом к сети, фильтрует и отклоняет запросы согласно заданным параметрам, включая запросы на несанкционированный доступ к конфиденциальным данным.

промежуточная система ~ **intermediate** system — оборудование для связи сетей (например, мосты, маршрутизаторы и шлюзы).

пропускная способность - throughput — скорость прохождения данных через какой-либо компонент, канал связи или систему. Служит хорошим индикатором общей производительности системы, так как определяет, насколько корректно совместно работают компоненты при передаче данных от одного компьютера к другому (сколько байт или пакетов передается по сети в единицу времени).

простой протокол передачи почты ~ Simple Mail Transfer Protocol (SMTP) — протокол семейства TCP/IP для обмена электронной почтой. *См. также* Transport Control Protocol/Internet Protocol (TCP/IP); протокол прикладного уровня.

простои протокол управления сетью - Simple Network Management Protocol (SNMP) — протокол прикладного уровня модели OSI для управления сетью. Опирается на протоколы нижних уровней (TCP/IP). В SNMP небольшие служебные программы-агенты собирают данные о компонентах сети, которые помещают затем в базу управляющей информации (MIB). Административная программа — диспетчер — регулярно опрашивает агенты и загружает эти данные (из MIB). Такой метод позволяет управлять сетью, передавая агентам административные распоряжения, и следить за состоянием сети. Если какие-то данные по своему значению выходят за установленные пределы, менеджер выдает на монитор описание проблемы и автоматически отправляет сообщение на пейджеры обслуживающего персонала.

пространство имен ~ namespace — набор уникальных имен ресурсов или элементов, используемых в разделяемой компьютерной среде. В MMC пространство имен представлено деревом консоли, отображающей все оснастки и ресурсы, доступные из данной консоли. В DNS пространство имен представляет собой иерархическую структуру дерева имен домена. Каждая метка домена (например host1 или example), используемая в полном доменном имени (например, host1.example.microsoft.com), указывает на ветвь дерева пространства имен домена. См. *также* MMC (Microsoft Management Console); оснастка; ресурс.

протоко.т ~ protocol — набор правил и соглашений, обеспечивающий максимально возможную скорость и наименьшее число ошибок при связи компьютеров друг с другом и с периферийными устройствами. Взаимосогласованные протоколы разных уровней составляют стек протоколов. Существует множество различных протоколов, не все из которых совместимы друг с другом; тем не менее если два устройства используют один протокол, они могут обмениваться данными. Существуют также подпротоколы, определяющие различные аспекты связи. Некоторые протоколы, например стандарт RS-232, управляют аппаратными соединениями. Другие стандарты управляют передачей данных, включая параметры и сигналы рукопожатия (например сигнал XON/OFF, используемый при асинхронной связи), а также методами кодирования данных (побитные и побайтовые протоколы). Протоколы, аналогичные широко используемому протоколу XMODEM, управляют передачей файлов, а такие протоколы, как CSMA/CD, определяют способы передачи сообщений между станциями ЛВС. Протоколы представляют собой попытку упростить сложный процесс связи между компьютерами разных моделей и производителей. В качестве примеров протоколов можно также принести модель OSI, протокол SNA компании IBM, а также набор Интернет-протоколов, включая TCP/IP. *См. также* Systems Network Architecture (SNA); Transport Control Protocol/Internet Protocol (TCP/IP).

протокол **динамической** конфигурации узла - Dynamic Host Configuration Protocol (DHCP) — протокол автоматической настройки узлов в сетях на базе протокола TCP/IP, предусматривающий динамическое выделение узлу IP-адресов и другой конфигурационной информации. См. *также* Transport Control Protocol/Internet Protocol (TCP/IP).

протокол передачи файлов - File Transfer Protocol (FTP) — протокол, обеспечивающий передачу файлов между локальным и удаленным компьютерами. Поддерживает несколько команд, реализующих двунаправленную передачу двоичных и ASCII-файлов между компьютерами. FTP-клиент поставляется с утилитами связи TCP/IP. *См. также* Transport Control Protocol/Internet Protocol (TCP/IP); американский стандартный набор символов для обмена информацией.

протокол **прикладного** уровня - application protocol — работает на верхнем уровне модели OSI и обеспечивает взаимодействие и обмен данными между программами. Наиболее популярные протоколы:

- FTAM (File Transfer, Access and Management) — протокол доступа к файлам;
- SMTP (Simple Mail Transfer Protocol) — TCP/IP-протокол передачи электронной почты;
- Telnet — TCP/IP-протокол для доступа к удаленному компьютеру и обработки данных на нем;
- NCP (NetWare Core Protocol) — основной протокол для передачи информации между сервером NetWare и его клиентами.

протокол связи имен - Name Binding Protocol, NBP — протокол фирмы Apple. Отвечает за сохранение соответствия между именованными объектами в сети и их Интернет-адресами. Работает на транспортном уровне модели OSI.

прямой доступ к памяти ~ direct memory access (DMA) — режим доступа к памяти, при котором не задействован микропроцессор. Используется при обмене информацией между памятью и «умным» периферийным устройством, например контроллером жесткого диска или сетевой платой.

пул принтеров ~ printer pool — принтер, подключенный к нескольким устройствам печати через несколько портов сервера печати. В качестве сервера печати могут выступать локальные или сетевые устройства печати. Устройства печати должны был. одинаковыми. Впрочем, можно объединять в пул и разные устройства печати, использующие одинаковый драйвер.

Р

рабочая группа - workgroup — набор «равноправных» компьютеров, объединенных в ЛВС для совместного использования ресурсов, таких, как данные и периферийные устройства. Каждая рабочая группа имеет уникальное имя. *См. также* домен; одноранговая сеть.

рабочая станция - workstation — любой сетевой персональный компьютер, использующий ресурсы сервера.

радиопередача в рассеянном спектре ~ spread-spectrum radio technology -- технология передачи в беспроводных сетях. Данные передаются в нескольких частотных диапазонах. За счет этого решаются коммуникационные проблемы, характерные для одночастотной передачи.

радиопередача в узком диапазоне (одночастотная передача) - narrowband (single-frequency) transmission — технология высокочастотной радиопередачи, похожая на обычное радиовещание. Пользователь настраивает приемник и передатчик на определенную частоту и обменивается данными по радиоканалу.

раздел ~ partition — часть физического диска, воспринимаемая ОС как отдельное логическое устройство.

разделение на уровни - layering — координация различных протоколов в определенной архитектуре, обеспечивающая совместную работу протоколов для подготовки, передачи, приема и обработки данных.

разделять - share — открывать общий доступ к ресурсам, например, папкам и принтерам.

разрешение имен - name resolution — процесс сопоставления (трансляции) имен, удобных для работы пользователей, с числовыми IP-адресами, необходимыми для работы TCP/IP. Может осуществляться программными компонентами, такими, как DNS и WINS.

разрешение доступа ~ access permissions — определяет тип доступа к разделяемым ресурсам. В Windows 2000 Server предусмотрено четыре уровня доступа:

- No Access — запрещает доступ к разделяемому каталогу, его подкаталогам и файлам;
- Read — разрешает просмотр списка имен файлов и подкаталогов, вход в подкаталог, просмотр данных в файлах, а также запуск приложений.
- Change — разрешает просмотр списка имен файлов и подкаталогов, вход в подкаталоги, просмотр данных в файлах, запуск приложений, добавление и удаление файлов и подкаталогов, а также изменение данных в файле;
- Full Control — включает все разрешения, предоставляемые уровнем доступа Change, позволяет изменять разрешения на доступ к ресурсам, а также брать во владение файлы и каталоги (только для файловой системы **NTFS).**

разъем BNC - BMC cable connector — разъем для коаксиального кабеля. Фиксируется поворотом замка на 90 градусов.

