Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Д. М. Романенко

ОСНОВЫ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ

**Лабораторный практикум
для студентов специальности 1-40 05 01-03
«Информационные системы и технологии
(издательско-полиграфический комплекс)»**

Минск 2015

УДК 004.7(076.5)
БКК 32.97я73
Р69

Рассмотрен и рекомендован редакционно-издательским советом университета.

Р е ц е н з е н т ы:
кандидат технических наук, доцент, доцент кафедры
информационных технологий автоматизированных систем
УО «Белорусский государственный университет информатики
и радиоэлектроники» *О. В. Герман*;
кандидат технических наук, доцент, доцент кафедры автоматизации
производственных процессов и электротехники
УО «Белорусский государственный
технологический университет» *О. Г. Барашко*

Романенко, Д. М.

Р69 Основы сетевого администрирования : лабораторный практикум для студентов специальности 1-40 05 01-03 «Информационные системы и технологии (издательско-полиграфический комплекс)» / Д. М. Романенко. – Минск : БГТУ, 2015. – 135 с.

В лабораторном практикуме приведены теоретические основы изучаемой предметной области, связанной с построением и администрированием информационных систем на основе операционных систем Windows Server. Описаны практические примеры работы с сетевой (статической и динамической), а также символьной (DNS, NetBios) адресацией, приведены методы планирования и управления Active Directory, удаленного администрирования, построения надежных и безопасных информационных систем.

Лабораторный практикум предназначен для выполнения заданий на лабораторных занятиях по курсу «Администрирование информационных систем», а также может быть полезен магистрантам и аспирантам, изучающим данную предметную область.

УДК 004.7(076.5)
БКК 32.97я73

ПРЕДИСЛОВИЕ

Дисциплина «Администрирование информационных систем» представляет собой продолжение изучения сетевой тематики и дает теоретические и практические знания по организации и управлению распределенных информационных систем на основе операционной системы Windows Server.

В данном лабораторном практикуме представлены основные методы настройки различных видов адресации (сетевой, символьной), построения администрирования распределенных информационных систем, обеспечения надежности и безопасности их функционирования. При этом предполагается, что читатель знаком с основами организации и использования компьютерных сетей.

Основная задача лабораторного практикума – дать студентам общие систематизированные знания о методах организации и администрирования информационных систем, которые затрагивают практически все сферы жизнедеятельности человека и динамично развиваются.

В результате изучения дисциплины и выполнения заданий на лабораторных занятиях студент должен освоить:

− правила и методы настройки статической и динамической адресации в информационных системах;

− методы разделения ресурсов в информационных системах;

− правила и методы настройки символьной DNS-адресации в информационных системах;

− методы организации и удаленного администрирования доменной системы на базе Active Directory;

− методы обеспечения надежности доменной системы на базе Active Directory (репликация);

− методы обеспечения безопасности доменной системы на базе Active Directory (шифрование сетевого траффика).

Студент должен научиться применять рассматриваемые методы администрирования на практике.

Тема 1

СЕТЕВАЯ АДРЕСАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

Для изучения основных приемов настройки адресации в информационных системах целесообразно использовать технологию виртуализации операционных систем.

1.1. Виртуализация операционных систем

Платформа Oracle VM VirtualBox представляет собой систему виртуализации для host-систем Windows, Linux и Mac OS и обеспечивает взаимодействие с гостевыми операционными системами Windows (2000, XP, 2003, Vista, Seven и др.), Linux (Ubuntu, Debian, OpenSUSE, Mandriva и др.), OpenBSD, FreeBSD, OS/2 Warp.

Ключевые возможности VirtualBox заключаются в следующем:

– x86-виртуализация (при этом поддержка аппаратной реализации Intel VT и AMD-V необязательна);

– поддержка многопроцессорности и многоядерности;

– поддержка виртуализации сетевых устройств;

– поддержка виртуализации USB-host;

– высокая производительность и скромное потребление ресурсов персонального компьютера;

– поддержка различных видов сетевого взаимодействия (NAT, HostNetwork, Bridge, Internal);

– возможность сохранения снимков виртуальной машины (snapshots), к которым может быть произведен откат из любого состояния гостевой системы;

– настройка и управление приложением VirtualBox и виртуальной системой из командной строки.

Установка данного программного продукта на компьютер является стандартной, поэтому уделять внимание данной процедуре не будем. Рассмотрим далее процесс создания и первичной настройки виртуальной машины.

Запустим приложение Oracle VM VirtualBox (при установке платформы на рабочем столе создается ярлык, которым далее можно будет пользоваться). Для создания виртуальной машины необходимо щелкнуть кнопку *Создать*/*New* (рис. 1.1).

После этого откроется новое окно, в котором будет сообщение о запуске мастера создания виртуальной машины.

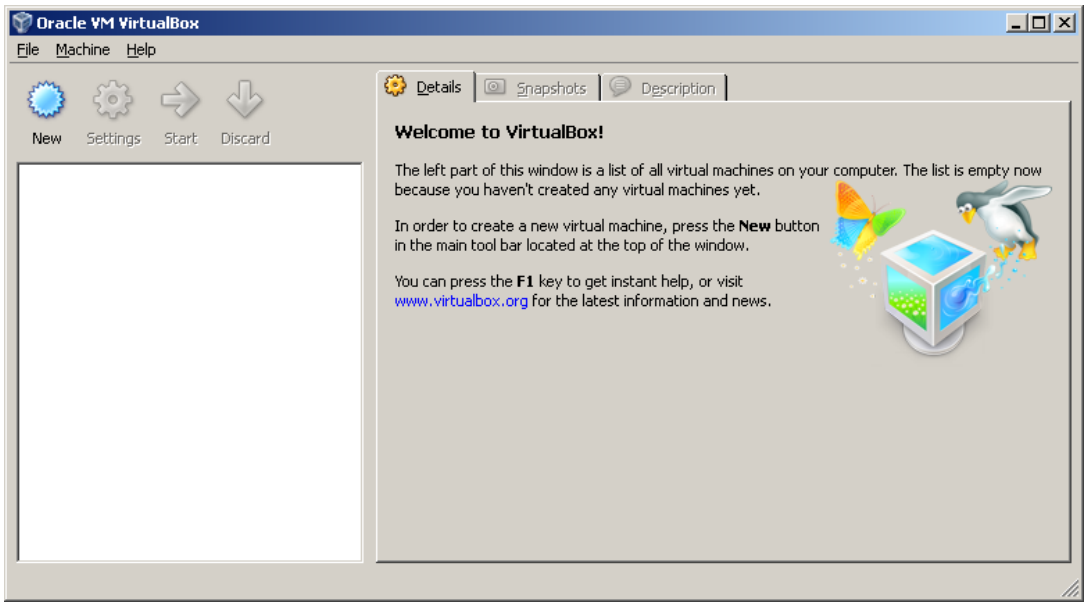

Рис. 1.1. Главное окно программы Oracle VM VirtualBox

Далее необходимо нажать кнопку *Next* и появится новое окно, предлагающее выбрать имя операционной системы, ее семейство и версию (рис. 1.2).

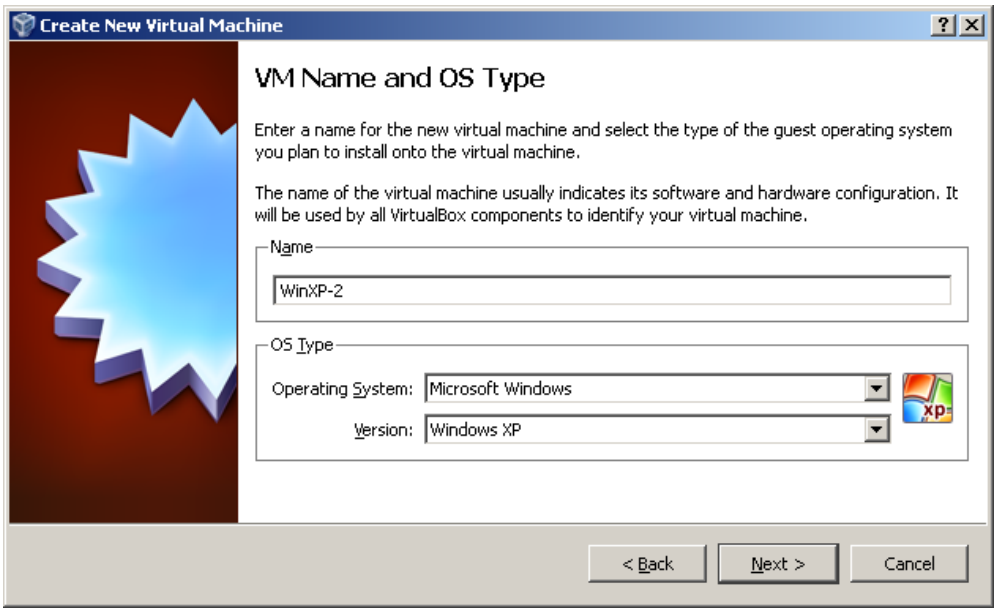

Рис. 1.2. Начальные параметры виртуальной машины

После нажатия кнопки *Next* будет предложено определить размер оперативной памяти, выделяемой виртуальной машине (рис. 1.3). Для стабильной работы с виртуальной системой Windows XP необходимо выделять не менее 256 Мбайт оперативной памяти. Отметим, что для стабильной работы 64-битных серверов типа Windows Server 2008 R2 и Windows Server 2012 R2 необходимо выделять не менее 1024 Мбайт.

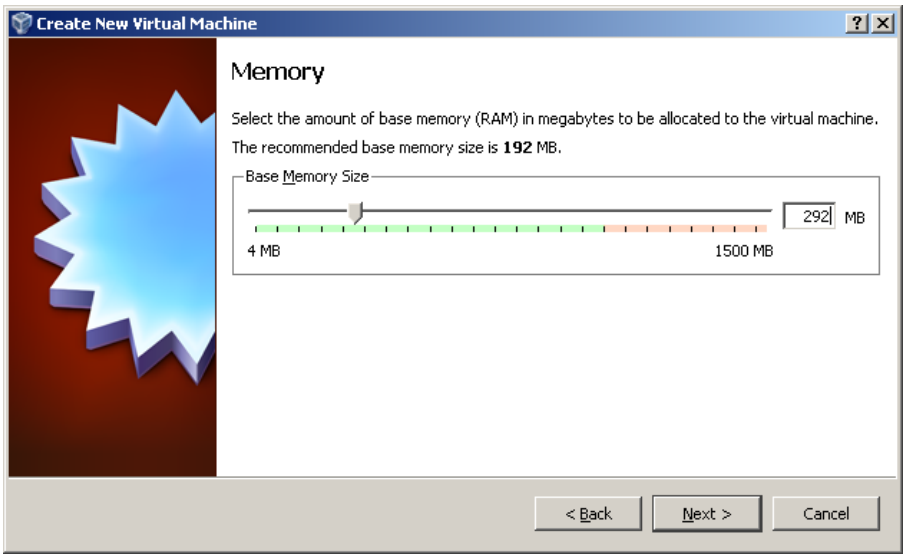

Рис. 1.3. Выделение оперативной памяти для виртуальной машины

Далее потребуется создать виртуальный жесткий диск (рис. 1.4).

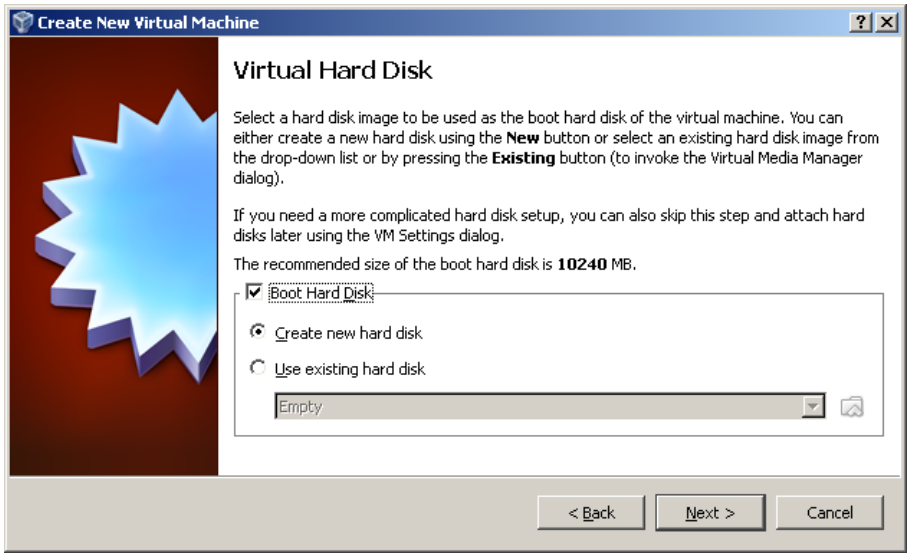

Рис. 1.4. Создание жесткого диска

Если ранее были созданы виртуальные диски, можно использовать их, но в данном случае будет рассмотрен именно процесс создания нового диска. Для подтверждения, что создаваемый жесткий диск является загрузочным, необходимо поставить флажок *Создать новый жесткий диск*/*Create new hard disk* и нажать кнопку *Next*.

Далее появится новое окно, которое сообщит, что запущенный мастер поможет в создании виртуального диска. Для продолжения работы необходимо нажать кнопку *Next*. В новом окне (рис. 1.5) будет предложено выбрать тип создаваемого диска – *динамически расширяющийся образ* или *образ фиксированного размера*. Разница объясняется в справке данного окна.

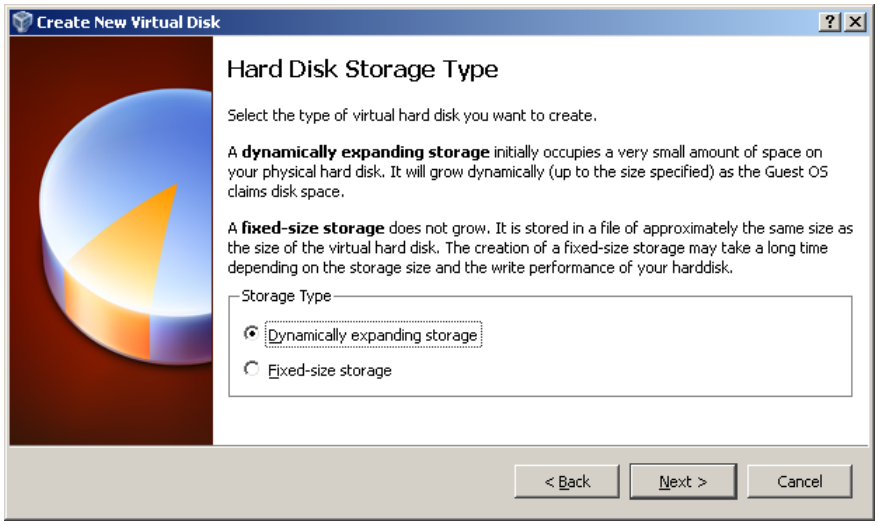

Рис. 1.5. Создание жесткого диска – выбор типа

В следующем окне (рис. 1.6) потребуется выбрать расположение создаваемого виртуального жесткого диска и его размер. Для загрузочного жесткого диска с системой Windows XP достаточно размера, установленного по умолчанию (10 Гб), а вот расположить его лучше вне системного раздела. Для установки Windows Server 2008 R2 и Windows Server 2012 R2 устанавливайте размер не менее 40–50 Гб.

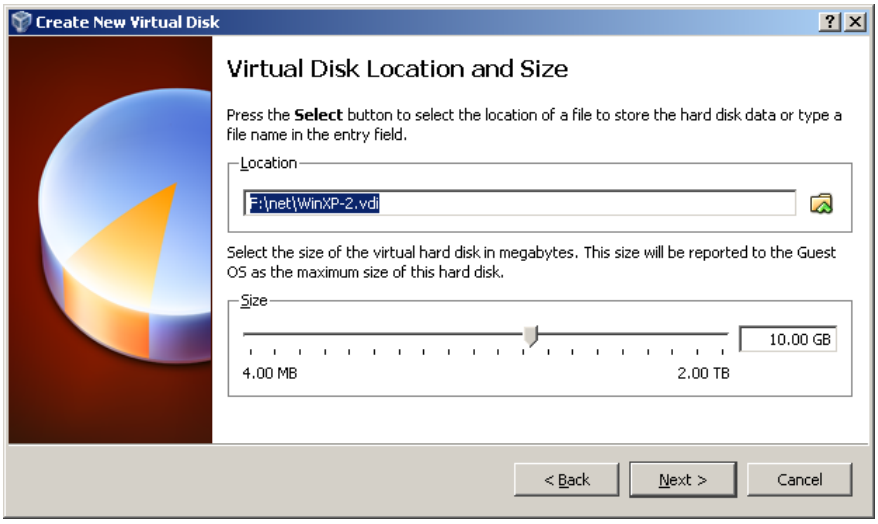

Рис. 1.6. Создание виртуального жесткого диска – выбор размера и расположения

После этого появится окно *Итог/Summary*, в котором будет указан тип, расположение и размер создаваемого вами жесткого диска. Для создания диска с такими параметрами необходимо нажать *Финиш/Finish*. Далее запустится процесс создания жесткого диска, по окончании которого появится новое окно *Итог/Summary* (рис. 1.7), в котором будут указаны параметры создаваемой виртуальной машины.

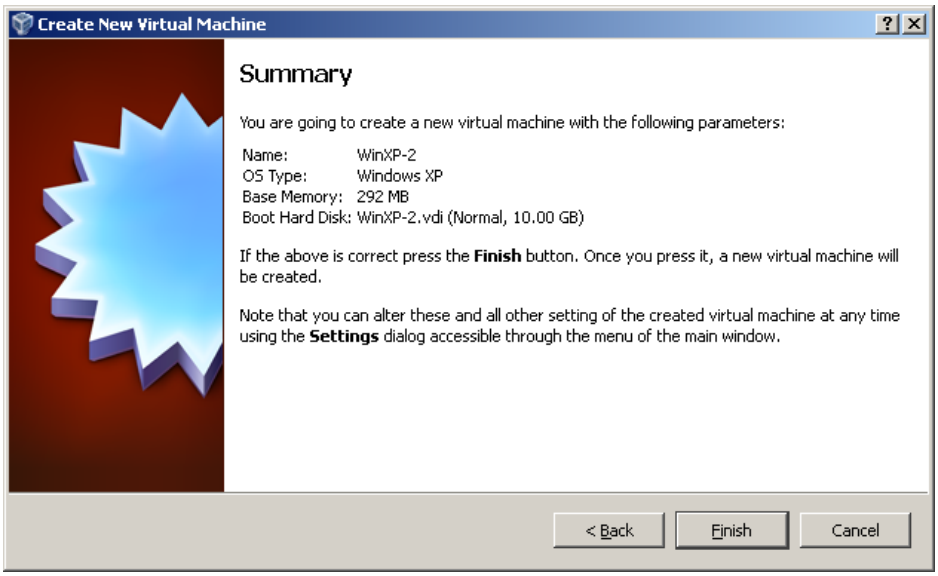

Рис. 1.7. Заключительная стадия создания виртуальной машины

Затем необходимо нажать *Финиш/Finish* и перейти к настройке аппаратной части виртуальной машины.

1.1.1. Настройка аппаратной части виртуальной машины

После создания виртуального жесткого диска настала очередь собрать виртуальный компьютер полностью. Для этого снова вернемся к главному окну VirtualBox (рис. 1.8), в нем уже можно увидеть только что созданную виртуальную машину WinXP-2, а в поле с правой стороны представлено ее описание, которое еще не похоже на описание полноценного персонального компьютера.

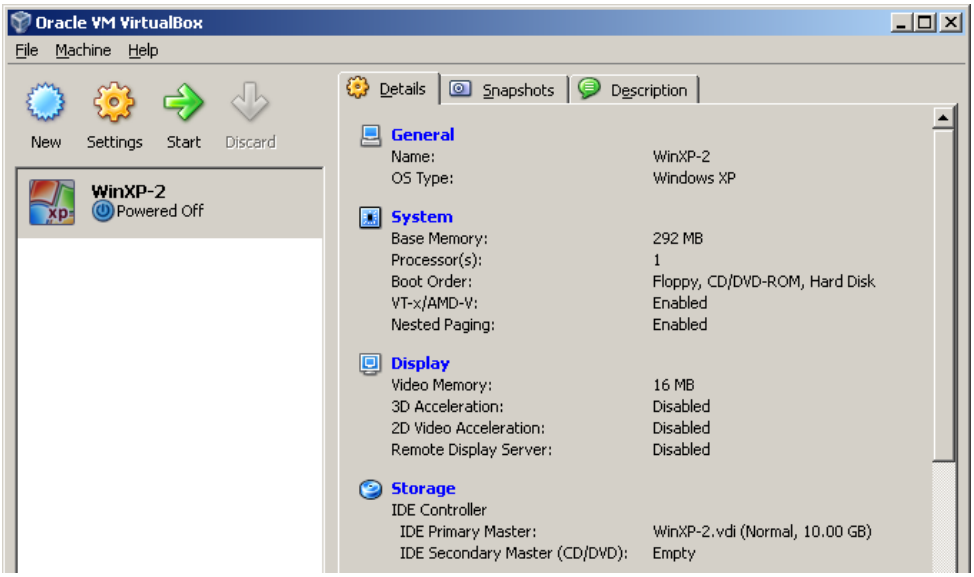

Рис. 1.8. Главное окно на этапе настройки аппаратной части

В колонке слева необходимо выбрать WinXP-2 и открыть ее свойства (*Settings*) (рис. 1.9), где колонка с левой стороны напоминает диспетчер устройств. На первой вкладке раздела *Общие*/*General* представлены основные параметры виртуальной машины.

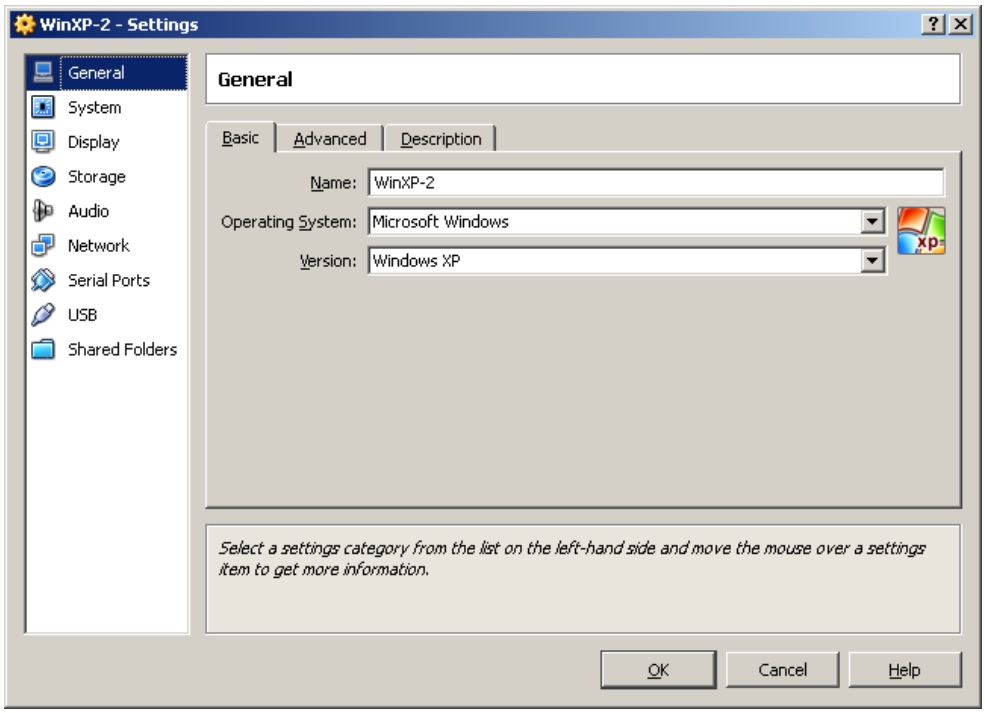

Рис. 1.9. Параметры виртуальной машины

На вкладке *Дополнительно*/*Advanced* (рис. 1.10) можно выбрать следующие параметры настройки системы.

Папка для снимков/*SnapshotFolder* – если жесткий диск размещен в отдельной директории, то лучше и эту папку перенести туда же, так как снимки имеют большой вес.

Общий буфер обмена/*SharedClipboard* – определение того, как будет работать буфер обмена между host-системой и виртуальной машиной. Вариантов работы буфера несколько, но предпочтительно выбирать *двунаправленный*/*Bidrectional*, так как это обеспечивает максимальное удобство в работе.

Сменные носители информации/*RemovableMedia* – лучше поставить флажок в поле *запоминать изменения в процессе работы*, так как данная опция позволит системе запомнить состояние CD\DVD-приводов.

Мини тулбар/*MiniToolbar* – это небольшая консоль, содержащая элементы управления виртуальной машиной. Ее лучше применять только в полноэкранном режиме, так как она полностью дублируется главным меню рабочего окна виртуальной машины. Располагать ее действительно лучше сверху, потому что можно случайно нажать на какой-нибудь элемент управления, пытаясь, например, развернуть окно из панели задач виртуальной машины.

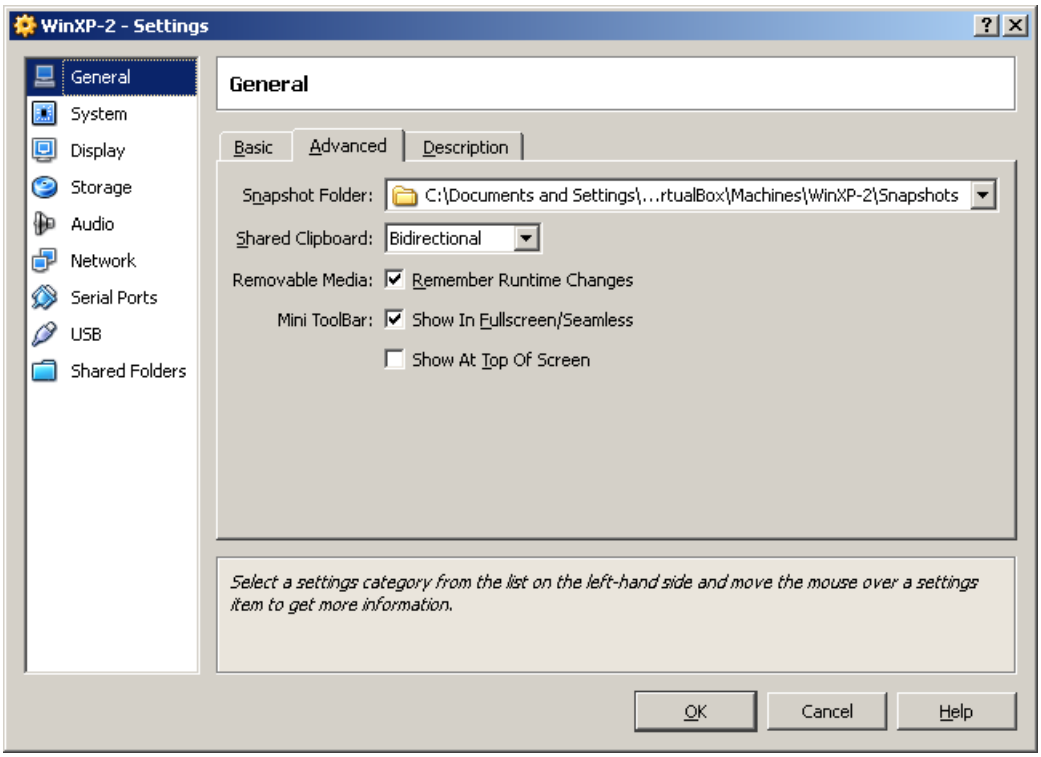

Рис. 1.10. Настройка дополнительных опций виртуальной машины

Перейдем далее к разделу *система* и на первой вкладке *Материнская плата*/*Motherboard* (рис. 1.11) произведем следующие настройки.