разъем-заглушка - hardware loopback — разъем, используемый при диагностике оборудования. Замыкает выходную линию на входную, позволяя компьютеру передавать данные самому себе. Если пересылаемые данные не поступают на вход, то налицо неисправность оборудования.

распределенная файловая система ~ distributed file system (DFS) — единая логическая иерархичная файловая система. Для отображения ресурсов файловой системы организует папки различных компьютеров сети в логическую древовидную структуру.

расширенный **двоично-десятичный код обмена информацией ~ Extended Binary Coded Decimal Interchange Code (EBCDIC)** — схема кодировки, разработанная IBM. Используется мэйнфреймами и персональными компьютерами как стандартный метод присвоения двоичных (численных) значений буквам, цифрам, знакам пунктуации и управляющим символам.

расширенный раздел ~ extended partition — часть базового диска, где могут размещаться логические диски. Позволяет создать на базовом диске более четырех томов. Только один из четырех томов может являться расширенным разделом; для создания расширенного раздела наличие основного раздела не требуется. Расширенные разделы разрешается создавать только на базовых дисках.

расширенный тестер кабеля - advanced cable tester — специальное средство, работающее на уровнях OSI выше физического — втором, третьем и даже четвертом. Выдает информацию **о физическом** состоянии кабеля, а также о числе кадров в сообщении, избыточных коллизиях, последних коллизиях, числе ошибочных кадров, ошибках, вызванных перегрузкой сети, и собственно перегрузке. Позволяет вести мониторинг трафика как всей сети, так и отдельного компьютера, выявлять определенные виды ошибок, неисправный кабель или сетевую плату.

редиректор - redirector — сетевое ПО, эмулирующее доступ к удаленной **файловой** системе, как к локальной. Принимает запросы ввода-вывода от приложения, а затем переадресует их сетевой службе сервера. Результаты обращения возвращаются приложению в том виде, как если бы файлы находились на локальном компьютере. См. *также* запросчик.

резервная копия - backup — копия программы, диска или данных, созданная во избежание потери важных файлов.

резервный контроллер домена ~ backup domain controller (BDC) — в домене Windows NT Server — компьютер, который хранит копию политики безопасности домена и базы учетных данных домена и производит аутентификацию регистрирующихся в сети пользователей. Служит резервом, если главный контроллер домена недоступен. Наличие резервного контроллера в домене необязательно, но рекомендуется. *См. также* главный контроллер домена; домен; контроллер домена.

ресурс ~ resource — любая часть компьютерной системы, используемая приложениями. Все, кто подключен к сети, могут совместно использовать такие ресурсы удаленных компьютеров, как жесткие диски, принтеры, модемы, CD-ROM-дисководы и даже процессор.

ретрансляция кадров ~ frame relay — передающий цифровая высокоскоростная технология передачи кадров переменной длины. Использует коммутацию кадров и технологию «точка-точка», которая применяет виртуальный канал (PVC) для передачи кадров переменной длины на канальном уровне модели OSI. Сети с ретрансляцией кадров способны предоставить абонентам такую полосу пропускания, которая им необходима. Это позволяет осуществлять любой тип передачи.

рефлектометр ~ time-domain reflectometer (TDR) — инструмент для выявления проблем. Посылая по кабелю короткие импульсы, определяет разрывы, короткие замыкания или дефекты, которые могут быть причиной сбоев. Обнаруживдефект, классифицирует его и выдает результат на экран. Хороший TDR способен локализовать разрыв с точностью до нескольких десятков сантиметров. *См. также* сетевой анализатор.

рукопожатие ~ handshaking — информация, передаваемая отправляющей и принимающей сторонами для поддержания потока данных и управления им. Обычно относится к модемной связи. Гарантирует, что принимающее устройство будет готово к получению данных, прежде чем передающее начнет их отправку.

С

сборщик/разборщик пакетов ~ packet assembler/disassembler (PAD) — устройство, которое перед отправкой разбивает потоки данных на пакеты, передаваемые по сетям с коммутацией пакетов (например CCITT X.25), а при получении восстанавливает из пакетов потоки данных. *См. также* коммутация пакетов.

связь «точка-точка» ~ point-to-point configuration — выделенный канал связи, также называемый арендуемой линией. Самый распространенный способ связи в ГВС. Гарантирует полнодуплексную полосу пропускания **между** двумя оконечными точками. Обычно используется для соединения двух ЛВС через мосты или маршрутизаторы. *См. также* Point-to-Point Protocol (PPP); Point-to-Point Tunneling Protocol (PPTP); дуплексная передача.

сеанс ~ session — цикл операций, при котором между станциями в сети устанавливается соединение, производится обмен информацией и завершается соединение.

сеансовый уровень ~ session layer — пятый уровень модели OSI. Позволяет двум приложениям на различных компьютерах устанавливать, поддерживать и завершать соединение, называемое сеансом. Выполняет распознавание имен и ряд других функций (например защиту, необходимую для поддержания связи двух приложений по сети). Обеспечивает синхронизацию между задачами и диалог между взаимодействующими процессами, решая, какой стороне передавать данные, когда, как долго и т. д. *См. также* эталонная модель взаимодействия открытых систем.

сегмент ~ segment — 1) Часть ЛВС, ограниченная связующими устройствами (повторителями, мостами, маршрутизаторами и *шлюзами*). 2) *Сообщения*, разбитые драйвером протокола на несколько частей.

сектор ~ sector — фрагмент дискового пространства. Диск подразделяется на стороны (верхняя и нижняя), дорожки (концентрические кольца на каждой стороне) и секторы (часть кольца). Сектор - наименьший элемент физической памяти на диске. **Имеет** фиксированный размер, обычно 512 байт данных.

сервер ~ server — 1) Компонент сетевой ОС, предоставляющий клиентам доступ к сетевым ресурсам. Для каждого вида ресурсов в сети может быть создан один или несколько серверов. Чаще всего применяются серверы файлов, печати, баз **данных,** удаленного доступа и т. д. 2) Компьютер, выполняющий программу сервера и предоставляющий свои ресурсы в совместное использование в сети. *См. также* клиент.

сервер DHCP ~ DHCP server — компьютер с Windows 2000 Server, выполняющий службу **DHCP,** обеспечивающую динамическое распределение IP-адресов и связанной информации для клиентов DHCP.

сервер доступа к сети ~ network access server (NAS) — устройство, принимающее PPP-соединения и подключающее клиентов к обслуживаемой сети.

сердечник ~ core — внутренняя часть кабеля, по которой передаются электронные сигналы, кодирующие данные. Сердечник может быть цельным (обычно медным) или многожильным. В оптоволоконном кабеле сигнал передается по сверхтонкому цилиндрическому стеклянному сердечнику, окруженному плакировкой.

сертификат ~ certificate — цифровой документ, обычно используемый для аутентификации и безопасного обмена информацией по общедоступным сет-м, например Интернету. Сертификат позволяет безопасным образом связать открытый ключ с владельцем соответствующего закрытого ключа. Сертификаты, скрепленные цифровой подписью выпустившего их центра сертификации; их выдают пользователю, компьютеру или службе. Наиболее широко применяемый формат сертификатов определен в международном стандарте ITU-TX.509.

сетевая плата ~ network adapter card — плата расширения для подключения компьютера к ЛВС. Пред-

ставляет собой физический интерфейс (соединение) между компьютером и сетевым кабелем.

сетевой анализатор ~ network analyzer — инструмент диагностики сети. Известен также как анализатор протоколов. При анализе сетевого трафика работает в реальном времени, а также выполняет захват, декодирование сетевых пакетов и передачу тестовых пакетов. Позволяет вести статистику о трафике в сети, которая затем поможет воссоздать сетевые события на разных уровнях протоколов. Большинство анализаторов имеет встроенный рефлектометр. *См. также* рефлектометр.

сетевой уровень - network layer — третий уровень модели OSI. Отвечает за адресацию пакетов и преобразование логических адресов и имен сетевых узлов в их физические адреса. Определяет маршрут данных от компьютера-отправителя к компьютеру-получателю на основе сведений о состоянии сети, приоритета услуг» и других факторов. Кроме того, выполняет такие задачи по управлению трафиком, как коммутация, маршрутизация и контроль за перегрузкой сети. *См. также* эталонная модель взаимодействия открытых систем.

сеть ~ network — два (или более) компьютера и подключенные к ним устройства, соединенные средствами связи.

сеть на основе сервера - server-based network — сеть, в которой функции компьютеров дифференцированы на функции серверов и клиентов. Стали стандартом для сетей, обслуживающих более 10 пользователей. См. *также* одноранговая сеть.

симметричная многопроцессорная обработка ~ symmetric multiprocessing (SMP) — способ организации вычислений, при котором и ОС, и приложения могут использовать любой доступный процессор.

симплексная передача ~ simplex transmission — *см.* дуплексная передача.

синхронная оптическая сеть - Synchronous Optical Network (SONET) — оптоволоконная технология, обеспечивающая скорость передачи данных более 1 Гбит/с. Построенные по этой технологии сети могут передавать речь, двоичные данные и видео. Стандарт оптической транспортной сети сформулирован Exchange Carriers Standards Association (ECSA) для ANSI.

синхронный... - synchronous — выполняемый согласованно. Синхронная связь базируется на согласовании таймеров передающего и принимающего устройств. При этом группы бит перелаются блоками — кадрами. Для начала синхронизации и периодической проверки ее точности используются специальные символы. Поскольку биты посылаются синхронно, необходимость в стартовом и стоповых битах отпадает. Передача прекращается по окончании блока и начинается при поступлении нового. Такой подход гораздо эффективнее, чем асинхронная передача. Обнаружив ошибку, схема определения и исправления ошибок просто посылает запрос на повторную передачу. Для синхронной передачи используется более сложное оборудование, поэтому она обходится дороже, чем асинхронная.

система доменных имен ~ Domain Name System (DNS) — базовая распределенная реплицируемая служба, используемая для разрешения имен узлов в IP-адреса.

система защиты - security — позволяет предотвратить повреждения и несанкционированный доступ к компьютерам и хранящимся на них данным.

система управления базами данных - DataBase Management System (DBMS) — программная прослойка между собственно базой данных и пользователем. Управляет всеми обращениями пользователя к базе, хранит подробности относительно расположения и форматов файлов, схем индексации и т. д. Кроме того, позволяет централизованно управлять безопасностью и целостностью данных.

скорость двоичной передачи в болах ~ baud rate — скорость, с которой модем может передавать данные. Часто путают со скоростью в бит/с (числе передаваемых за секунду бит). Скорость в бод показывает количество осциллящий, или изменений, несущего сигнала в секунду. При высокоскоростной цифровой передаче данных за одно событие может кодироваться несколько бит, поэтому скорость в бод и в бит/с не всегда одно и то же, и по отношению к модемам правильнее пользоваться битами в секунду, бит/с. Например, модем, который перелает за одну осциллящию 4 бит, на самом деле работает со скоростью 2400 бод, но передает данные со скоростью 9600 бит/с. Его следует считать модемом на 9600 бит/с.

служба T1 ~ T1 service — стандартная служба цифровой связи. Обеспечивает пропускную способность 1,544 Мбит/с. Может одновременно передавать и речь, и двоичные данные.

служба каталогов Active Directory ~ Active Directory services — служба каталогов, поставляемая с Windows 2000 Server. Хранит информацию обо всех объектах сети и предоставляет ее пользователям и администраторам сети. Благодаря Active Directory пользователю для доступа к любым ресурсам сети, на которые у него есть соответствующие разрешения, достаточно один раз зарегистрироваться в системе. Active Directory предоставляет администраторам сети интуитивное иерархическое представление сети и позволяет централизованно управлять всеми ее объектами.

служба коммутируемых мультигигабитных данных - Switched Multimegabit Data Services (SMDS) — высокоскоростная служба с коммутацией пакетов, обеспечивающая передачу данных со скоростью до 34 Мбит/с.

служба репликации файлов - file replication service (FRS) — обеспечивает тиражирование с несколькими хозяевами операций для указанных деревьев каталогов между серверами Windows 2000. Реплицируемые деревья каталогов должны размещаться на разделах с NTFS версии 5.0. FRS используется распределенной файловой системой (DFS) для автоматической синхронизации копий реплик и службой каталогов Active Directory для автоматической синхронизации данных системного тома между контроллерами домена.

службы терминалов - Terminal Services — программные службы, позволяющие запускать клиентские приложения на сервере, после чего клиентские ком-

пьютеры могут функционировать как терминалы, а не как независимые системы. Сервер предоставляет многосеансовую среду и выполняет программы Windows, используемые клиентами.

смарт-карта ~ smart card — устройство размером с кредитную карточку, активизируемое PIN-кодом и используемое для проверки подлинности с применением **сертификатов** и организации разового входа в систему предприятия. Для использования смарт-карт к компьютеру надо присоединить устройство чтения.

смешанный режим - mixed mode — режим, используемый по умолчанию для контроллеров домена Windows 2000. В этом режиме в домене могут одновременно существовать резервные контроллеры домена Windows NT и контроллеры домена Windows 2000. **Кроме того**, для него не поддерживаются расширения универсальных и вложенных групп Windows 2000. Режим домена может быть переключен на основной режим домена Windows 2000, если все контроллеры Windows NT удалены из домена.

смонтированный диск - mounted drive — диск, подключенный к пустой папке тома NTFS. Работает аналогично любым другим дискам, однако вместо буквы смонтированному диску присваивается **метка** или имя, которое разрешается как полный путь файловой системы, а не просто как буква диска. Члены группы Administrators (Администраторы) могут монтировать диски или менять буквы дисков средствами утилиты Disk Management.

событие - event — 1) Действие, на которое реагирует программа (например, щелчок кнопкой мыши, перемещение мыши, нажатие клавиши). 2) Любое значительное происшествие в системе или программе, о котором следует сообщить пользователю или записать в журнал.

совместимость - interoperability — способность компонентов одной системы взаимодействовать с компонентами других систем.

совместное использование ~ sharing — способ размещения файлов в сети, при котором файлы становятся доступными всем пользователям.

совокупная стоимость владения ~ total cost of ownership <TCO) — сумма материальных и временных затрат, связанных с приобретением, развертыванием, конфигурированием **и обслуживанием** программного и аппаратного обеспечения. Включает затраты на обновление **ПО** и оборудования, обучение, обслуживание, администрирование и техническую поддержку. На стоимости владения отрицательно отражается потеря производительности в результате ошибок пользователей, неисправности оборудования, неэффективных обновлении ПО и переквалификации персонала.

соединительный кабель - crossover cable — применяется для прямого соединения двух компьютеров. При этом передающий **кабель одного** из компьютеров подключается к принимающему порту другого. Соединительные кабели полезны при устранении проблем с сетевыми соединениями.

сопротивление терминатора ~ terminator resistance — сопротивление резистора терминатора, выраженное в Ом. Должно соответствовать волновому сопротивлению кабеля. Например, Ethernet, использующий тонкий кабель RG-58 A/U с волновым сопротивлением 50 Ом, требует подключения терминатора сопротивлением 50 **Ом.** Несоответствие сопротивления терминатора спецификациям может вызвать сбои в сети. *См. также* Ом.