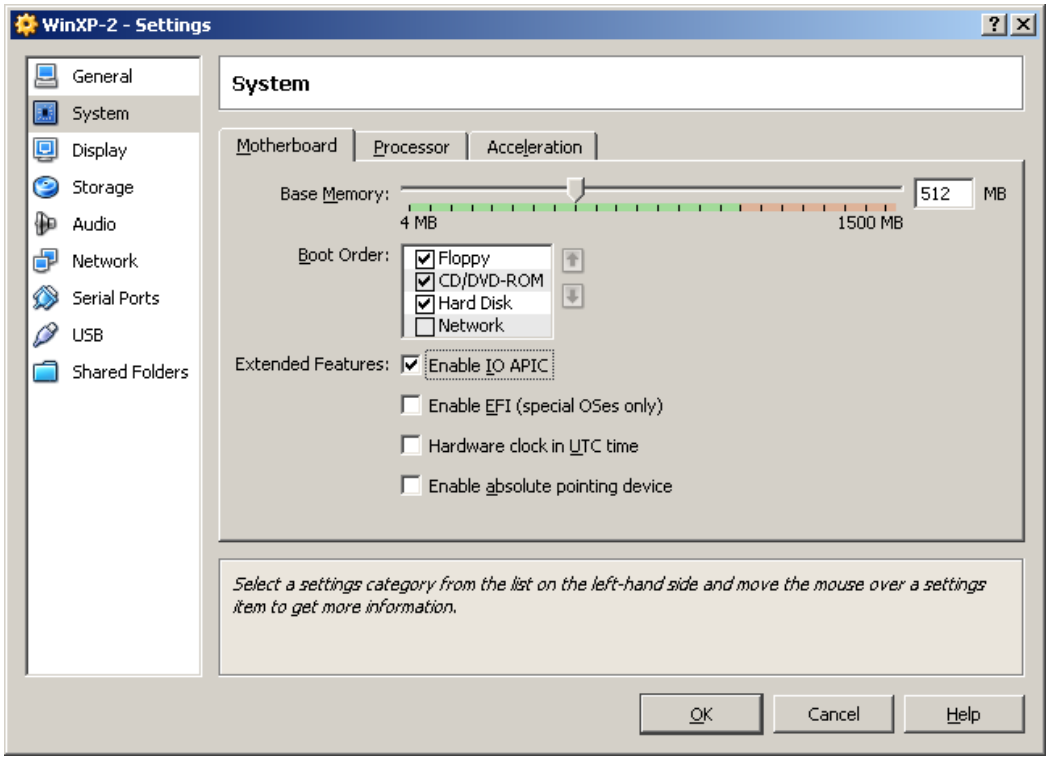

Рис. 1.11. Настройка параметров материнской платы

1. Целесообразно откорректировать размер оперативной памяти виртуальной машины, хотя окончательно убедиться в правильности выбранного объема можно только после запуска виртуальной машины. Выбирать размер можно исходя из объема доступной физической памяти, установленной на ПК. Например, при наличии 2 Гбайт ОЗУ оптимальным будет выделение 512 Мбайт, т. е. одной четвертой части, что позволит виртуальной машине работать без малейших зависаний.

2. Рекомендуется изменить порядок загрузки – дисковод гибких дисков (floppy) можно вообще отключить, а первым обязательно поставить CD/DVD-ROM, чтобы обеспечить возможность установки ОС с загрузочного диска. При этом в роли загрузочного диска может выступать как компакт-диск, так и образ ISO.

3. Все остальные настройки описаны в динамической справке снизу, и их применение зависит от аппаратной части вашего реального ПК, причем если выставить настройки, неприменимые к используемому ПК, система с виртуальной машиной просто не запустится.

На вкладке *Процессор*/*Processor* (рис. 1.12) можно выбрать количество процессоров, установленных на виртуальную материнскую плату.

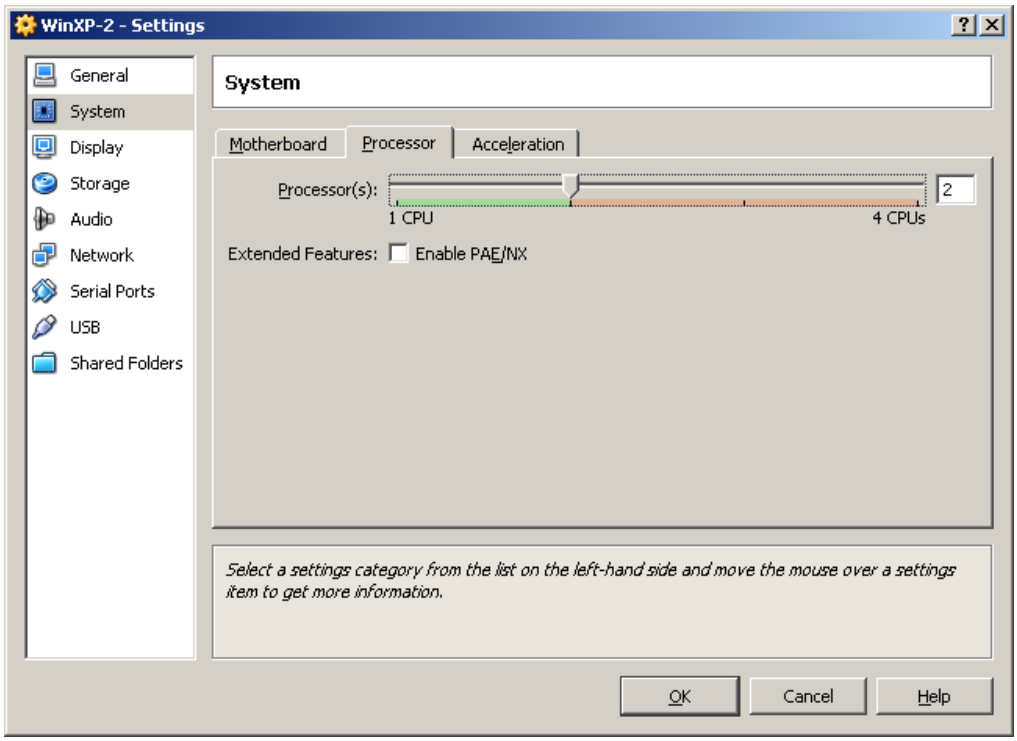

Рис. 1.12. Настройка параметров процессора

Необходимо обратить внимание, что данная опция будет доступна только при условии поддержки аппаратной виртуализации AMD-V или VT-x (рис. 1.13), а также включенной опции OI APIC на предыдущей вкладке.

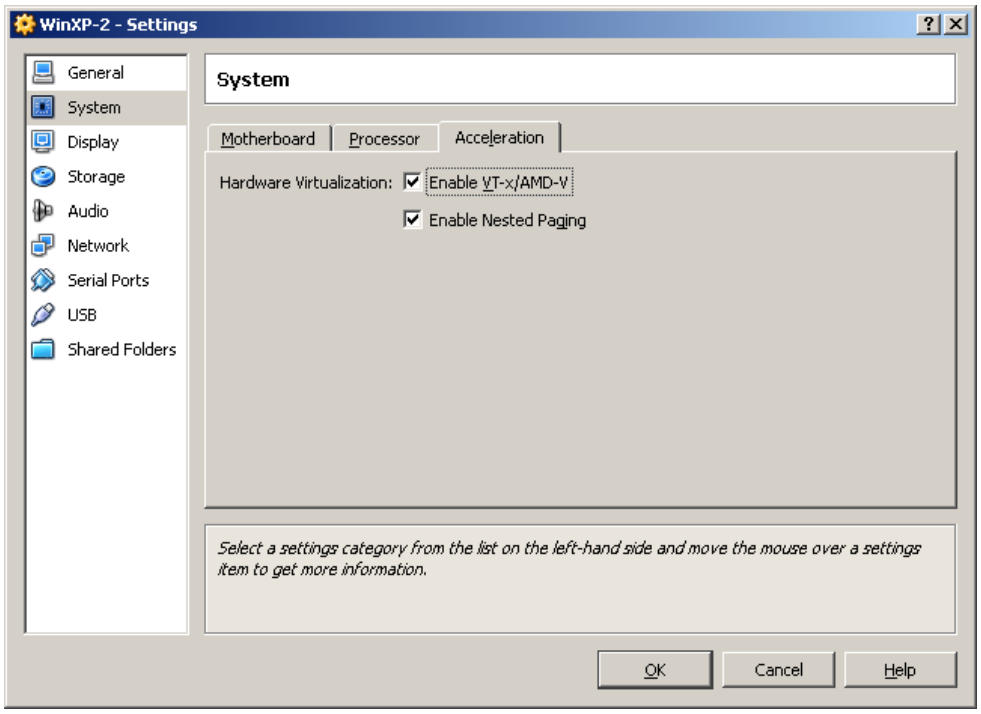

Рис. 1.13. Настройка аппаратной виртуализации

В разделе *Дисплей*/*Display* (рис. 1.14) на вкладке *Видео*/*Video* можно установить размер памяти виртуальной видео карты, а также включить 2D- и 3D-ускорение, причем включение 2D-ускорения желательно, а 3D – необязательно.

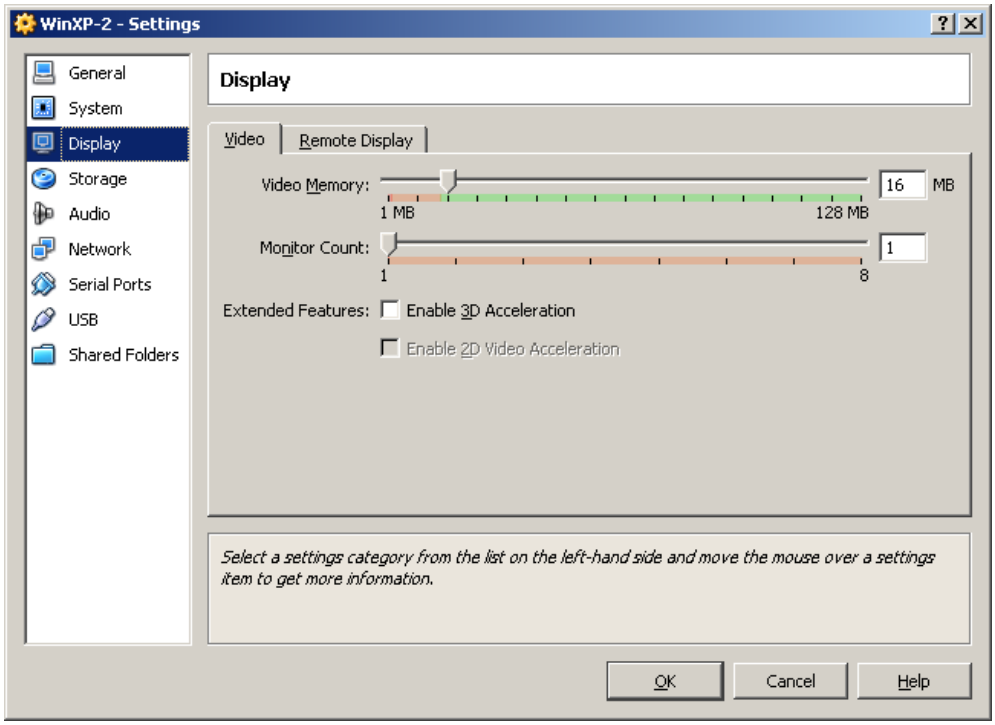

Рис. 1.14. Настройка параметров виртуального видеоадаптера

На вкладке *Удаленный дисплей*/*RemoteDisplay* можно включить опцию, при которой виртуальная машина будет работать как сервер удаленного рабочего стола (RDP).

В разделе *Носители*/*Storage* (рис. 1.15) отображен созданный ранее виртуальный жесткий диск и позиция с надписью *Пусто*/*Empty*.

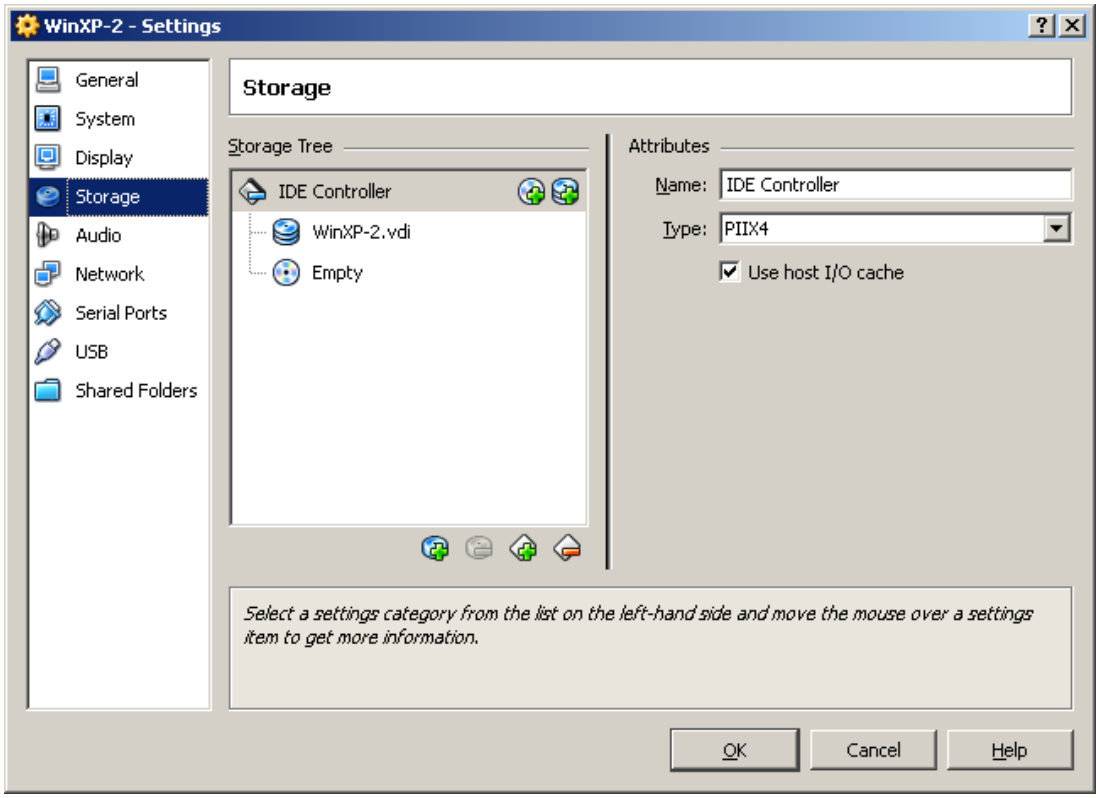

Рис. 1.15. Настройка виртуально CD-ROM

Далее необходимо выделить данную позицию и осуществить ее настройку. Для этого нужно щелкнуть по пиктограмме папки и в отрывшемся окне (рис. 1.16) добавить ISO-образ загрузочного диска операционной системы Windows. На рис. 1.17 представлена процедура добавления ISO-образов в менеджер виртуальных носителей. В него можно внести любое количество образов различного назначения, например игры, дистрибутивы приложений, базы данных и т. д.

Далее (рис. 1.18 и 1.19) необходимо настроить слоты подключения накопителей.

При этом устанавливается привод компакт-дисков как *Первичный мастер IDE*/*IDEPrimaryMaster*, жесткий диск, содержащий загрузочный раздел, как *Вторичный мастер IDE*/*IDESecondaryMaster*, а дополнительный виртуальный жесткий диск – как *Первичный слейв IDE*/*IDEPrimarySlave*.

При настройке сети в качестве типа подключения необходимо использовать *сетевой мост*, как показано на рис. 1.20.

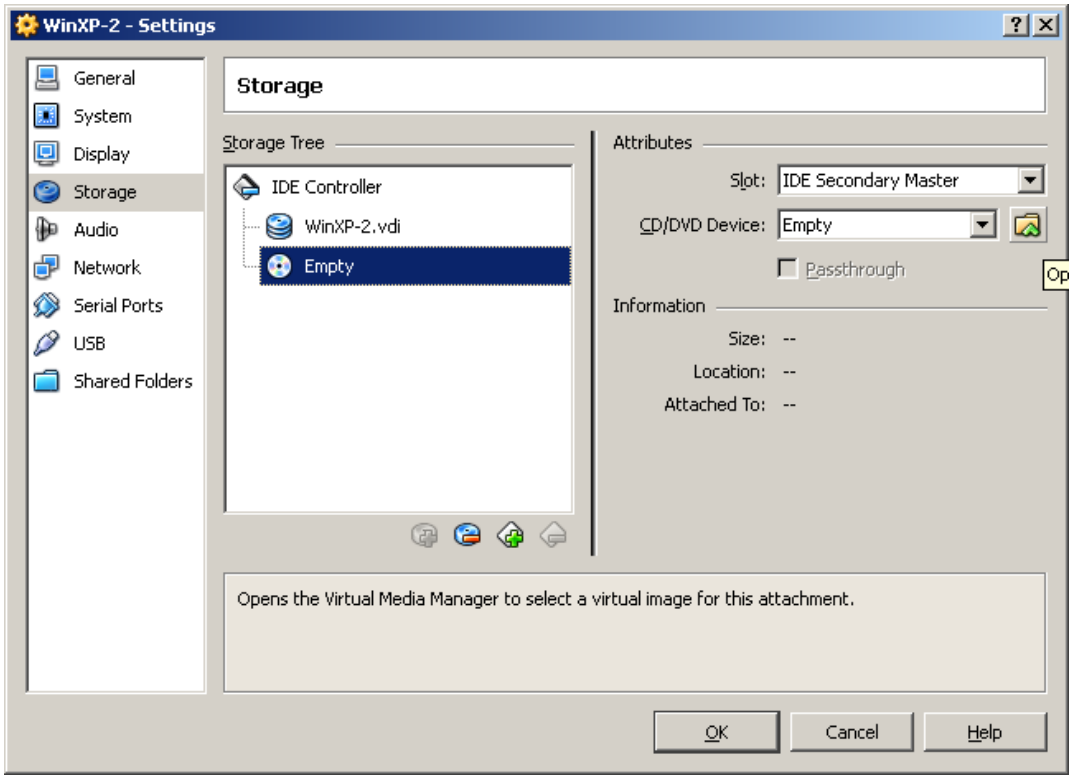

Рис. 1.16. Менеджер виртуальных носителей

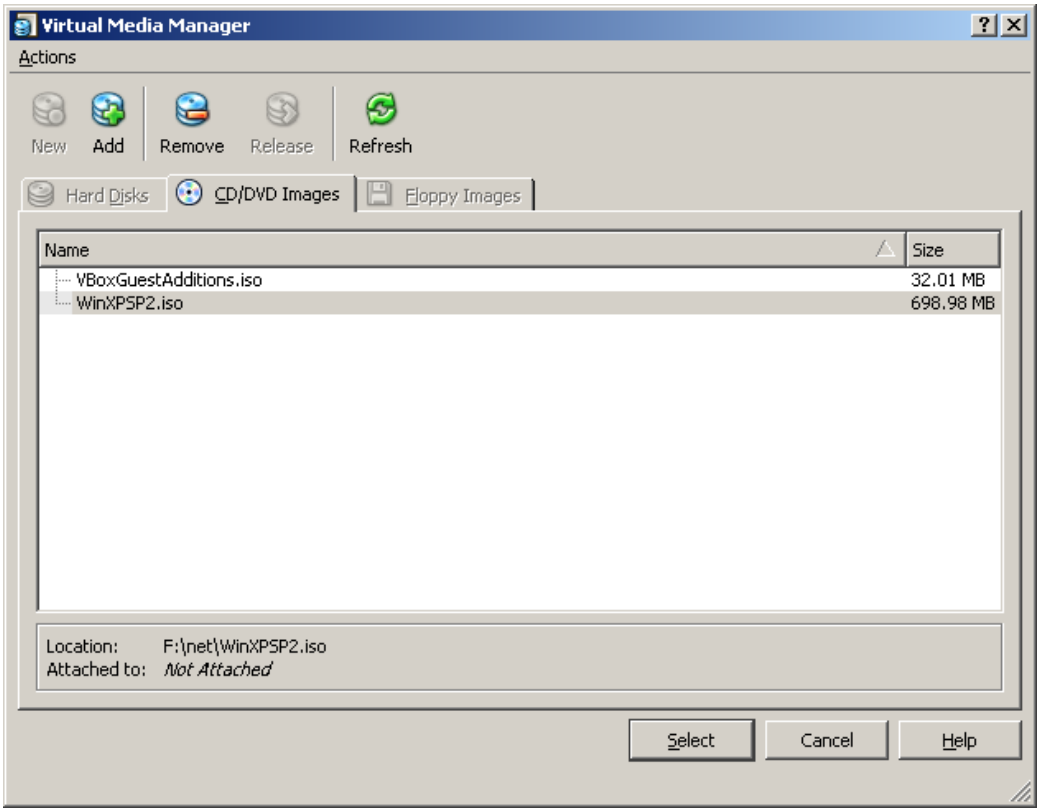

Рис. 1.17. Добавление виртуальных носителей

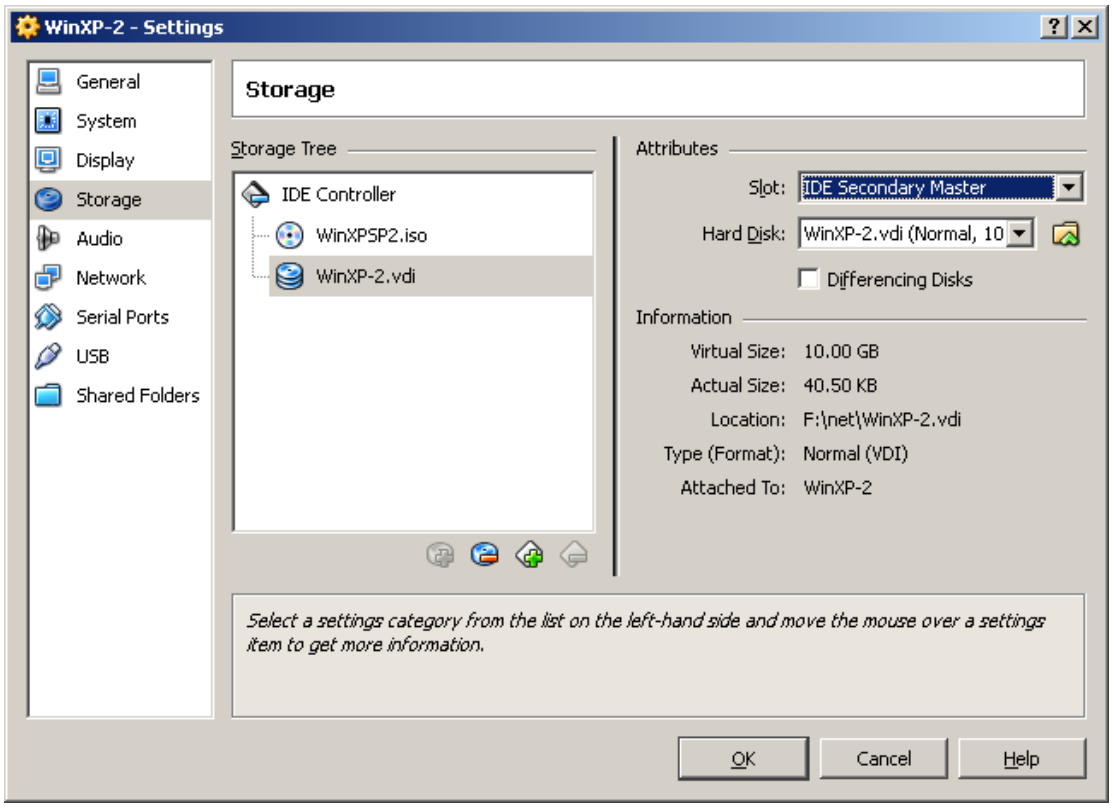

Рис. 1.18. Настройка слота подключения виртуального жесткого диска

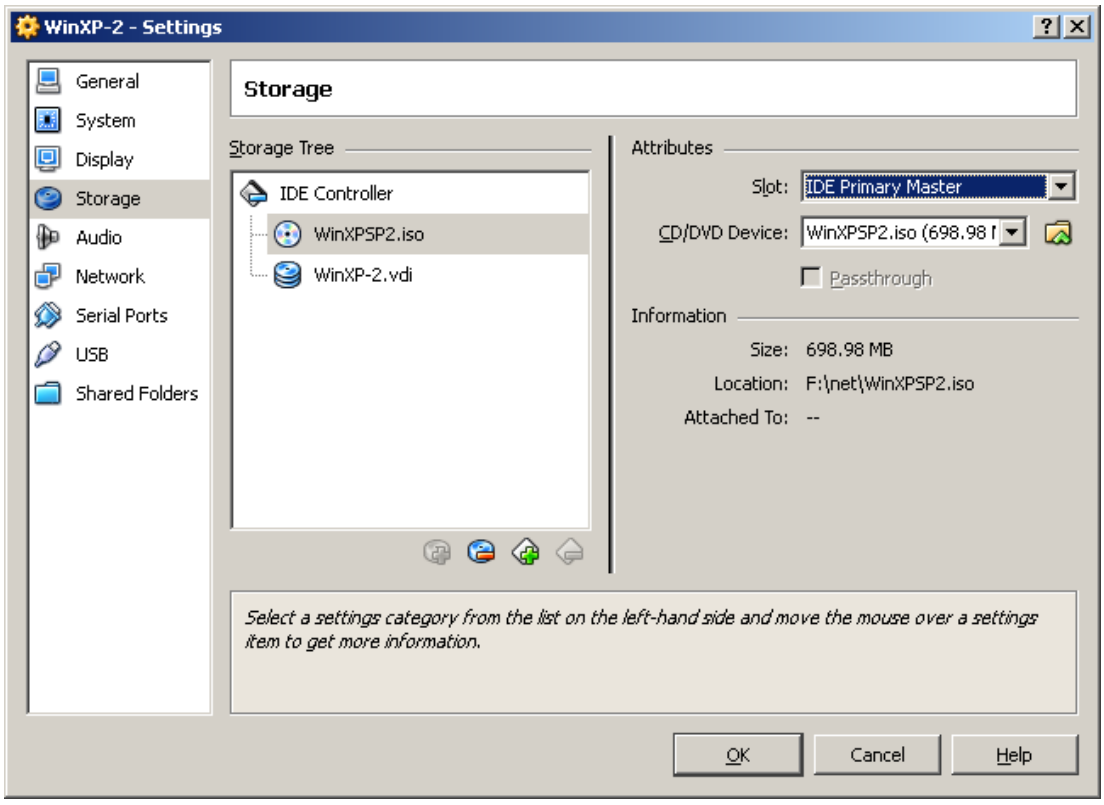

Рис. 1.19. Настройка слота подключения
виртуального привода оптических дисков

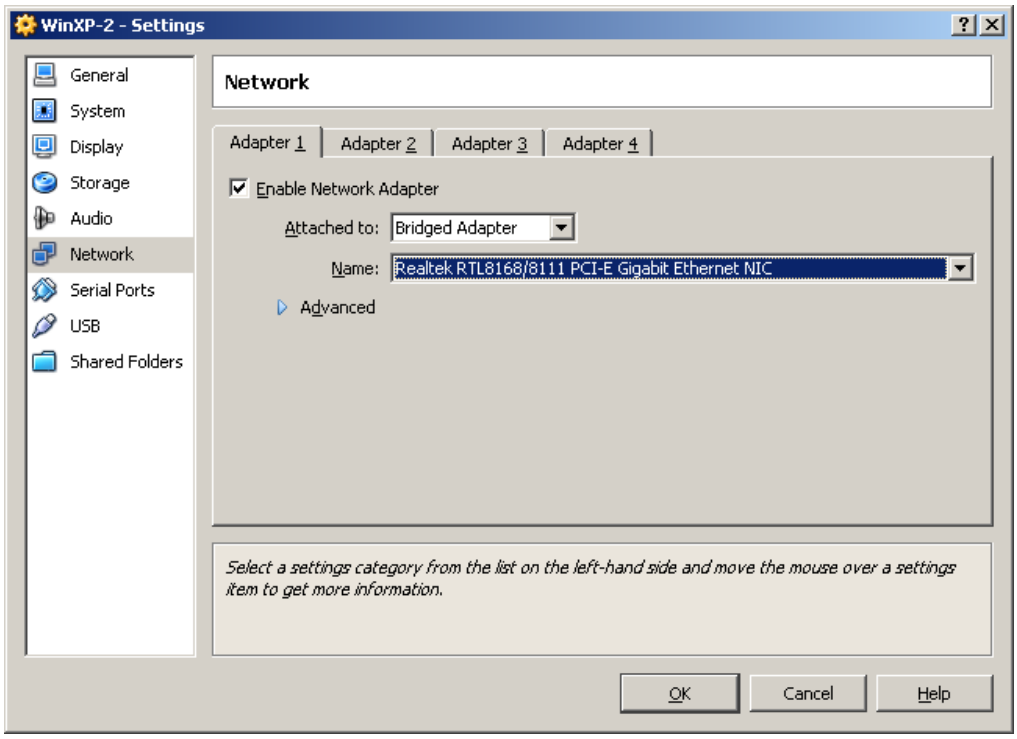

Рис. 1.20. Настройка сетевого адаптера виртуальной машины

Далее переходим к разделу USB (рис. 1.21), где необходимо поставить оба доступных флажка, а затем, используя кнопку с изображением *вилки* USB и *плюса*, добавить все доступные контроллеры.