соотязание - contention — состязание между сетевыми станциями за право использовать линию связи или сетевой ресурс. Попытка нескольких компьютеров одновременно осуществить передачу по одному и тому же кабелю приводит к *коллизии*. **Такие** системы нуждаются в регулирующих правилах, которые позволяют устранять коллизии (они могут привести к разрушению данных и остановке сети). *См. также* множественный доступ с контролем несущей и обнаружением коллизий.

спецификация интерфейса сетевых устройств - Network Device Interface Specification (NDIS) — стандарт определяющий интерфейс между драйверами сетевых плат и драйверами сетевых протоколов. Преимущество возможность использования нескольких стеков протоколов с одной сетевой платой и наоборот. *См. также* Open Data-Link Interface (ODI).

список совместимого оборудования ~ hardware compatibility list (HCL) — список компьютеров и периферийного оборудования, проверенных на совместимость с продуктом, для которого приведен список. Например, список для Windows NT 4.0 содержит названия аппаратных средств, успешно прошедших тест на совместимость с Windows NT 4.0.

способ доступа - access method — набор правил, определяющих порядок передачи/приема данных компьютером по сетевому кабелю; позволяет управлять сетевым трафиком при перемещении данных по сети.

среда передачи - media — кабели или провода, выступающие в качестве среды передачи ЛВС, которая обеспечивает пересылку данных между компьютерами. Средой передачи часто называют систему кабелей.

стандарт RS-232 — промышленный стандарт (Recommended Standard, RSI для последовательных соединений. Принят Electrical Industries Association (EIA). Определяет конкретные линии и характеристики сигнала, используемые контроллерами последовательных соединений. В результате достигается единообразие способа передачи последовательных данных между устройствами.

стандартный Ethernet - standard Ethernet — *см.* «толстый стандартный Ethernet».

стек протокола - protocol slack — многоуровневый набор протоколов, работающих совместно и реализующих различные сетевые функции.

Т

таблица размещения файлов ~ file allocation (able (FAT) — таблица, поддерживаемая некоторыми ОС для отслеживания состояния разных сегментов дискового пространства, где хранятся файлы.

телекоммуникационное оборудование ~ Data Communications Equipment (DCE) — один из двух типов устройств, соединяемых с последовательным интерфейсом RS-232; другой тип — терминальное оборудование (DTE). DCE-устройство принимает данные от DTE-устройства и выполняет посреднические функции, преобразуя **входной** сигнал перед его отправкой получателю. Например, внешний модем — это DCE-устройство, которое принимает данные от микрокомпьютера (DTE), выполняет их модуляцию и посылает модулированные данные по телефонной линии. В коммуникациях DCE-устройство, соединенное с RS-232, принимает данные по линии 2 и перелает их по линии 3. А DTE-устройство, наоборот, принимает данные по линии 3 и передает их по линии 2. *См. также* терминальное оборудование.

терабайт ~ terabyte — *см.* **байт.**

терминал ввода-вывода ~ dumb terminal — устройство сети для ввода-вывода данных, которое не имеет собственных вычислительных возможностей (отсутствует микропроцессор).

терминальное оборудование ~ Data Terminal Equipment (DTE) — согласно стандарту RS-232, DTE любое устройство, например микрокомпьютер или терминал, способное передавать информацию в цифровой форме по кабелю или по линии связи. DTE — один из двух типов устройств, соединяемых с последовательным интерфейсом RS-232; другим типом является телекоммуникационное оборудование (DCE), например модем, который обычно соединяет DTE с **линией** связи. **В** коммуникациях DTE-устройство, соединенное с RS-232, передает данные по линии 2 и принимает их по линии 3. DCE принимает данные по линии 2 и передает их по линии 3. *См. также* телекоммуникационное оборудование.

терминатор ~ terminator — резистор, подключенный к каждому концу кабеля Ethernet, чтобы предотвратить отражение сигнала. **Один** из терминаторов обычно заземляют. *См. также* отражение сигнала.

тестер кабеля ~ cable tester — *см.* расширенный тестер кабеля.

«толстый (стандартный) Ethernet» - Thicknet (standard) Ethernet — относительно жесткий коаксиальный кабель диаметром чуть больше 1 см. Способен передавать сигнал без усиления на расстояние до 500 м (около 1 640 футов). Благодаря своей способности пересылать данные на большие расстояния, используется как магистраль, соединяющая несколько небольших сетей, построенных на основе «тонкого Ethernet».

«тонкий Ethernet» ~ thinnet (thin-wire) Ethernet - гибкий коаксиальный кабель диаметром около 0,5 см. Способен передавать сигнал без усиления на расстояние до 185 м (около 600 футов). Используется для соединения относительно близких устройств (фактически для соединения компьютеров между собой).

тоновый генератор ~ tone generator — прибор, используемый в диагностике. Генерирует в кабеле переменный или непрерывный тоновый сигнал, по которому тоновый определитель проверяет целостность и качество кабеля. *См. также* тоновый определитель.

тоновый определитель ~ tone locator — прибор, используемый в диагностике. Определяет целостность и качество кабеля, анализируя сигналы, испускаемые тоновым генератором. См. *также* тоновый генератор.

топология ~ topology — схема соединения компьютеров, кабельной системы и других сетевых компонентов. «Топология» — стандартный термин, которым пользуется большинство профессионалов при описании базовой компоновки сети.

топология «звезда» - star topology — схема соединения, при которой каждый компьютер подключен к центральному компоненту — концентратору. Сигналы компьютера **через** концентратор поступают ко всем станциям в сети. Обеспечивает централизованное управление и доступ к ресурсам. Создана на заре развития компьютерных технологий, когда терминалы подключались к централизованному мэйнфрейму. Требует **много** кабеля (поскольку каждый компьютер подключается к центральному модулю). Недостаток: выход всей сети из строя при сбое центрального узла. *См. также* концентратор.

топология «кольцо» ~ ring topology — последовательное соединение компьютеров, при котором последний соединен с первым. Данные перемешаются по кольцу от **компьютера к** компьютеру в одном направлении. Каждый компьютер работает как повторитель, усиливая сигнал и передавая его дальше. Поскольку сигнал проходит через каждый компьютер, сбой одного часто приводит к сбою всей сети. В кольцо можно встроить дополнительные средства, которые отключают неисправный компьютер, чтобы сеть продолжала работу. *См. также* Token Ring, передача маркера.

топология «шина» - bus topology — схема подключения сетевых станций к одному общему кабелю — шине. На его концах находятся терминаторы (резисторы), которые предотвращают отражение электромагнитной волны. Во время передачи данные проходят по всему кабелю и достигают всех станций. Каждая станция прослушивает шину и принимает кадр только в том случае, если адрес станции совпадает с адресом получателя, установленным в кадре.

точка доступа к услугам - service access point (SAP) — интерфейс между соседними уровнями в стеке протоколов OSI. Протоколы могут иметь несколько активных SAP одновременно.

транзит ~ hop — для маршрутизации в сети это факт прохода пакета через маршрутизатор.

трансивер - transceiver — устройство для подключения компьютера к сети. Термин образован от англ. слов *передатчик — приемник* (TRANSmitter/reCEIVER — transceiver), так как данное устройство осуществляет прием и передачу сигналов. Преобразует **поток** параллельных данных, пересылаемый по шине компьютера, в поток последовательных данных, который передается по кабелю, соединяющему компьютеры.