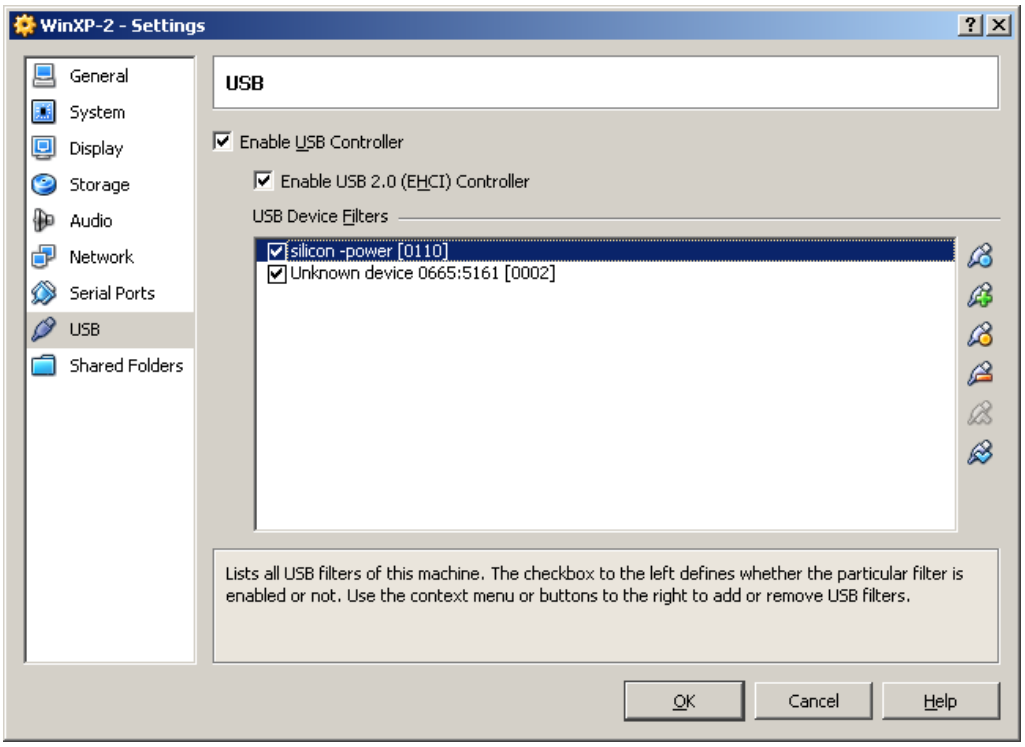

Рис. 1.21. Настройка USB контроллера виртуальной машины

В разделе *Общие папки*/*Shared Folders* (рис. 1.22) можно выбрать папки, которые необходимо сделать доступными для виртуальной машины.

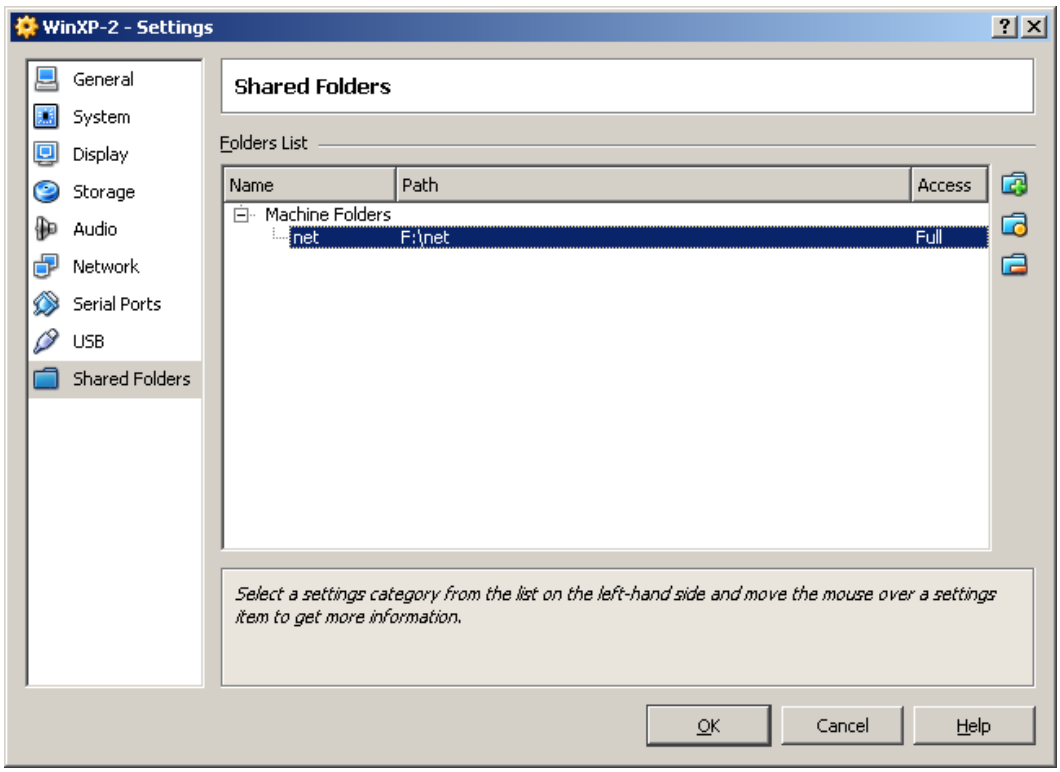

Рис. 1.22. Настройка общих папок

На этом настройка аппаратной части виртуальной машины может считаться законченной, и далее переходим к установке операционной системы.

1.1.2. Настройка операционной системы виртуальной машины

Описание установки операционной системы рассматриваться не будет, так как данная процедура является стандартной. Запуск установки операционной системы осуществляется из главного окна VirtualBox путем выбора соответствующей виртуальной машины и нажатия кнопки *Старт*/*Start* (рис. 1.23).

После проведения действий, описанных выше, появится окно с установкой операционной системы. Это означает, что все настройки выполнены правильно, и остается установить и настроить операционную систему. После того как система будет установлена и загружена (рис. 1.24), можно приступать к настройке операционной системы виртуальной машины. Отметим, что для выполнения лабораторных работ вам потребуется минимум 4 виртуальные машины с операционными системами: две из них типа Windows Server (можно использовать 2003, 2008 либо 2012 версии), а две – клиентские машины типа Windows XP, Windows 7, Windows 8. Установка других ОС выполняется аналогично.

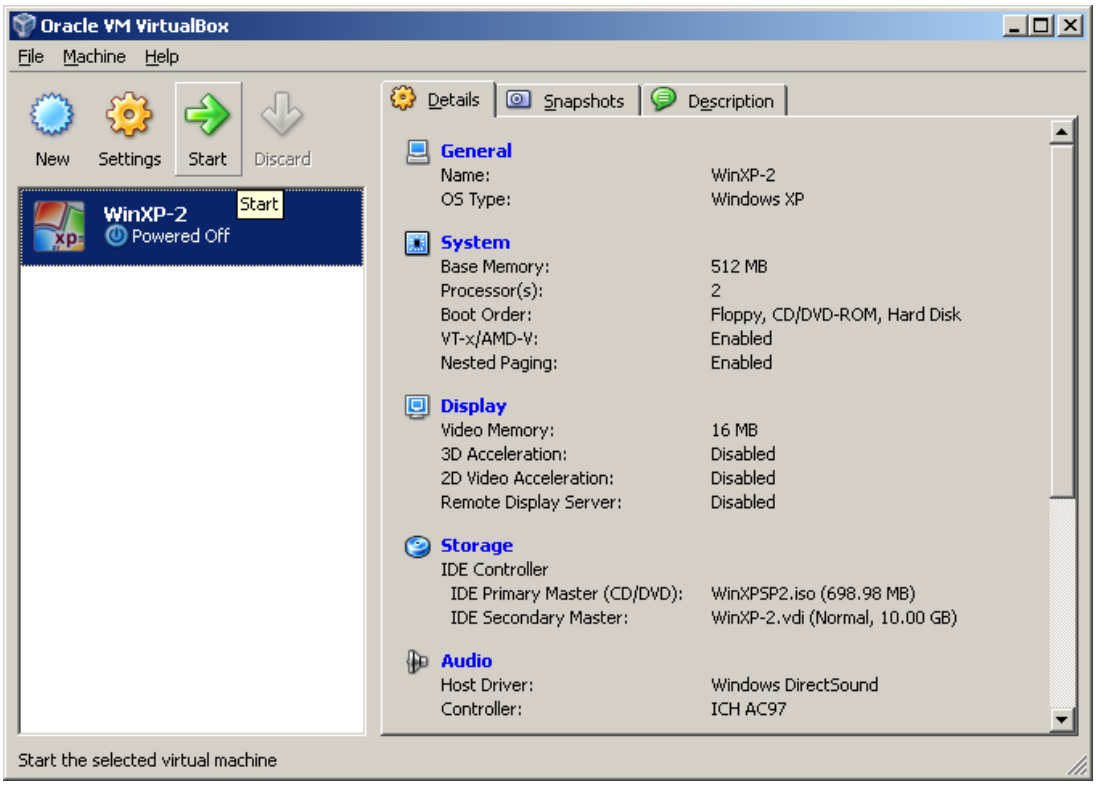

Рис. 1.23. Запуск установки операционной системы

Рис. 1.24. Настройка операционной системы

Для начала необходимо установить драйверы для всех виртуальных аппаратных компонентов виртуального ПК. Для этого в главном меню (рис. 1.25) нужно выбрать пункт *Устройства*/*Приводы оптических дисков*/*VboxGuestAdditions.iso*. Впоследствии таким же образом можно подключить к виртуальной машине физический CD-ROM или загрузить ISO-образ.

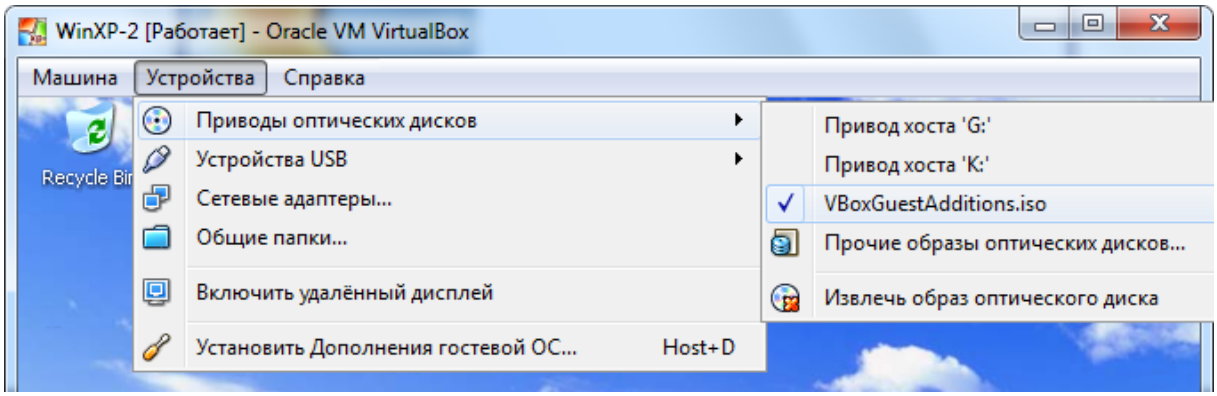

Рис. 1.25. Загрузка *VboxGuestAdditions.iso*
при настройке операционной системы

После подключения образа *VboxGuestAdditions.iso* в папке *Мой компьютер* в привод компакт-дисков загрузится данный виртуальный диск – далее его необходимо запустить двойным щелчком левой кнопки мыши (рис. 1.26).

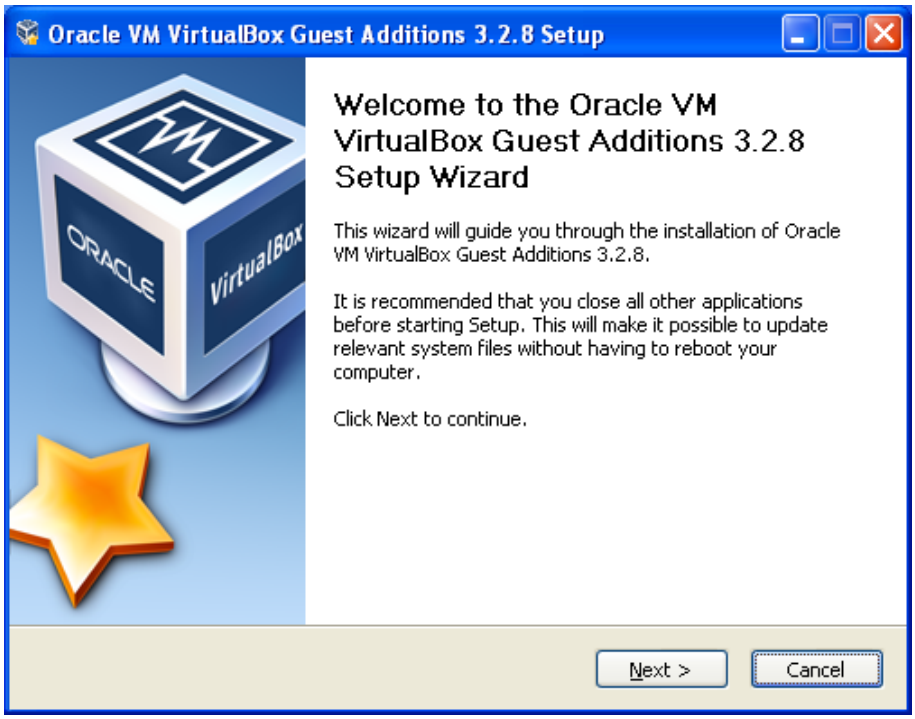

Рис. 1.26. Установка *VboxGuestAdditions.iso*
при настройке операционной системы

Сам процесс установки происходит практически без участия пользователя, и только в случае, если ранее было включено 3D-ускорение, следует выбрать соответствующий компонент (Direct3DSupport) (рис. 1.27) для дополнительной установки.

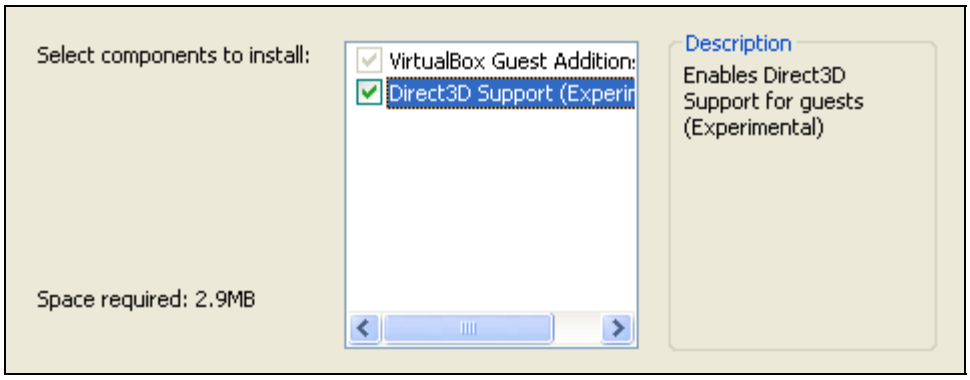

Рис. 1.27. Выбор дополнений при настройке операционной системы

Далее подключим общие папки, чтобы получить возможность переносить в созданную виртуальную машину нужные для работы файлы и устанавливать приложения. Это можно сделать с помощью командной строки, следуя справке *VirtualBox*, но лучше использовать следующий способ: необходимо открыть папку *Мой компьютер*, в главном меню выбрать *Сервис*/*Подключить сетевой диск* и открывшемся окне в поле *папка* ввести *\\vboxsrv\имя_общей_папки*, например как показано ниже.

```
\\vboxsrv\WinXP-2-Share
```

После этих действий в папке *Мой компьютер* появится общая папка, доступная в качестве сетевого диска.

Для создания второй виртуальной машины зачастую будет целесообразным сделать ее копию, выполнив щелчок правой кнопкой мыши по названию виртуальной машины (т. е. вызвав контекстное меню) и выбрав операцию копирования. При этом на последующем этапе важным является выбрать пункт, связанный с изменением всех адресов.

1.2. Организация статической и динамической адресации в компьютерных сетях

Каждый компьютер в сетях TCP/IP имеет адреса трех уровней: физический (MAC-адрес), сетевой (IP-адрес) и символьный (DNS-имя).

При построении информационных систем с большим числом узлов целесообразно использовать методы как статической, так и динамической

адресации. Так, серверы, выполняющие все необходимые функции, связанные с управлением, используют всегда статические адреса, но при этом все клиенты, как правило, получают IP-адрес и другие параметры сети динамически. Это связано с тем, что в больших информационных системах число узлов может составлять тысячи, соответственно ручная настройка каждого из них затруднительна. Поэтому целесообразно использовать методы автоматической настройки IP-параметров клиентских компьютеров, основанные на динамической адресации.

1.2.1. Статическая адресация в компьютерных сетях

Ключевую роль в организации любой компьютерной сети играет сетевой адрес (IP-адрес), который представляет собой 32-разрядное двоичное число, разделенное на группы по 8 бит, называемые *октетами*. Например, 00010001 11101111 00101111 01011110.

Обычно IP-адреса записываются в виде четырех десятичных октетов и разделяются точками. Таким образом, приведенный выше IP-адрес можно записать в следующей форме: 17.239.47.94.

Следует заметить, что максимальное значение октета равно 11111111_2 (двоичная система счисления), что соответствует в десятичной системе 255_{10}. Поэтому IP-адреса, в которых хотя бы один октет превышает это число, являются недействительными, например 172.16.123.1 – действительный адрес, а 172.16.123.256 – несуществующий адрес, поскольку 256 выходит за пределы допустимого диапазона: от 0 до 255.

IP-адрес состоит из двух логических частей – *номера подсети* (ID подсети) и *номера узла* (ID хоста) в этой подсети. При передаче пакета из одной подсети в другую используется ID подсети. Когда пакет попал в подсеть назначения, ID хоста указывает на конкретный узел в рамках этой подсети.

Чтобы записать ID подсети, в поле номера узла в IP-адресе ставят нули. Чтобы записать ID хоста, в поле номера подсети ставят нули.

Например, если в IP-адресе 172.16.123.1 первые два байта отводятся под номер подсети, остальные два байта – под номер узла, то номера записываются следующим образом: ID подсети 172.16.0.0; ID хоста 0.0.123.1.

По числу разрядов, отводимых для представления номера узла (или номера подсети), можно определить общее количество узлов (или подсетей) по простому правилу: если число разрядов для представления номера узла равно N, то общее количество узлов равно $2^N - 2$. Два узла вычитаются вследствие того, что адреса со всеми разрядами, равными нулям или единицам, являются особыми и используются в специальных целях.

Например, если под номер узла в некоторой подсети отводится два байта (16 бит), то общее количество узлов в такой подсети равно $2^{16} - 2 =$ 65 534 узлов.

Общее правило: под ID подсети отводятся *первые* несколько бит IP-адреса, оставшиеся биты обозначают ID хоста.

Служба распределения номеров IANA (Internet Assigned Numbers Authority) зарезервировала для частных (локальных) сетей три блока адресов:

10.0.0.0 – 10.255.255.255 (префикс 10/8);

172.16.0.0 – 172.31.255.255 (префикс 172.16/12);

192.168.0.0 – 192.168.255.255 (префикс 192.168/16).

Будем называть первый блок 24-битовым, второй – 20-битовым, а третий – 16-битовым. Отметим, что первый блок представляет собой не что иное, как одну сеть класса *A*, второй блок – 16 последовательных сетей класса *B*, а третий блок – 256 последовательных сетей класса *C*.

Любая организация может использовать IP-адреса из этих блоков без согласования с IANA или Internet-регистраторами. В результате эти адреса используются во множестве организаций. Таким образом, уникальность адресов сохраняется только в масштабе одной или нескольких организаций, согласованно использующих общий блок адресов. В такой сети каждая рабочая станция может обмениваться информацией с любой другой рабочей станцией частной сети.

Если организации требуются уникальные адреса для связи с внешними сетями, такие адреса следует получать обычным путем через регистраторов Internet. Такие адреса никогда не будут входить ни в один из указанных выше блоков частных адресов.

Рассмотрим конфигурирование IP-адресации (v4) в операционных системах типа Windows.

Пример 1. Рассмотрим настройку протокола TCP/IPv4.

1. Запустите папку *Сетевые подключения*. Для этого в операционных системах типа Windows Seven необходимо нажать кнопку *Пуск*, ввести в строке поиска начальные буквы слова *Центр*. Из списка выберите пункт *Центр управления сетями и общим доступом* (рис. 1.28).

2. В окне *Центра управления сетями и общим доступом* щелкните по *Изменению параметров адаптера* (рис. 1.29). Далее откроется окно с сетевыми подключениями (рис. 1.30).

3. Щелкните правой кнопкой мыши по подключению, которое требуется настроить, а затем выберите команду *Свойства*. Если появится диалоговое окно *Управление учетной записью пользователя*, убедитесь, что действие, указанное в окне, совпадает с тем, которое вы хотите выполнить, и нажмите *Продолжить*.

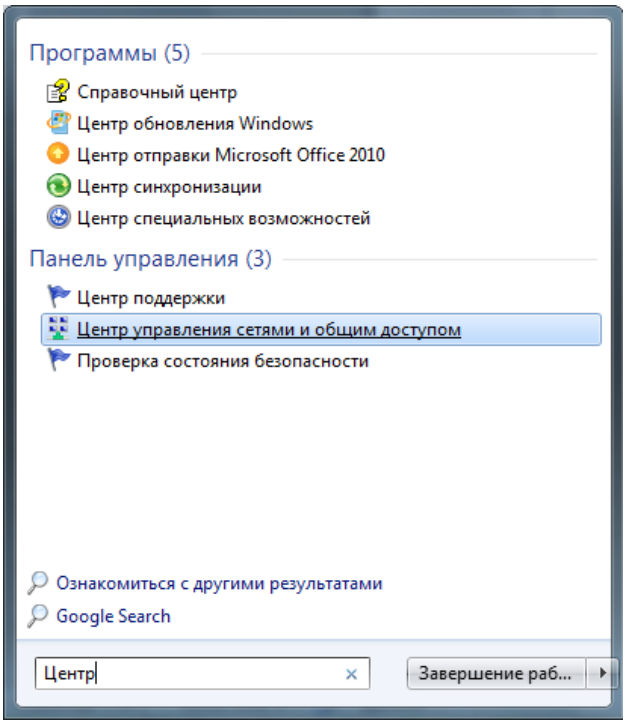

Рис. 1.28. Пример вызова *Центра управления сетями и общим доступом*

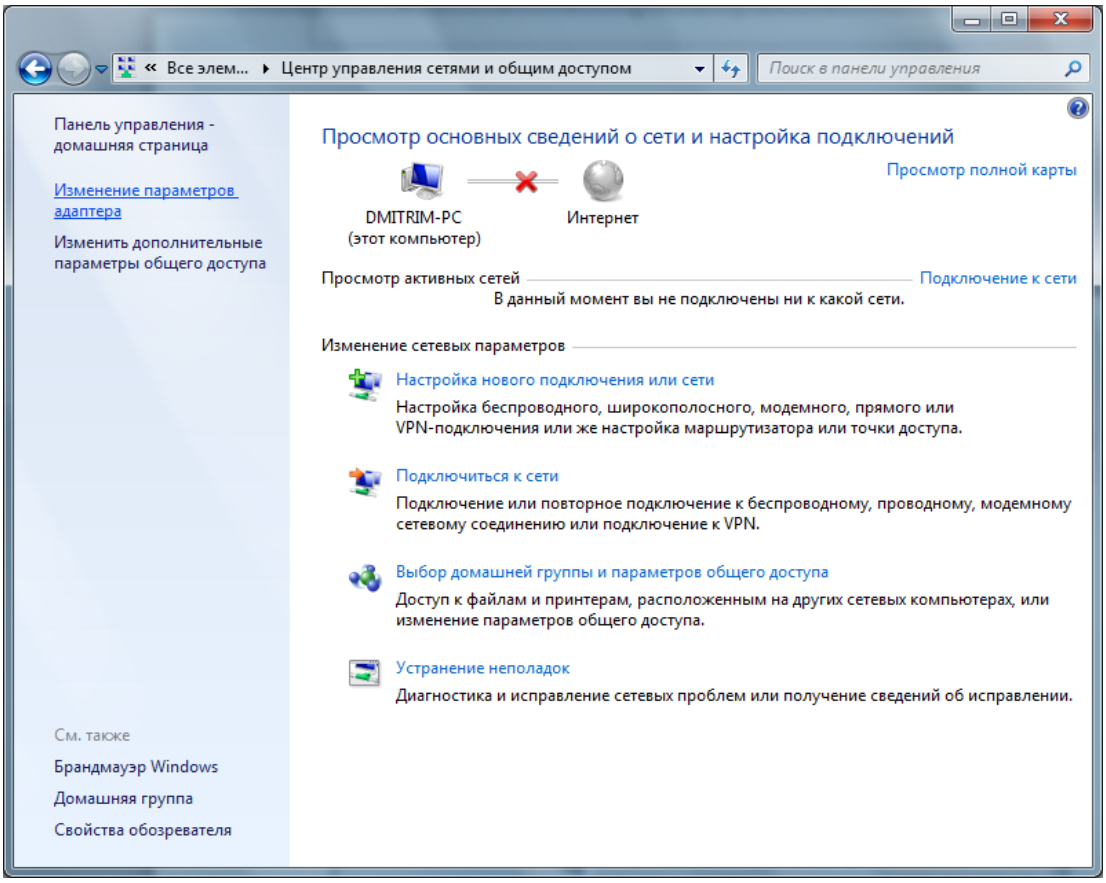

Рис. 1.29. Общий вид *Центра управления сетями и общим доступом*

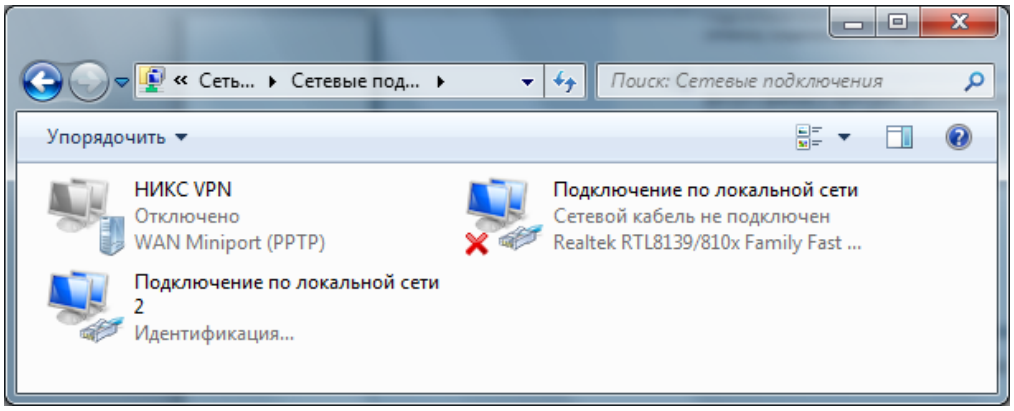

Рис. 1.30. Общий вид папки *Сетевые подключения*

4. Далее выполните одно из указанных ниже действий:

– в случае подключения по локальной сети на вкладке *Общие* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства*;

– в случае подключения удаленного доступа, VPN-подключения или высокоскоростного подключения на вкладке *Сеть* в списке *Компоненты*, используемые этим подключением, выберите пункт *Протокол Интернета версии 4 (TCP/IPv4)* и нажмите кнопку *Свойства* (рис. 1.31). В результате откроется окно с настройками протокола TCP/IP (рис. 1.32).