транспортный протокол - transport protocol — протокол, выполняющий функции транспортного уровня модели OSI. Си. *также* транспортный уровень,

транспортный уровень - transport layer — четвертый уровень модели OSI. Предоставляет услуги сеансовому уровню по транспортировке пакетов данных. Управляет передачей пакетов, обеспечивая их целостность; обнаруживает и устраняет ошибки, укрупняет либо разукрупняет пакеты данных, устанавливает приоритеты при передаче, восстанавливает пакеты, потерянные нижними уровнями протоколов. См. *также* транспортный протокол; эталонная модель взаимодействия открытых систем.

трейлер ~ trailer — один из трех компонентов сетевого пакета. Его наполнение зависит от протокола, но обычно содержит CRC-код.

«троянский конь» ~ «trojan horse» virus — вирус, выдающий себя за обычное приложение. Способен разрушать данные, перехватывать пароли и выводить из строя физические диски.

У

удаленная установка - remote installation — процесс подключения к RIS-серверу (на котором выполняется служба Remote Installation Service) и запуска автоматической установки Windows 2000 на локальном компьютере.

удаленное соединение - dial-up connection — соединение с сетью посредством устройства, использующего телефонную линию. Сюда относятся модемы, подключенные по обычной телефонной линии, платы ISDN с высокоскоростными каналами ISDN и сети X.25. Как правило, обычный пользователь применяет одно или два удаленных соединения, например, с Интернетом и корпоративной сетью. В более сложных ситуациях, например на сервере, для обеспечения сложной маршрутизации должно иметься несколько сетевых модемных соединений.

удаленный компьютер - remote computer — компьютер, доступный пользователю только с применением коммуникационных линий и устройств, таких, как сетевая плата или модем.

удаленный пользователь - remote user — пользователь, подключающийся к серверу по модему и телефонной линии.

узел - host — устройство, подключенное к сети и способное взаимодействовать с другими сетевыми устройствами (например, рабочая станция, сервер).

«узкое» место ~ bottleneck — устройство, программа или другой ресурс, которые ограничивают производительность компьютерной системы. Большинство операций состоит из согласованных действий нескольких устройств. Каждое, выполняя свою часть работы, вызывает временную задержку. Низкая производительность является результатом того, что одно из устройств расходует гораздо больше времени, чем остальные. Потенциальными «узкими» местами считаются центральный процессор, память, плата сетевого адаптера и т. п.

универсальная последовательная шина ~ Universal Serial Bus (USB) — последовательная шина со скоростью передачи данных 12 Мбит/с, предназначенная для подключения к компьютеру периферийных устройств. Позволяет подключить к одному порту до 127 устройств, выстраивая из них цепи-цепочку. Поддерживает «горячее» подключение, автомагическое распознавание и настройку оборудования.

универсальные правила именования ~ Universal Naming Convention (UNC) — стандарт записи полных имен сетевых ресурсов в Windows 2000. UNC-имя имеет вид *\\имя_сервера\имя_ресурса*. UNC-имена каталогов или файлов после имени ресурса также могут включать путь к каталогу: *\\имя_сервера\имя_ресурса\каталог\имя_файла*.

универсальный асинхронный приемник-передатчик - universal asynchronous receiver transmitter (UART) — модуль, обычно организованный в виде одной микросхемы. Широко применяется в модемах. Содержит цепи и передатчика, и приемника, необходимые для асинхронной связи. Два компьютера, оборудованные UART, могут взаимодействовать через просто; проводное соединение. Работа передающего и принимающего модулей не синхронизируется, поэтому поток данных должен содержать сигналы о начале и конце байта данных — стартовый и стоповый биты.

универсальный указатель ресурса ~ Uniform Resource Locator (URL) — идентификатор, или адрес ресурсов, в Интернете. Обеспечивает гипертекстовые связи между документами World Wide Web (WWW). Определяет сервер и способ доступа к нему, а также местонахождение ресурса. Может использовать разные протоколы, в том числе **FTP, HTTP** или Gopher.

управление потоком - flow control — в сетях это регулирование потока данных через маршрутизаторы для равномерного распределения нагрузки по всем сегментам.

управление сеансами - session management — установка, поддержка и завершение соединения между станциями в сети.

усилитель ~ amplifier — устройство, например повторитель или мост, повышающее мощность электрических сигналов, ослабленных в результате затухания. Усилитель обеспечивает передачу сигналов по дополнительным сегментам кабеля с сохранением исходной мощности.

устройство ~ device — общий термин для любой подсистемы компьютера. Это может быть принтер, последовательный порт, дисковый накопитель и др.

устройство чтения смарт-карт ~ smart card reader — стандартное устройство в системе считывания смарт-карт. Представляет собой интерфейсное устройство (interface device, IFD), поддерживающее двусторонний обмен данными.

учетная запись пользователя ~ user account — информация о сетевом пользователе: его имя, пароль для регистрации при входе в сеть группы, к которым принадлежит данная учетная запись, права доступа к ресурсам и привилегии при работе в системе. В Windows NT Workstation управление учетными записями осуществляется через программу User Manager. В Windows NT Server для этого служит User Manager for Domains.

учетная политика ~ account policy — метод управления характеристиками паролей всех учетных записей домена или отдельного компьютера.

Ф

файл подкачки - paging file — специальный файл, размещающийся на одном или нескольких дисках компьютера. Windows 2000 распределяет виртуальную память для хранения программного кода и прочей информации между ОЗУ и жесткими дисками компьютера. Это позволяет увеличить доступный объем памяти.

файловая система NTFS ~ NTFS file system -- усовершенствованная файловая система, специально предназначенная для использования с Windows 2000. Поддерживает операцию восстановления, носители с большим объемом памяти, длинные имена файлов, а также расширенные возможности подсистемы POSIX. Также поддерживает объектно-ориентированные приложения, поскольку все файлы рассматриваются как объекты с пользовательскими и системными атрибутами.

файловый вирус ~ file infector — вирус, прикрепляющий себя к файлу или программе и активизирующийся при каждом использовании файла. Существует много разновидностей таких вирусов. *См. также* вирус-компаньон; вирус-невидимка; макровирус; **полиморфный** вирус.

файловый протокол AppleTalk ~ AppleTalk filing protocol (AFP) — определяет порядок хранения файлов в сети и доступа к **ним.** Соответствует иерархической файловой структуре томов, папок и файлов, применяемой в сетях Apple, и обеспечивает совместное использование файлов компьютерами Macintosh и компьютерами под управлением **MS-DOS.** Предоставляет интерфейс для взаимодействия между AppleTalk и другими сетевыми **ОС. что** позволяет интегрировать компьютеры Macintosh и любую сеть, где используется ОС, поддерживающая AFP.

физический уровень - physical layer — первый (самый нижний) уровень модели OSI. **Обеспечивает** передачу данных в виде потока битов по физическому носителю (сетевому кабелю). Реализует электрический (или оптический), механический и **функциональный** интерфейсы с кабелем, а также передает данные, генерируемые всеми вышестоящими уровнями модели OSI. См. *также* эталонная модель взаимодействия открытых систем.

Ц

центр сертификации - certificate **authority (CA)** — удостоверяет аутентичность открытых ключей пользователей или других центров сертификации. В обязанности центров **сертификации** может входить связывание открытых ключей с уникальными именами посредством подписанных сертификатов, управление порядковыми и номерами сертификатов и отзыв сертификатов.

центральный процессор ~ central processing unit (CPU) — вычислительный и управляющий модуль компьютера; устройство, которое интерпретирует и выполняет команды. Создание одиночных центральных процессоров, называемых микропроцессорами, сделало возможным появление персональных компьютеров.

центральный сервер файлов ~ central file server — модель сети, в которой специальному компьютеру отводится роль сервера файлов по отношению к остальным компьютерам. *См. также* клиент/сервер.