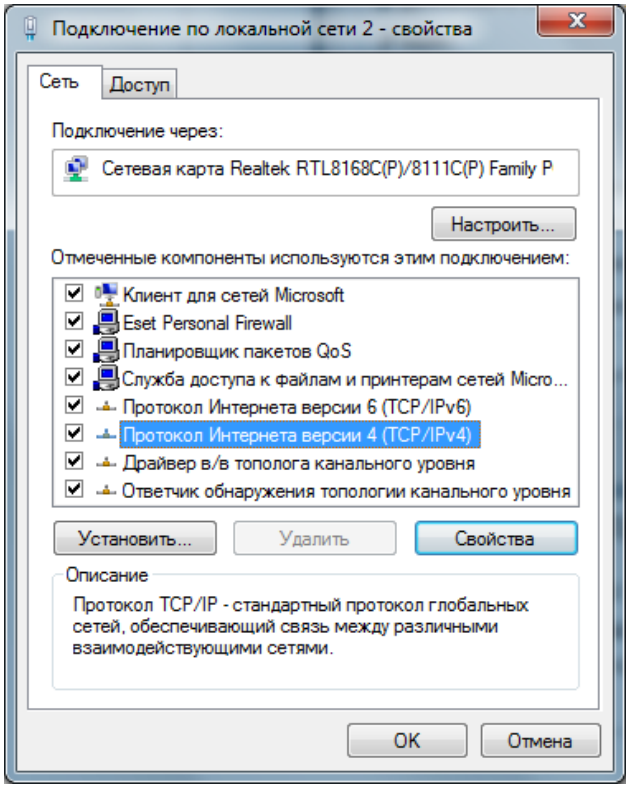

Рис. 1.31. Свойства: *Подключение по локальной сети*

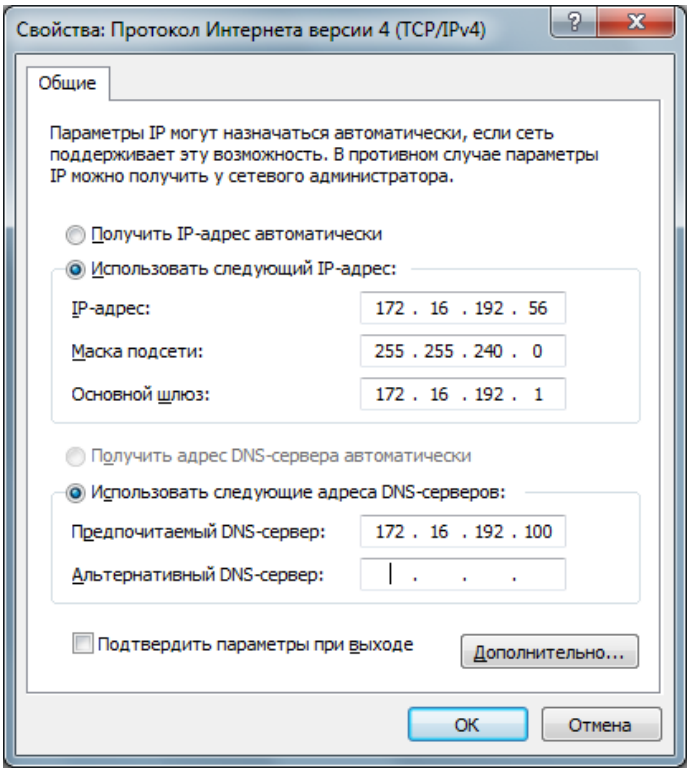

Рис. 1.32. Свойства: *Протокол Интернета версии 4* (*TCP/IPv4*)

5. Выполните далее одно из указанных ниже действий:

– если необходимо, чтобы параметры IP-адреса назначались автоматически (для клиентских компьютеров информационной системы), выберите пункт *Получить IP-адрес автоматически* и нажмите кнопку *OK*;

– если необходимо указать IP-адрес IPv4 или адрес DNS-сервера (также могут быть получены автоматически), выполните следующие действия:

а) выберите пункт *Использовать следующий IP-адрес* и в поле *IP-адрес* введите IP-адрес, соответствующую маску подсети и адрес шлюза по умолчанию (в примере на рис. 1.32 IP адрес: 172.16.192.56; маска подсети: 255.255.240.0; основной шлюз: 172.16.192.1);

б) выберите пункт *Использовать следующие адреса DNS-серверов* и в полях *Предпочитаемый DNS-сервер* и *Альтернативный DNS-сервер* введите адреса основного и, при необходимости, дополнительного DNS-сервера (в примере на рис. 1.32 IP-адрес предпочитаемого DNS сервера: 172.16.192.100);

в) для настройки параметров DNS, WINS и IP нажмите кнопку *Дополнительно* (рис. 1.33).

6. В подключении по локальной сети при выборе параметра *Получить IP-адрес автоматически* включается вкладка *Альтернативная конфигурация*. Если компьютер используется более чем в одной сети, используйте

эту вкладку для ввода альтернативных параметров IP-адреса. Для настройки параметров DNS, WINS и IP откройте вкладку *Настраиваемый пользователем* или *Альтернативная конфигурация.*

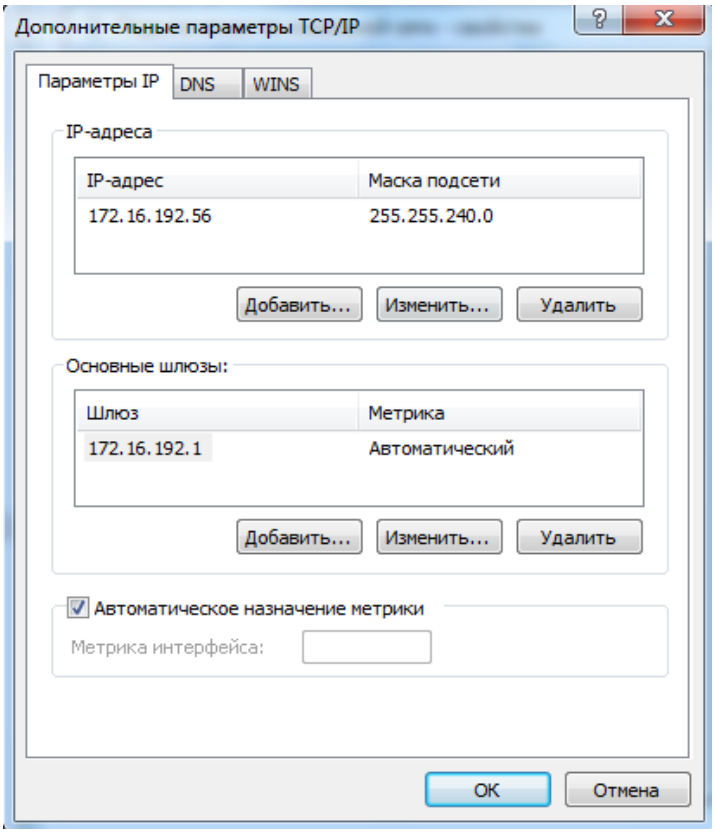

Рис. 1.33. Окно с дополнительными параметрами TCP/IP

Параметры *Альтернативная конфигурация* определяют второй набор параметров протокола IP, который используется при недоступности DHCP-сервера. Это весьма полезно для пользователей портативных компьютеров, которые часто перемещаются между двумя различными сетевыми средами (например, между средой со службой DHCP и средой со статическими IP-адресами).

Отметим, что аналогично осуществляется конфигурирование TCP/IPv6 (используются *свойства*: *Протокол Интернета версии 6 (TCP/IPv6)*).

1.2.2. Динамическая адресации в компьютерных сетях

Как уже было сказано, IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора утомительную процедуру. Ситуация усложняется еще тем, что многие пользователи не обладают достаточными знаниями для того, чтобы конфигурировать свои компьютеры для работы в интерсети, и должны поэтому полагаться на администраторов.

Протокол Dynamic Host Configuration Protocol (DHCP) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. Однако, кроме динамического, DHCP может поддерживать и более простые способы ручного и автоматического статического назначения адресов.

В ручной процедуре назначения адресов активное участие принимает администратор, который предоставляет DHCP-серверу информацию о соответствии IP-адресов физическим адресам или другим идентификаторам клиентов. Эти адреса сообщаются клиентам в ответ на их запросы к DHCP-серверу.

При автоматическом статическом способе DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула наличных IP-адресов (его также называют scope или диапазоном IP-адресов) без вмешательства оператора. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом по-прежнему, как и при ручном назначении, существует постоянное соответствие. Оно устанавливается в момент первичного назначения сервером DHCP IP-адреса клиенту. При всех последующих запросах сервер возвращает тот же самый IP-адрес.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время, что дает возможность впоследствии повторно использовать IP-адреса другими компьютерами. Служба DHCP обеспечивает надежный и простой способ конфигурации сети TCP/IP, гарантируя отсутствие конфликтов адресов за счет централизованного управления их распределением. Администратор управляет процессом назначения адресов с помощью параметра «продолжительности аренды», который определяет, как долго компьютер может использовать назначенный IP-адрес, перед тем как снова запросить его от сервера DHCP в аренду.

1.2.3. Принцип работы протокола DHCP

Выделяют 3 типа областей:

– стандартные (описывает одну IP-сеть);

– суперобласть (совокупность стандартных);

– многоадресные (описывают IP-сети, предназначенные для многократной рассылки).

Стандартные. Служат для объединения компьютеров в логические подсети в рамках одной физической сети. При этом администратор сначала создает область для каждой подсети, а затем использует ее для определения параметров клиентов.

Любая стандартная область характеризуется следующими свойствами:

1) диапазон IP-адресов, из которых службой DHCP выбираются либо исключаются IP-адреса;

2) маска подсети;

3) срок аренды, назначаемый клиентам DHCP, которые динамически получают адреса.

В большинстве случаев на DHCP-серверы настраивается одна стандартная область, но если один DHCP-сервер обслуживает несколько сетей, то создается несколько стандартных областей, которые в дальнейшем объединяются в суперобласти. При этом важно следить, чтобы диапазон IP-адресов отдельных стандартных областей не пересекались.

Суперобласти. С помощью их можно получить ряд дополнительных возможностей.

1. Поддержка DHCP-клиентов, расположенных на отдельном сегменте физической сети, в которой используется несколько логических IP-сетей. Если в каждой физической сети или подсети используется несколько логических сетей или подсетей, то такие конфигурации называются *мультисетевыми*.

2. Поддержка удаленных DHCP-клиентов, расположенных на удаленной стороне агентов-ретрансляторов.

Суперобласти позволяют разрешать следующие проблемные ситуации:

1) доступный диапазон в настоящее время исчерпан почти полностью, исходная область включает весь диапазон IP-сети для расширения адресного пространства для одного и того же физического сегмента сети с последующим объединением в суперобласти;

2) клиенты должны перейти со временем на другую область, например для перенумерации текущей IP-сети, в таком случае также создается новая область с последующим объединением в суперобласти;

3) необходимость использования два DHCP-сервера в физическом сегменте для управления различными логическими сетями.

Многоадресная область. В качестве диапазона адресов многоадресной групповой рассылки использует класс адресов D. Данные адреса не могут использоваться в стандартных областях.

Во всех TCP/IP сетях каждый узел сначала должен получить индивидуальный IP (классы A, B, C). Без назначения такого адреса настройка узла на поддержку и использование вторичных IP-адресов (адреса многоадресной рассылки) невозможна.

Членство в группе многоадресной рассылки является динамическим, что означает возможность присоединения в любое время IP-узлов или их выход.

Создается область многоадресной рассылки, которая будет назначать клиенту групповой адрес после получения индивидуального.

В DHCP-серверах можно резервировать за определенным MAC-адресом соответствующий IP-адрес, так же можно в области добавлять исключения.

Исключения – это диапазон IP-адресов, из которого клиентам адреса не будут выдаваться. Как правило, в диапазон исключений попадают все статически заданные IP-адреса в сети.

Перечислим только *основные параметры DHCP*:

– Subnet mask – маска подсети;

– Router – список IP-адресов маршрутизаторов;

– Domain Name Servers – список адресов DNS-серверов;

– DNS Domain Name – DNS-суффикс клиента;

– WINS Server Names – список адресов WINS-серверов;

– LeaseTime – срок аренды (в секундах);

– Renewal Time (T1) – период времени, через который клиент начинает продлевать аренду;

– Rebinding Time (T2) – период времени, через который клиент начинает осуществлять широковещательные запросы на продление аренды.

Параметры могут применяться на следующих *уровнях*:

– уровень сервера;

– уровень области действия;

– уровень класса;

– уровень клиента (для зарезервированных адресов).

Параметры, определенные на нижележащем уровне, перекрывают параметры вышележащего уровня: например, параметры клиента имеют больший приоритет, чем параметры сервера. Самый высокий приоритет имеют параметры, настроенные вручную на клиентском компьютере.

Уровень класса используется для объединения клиентов в группы и применения для этой группы отдельных параметров. Отнести клиента к определенному классу можно, применив утилиту IPconfig с ключом /setclassid.

Процесс функционирования служб DHCP заключается в обмене сообщениями между сервером и клиентом. Список используемых сообщений представлен в табл. 1.1.

Диаграмма переходов, иллюстрирующая принципы работы протокола DHCP, приведена на рис. 1.34. На схеме овалами обозначены состояния, в которых может находиться DHCP-клиент. Из одного состояния в другое клиент может переходить только по дугам. Каждая дуга помечена дробью, числитель которой обозначает событие (чаще всего это сообщение от DHCP-сервера), после которого клиент переходит в соответствующее состояние, а знаменатель описывает действия DHCP-клиента при переходе. Черточка в числителе означает безусловный переход.

Таблица 1.1

Типы DHCP-сообщений

Тип сообщения	Направление	Значение
DHCPDISCOVER (DHCP-обнаружение)	Клиент → сервер	Широковещательный запрос для обнаружения DHCP-сервера
DHCPOFFER (DHCP-предложение)	Сервер → клиент	Ответ на DHCPDISCOVER, содержит предлагаемые сетевые параметры
DHCPREQUEST (DHCP-запрос)	Клиент → сервер	Запрос предложенных параметров
DHCPACK (DHCP-подтверждение)	Сервер → клиент	Подтверждение сетевых параметров
DHCPNAK (DHCP-несогласие)	Сервер → клиент	Отклонение запроса клиента
DHCPDECLINE (DHCP-отказ)	Клиент → сервер	Отказ клиента от предложенных параметров
DHCPRELEASE (DHCP-освобождение)	Клиент → сервер	Освобождение арендованного IP-адреса
DHCPINFORM (DHCP-информация)	Клиент → сервер	Запрос дополнительных параметров

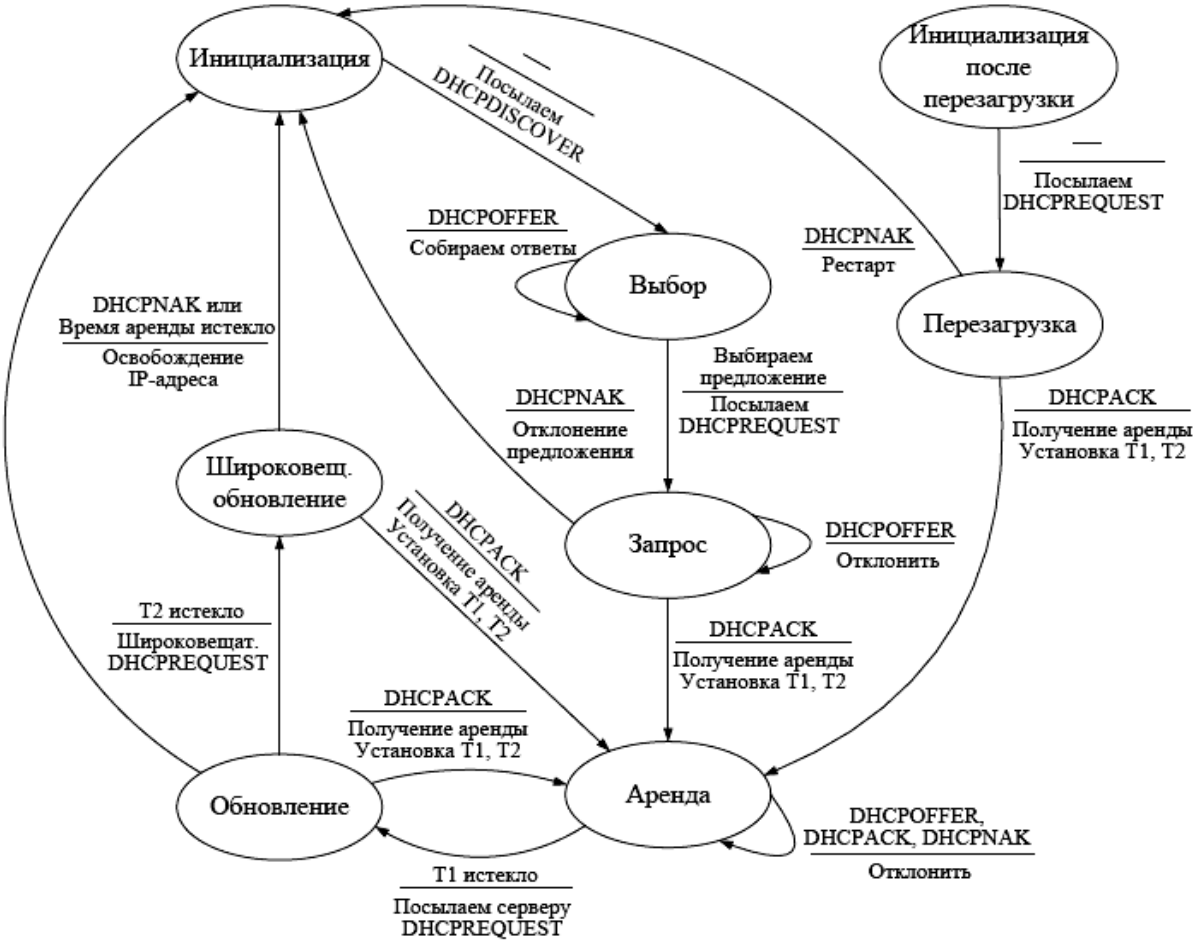

Рис. 1.34. Диаграмма переходов, иллюстрирующая принципы работы протокола DHCP

Начальное состояние, в котором оказывается служба DHCP-клиента при запуске, – это «Инициализация». Из этого состояния происходит безусловный переход в состояние «Выбор» с рассылкой широковещательного сообщения DHCPDISCOVER. DHCP-серверы (в одной сети их может быть несколько), принимая сообщение, анализируют свою базу данных на предмет наличия свободных IP-адресов. В случае успеха серверы отправляют сообщение DHCPOFFER, которое помимо IP-адреса содержит дополнительные параметры, призванные помочь клиенту выбрать лучшее предложение. Сделав выбор, клиент посылает широковещательное сообщение DHCPREQUEST, запрашивая предложенный IP-адрес и требуемые параметры (например, маска подсети, шлюз по умолчанию, IP-адреса DNS-серверов и др.), и переходит в состояние «Запрос». Данное сообщение требуется посылать широковещательно (т. е. оно должно доставляться всем компьютерам подсети), чтобы DHCP-серверы, предложения которых клиент отклонил, знали об отказе.

В состоянии «Запрос» клиент ожидает подтверждение сервера о возможности использования предложенных сетевых параметров. В случае прихода такого подтверждения (сообщение DHCPACK) клиент переходит в состояние «Аренда», одновременно начиная отсчет интервалов времени T1 и T2. Если сервер по каким-либо причинам не готов предоставить клиенту предложенный IP-адрес, он посылает сообщение DHCPNAK. Клиент реагирует на это сообщение переходом в исходное состояние «Инициализация», чтобы снова начать процесс получения IP-адреса.

Состояние «Аренда» является основным рабочим состоянием – у клиента присутствуют все необходимые сетевые параметры, и сеть может успешно функционировать.

Через временной интервал T1 от момента получения аренды (обычно T1 равно половине общего времени аренды) DHCP-клиент переходит в состояние «Обновление» и начинает процесс обновления аренды IP-адреса. Сначала клиент посылает DHCP-серверу сообщение DHCPREQUEST, включающее арендованный IP-адрес. Если DHCP-сервер готов продлить аренду этого адреса, то он отвечает сообщением DHCPACK, клиент возвращается в состояние «Аренда» и заново начинает отсчитывать интервалы T1 и T2.

В случае, если в состоянии «Обновление» по истечении интервала времени T2 (который обычно устанавливается равным 87,5% от общего времени аренды) все еще не получено подтверждение DHCPACK, клиент переходит в состояние «Широковещательное обновление» с рассылкой широковещательного сообщения DHCPREQUEST. Такая рассылка делается в предположении, что DHCP-сервер поменял свой IP-адрес (или перешел в другую подсеть) и передал свою область действия другому серверу. В этом состоянии получение DHCPACK возвращает клиента в состояние «Аренда» и аренда данного IP-адреса продлевается. Если клиент получает от сервера сообщение

DHCPNAK или общее время аренды истекает, то происходит переход в состояние «Инициализация» и клиент снова пытается получить IP-адрес.

В процессе работы может оказаться, что время аренды не истекло, а служба DHCP-клиента прекратила работу (например, при перезагрузке). В этом случае DHCP-клиент начинает работу в состоянии «Инициализация после перезагрузки», рассылает широковещательное сообщение DHCPREQUEST и переходит в состояние «Перезагрузка». В случае подтверждения продления аренды (сообщение DHCPACK от DHCP-сервера) клиент переходит в состояние «Аренда». Иначе (сообщение DHCPNAK) клиент оказывается в состоянии «Инициализация».

1.2.4. Установка и настройка DHCP-сервера

Рассмотрим настройку DHCP-сервера на примере ОС Windows Server 2012.

1. Установка и авторизация сервера DHCP

Установка службы DHCP выполняется так же, как и установка любой другой компоненты Windows Server: *Пуск – Панель управления –Установка и удаление программ – Установка компонентов Windows – Сетевые службы* – кнопка *Состав – выбрать пункт DHCP* – кнопки *OK*, *Далее* и *Готово* (если потребуется, то указать путь к дистрибутиву системы). Также можно установить DHCP-сервер, используя *Server Manager (Диспетчер серверов)*, а именно *Start (Пуск) – Server Manager (Диспетчер серверов)*, общий вид которого показан на рис 1.35.

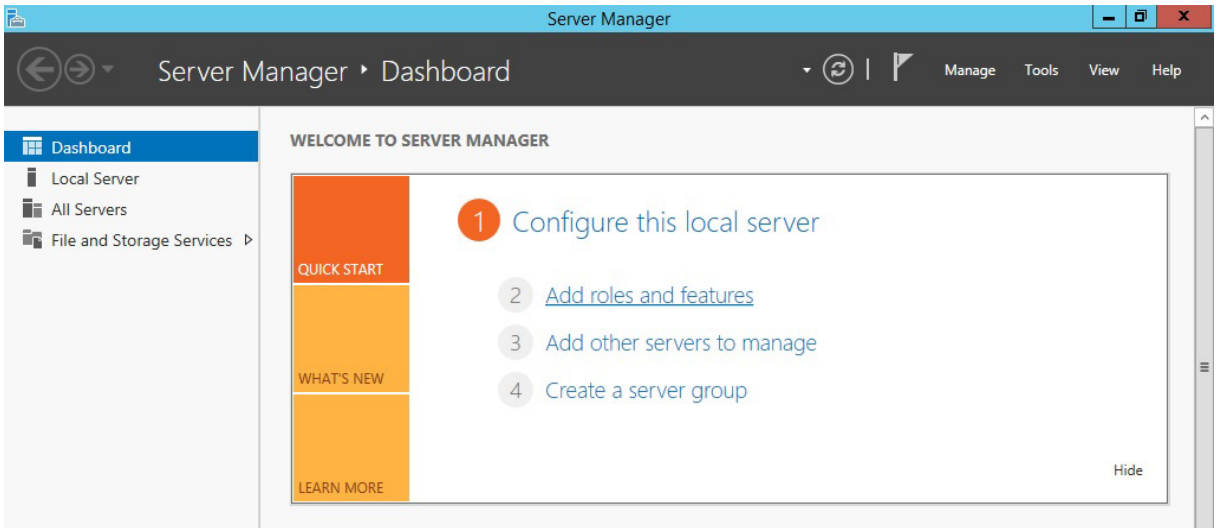

Рис. 1.35. Общий вид *Server Manager*

Далее нажимаем *Add roles and features (Добавить роль сервера)*, можно непосредственно через быстрый запуск, а можно через меню *Управление*, и на странице приветствия жмем *Next (Далее)* (рис. 1.36).

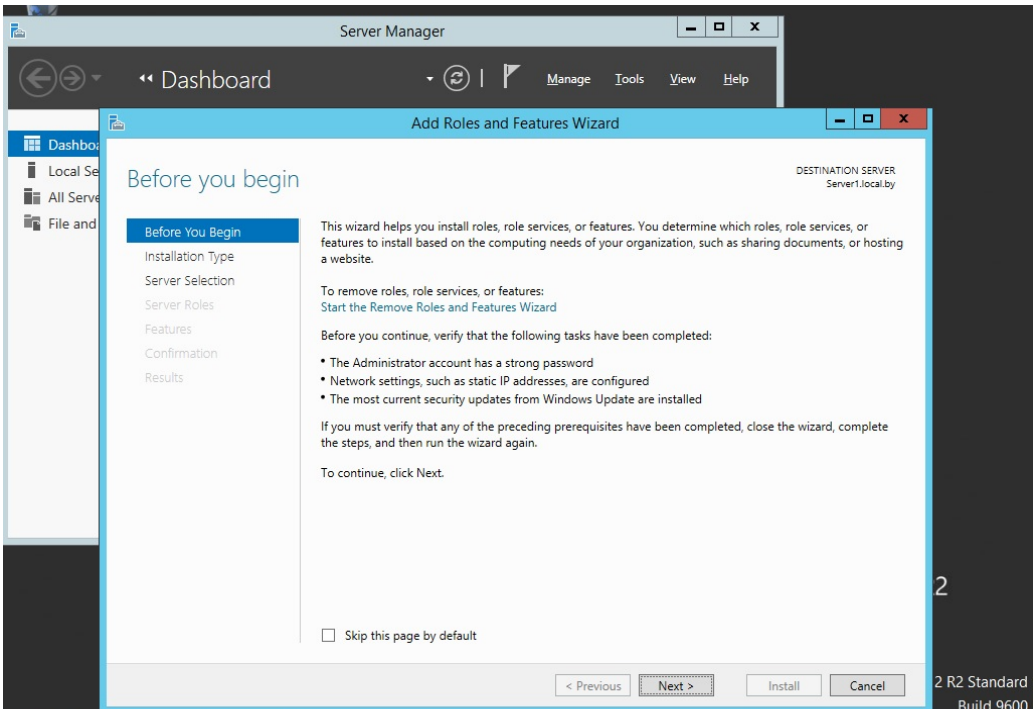

Рис. 1.36. Старт работы мастера установки роли сервера

Далее уже по умолчанию выбран необходимый пункт, т. е. *Role-based or feature-based installation (Установка ролей или компонентов)*, и поэтому жмем *Далее* (рис. 1.37).

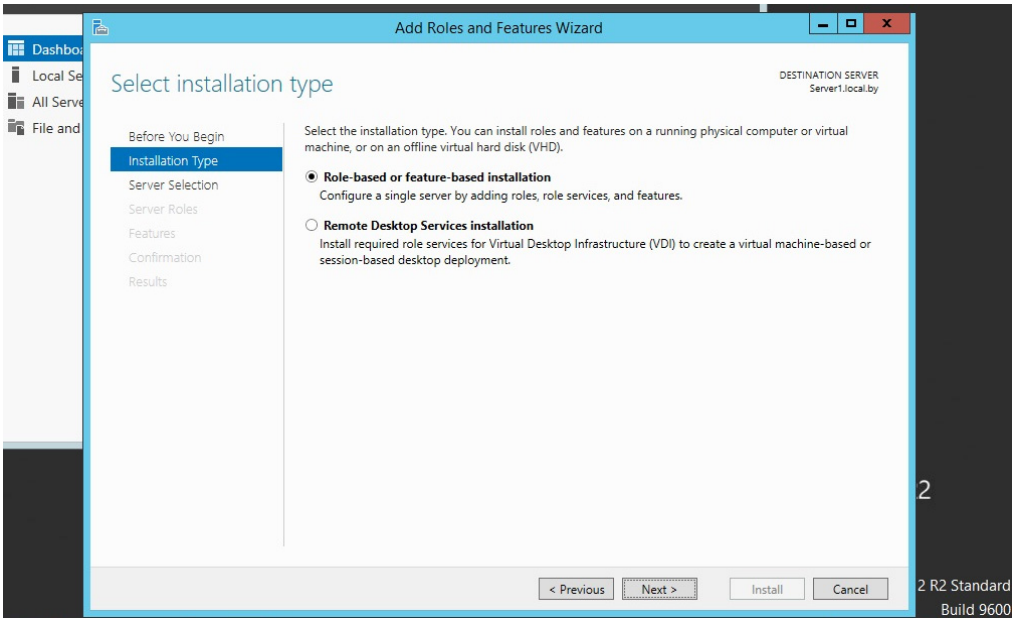

Рис. 1.37. Выбор опции установки ролей и компонент

Затем необходимо выбрать, на какой сервер или виртуальный жесткий диск будет устанавливаться DHCP-сервер (в нашем случае локально, т. е.

этот же самый сервер). Далее необходимо выбрать, какую роль собираемся устанавливать, и соответственно выбираем DHCP-сервер (рис. 1.38).

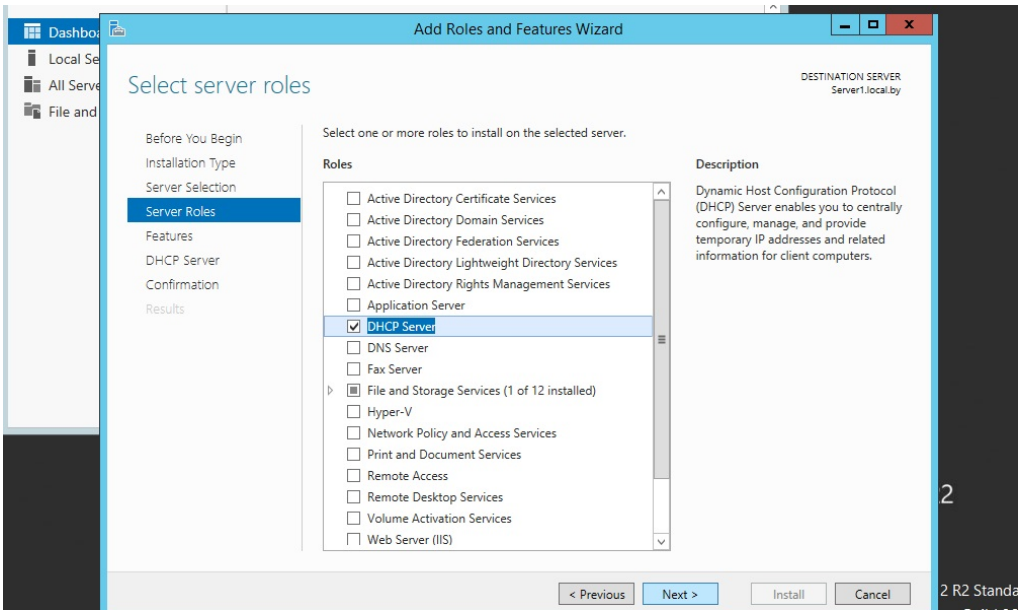

Рис. 1.38. Выбор устанавливаемой роли

После нажатия откроется окно, в котором сразу предложат выбрать для установки средства администрирования DHCP-сервера. Необходимо согласиться, иначе далее все равно придется это выбирать, так как администрировать DHCP будем с данного компьютера, и затем жмем *Add Features (Добавить компоненты)* (рис. 1.39).

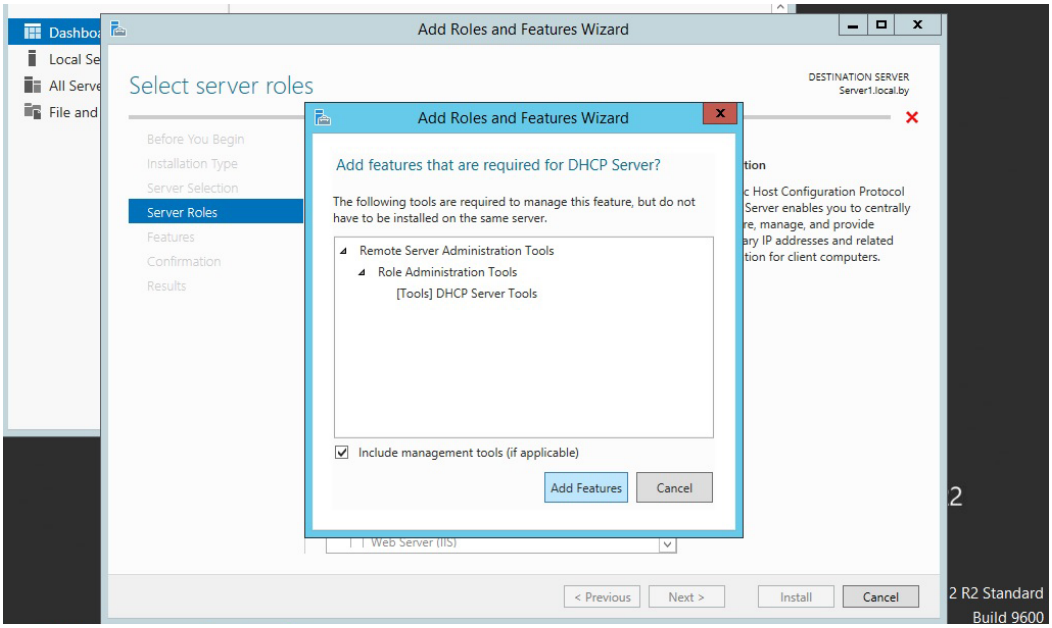

Рис. 1.39. Выбор средств администрирования

Далее будет предложено выбрать необходимые компоненты. Если на прошлом шаге было выбрано *Добавить компоненты*, то необходимые компоненты уже будут выбраны, а соответственно, жмем *Next (Далее)* (рис. 1.40).

Еще на нескольких последующих этапах также жмем *Next (Далее)* и затем начнется установка DHCP-сервера (рис. 1.41).

После завершения установки будет предложено выполнить предварительную настройку. Рассмотрим настройку DHCP-сервера далее отдельно.

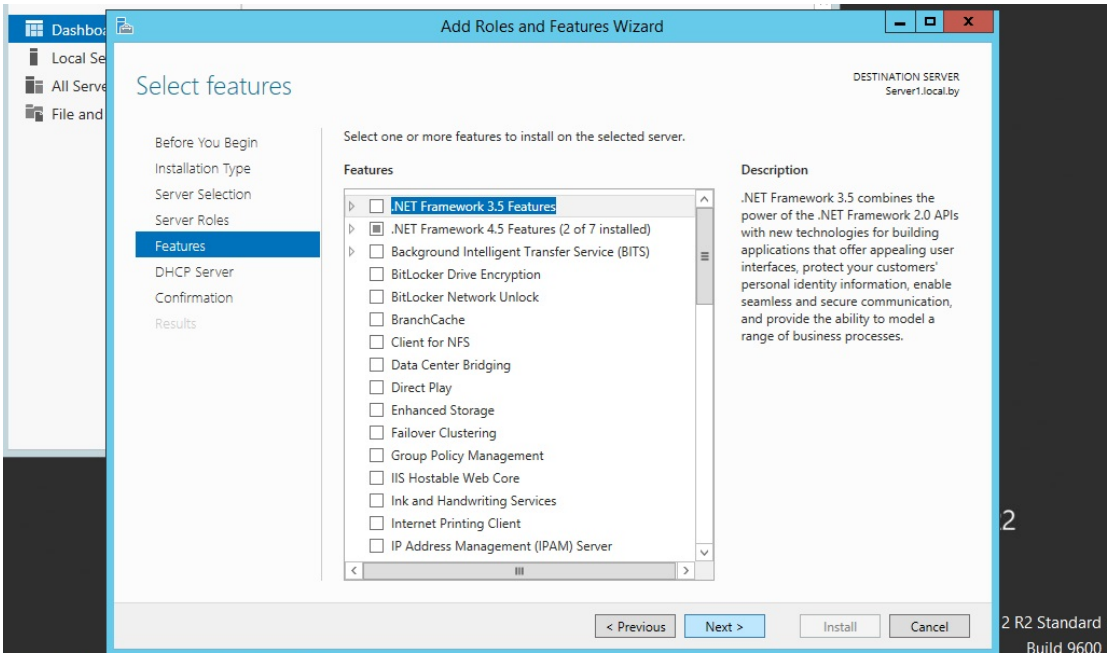

Рис. 1.40. Выбор компонент устанавливаемой роли

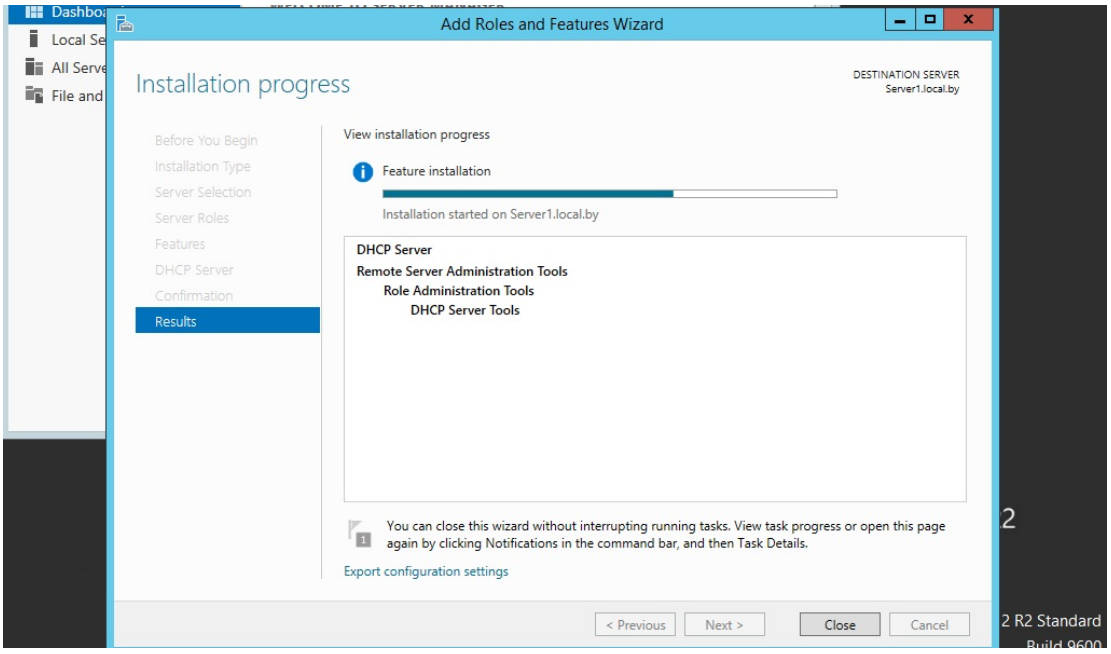

Рис. 1.41. Установка DHCP-сервера

2. Настройка параметров DHCP-сервера

После установки DHCP-сервер и средства его администрирования необходимо настроить. Для этого запускаем оснастку управления DHCP-сервером. Это можно сделать через *Server Manager (Диспетчер серверов)*, меню *Tools (Средства)* (рис. 1.42).

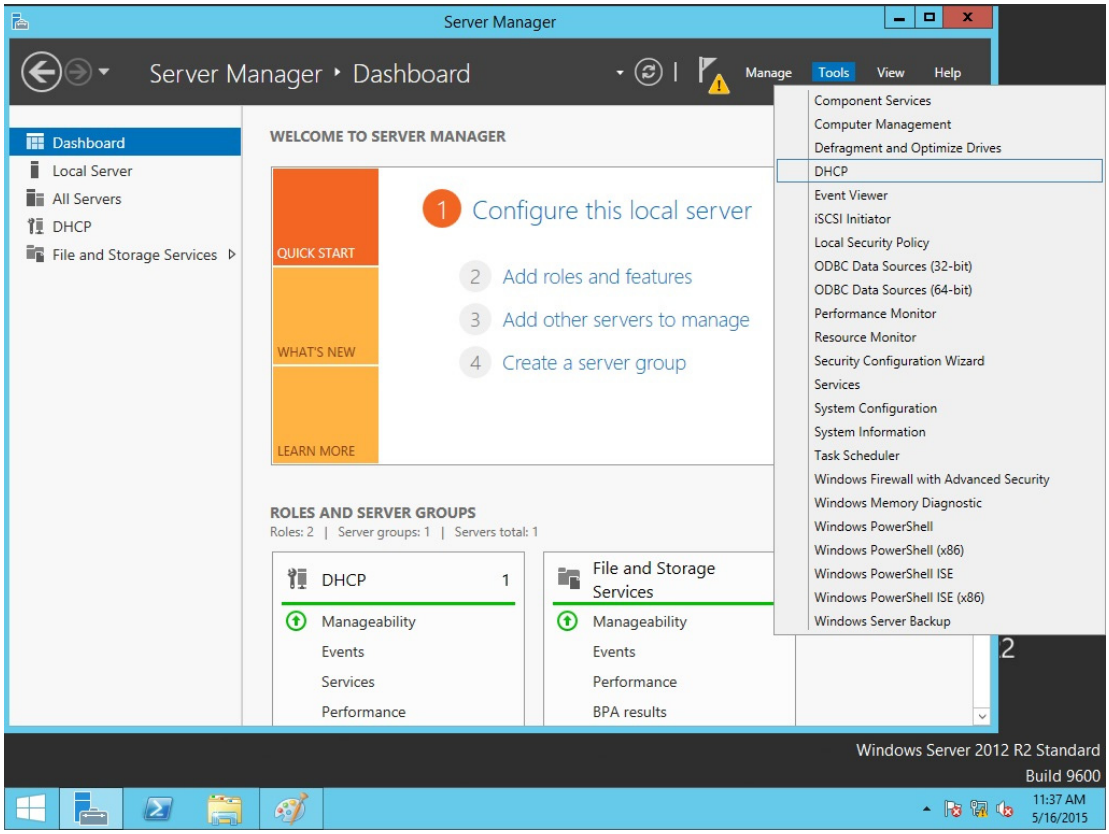

Рис. 1.42. Запуск DHCP-сервера

Создать область можно, щелкнув правой кнопкой мыши на имени сервера и выбрав пункт меню *New Scope (Создать область)* (или аналогичный пункт в меню *Действие* консоли DHCP) (рис. 1.43). Консоль запустит *Мастер создания области*, который позволяет по шагам определить все необходимые параметры.

Имя и описание области. В больших сетях именование областей и задание их краткого описания облегчает работу администратора за счет более наглядного отображения в консоли всех созданных областей (рис. 1.44).

Дальнейший процесс создания и настройки области в Windows Server 2012 практически ничем не отличается от настройки Windows Server 2003, которая была рассмотрена и изучена в курсе «Компьютерные сети». Фактически необходимо определить диапазон IP-адресов и маски подсети (в данном примере используется подсеть с Network ID 192.168.1.0 и маской 24 бита) (рис. 1.45). Отметим, что при настройке каждый должен исполь-

зовать диапазон IP-адресов и другие параметры исходя из выбранного варианта задания.

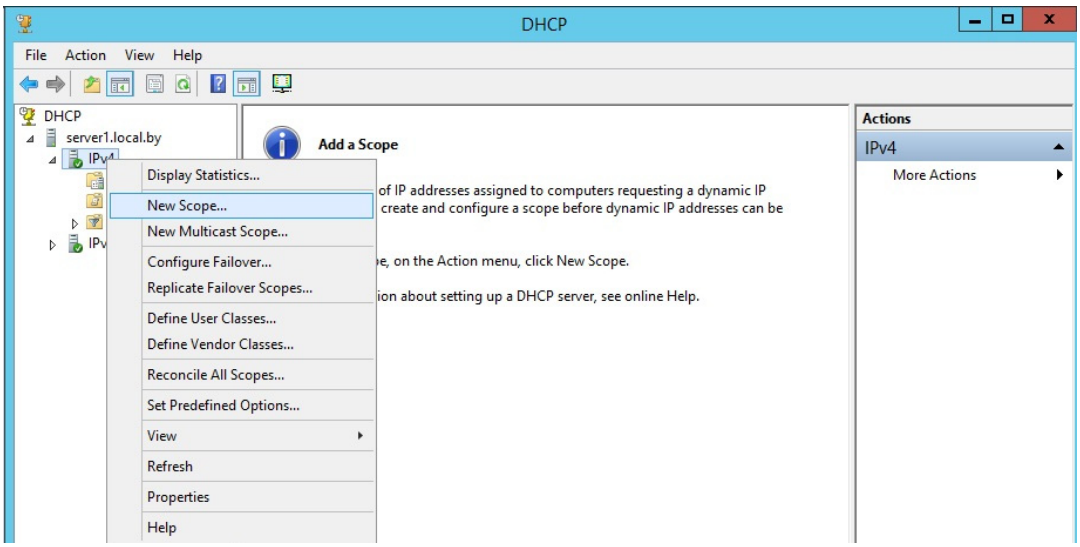

Рис. 1.43. Создание новой области DHCP-сервера

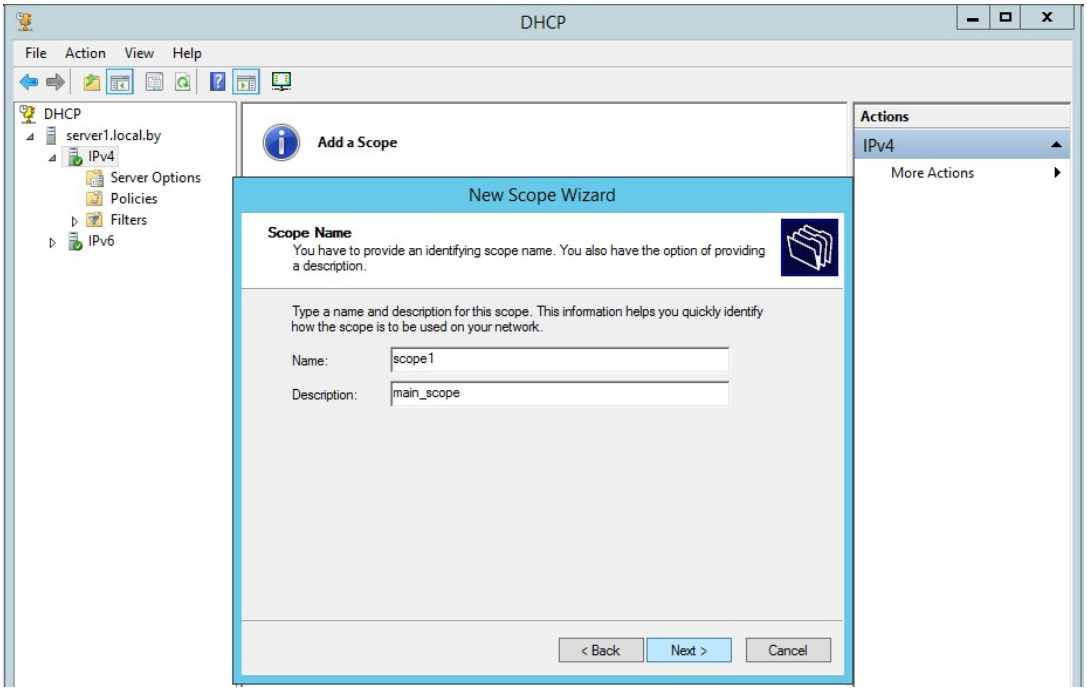

Рис. 1.44. Создание области DHCP-сервера

Добавление исключений. На данном шаге задаются диапазоны IP-адресов, которые будут исключены из процесса выдачи адресов клиентам (все статические IP-адреса должны быть обязательно исключены из действующего диапазона адресов). В рассмотренном на рис. 1.46 примере исключаются адреса обоих серверов: 192.168.100 и 192.168.1.101.

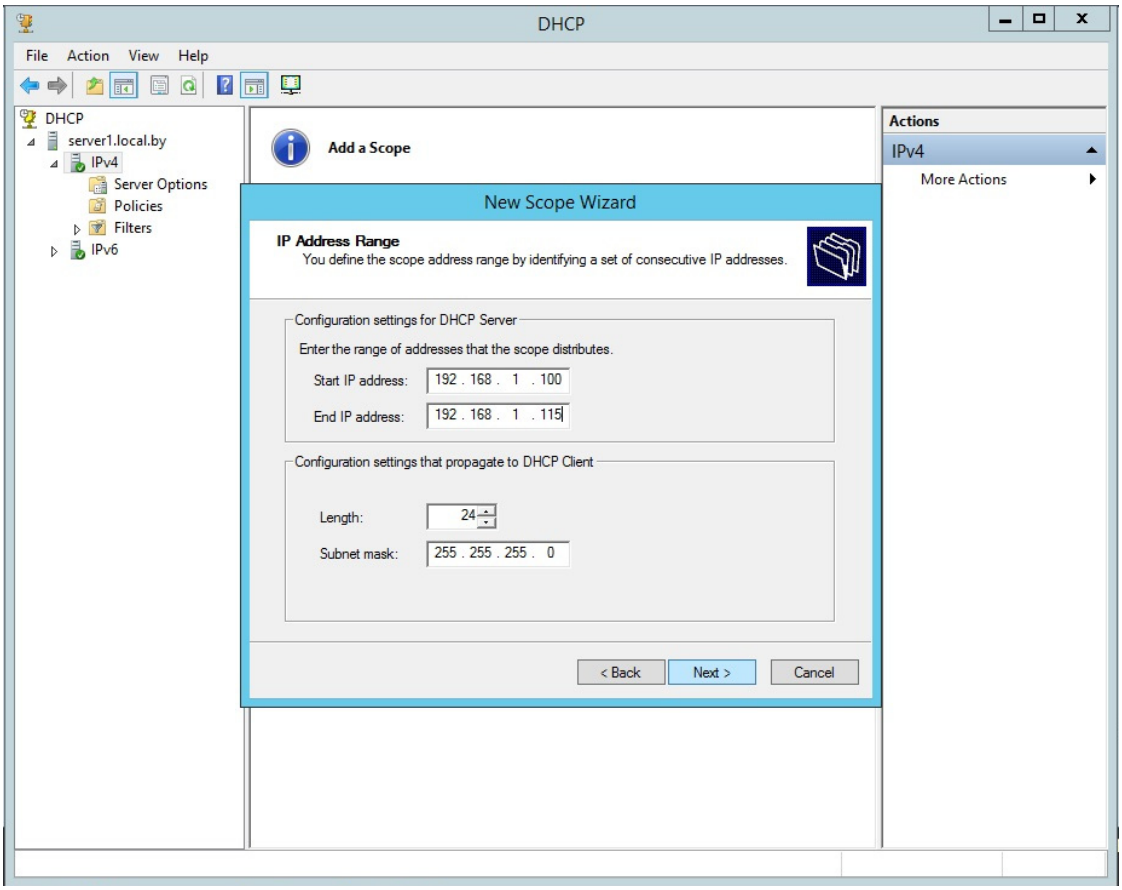

Рис. 1.45. Определение диапазона адресов области

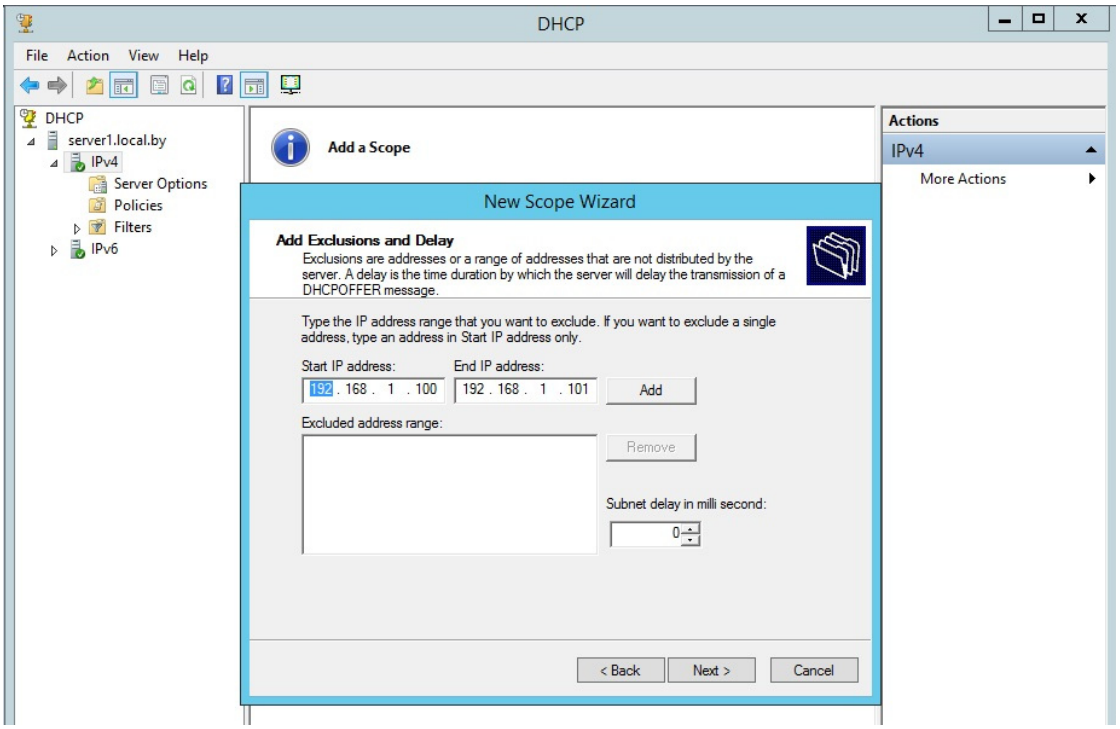

Рис. 1.46. Добавление исключающего диапазона адресов области

Срок действия аренды. Стандартный срок действия – 8 дней (рис. 1.47).