цикличный избыточный код - Cyclical Redundancy Check (CRC) — число, получаемое в результате математических преобразований над пакетом данных и исходными данными, помещенными в пакет. Когда пакет приходит к получателю, вычисления повторяются. Если результаты обоих вычислений совпадают, считается, что пакет принят без ошибок, если нет — данные приняты с ошибками. В таком случае CRC-процедура сообщает передающему компьютеру о необходимости повторить передачу пакета.

цилиндрический разъем ~ barrel connector — позволяет удлинить кабель путем соединения двух его отрезков.

цифровая линия ~ digital line — линия связи, передающая информацию только в двоичной (цифровой) форме. Для минимизации искажений и влияния помех вдоль цифровой линии периодически подключаются повторители, которые восстанавливают форму сигнала. Си. *также* аналоговая линия.

цифровая подпись ~ digital signature — средство подтверждения авторства зашифрованного **сообщения.** файла или любой другой зашифрованной цифровой информации. Скрепление цифровой подписью подразумевает преобразование информации и некоторых конфиденциальных сведений, которыми обладает отправитель, в метку, называемую подписью. Цифровые подписи применяются и средах с открытыми ключами и предоставляют функции обеспечения целостности и предотвращения несанкционированного изменения передаваемой информации.

цифровая сеть комплексных услуг ~ Integrated Services Digital Network (ISDN) — цифровая сеть связи. Возникла в результате совершенствования обычных телефонных служб. Цель внедрения **ISDN** - заменить все телефонные линии, которые требуют цифро-аналоговых преобразований, на полностью цифровые средства связи, способные передавать речь, цифровые данные, музыку и видео. Строится на основе двух основных типов каналов связи: B-каналах, которые передают речь, двоичные данные и изображения со скоростью 64 кбит/с, и D-канале, работающем со скоростью 16 кбит/с. Стандартная служба ISDN называется «2B+D». Компьютеры и другие устройства подключаются к линиям **ISDN** через стандартные интерфейсы.

цифровой... ~ digital — описываемый дискретной функцией. Цифровые устройства работают с информацией, представленной в двоичном виде (нулями и единицами). Например, компьютеры обрабатывают представленные в цифровой форме данные. Цифровые сигналы — это дискретные состояния; есть сигнал — нет сигнала. *См. также* аналоговый.

цифровой видеодиск - digital video disc (DVD) — оптическая среда хранения информации. Обладает высокой плотностью записи и пропускной способностью компакт-диска. Может хранить высококачественный видеофильм в формате MPEG-2 продолжительностью до 133 мин. Также известен под названием универсальный цифровой диск (digital versatile disc).

цифровой вольтметр ~ digital voltmeter (DVM) — электронное измерительное устройство общего назначения. Позволяет измерять напряжение тока, проходящего через резистор, и определять целостность сетевых кабелей.

Ч

чередование дисков - disk striping — данные делятся на блоки размером 64 кб и равномерно, в фиксированном соотношении и порядке распределяются по дискам массива. Тем не менее чередование дисков не обеспечивает отказоустойчивости, поскольку отсутствует избыточность данных — при отказе любого из разделов будут потеряны все данные. *См. также* зеркальные диски; отказоустойчивость.

чередующийся набор ~ stripe set — разновидность отказоустойчивой дисковой подсистемы, в которой несколько областей неотформатированного *свободного пространства объединяются* и один большой логический диск и данные одновременно распределяются по всем дискам. В Windows NT чередующийся набор можно создать на 2–32 физических дисках. **Допускает** сочетание пространства дисков различных типов, например SCSI-, ESDI- и IDE-дисков.

четность ~ parity — способ *контроля* за безошибочной передачей блоков данных с помощью добавления контрольных бит. Число единичных битов всегда должно быть либо четным, либо нечетным. Нарушение этого принципа свидетельствует об ошибке передачи. **Если** четность проверяется для каждого символа, метод называется вертикальным контролем (Vertical Redundancy Cheek, VRC). Если проверка проводится поблочно (блок состоит из нескольких байт), метод носит название продольного контроля (Longitudinal Redundancy Checking, LRC). Четность применяется для контроля данных, передаваемых внутри компьютера или между компьютерами.

четырехслойная экранирующая оболочка - quad shielding — кабель, который содержит два слоя фольги и два слои металлической оплетки.

Ш

шина - bus — параллельные проводники, связывающие компоненты компьютера.

широковещательная передача - broadcast — передача одного сообщения всем станциям сети.

широковещательный «шторм» ~ broadcast storm — число широковещательных сообщений в сети, достигающее пропускной способности сети или превышающее ее. Это может быть связано с тем, что каждая станция или маршрутизатор, получившие широковещательное сообщение, в соответствии с протоколом должны широковещательно ответить на него либо выдать новый широковещательный запрос другим станциям. В результате сеть оказывается «забитой», причем только служебными сообщениями, возможность же передать прикладную информацию отсутствует.

шифрование ~ encryption — преобразование данных с целью защиты от несанкционированного просмотра, использования или модификации, особенно при передаче по линиям связи или транспортировке на сменных магнитных носителях. Для обратного преобразования — расшифровки — нужен специальный ключ. *См. также* **Commercial** COMSEC Endorsement Program (CCEP), Data Encryption Standard (DES).

шифрование данных ~ data encryption — *см.* шифрование.

шифрование с открытым ключом ~ public key cryptography — криптографический метод, в котором для обеспечения безопасности применяется схема двух взаимодополняющих ключей — открытого и закрытого. Первый служит для шифрования сообщения, второй — для расшифровки.

шифрованная файловая система ~ encrypting file system (EFS) — файловая система Windows 2000, позволяющая защитить от несанкционированного доступа файлы и папки, хранимые на диске с файловой системой NTFS.

шлюз - gateway — устройство для **объединения** информационных сетей, использующих различные протоколы. Работает на прикладном уровне модели OSI.

«шум» - noise — случайные электрические сигналы в кабеле, которые могут искажать данные. Генерируются любыми электроустановками — двигателями электропередачи, лифтами, кондиционерами и др. *См. также* экран.

Э

экран - shielding — металлическая оплетка или цилиндр из фольги. Защищает передаваемые данные, уменьшая внешние электрические помехи - «шум». Ср. *также* «шум».

экранированная витая пара - shielded twisted pair (STP) cable — витая пара, окруженная заземленной металлической фольгой, которая служит экраном. *См. также* витая пара.

эксабайт - exabyte — *см.* байт.

электронная доска объявлений ~ bulletin board system, BBS — компьютер, оборудованный одним или несколькими модемами или другими средствами сетевого доступа и выступающий в роли центра обмена информацией для удаленных пользователей. У многих компаний по разработке **ПО** и оборудования имеются собственные BBS, где пользователи могут получить **информацию** о новых товарах, техническую поддержку или пакеты обновлений ПО.

эталонная модель взаимодействия открытых систем ~ Open Systems Interconnection (OSI) reference model — семиуровневая архитектура, которая стандартизирует уровни услуг и виды взаимодействия для компьютеров, обменивающихся информацией по сети.

Эта модель наиболее известна и широко применяется при описании сетевой среды или прохождении данных между физическим соединением с сетью и конечным приложением.

Уровень OSI	Вид услуг
7. прикладной	Передача иформации между программами
6. прелстави-тельский	Шифрование, кодирование, иногда сжатие данных
5. сеансовый	Установка, поддержка и разрыв соединения
4. транспортный	Точность доставки, уровень качества услуг
3. сетевой	Маршруты передачи, обработка и передача сообщений
2. канальный	Управление каналом связи, доступ к среде передачи и адресация
1. физический	Связи на уровне аппаратуры

Я

язык описания страниц ~ page-description language (PDL) — язык, на котором сообщается принтеру как должна выглядеть печатаемая страница. На нем задаются основные ее параметры, например, размер и гарнитура шрифта, местоположение иллюстраций и т. д. Однако создание конечного оттиска поручается принтеру.

язык структурированных запросов ~ structured query language (SQL) — язык управления базами данных, применяемый для запроса, обновления и управления реляционными БД. **Не** являясь **языком** программирования в том понимании, как С или Pascal, SQL способен формулировать интерактивные запросы или, будучи встроенным к приложение, выступать в качестве инструкций по управлению данными. Стандарт SQL, кроме того, содержит компоненты для определения, изменения, проверки и защиты данных.

ячеистая топология сети - mesh network topology — топология, которая в основном используется в ГВС. Ее отличительный признак: к любому узлу существует два (или более) маршрута. Для выбора оптимального на данный момент маршрута из нескольких возможных применяются маршрутизаторы.

Предметный указатель

M

N

O

P

Q

R

S

T

U

V

W

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ MICROSOFT

прилагаемый к книге компакт-диск

ЭТО ВАЖНО — ПРОЧИТАЙТЕ **ВНИМАТЕЛЬНО.** Настоящее лицензионное соглашение (далее «Соглашение») является юридическим документом, оно заключается между Вами (физическим или юридическим лицом) и Microsoft Corporation (далее «корпорация Microsoft») на указанный выше продукт Microsoft, который включает программное обеспечение и может включать сопутствующие мультимедийные и печатные материалы, а также электронную документацию (далее «Программный Продукт»). Любой компонент, входящий в Программный Продукт, который сопровождается отдельным Соглашением, подпадает под действие именно того Соглашения, а не условий, изложенных ниже. Установка, копирование или иное использование данного Программного Продукта означает принятие Вами данного Соглашения. Если Вы не принимаете его условия, то не имеете права устанавливать, копировать или как-то иначе использовать этот Программный Продукт.

ЛИЦЕНЗИЯ НА ПРОГРАММНЫЙ ПРОДУКТ

Программный Продукт защищен законами Соединенных Штатов по авторскому праву и международными договорами по авторскому праву, а также другими законами и договорами по правам на интеллектуальную собственность.

1. **ОБЪЕМ ЛИЦЕНЗИИ.** Настоящее Соглашение дает Вам право:
   a) Программный **продукт.** Вы можете установить и использовать одну копию Программного Продукта на одном компьютере. Основной пользователь компьютера, на котором установлен данный Программный Продукт, может сделать только для себя вторую копию и использовать ее на портативном компьютере.
   b) Хранение или **использование** в **сети.** Вы можете также скопировать или установить экземпляр Программного Продукта на устройстве хранения, например на сетевом сервере, исключительно для установки или запуска данного Программного Продукта на других компьютерах в своей внутренней сети, но тогда Вы должны приобрести лицензии на каждый такой компьютер. Лицензию на данный Программный продукт нельзя использовать совместно или одновременно на других компьютерах.
   c) License **Pak.** Если Вы купили эту лицензию в составе Microsoft License Pak, можете сделать ряд дополнительных копий программного обеспечения, входящего в данный Программный Продукт, и использовать каждую копию так, как было описано выше. Кроме того, Вы получаете право сделать соответствующее число вторичных копий для портативного компьютера в целях, также оговоренных выше.
   d) **Примеры кода.** Это относится исключительно к отдельным частям Программного Продукта, заявленным как примеры кода (далее «Примеры»), если таковые входят в состав Программного Продукта.
      i) **Использование и модификация.** Microsoft дает Вам право использовать и модифицировать исходный код Примеров при условии соблюдения пункта (d)(iii) ниже. Вы не имеете права распространять в виде исходного кода ни Примеры, ни их модифицированную версию.
      ii) **Распространяемые файлы.** При соблюдении пункта (d)(iii) Microsoft дает Вам право на свободное от отчислений копирование и распространение в виде объектного кода Примеров или их модифицированной версии, кроме тех частей (или их модифицированных версий), которые оговорены в файле Readme, относящемся к данному Программному Продукту, как не подлежащие распростране[illegible]
      iii) **Требования к распространению** файлов. Вы можете распространять файлы, разрешенные к распространению, при условии, что: а) распространяете их в виде объектного кода только в сочетании со своим приложением и как его часть; б) не используете название, эмблему или товарные знаки Microsoft для продвижения своего приложения; в) включаете имеющуюся в Программном Продукте ссылку на авторские права в состав этикетки и заставки своего приложения; г) согласны освободить от ответственности и взять на себя защиту корпорации Microsoft от любых претензий или преследований по закону, включая судебные издержки, если таковые возникнут в результате использования или распространения Вашего приложения; и д) не допускаете дальнейшего распространения конечным пользователем своего приложения. По поводу отчислений и других условий лицензии применительно к иным видам использования или распространения распространяемых файлов обращайтесь в Microsoft.

2. **ПРОЧИЕ ПРАВА И ОГРАНИЧЕНИЯ**
   - Ограничения на **реконструкцию, декомпиляцию и дизассемблирование.** Вы не имеете права реконструировать, декомпилировать или дизассемблировать данный Программный Продукт, кроме того случая, когда такая деятельность (только в той мере, которая необходима) явно разрешается соответствующим законом, несмотря на это ограничение.

- **Разделение компонентов.** Данный Программный Продукт лицензируется как единый продукт. Его компоненты нельзя отделять друг от друга для использования более чем на одном компьютере.
- **Аренда.** Данный Программный Продукт нельзя сдавать в прокат, передавать во временное пользование или уступать для использования в целях почты.
- **Услуги потехнической поддержке.** Microsoft может (но не обязана) предоставить Вам услуги по технической поддержке данного Программного Продукта (далее «Услуги»). Предоставление Услуг регулируется соответствующими правилами и программами Microsoft, описанными в руководстве пользователя, электронной документации и/или других материалах, публикуемых Microsoft. Любой дополнительный программный код, предоставленный в рамках Услуг, следует считать частью данного Программного Продукта и подпадающим под действие настоящего Соглашения. Что касается технической информации, предоставляемой Вами корпорации Microsoft при использовании ее Услуг, то Microsoft может использовать эту информацию в целях, в том числе для технической поддержки продукта и разработки. Используя такую техническую информацию, Microsoft не будет связываться ни Вас.
- **Передача прав на программное обеспечение.** Им можете безвозвратно уступить все права, регулируемые настоящим Соглашением, при условии, что не оставите себе никаких копий, передадите все составные части данного Программного Продукта (включая компоненты, мультимедийные и печатные материалы, любые обновления, Соглашение и сертификат подлинности, если таковой имеется) и принимающая сторона согласится с условиями настоящего Соглашения.
- **Прекращение действия Соглашения.** Без ущерба для любых других прав Microsoft может прекратить действие настоящего Соглашения, если Вы нарушите его условия. В этом случае Вы должны будете уничтожить все копии данного Программного Продукта вместе со всеми его компонентами.

3. АВТОРСКОЕ ПРАВО. Все авторские права и право собственности на Программный Продукт (в том числе любые изображения, фотографии, анимация, видео, аудио, музыку, текст, примеры кода, распространяемые файлы и апплеты, включенные в состав Программного Продукта) и любые его копии принадлежат корпорации Microsoft или ее поставщикам. Программный Продукт охраняется законодательством об авторских правах и положениями международных договоров. Таким образом, Вы должны обращаться с данным Программным Продуктом, как с любым другим материалом, охраняемым авторскими правами, с тем **исключением**, что Вы можете установить Программный Продукт на один компьютер при условии, что храните оригинал исключительно как резервную или архивную копию. Копирование печатных материалов, поставляемых вместе с Программным Продуктом, запрещается.