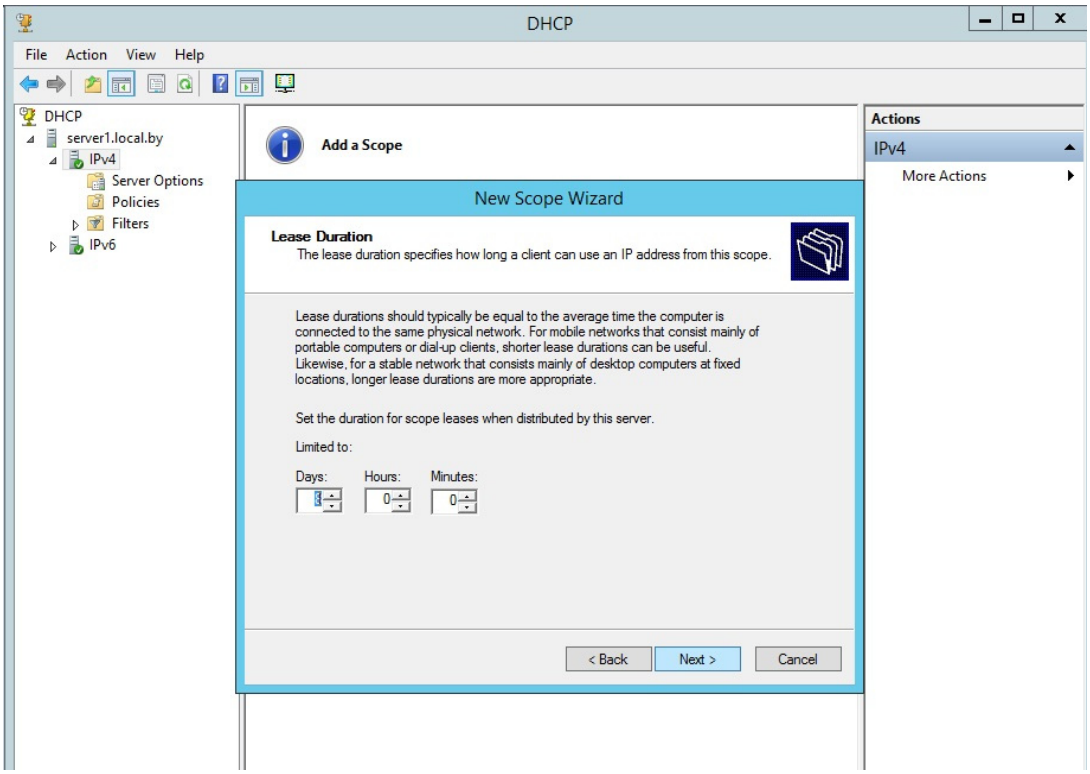

Рис. 1.47. Определение срока аренды клиентом адресов

Если в сети редко происходят изменения (добавление или удаление сетевых узлов, перемещение сетевых узлов из одной подсети в другую), то срок действия можно увеличить, это сократит количество запросов на обновление аренды. Если же сеть более динамичная, то срок аренды можно сократить, это позволит быстрее возвращать в пул IP-адреса, которые принадлежали компьютерам, уже удаленным из данной подсети.

Далее мастер предложит настроить параметры, специфичные для узлов IP-сети, относящихся к данной области, например маршрутизатор (основной шлюз), адрес DNS-сервера (можно назначить несколько адресов, рис. 1.48); адрес WINS-сервера (аналогично серверу DNS; можно также назначить несколько адресов).

Запрос на активацию области. IP-адреса, заданные в созданной области, не будут выдаваться клиентам, пока область не будет активирована (рис. 1.49).

Далее завершаем работу мастера, и область готова к использованию. Если какие-либо параметры (например, адреса серверов DNS или WINS) являются общими для всех областей, управляемых данным DHCP-сервером, то такие параметры лучше определять не в разделе параметров каждой области, а в разделе параметров самого сервера.

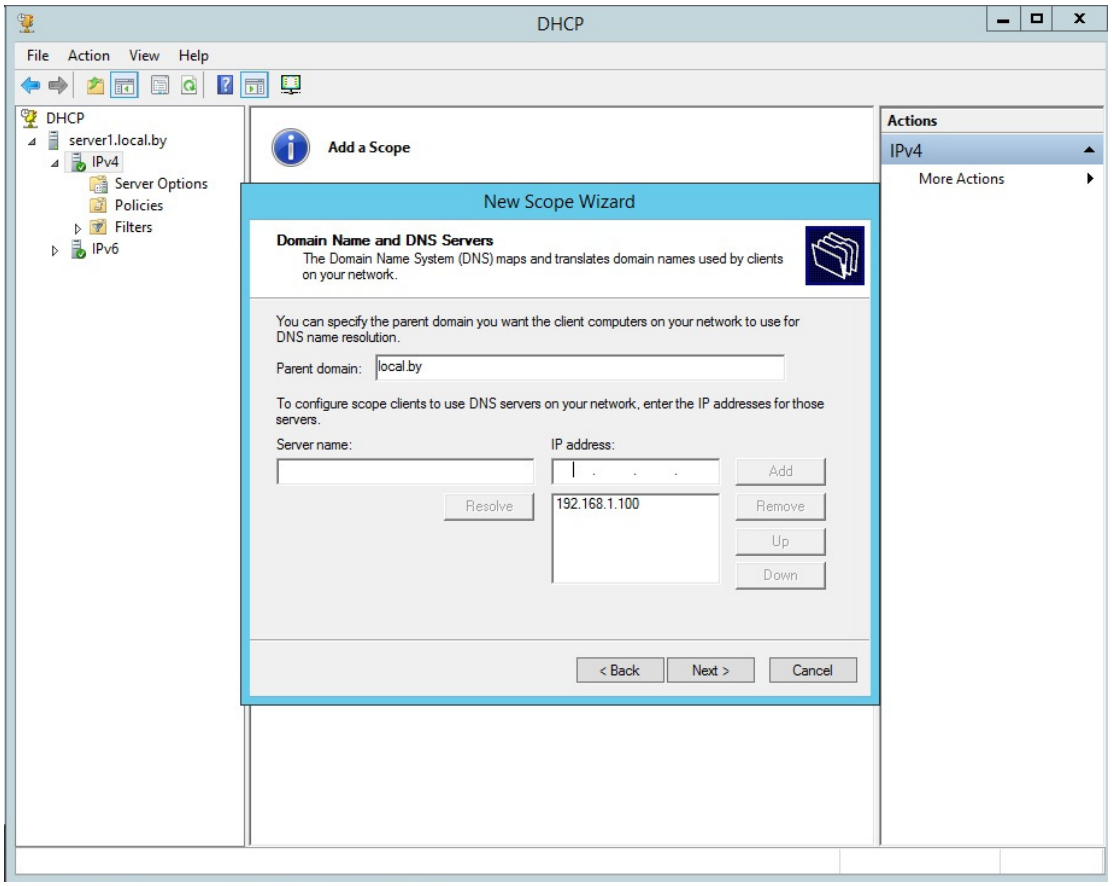

Рис. 1.48. Добавление адреса DNS-сервера, распределяемого областью

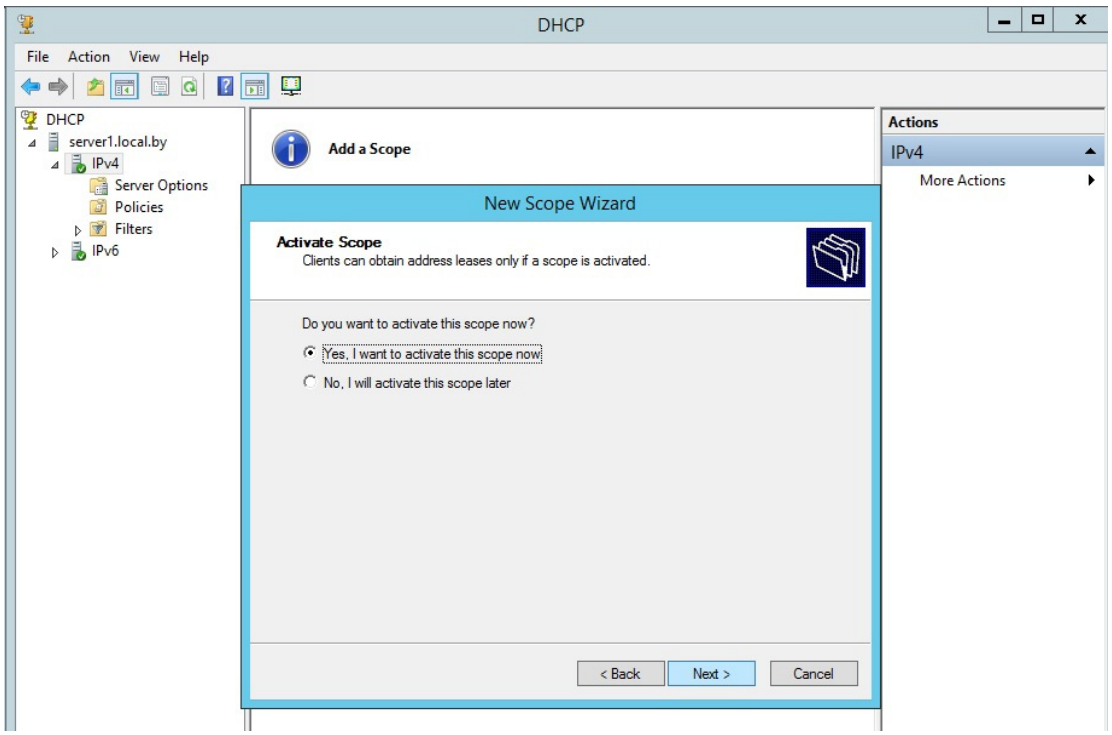

Рис. 1.49. Запрос на активацию области DHCP-сервера

1.2.5. Распределение ресурсов по сети

Распределение ресурсов в сетях TCP/IP при поддержке операционных систем Windows осуществляется в два этапа. Рассмотрим открытие ресурсов в сеть на примере клиентской Windows Seven (в Windows Server 2003, 2008 и 2012 данные операции будут выполняться аналогично).

1. Для того чтобы клиенты в дальнейшем получили доступ к разделяемым ресурсам, на компьютере создаются папки или структура папок каким-либо стандартным способом (используемая файловая система – NTFS). Будем их называть далее сетевыми папками или сетевыми ресурсами. Данные ресурсы открываются в сеть вызовом контекстного меню и выполнением из него команды *Общий доступ и безопасность* (*или Свойства*/*Доступ*) (рис. 1.50).

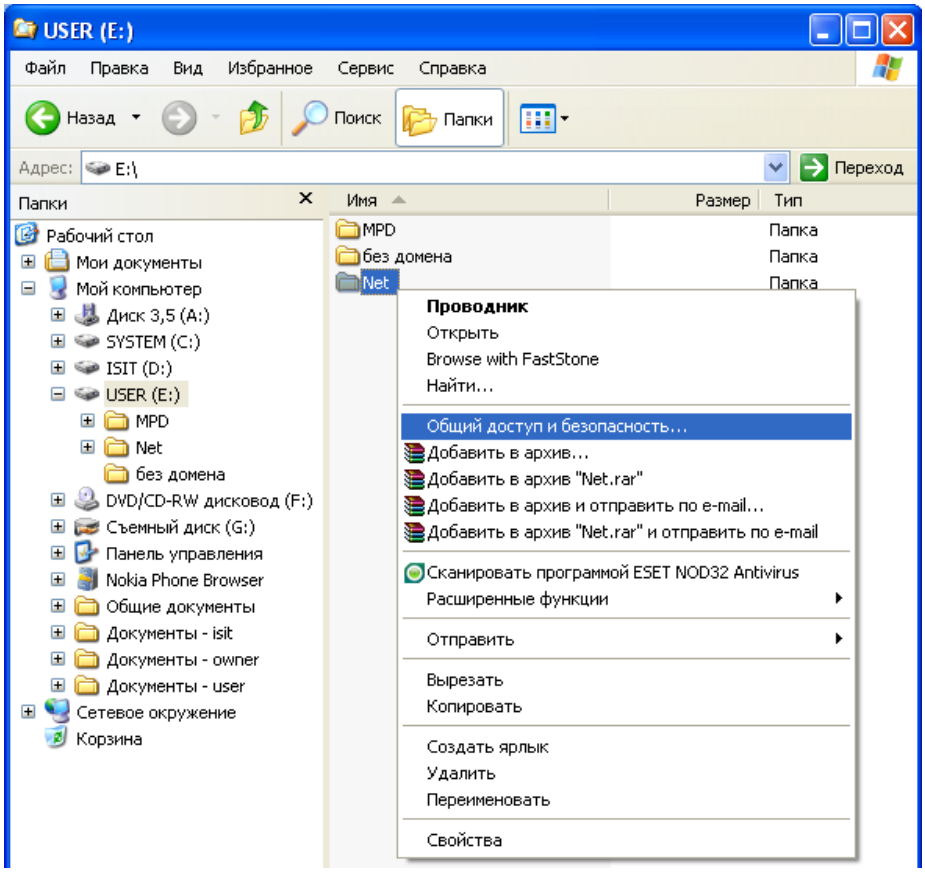

Рис. 1.50. Открытие доступа к папке по сети

В результате появится окно следующего вида (рис. 1.51), в котором необходимо выбрать *Открыть общий доступ к этой папке*. Целесообразно также установить предельное число пользователей, например как показано на рис. 1.51.

Далее для выбора и настройки правил доступа к папке по сети необходимо щелкнуть по кнопке *Разрешения*. Откроется стандартное окно, пока-

занное на рис. 1.52, из которого видно, что папка будет открыта по сети для всех пользователей с правами *Только чтение*. Если необходимо просто предоставить всем пользователям сети просмотр информации, хранящейся в сетевой папке, то данный стандартный вариант можно считать приемлемым.

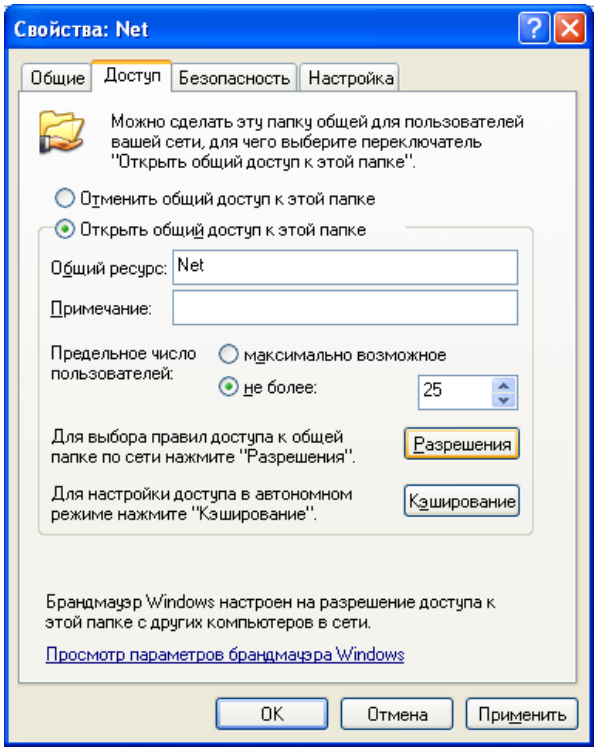

Рис. 1.51.Окно настройки общего доступа

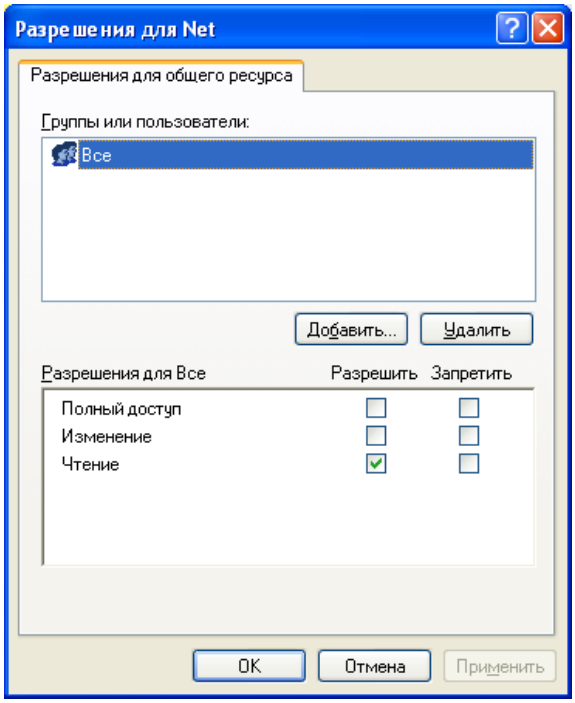

Рис. 1.52. Окно для выбора правил доступа к сетевой папке

Однако чаще всего требуется более тонкая настройка правил общего доступа. Для этого необходимо удалить группу пользователей *Все*, а добавить отдельных пользователей. Так, согласно рис. 1.53, для пользователя *user* предоставлен доступ типа *Чтение*, а для пользователя *user1 – Полный доступ* (рис. 1.54).

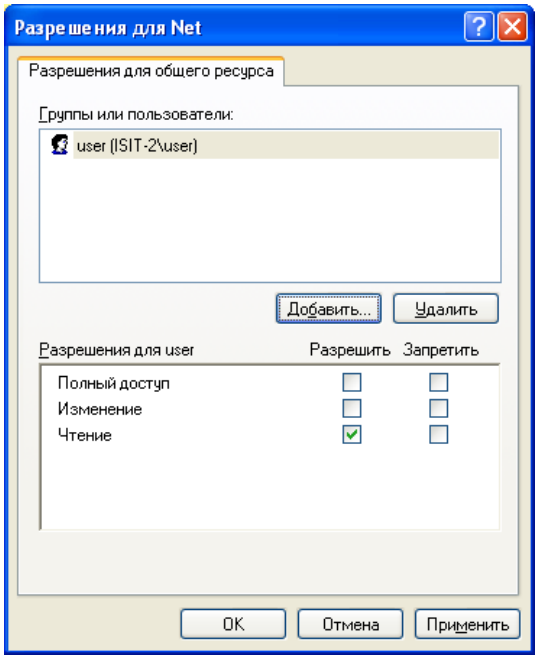

Рис. 1.53. Предоставление ограниченного доступа для пользователя *user*

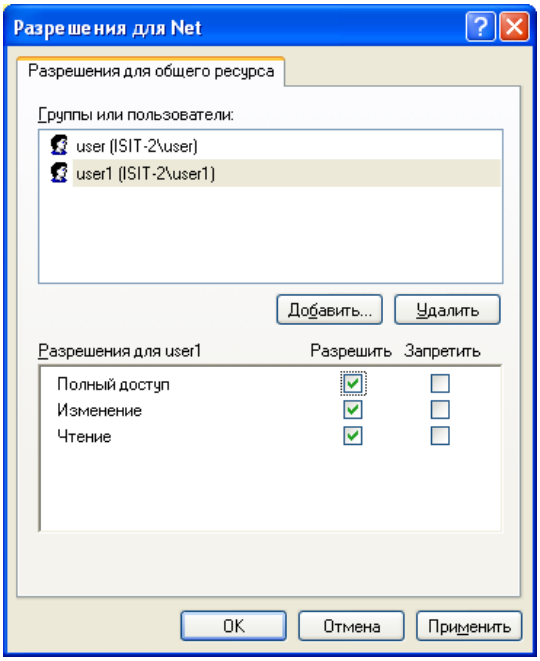

Рис. 1.54. Предоставление полного доступа для пользователя *user1*

Во всех операционных системах Windows существует важное правило: *запрещающие правила всегда имеют более высокий приоритет, чем разрешающие правила*. Из чего следует существенный момент: если на этапе открытия доступа к папке будут использованы запрещающие правила, то их действие на всех последующих этапах настройки сетевого ресурса отменить будет невозможно.

2. Далее перейдем к настройке вкладки *Безопасность*, общий вид которой представлен на рис. 1.55.

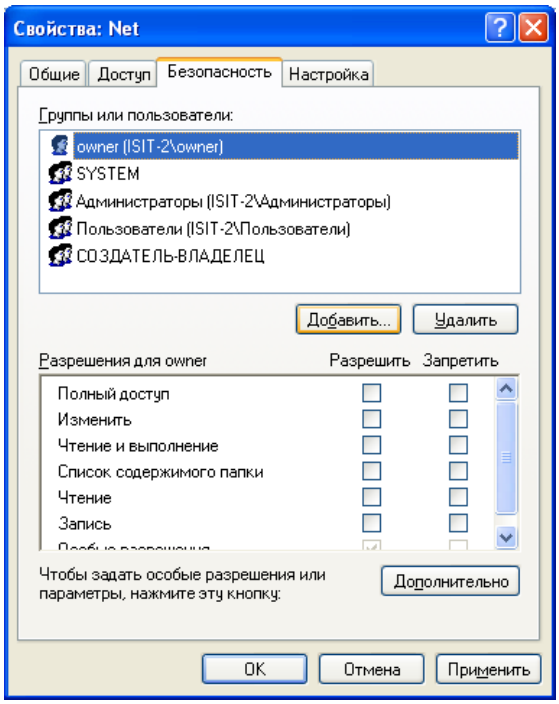

Рис. 1.55. Вид окна для настройки безопасности сетевой папки

Для тонкой настройки безопасности сетевой папки рекомендуется удалить из перечня *групп или пользователей* группу пользователей *Пользователи*. Для этого необходимо сначала отменить в дополнительных параметрах наследование от родительского объекта применимых к дочерним объектам разрешений (рис. 1.56), а лишь затем выполнить операцию удаления группы *Пользователи*.

Далее можно приступать к добавлению отдельных пользователей (согласно рис. 1.57, добавлен пользователь *user1*). Детальную настройку разрешений и запретов для определенного пользователя можно выполнить в окне дополнительных параметров безопасности сетевой папки, щелкнув по кнопке *Изменить* (рис. 1.58).

Просмотреть открытые ресурсы для доступа по сети, а также подключенных к ним пользователей можно, открыв *Управление компьютером* (рис. 1.59) (вызывается при помощи контекстного меню для объекта *Мой*

компьютер с дальнейшим выполнением команды *Управление* или через *Панель управления*).

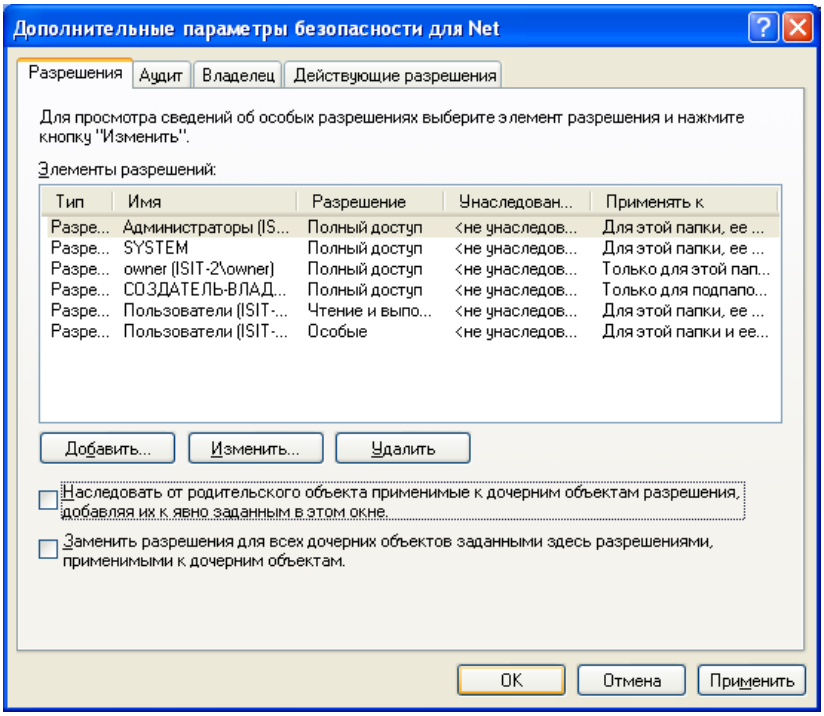

Рис. 1.56. Вид окна для настройки дополнительных параметров безопасности сетевой папки

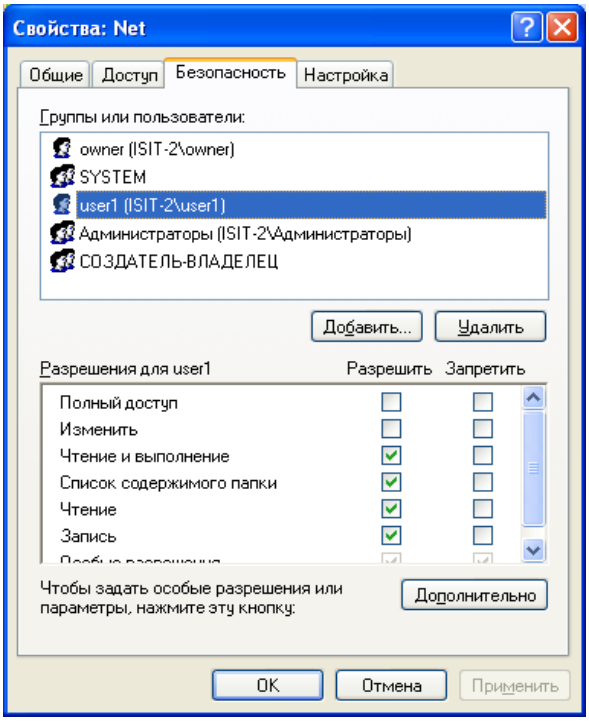

Рис. 1.57. Вид окна для настройки безопасности сетевой папки с добавленным пользователем *user1*

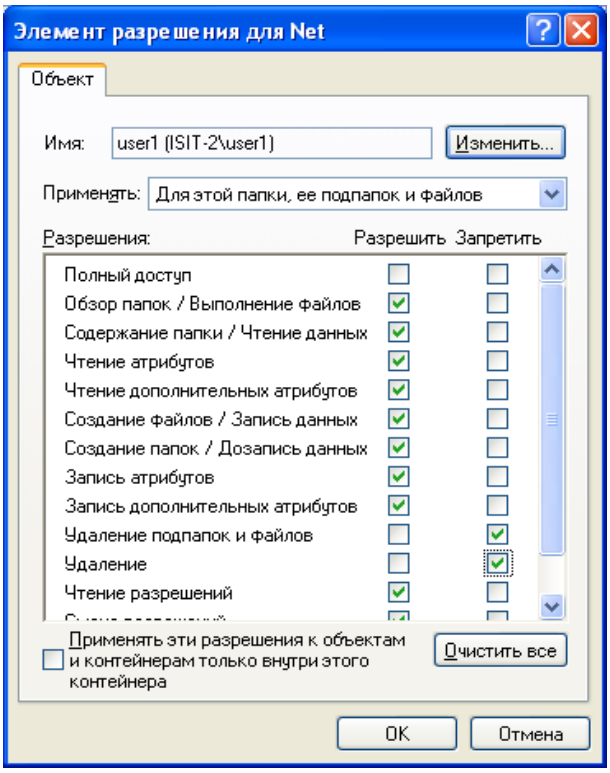

Рис. 1.58. Вид окна для тонкой настройки безопасности сетевой папки

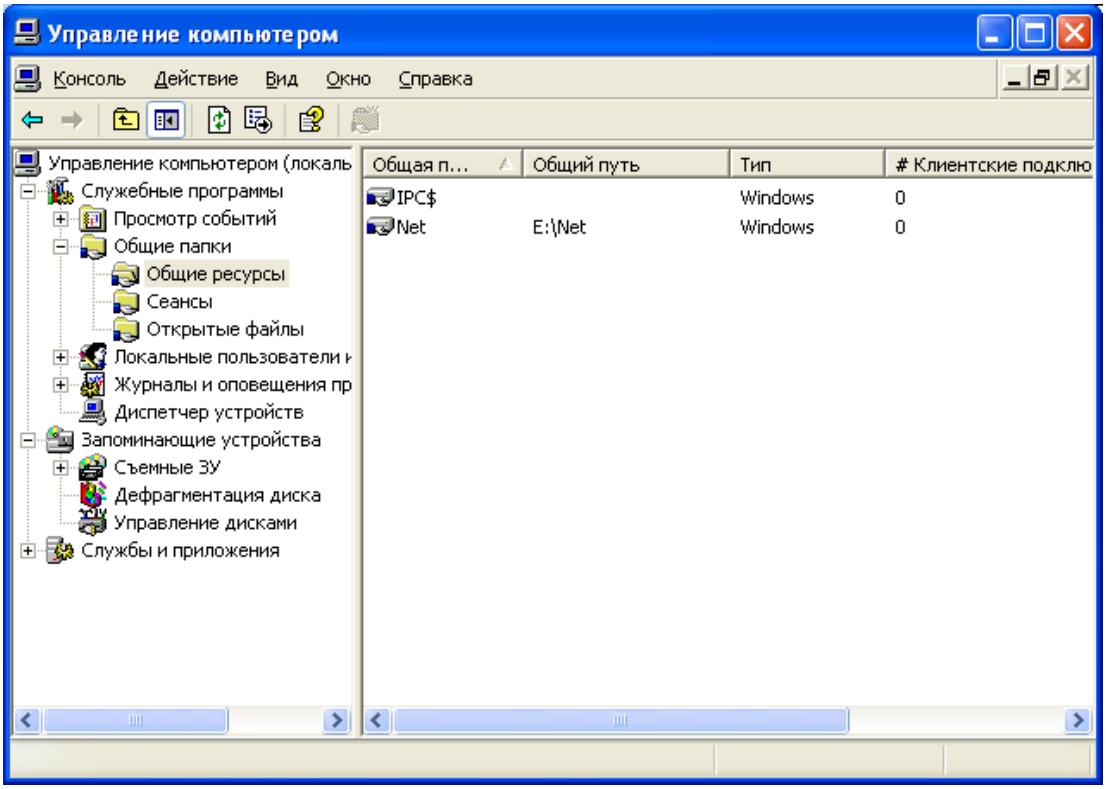

Рис. 1.59. Вид окна консоли *Управление компьютером*

1.3. Утилиты диагностики TCP/IP и DNS

Любая операционная система имеет набор диагностических утилит для тестирования сетевых настроек и функционирования коммуникаций. Большой набор диагностических средств есть и в системах семейства Windows (как графических, так и в режиме командной строки).

Утилиты командной строки, являющиеся инструментами первой необходимости для проверки настроек протокола TCP/IP и работы сетей и коммуникаций, изучались в рамках дисциплины «Компьютерные сети» и подробно рассмотрены с соответствующих пособиях.

Лабораторная работа № 1

Цель: изучение методов установки и первичной настройки операционных систем Windows.

Задание: для выполнения последующих лабораторных работ необходимо установить минимум две операционные системы (в виде виртуальных машин) типа Server (например, Windows Server 2003 R2, Windows Server 2008 R2, Windows Server 2012), а также две клиентские операционные системы типа Windows XP, Windows 7, Windows 8. Отметим, что можно установить одну ОС типа Server, а также одну клиентскую машину и сделать их копии, как описано в подразделе 1.1.

Лабораторная работа № 2–3

Цель: изучение методов организации информационных систем со статической и динамической адресацией на базе операционных систем Windows.

Задание: лабораторная работа представляет собой организацию сети с элементами статической и динамической адресацией между четырьмя ОС. В качестве хостов должны выступать виртуальные операционные системы типа Windows со статически заданными сетевыми адресами для серверов, а также динамически заданными – для клиентских машин согласно варианту (см. табл. 1.2).

Таблица 1.2

Варианты заданий для лабораторной работы № 2–3

Номер варианта	Имя хоста	Scope (Диапазон IP-адресов)	IP-адрес хоста
1	Server1_1	172.16.192.131–172.16.192.150 маска 255.255.240.0	172.16.192.131
	Server1_2		172.16.192.132
	Client1_1		любой из scope
	Client1_2		любой из scope

Окончание табл. 1.2

Номер варианта	Имя хоста	Scope (Диапазон IP-адресов)	IP-адрес хоста
2	Server2_1	172.16.192.151–172.16.192.170 маска 255.255.240.0	172.16.192.151
	Server2_2		172.16.192.170
	Client2_1		любой из scope
	Client2_2		любой из scope
3	Server3_1	172.16.192.171–172.16.192.190 маска 255.255.240.0	172.16.192.175
	Server3_2		172.16.192.176
	Client3_1		любой из scope
	Client3_2		любой из scope
4	Server4_1	172.16.192.191–172.16.192.210 маска 255.255.240.0	172.16.192.191
	Server4_2		172.16.192.192
	Client4_1		любой из scope
	Client4_2		любой из scope
5	Server5_1	172.16.192.211–172.16.192.230 маска 255.255.240.0	172.16.192.229
	Server5_2		172.16.192.230
	Client5_1		любой из scope
	Client5_2		любой из scope
6	Server6_1	172.16.192.231–172.16.192.250 маска 255.255.240.0	172.16.192.241
	Server6_2		172.16.192.249
	Client6_1		любой из scope
	Client6_2		любой из scope

Схема соединения компьютеров в сети представлена на рис. 1.60 (на примере первого варианта).

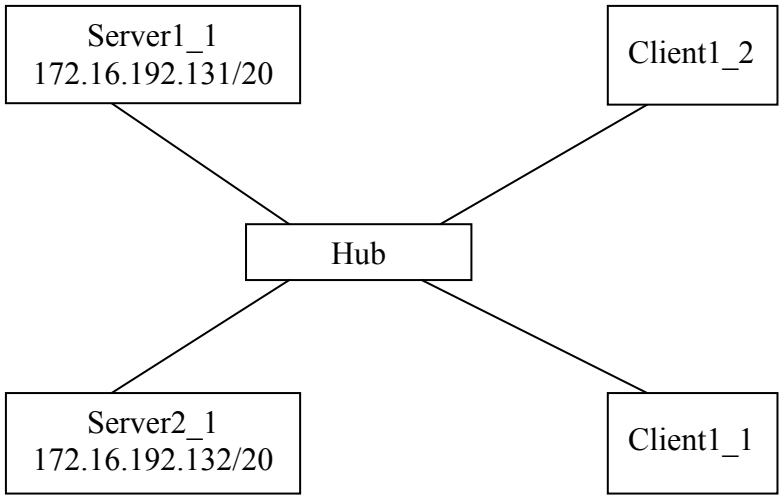

Рис. 1.60. Схема соединения компьютеров в сети

Согласно заданию предполагается, что серверы (Server1_1 и Server1_2) должны быть настроены с резервированием друг друга, при этом каждый из них будет обслуживать определенную часть адресного пространства (scope), т. е. Client1_2 и Client1_1 должны получить IP-адреса от разных DHCP-серверов. Таким образом, имеем следующее:

Для Server1_1

Scope: 172.16.192.131–172.16.192.150, маска 255.255.240.0

Exclusion range: 172.16.192.131–172.16.192.132 (адреса серверов);
172.16.192.143–172.16.192.150 (данный диапазон обслуживается Server1_2, но при выходе его из строя исключение может быть снято).

Оставшаяся часть диапазона IP-адресов (172.16.192.133–172.16.192.142) используется для выдачи клиентским компьютерам. При этом отметим, что это необходимо осуществлять с «жестким привязыванием» выдаваемого IP-адреса к MAC-адресу клиента (т. е. используя так называемую таблицу соответствия MAC и IP-адресов – reservations).

Соответственно для server1_2 получим:

Scope: 172.16.192.131–172.16.192.150, маска 255.255.240.0

Exclusion range: 172.16.192.131–172.16.192.132 (адреса серверов);
172.16.192.133–172.16.192.142 (данный диапазон обслуживается Server1_1, но при выходе его из строя исключение может быть снято).

Отметим, что при использовании Windows Server 2003 и Windows Server 2008 нет каких-либо средств автоматизации резервирования DHCP-серверов, т. е. администратор при возникновении неполадок с одним из серверов принимает решение о снятии исключающего диапазона на втором (рабочем) сервере, чтобы выдавать адреса из всего адресного пространства. При использовании Windows Server 2012 такая возможность уже появилась.

Результаты всей системы в целом можно продемонстрировать, используя утилиты *ping* и *ipconfig*.

СИМВОЛЬНАЯ АДРЕСАЦИЯ В КОМПЬЮТЕРНЫХ СЕТЯХ

2.1. Символьный адрес DNS

В стеке протоколов TCP/IP, как уже ранее говорилось, используются три типа адресов – физические, IP-адреса и символьные доменные имена. Физические адреса служат для адресации на канальном уровне. IP-адреса применяются на сетевом уровне. Доменные имена кажутся в этом ряду необязательными, ведь сеть будет работать и без них. Однако пользователю сети неудобно запоминать числовые IP-адреса, ассоциируя их с конкретными сетевыми объектами. Все привыкли к символьным именам, и именно поэтому в стек TCP/IP была введена система доменных имен DNS (Domain Name System). Она описывается в RFC 1034 и RFC 1035. Полное название доменных имен – FQDN (Fully Qualified Domain Name – полностью определенное имя домена). Кроме DNS-имен операционные системы Windows Server поддерживают символьные имена NetBIOS.

DNS (*Domain Name System*) – это распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Internet.

Служба DNS предназначена для автоматического поиска IP-адреса по известному символьному имени узла. DNS требует статической конфигурации своих таблиц, разрешающих имена компьютеров в IP-адреса.

Протокол DNS является служебным протоколом прикладного уровня. Этот протокол несимметричен – в нем определены DNS-серверы и DNS-клиенты.

DNS-серверы хранят часть распределенной базы данных о соответствии символьных имен и IP-адресов. Эта база данных распределена по административным доменам сети Internet. Клиенты сервера DNS знают IP-адрес сервера DNS своего административного домена и по протоколу IP передают запрос, в котором сообщают известное символьное имя и просят вернуть соответствующий ему IP-адрес. Если данные о запрошенном соответствии хранятся в базе данного DNS-сервера, то он сразу посылает ответ клиенту, если же нет – то он посылает запрос DNS-серверу другого домена, который может сам обработать запрос либо передать его другому DNS-серверу. Все DNS-серверы соединены иерархически в соответствии с иерархией доменов сети Internet. Клиент опрашивает эти серверы имен, пока не найдет нужные отображения. Этот процесс ускоряется

из-за того, что серверы имен постоянно кэшируют информацию, предоставляемую по запросам. Клиентские компьютеры могут использовать в своей работе IP-адреса нескольких DNS-серверов для повышения надежности своей работы.

База данных DNS имеет структуру дерева, называемого *доменным пространством имен*, в котором каждый домен (узел дерева) имеет имя и может содержать поддомены.

Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, причем точки в имени отделяют части, соответствующие узлам домена.

Корень базы данных DNS управляется центром Internet Network Information Center. Домены верхнего уровня назначаются для каждой страны, а также на организационной основе. Имена этих доменов должны отвечать международному стандарту ISO 3166. Для обозначения стран используются трехбуквенные и двухбуквенные аббревиатуры, а для различных типов организаций применяются следующие аббревиатуры:

– *com* – коммерческие организации (например, microsoft.com);

– *edu* – образовательные (например, mit.edu);

– *gov* – правительственные организации (например, nsf.gov);

– *org* – некоммерческие организации (например, fidonet.org);

– *net* – организации, поддерживающие сети (например, nsf.net).

Каждый домен DNS администрируется отдельной организацией, которая обычно разбивает свой *домен* на *поддомены* и передает функции администрирования этих поддоменов другим организациям. Каждый домен имеет уникальное имя, а каждый из поддоменов имеет уникальное имя внутри своего домена. Имя домена может содержать до 63 символов. Каждый хост в сети Internet однозначно определяется своим полным доменным именем (Fully Qualified Domain Name, FQDN), которое включает имена всех доменов по направлению от хоста к корню.

В процессе разрешения участвуют DNS-клиент и DNS-сервер. Системный компонент DNS-клиента, называемый DNS-распознавателем, отправляет запросы на DNS-серверы. Бывает двух видов:

− интерактивный – DNS-сервер обращается к DNS-серверу с просьбой разрешить имя без обращения к другим DNS-серверам;

− рекурсивный – всю работу по разрешению имени выполняет DNS-сервер путем отправки запросов другим DNS-серверам. DNS-сервер всегда сначала ищет имя в собственной базе данных или в кэше, а в случае отсутствия обращается к другим серверам.

В основном DNS-клиентами используются рекурсивные запросы. На рис. 2.1 проиллюстрирован процесс разрешения доменного имени с помощью рекурсивного запроса.

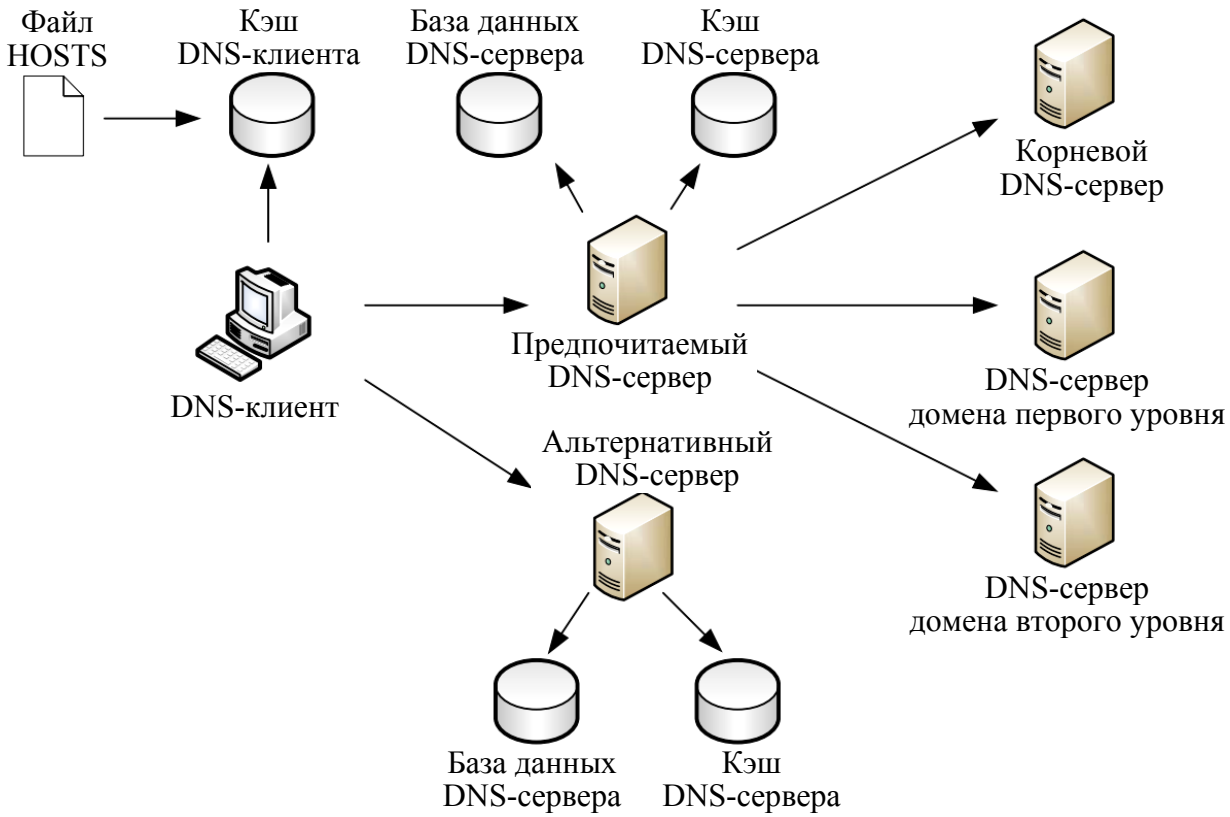

Рис. 2.1. Процесс рекурсивного разрешения имен

Сначала DNS-клиент осуществляет поиск в собственном локальном кэше DNS-имен. Это память для временного хранения ранее разрешенных запросов. В эту же память переносится содержимое файла hosts (каталог windows/system32/drivers/etc). Утилита IPconfig с ключом /displaydns отображает содержимое DNS-кэша. Если кэш не содержит требуемой информации, DNS-клиент обращается с рекурсивным запросом к предпочитаемому DNS-серверу (Preferred DNS server), адрес которого указывается при настройке стека TCP/IP. DNS-сервер просматривает собственную базу данных, а также кэш-память, в которой хранятся ответы на предыдущие запросы, отсутствующие в базе данных. В том случае, если запрашиваемое доменное имя не найдено, DNS-сервер осуществляет итеративные запросы к DNS-серверам верхних уровней, начиная с корневого DNS-сервера.

Рассмотрим процесс разрешения доменного имени на примере. Пусть требуется разрешить имя www.microsoft.com. Корневой домен содержит информацию о DNS-сервере, содержащем зону .com. Следующий запрос происходит к этому серверу, на котором хранятся данные о всех поддоменах зоны .com, в том числе о домене microsoft и его DNS-сервере. Сервер зоны microsoft.com может непосредственно разрешить имя www.microsoft.com в IP-адрес. Обращение к альтернативному серверу происходит, только если основной сервер недоступен.

Просмотр DNS-кэша осуществляется утилитой *ipconfig /displaydns*, очистка кэша – *ipconfig /flushdns*.

2.2. Символьный адрес NETBIOS

Протокол *NetBIOS* (Network Basic Input/Output System – сетевая базовая система ввода/вывода) был разработан в 1984 г. для корпорации IBM как сетевое дополнение стандартной BIOS на компьютерах IBM PC. В операционных системах Microsoft Windows NT, а также в Windows 98 протокол и имена NetBIOS являлись основными сетевыми компонентами. Начиная с Windows 2000, операционные системы Microsoft ориентируются на глобальную сеть Интернет, в этой связи фундаментом сетевых решений стали протоколы TCP/IP и доменные имена. Однако поддержка имен NetBIOS осталась и в операционной системе Windows Server 2008, а также Windows Server 2012.

Система имен NetBIOS представляет собой простое неиерархическое пространство, т. е. в имени NetBIOS отсутствует структура, деление на уровни, как в DNS-именах. Длина имени не более 15 символов (плюс один служебный).

Для преобразования NetBIOS-имен в IP-адреса в операционной системе Windows Server используется служба *WINS* – Windows Internet Naming Service (служба имен в Интернете для Windows).

Служба WINS работает, как и служба DNS, по модели клиент – сервер. WINS-клиенты используют WINS-сервер для регистрации своего NetBIOS-имени и преобразования неизвестного NetBIOS-имени в IP-адрес. Функции сервера NetBIOS-имен описаны в RFC 1001 и 1002.

Процесс разрешения имен в пространстве NetBios может быть выполнен одним из трех способов:

1) широковещательный запрос;

2) обращение к локальной базе данных NetBios-имен (LMhosts), хранящихся в папке, где и файл hosts, отображающий FQDN-имена;

3) обращение к централизованной базе данных имен NetBios, хранящихся на сервере WINS.

В зависимости от типа узла NetBios разрешение имен осуществляется с помощью различных комбинаций перечисленных способов. Выделяют четыре типа узла:

– b-узел (broadcast node, широковещательный) – разрешает имена в IP-адресах посредством широковещательных сообщений broadcast node;

– p-узел (peer node) – разрешает имена в IP-адреса с помощью WINS-сервера;

– m-узел (mixed node, смешанный узел) – комбинирует запросы b- и p-узлов, первоначально узел пытается применить широковещательный запрос, а в случае неудачи – обращается к WINS-серверу;

– h-узел (hybrid node, гибридный) – комбинирует запросы b- и p-узлов, но при этом сначала обращается к WINS-серверу, а при неудаче выполняет широковещательную рассылку.

Наиболее эффективным является h-узел. Тип узла определяется следующим образом: если в свойствах протокола TCP/IP нет адреса WINS-сервера, то данный компьютер считается b-узлом, в противном случае является h-узлом. Использование других типов узлов настраивается через реестр Windows.

В больших сетях для распределения нагрузки по регистрации и разрешению NetBios-имен необходимо использовать несколько WINS-серверов. Считается, что один WINS-сервер должен обслуживать порядка нескольких сотен компьютеров. При использовании нескольких серверов часть клиентов настраивается на регистрацию и разрешение имен на один WINS-сервер, вторая – на другой, а между серверами, по аналогии с системой DNS, настраивается репликация.

2.3. Настройка DNS-сервера

Рассмотрим организацию DNS-адресации в локальной сети на примере Windows Server 2012 R2. Для организации DNS-адресации необходимо выполнить определенные действия на двух серверах (с именами Server1 и Server2) и клиенте.

1. Установка DNS-сервера

Установка службы DNS производится в целом аналогично установке DHCP-сервера, описанной ранее в пункте 1.2.4, с той лишь разницей, что выбирается установка службы DNS.

2. Создание основной зоны прямого просмотра

На сервере DC1 создадим стандартную основную зону с именем world.ru:

– откройте консоль DNS (рис. 2.2);

– выберите раздел *Forward Lookup Zones (Зоны прямого просмотра)* и запустите мастер создания зоны (тип зоны – *Primary (Основная)*, динамические обновления – *разрешить*, остальные параметры – по умолчанию) (рис. 2.3);

– введите тип зоны и имя – в примере используется название local.by (рис. 2.4 и 2.5); имя файла, хранящего информацию о зоне, сформируется автоматически (рис. 2.6);

– разрешите передачу данной зоны на любой сервер DNS (*консоль DNS* – зона local.by – *Properties (Свойства)* – закладка *Zone Transfers (Передачи зон)* – Отметьте *Allow zone transfers (Разрешить передачи)* и *To any server (На любой сервер)*) (рис. 2.7);

– в итоге получим зону прямого просмотра DNS-сервера, как показано на рис. 2.8.