ОГРАНИЧЕНИЕ ГАРАНТИИ

ДАННЫЙ ПРОГРАММНЫЙ ПРОДУКТ (ВКЛЮЧАЯ ИНСТРУКЦИИ ПО ЕГО ИСПОЛЬЗОВАНИЮ) ПРЕДОСТАВЛЯЕТСЯ БЕЗ КАКОЙ-ЛИБО ГАРАНТИИ. КОРПОРАЦИЯ MICROSOFT СНИМАЕТ С СЕБЯ ЛЮБУЮ ВОЗМОЖНУЮ ОТВЕТСТВЕННОСТЬ, В ТОМ ЧИСЛЕ ОТВЕТСТВЕННОСТЬ ЗА КОММЕРЧЕСКУЮ ЦЕННОСТЬ ИЛИ СООТВЕТСТВИЕ ОПРЕДЕЛЕННЫМ ЦЕЛЯМ. ВЕСЬ РИСК ПО ИСПОЛЬЗОВАНИЮ ИЛИ РАБОТЕ С ПРОГРАММНЫМ ПРОДУКТОМ ЛОЖИТСЯ НА ВАС.

НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ КОРПОРАЦИЯ MICROSOFT, ЕЕ РАЗРАБОТЧИКИ, А ТАКЖЕ ВСЕ, ЗАНЯТЫЕ В СОЗДАНИИ, ПРОИЗВОДСТВЕ И РАСПРОСТРАНЕНИИ ДАННОГО ПРОГРАММНОГО ПРОДУКТА, НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА КАКОЙ-ЛИБО УЩЕРБ, (ВКЛЮЧАЯ ВСЕ, БЕЗ ИСКЛЮЧЕНИЯ, СЛУЧАИ УПУЩЕННОЙ ВЫГОДЫ, НАРУШЕНИЯ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ, ПОТЕРИ ИНФОРМАЦИИ ИЛИ ДРУГИХ УБЫТКОВ) ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ ДАННОГО ПРОГРАММНОГО ПРОДУКТА ИЛИ ДОКУМЕНТАЦИИ, ДАЖЕ ЕСЛИ КОРПОРАЦИЯ MICROSOFT БЫЛА ИЗВЕЩЕНА О ВОЗМОЖНОСТИ ТАКИХ ПОТЕРЬ, ТАК КАК В НЕКОТОРЫХ СТРАНАХ НЕ РАЗРЕШЕНО ИСКЛЮЧЕНИЕ ИЛИ ОГРАНИЧЕНИЕ ОТВЕТСТВЕННОСТИ ЗА НЕПРЕДНАМЕРЕННЫЙ УЩЕРБ, УКАЗАННОЕ ОГРАНИЧЕНИЕ МОЖЕТ ВАС НЕ КОСНУТЬСЯ.

РАЗНОЕ

Настоящее Соглашение регулируется законодательством штата Вашингтон (США), кроме случаев (в той мере, насколько это необходимо) исключительной юрисдикции того государства, на территории которого используется Программный Продукт.

Если у Вас возникли какие-либо вопросы, касающиеся настоящего Соглашения, или если Вы желаете связаться с Microsoft по любой другой причине, пожалуйста, обращайтесь в местное представительство Microsoft или напишите по адресу: Microsoft Sales Information Center, One Microsoft Way, Redmond, WA 98052-6399.

Microsoft Corporation

Администрирование сети на основе Microsoft Windows 2000

Учебный курс MCSA/MCSE

3-е издание, исправленное

Перевод с английского под общей редакцией **А. В. Иванова**

Редактор **Ю. Н. Леонова**

Технический редактор **Н. Г. Тимченко**

Компьютерная верстка **Е. В. Козлова**

Оригинал-макет выполнен с использованием
издательской системы Adobe PageMaker 6.0

ParaGraph TypeMarketFontLibrary

Главный редактор **А. И. Козлов**

Подготовлено к печати издательством «Русская Редакция»
123182, Москва, ул. Антонова-Овсеенко, д. 13
тел. (095) 256-5120, тел./факс: (095) 256-4541
e-mail: info@ruscedit.ru, http://www.ruscedit.ru

РУССКАЯ РЕДАКЦИЯ

Подписано в печать 26.02.2004 г. Тираж 1 500 экз. Зак. № 1079
Формат 70x100 1/16. Физ. п. л. 26

При участии ООО «ПФ «Сашко»

Отпечатано с готовых диапозитивов
во ФГУП ИПК «Ульяновский Дом печати»
432980, г. Ульяновск, ул. Гончарова, 14

как повысить отдачу от вложений в информационную инфраструктуру компании?

обучить специалистов в учебном центре SoftLine

Непрерывное обучение. Информационные технологии быстро меняются. Так же быстро устаревают знания сотрудников. Мы предлагаем экономичный и эффективный способ непрерывного обучения. *Мы* готовы разработать корпоративную программу обучения специально **для** сотрудников вашей компании.

Широкий майор курсов для профессионалов в области IT, которые хотят повысить свой уровень. Большое внимание уделяется вопросам построения правильной IT-инфраструктуры современной компании - вопросам безопасности, защиты данных, резервному копированию, администрированию сети и др.

Авторизованное обучение. SoftLine является авторизованным учебным центром компаний Microsoft, Symantec, Citrix, VERITAS, и др.

Высокое качество обучения. Обучение ведут сертифицированные преподаватели по официальным **методическим** материалам. Высокое **качество** обучения подтверждается откликами крупнейших компаний, входящих в **ТОП** 100 Российского рынка.

Корпоративные программы обучения. SoftLine ориентируется на долгосрочные отношения с корпоративными клиентами. Мы предлагаем разработку непрерывной программы обучения сотрудников, которая позволит экономить ресурсы, выделяемые на обучение.

Обратитесь **К консультантам учебного центра Анне Дмитраковой или Инне Домино по тел.: +7(095)232-0023 и** закажите бесплатный каталог учебных курсов.

программное обеспечение – лицензирование, обучение, консалтинг

+7(095)232-0023 www.softline.ru

конкурс
«Читатель месяца»

Хотите сэкономить на обучении до $1000?

Издательство «Русская Редакция» и учебный центр компании «Инвента» проводят конкурс «Читатель месяца» и будут ежемесячно выбирать двух самых активных читателей книг серии «Учебный курс».

Просто вырежьте купон из книги, помеченной на обложке специальным значком «Читатель месяца», и пришлите нам по адресу. **123317, Россия, г. *Москва, ул. Антонова-Овсеенко*, д. 13. *Издательство «Русская Редакция»*.**

Лотерея определит победителей месяца. Один купон — один голос!
Чем больше купонов вы пришлете, тем больше у вас шансов выиграть!

Призы победителям — ***бесплатное обучение*** *в учебном центре «Инвента» в Москве!*

Но это не все! Помимо выбранного вами курса по программе сертификации Microsoft, победителей ждут и другие призы — скидка на дальнейшее обучение в учебном центре и подарок от «Русской Редакции».

Подробности конкурса — на сайте издательства "Русская Редакция" (*www.rusedit.ru/bonus*) и на сайте компании «Инвента» (*www.inventa.ru*). Там же все новости о конкурсе и о победителях. Телефон для справок (095) 775-8777

Купон участника конкурса «Читатель месяца»

РУССКАЯ РЕДАКЦИЯ учебный центр ИНВЕНТА

Ф. И. О.:

E-mail:

Телефон:

Род занятий:

ВНИМАНИЕ! Незаполненные купоны не принимаются.

Конкурс проводится исключительно за счет устроителей. Данный купон не может рассматриваться как коммерческое предложение.

Купон из книги **Администрирование сети на основе Microsoft Windows 2000. Учебный курс MCSA/MCSE.** Экз. № 70-216. ISBN 5-7502-0148-1