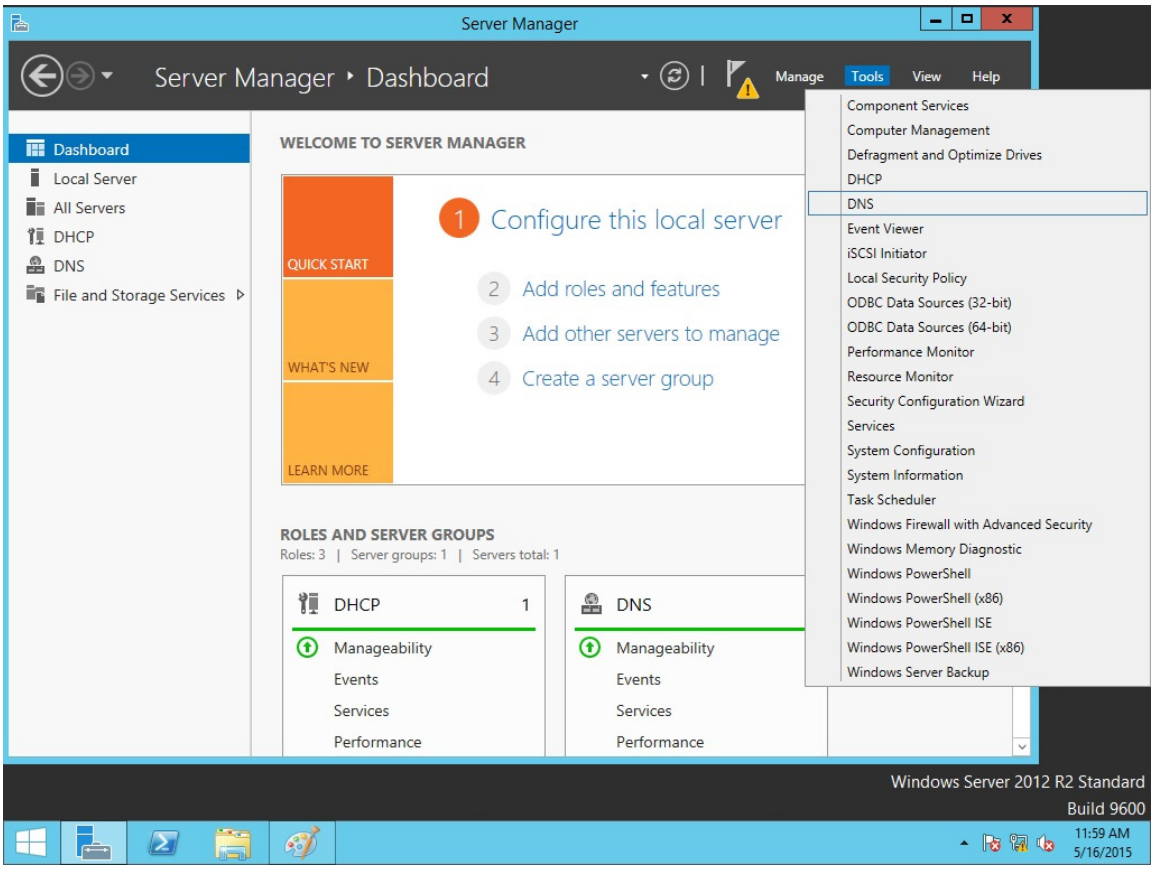

Рис. 2.2. Открытие консоли DNS-сервера

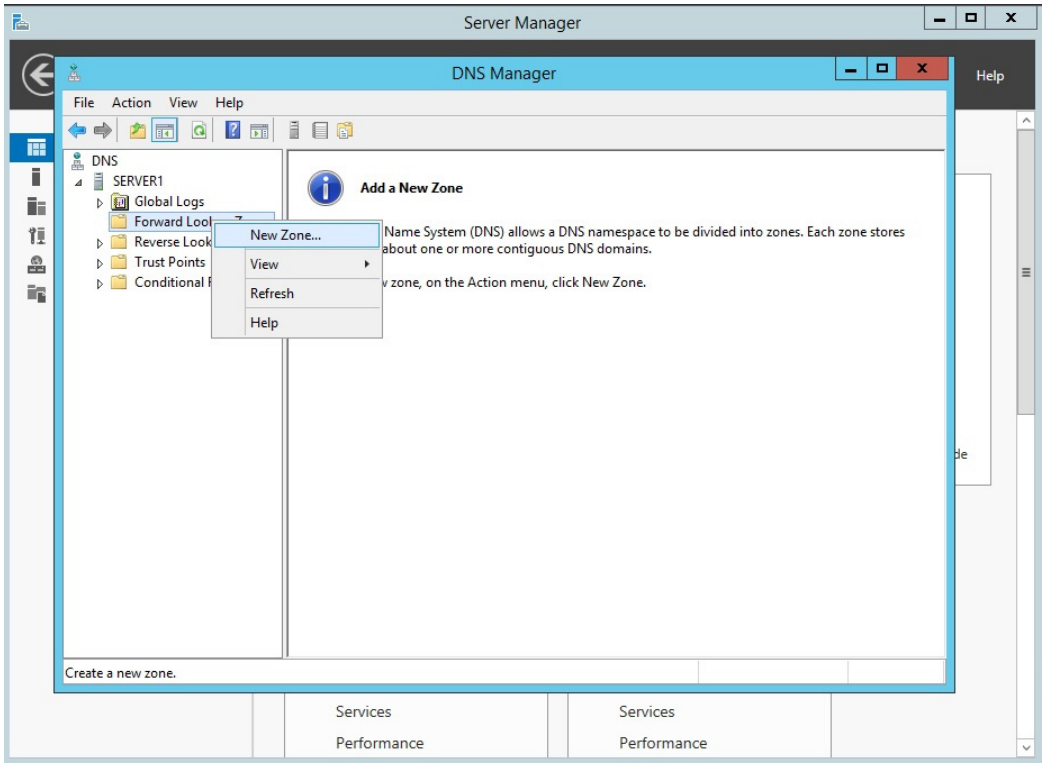

Рис. 2.3. Запуск мастера для создания новой зоны DNS-сервера

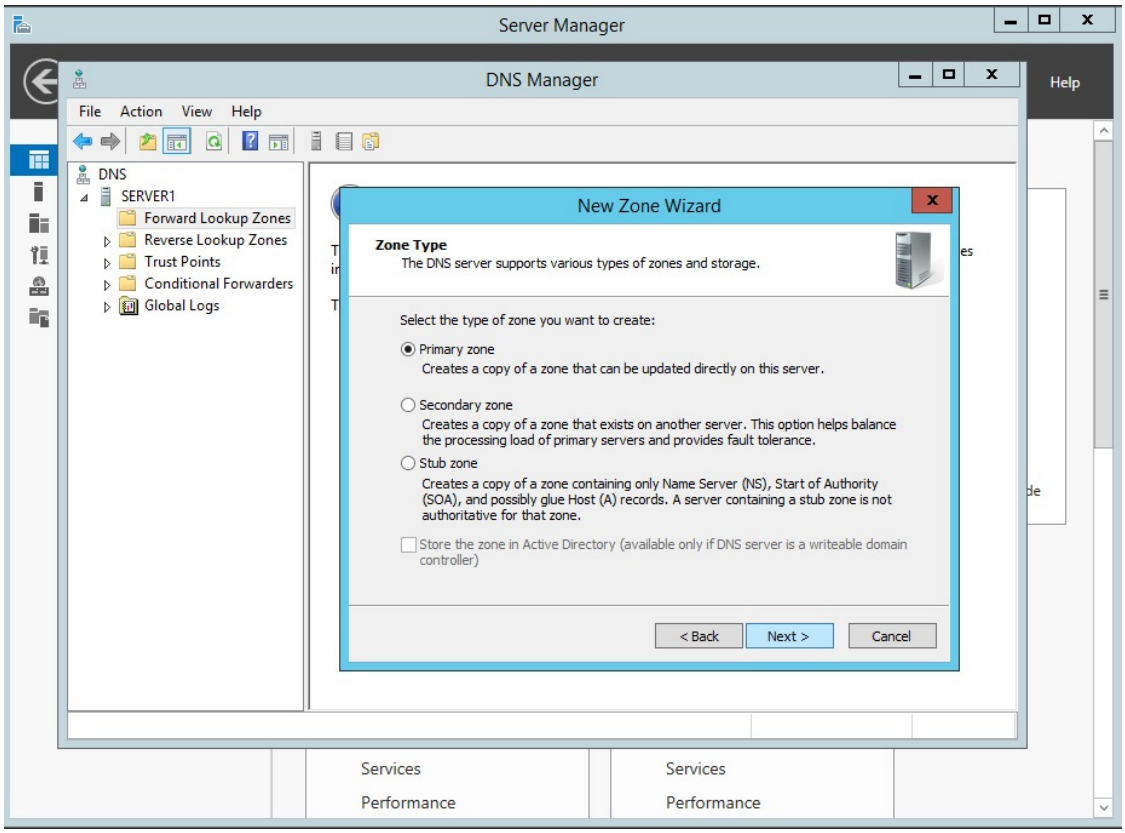

Рис. 2.4. Выбор типа новой зоны DNS-сервера

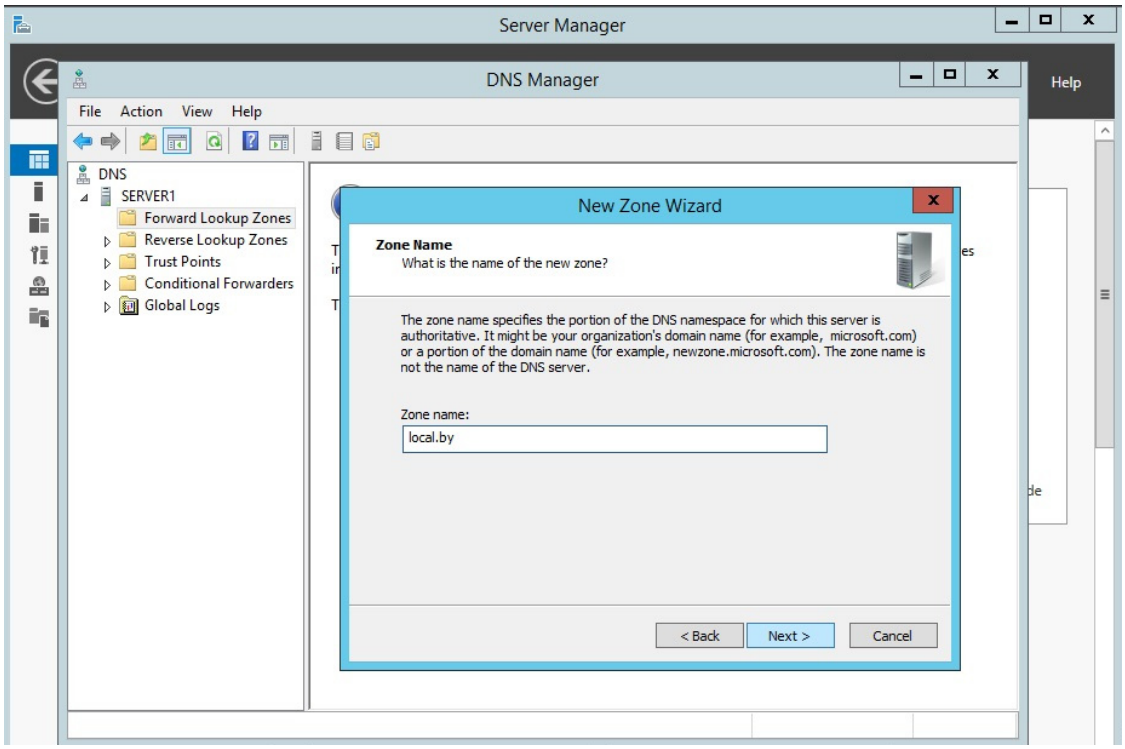

Рис. 2.5. Выбор названия новой зоны DNS-сервера

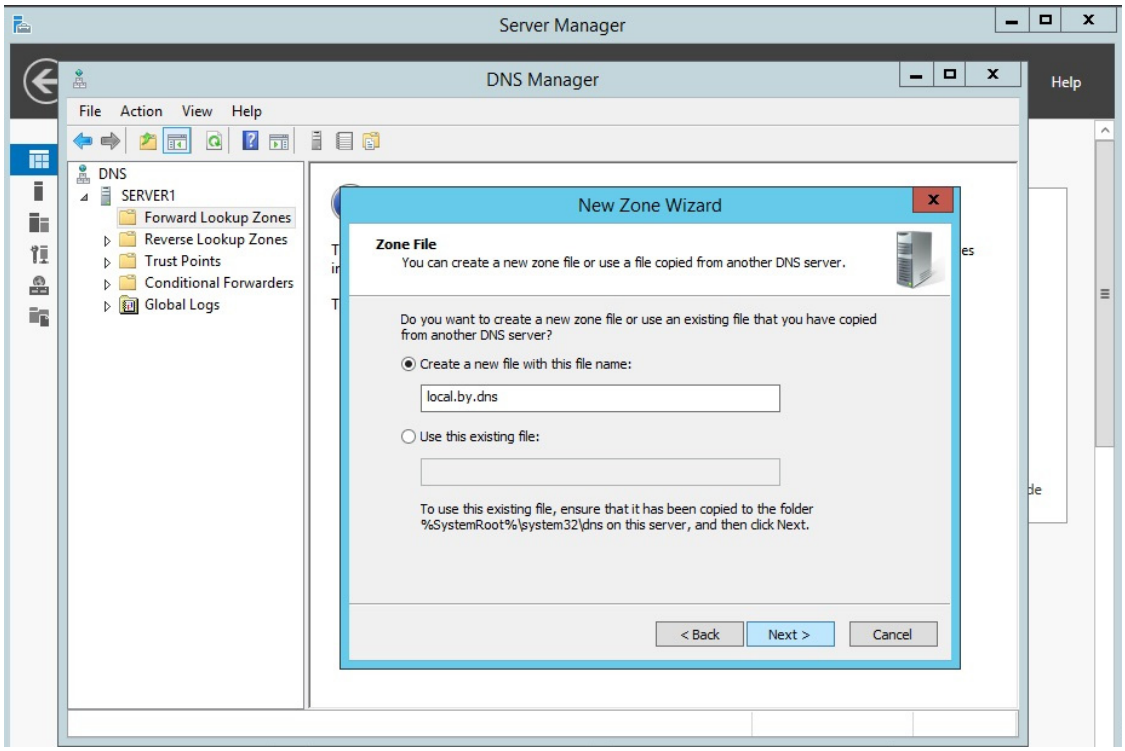

Рис. 2.6. Название файла новой зоны DNS-сервера

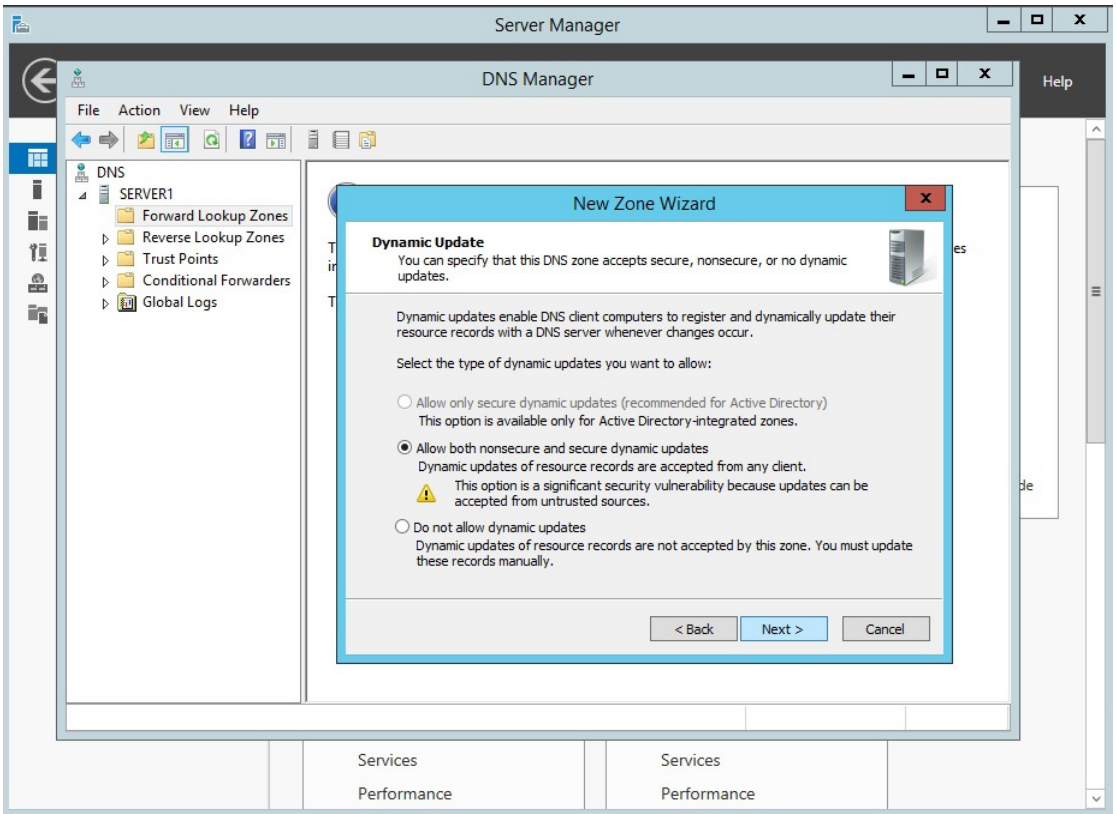

Рис. 2.7. Разрешение на передачу зоны на другой сервер

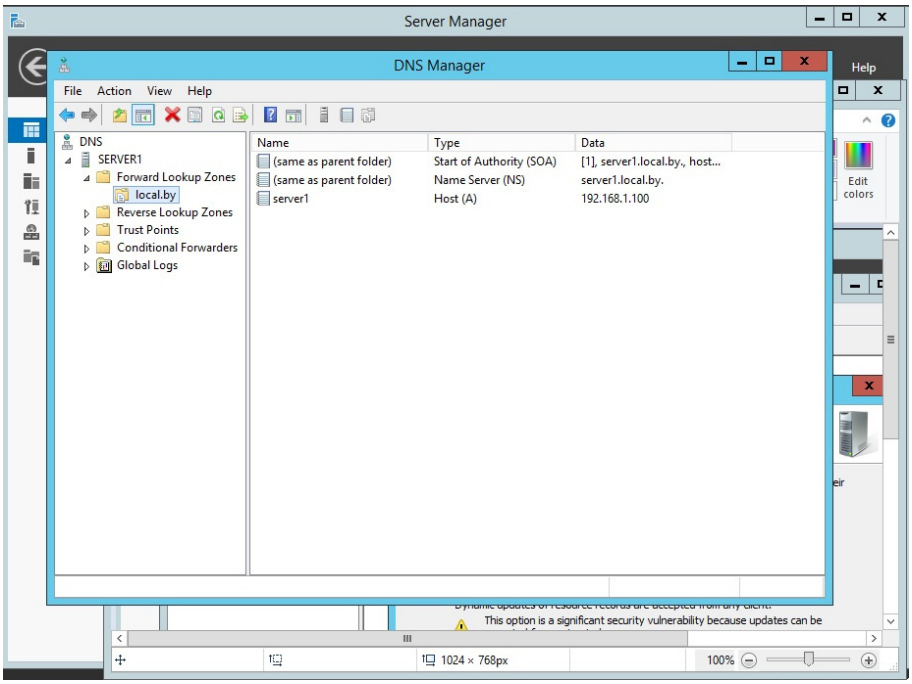

Рис. 2.8. DNS-сервер с созданной зоной прямого просмотра

Чтобы на DNS-сервере автоматически зарегистрировалось имя сервера (в нашем случае server1), необходимо указать в свойствах компьютера DNS-суффикс (рис. 2.9), а также в IP-конфигурации должен быть указан адрес DNS-сервера (в нашем случае это все тот же 192.168.1.100).

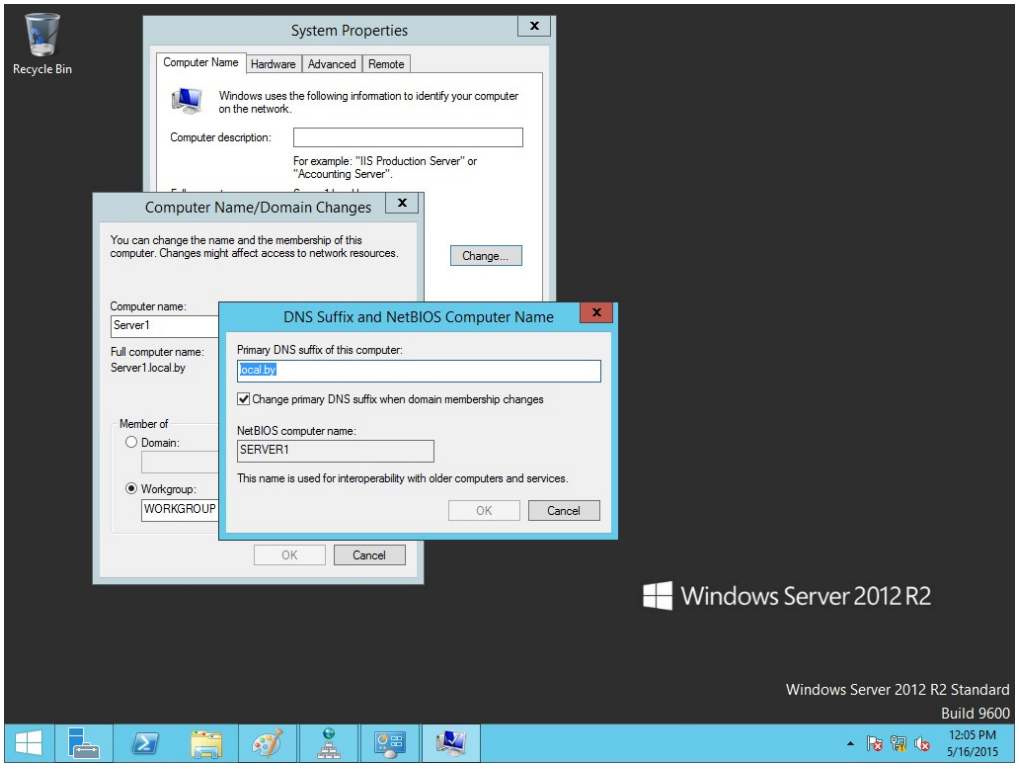

Рис. 2.9. DNS-суффикс для символьного имени компьютера

3. Создание дополнительной зоны прямого просмотра

На втором сервере создадим стандартную дополнительную зону с именем local.by (все действия выполняются на втором сервере аналогично установке службы DNS на первом сервере с отличием типа зоны прямого просмотра):

– откройте консоль DNS;

– выберите раздел *Primary Zone (Зоны прямого просмотра)*;

– запустите мастер создания зоны (выберите: тип зоны – *Secondary Zone (Дополнительная зона)*, IP-адрес master-сервера (с которого будет копироваться зона) – адрес сервера *server1*, остальные параметры – по умолчанию);

– введите имя зоны – local.by.

В итоге получим совместную работу DNS-серверов с реализации функции резервирования.

4. Настройка узлов для выполнения динамической регистрации на сервер DNS

Для выполнения данной задачи нужно выполнить ряд действий как на серверах (если требуемые настройки не были выполнены ранее), так и в настройках клиента DNS. Рассмотрим пример настройки клиента с его регистрацией в DNS-сервере.

На сервере DNS должна быть создана соответствующая зона, а также разрешены динамические обновления.

На клиенте DNS необходимо сделать следующее:

– указать в настройках протокола TCP/IP адрес предпочитаемого DNS-сервера – тот сервер, на котором разрешены динамические обновления (в нашем примере – сервер с адресом 192.168.1.100);

– в полном имени компьютера указать соответствующий DNS-суффикс (в нашем примере – local.by). Для этого последовательно инициировать: *Мой компьютер – Свойства* – закладка *Имя компьютера* – кнопка *Изменить* – Кнопка *Дополнительно* – в пустом текстовом поле вписать название домена local – кнопка *OK* (3 раза)) (рис. 2.10).

После этого система предложит перезагрузить компьютер. После выполнения перезагрузки на сервер DNS в зоне local.by автоматически создадутся записи типа A для наших серверов (рис. 2.11). В случае не создания записи для клиента (в нашем примере это client1) можно на стороне клиента в командной строке выполнить команду *ipconfig / registerdns.*

Аналогичные операции необходимо выполнить на всех компьютерах сети.

Если автоматически записи не создались, то их можно создать вручную (рис. 2.12), однако при этом могут возникнуть сложности с автоматическим обновлением записей при изменении IP-адресов.

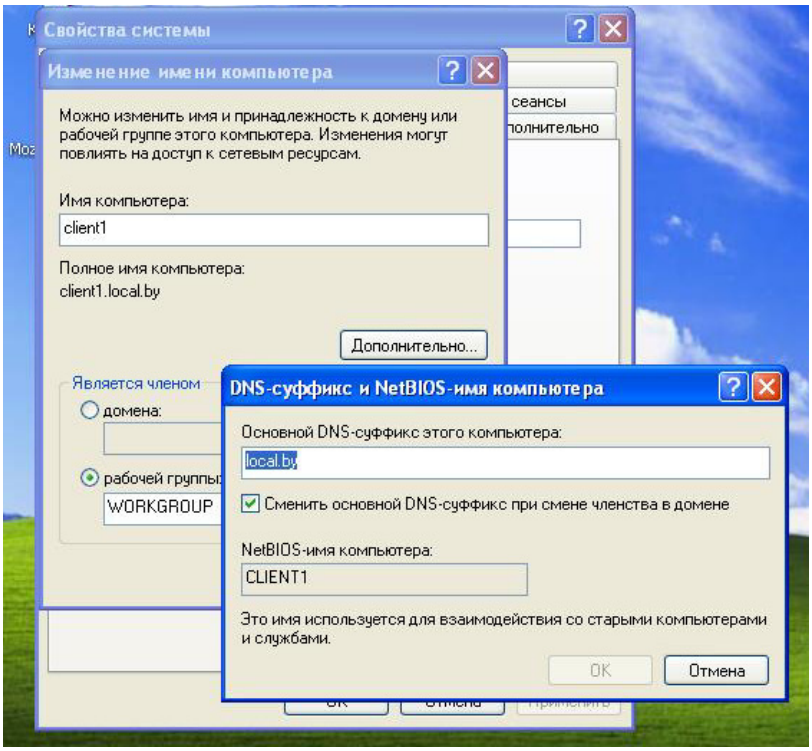

Рис. 2.10. Заполнение поля *DNS-суффикс* на клиенте

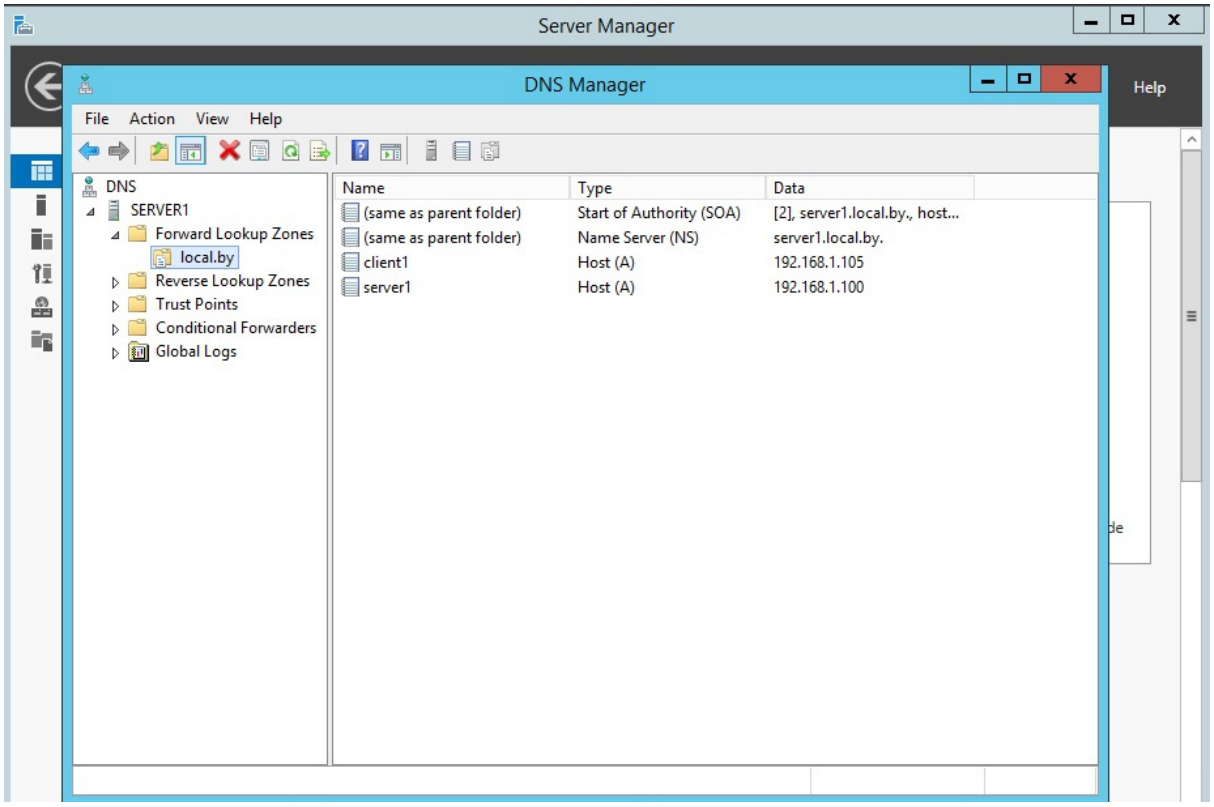

Рис. 2.11. Пример DNS-сервера с записями для клиента и сервера

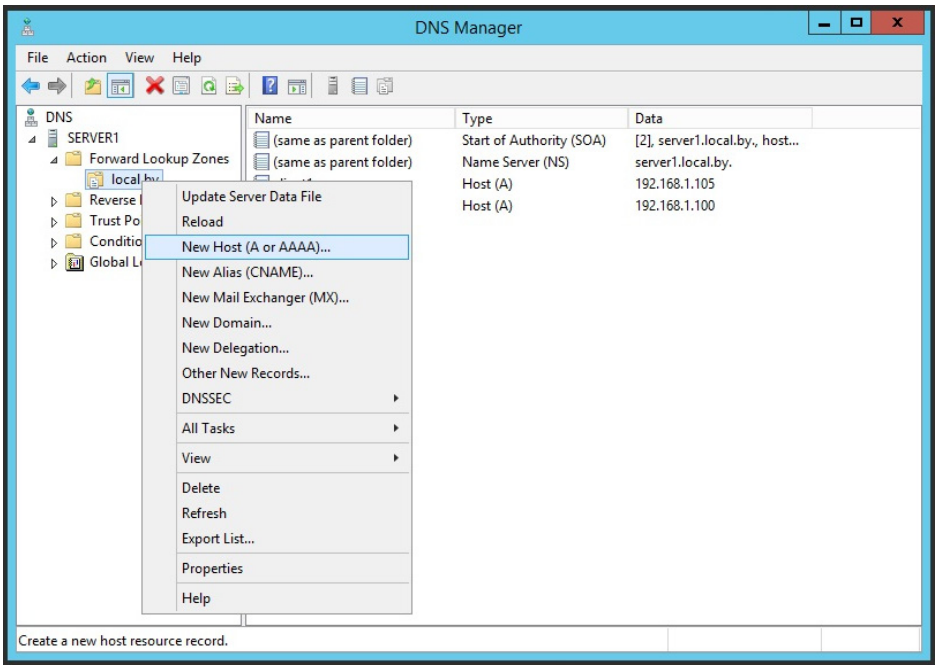

Рис. 2.12. Создание записи типа A на DNS-сервере вручную

5. Создание зоны обратного просмотра

Выполняется по следующим шагам:

– откройте консоль DNS;

– выберите раздел *Reverse Lookup Zone (Зоны обратного просмотра)*;

– запустите мастер создания зоны (выберите: тип зоны – *Primary (Основная)*, динамические обновления – разрешить, остальные параметры – по умолчанию) (рис. 2.13);

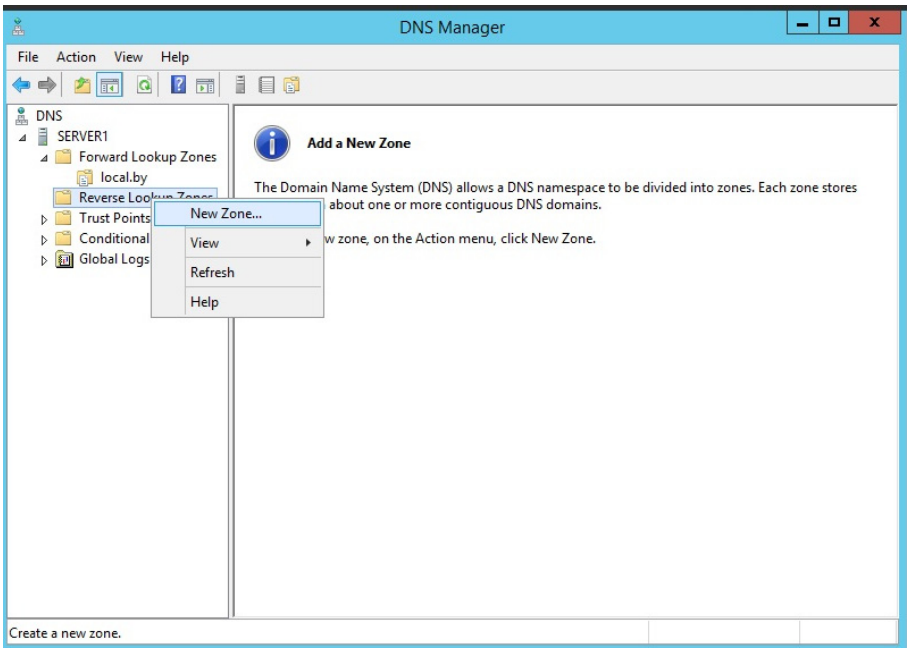

Рис. 2.13. Создание зоны обратного просмотра

– в поле *Код сети* (*ID*) введите параметры идентификатора сети – «192.168.1», а затем выполните команду принудительной регистрации компьютеров на сервере DNS – *ipconfig* / *registerdns*.

В итоге компьютеры зарегистрируются в обратной зоне DNS.

Лабораторная работа № 4

Цель: изучение методов организации символьной адресации в информационных системах на базе клиент-серверной сети и операционных систем Windows с использованием DNS-сервера.

Задание: лабораторная работа представляет собой настройку в сети с клиент-серверной архитектурой, организованной при выполнении лабораторной работы № 2–3, DNS-сервера и регистрации DNS-клиентов. В качестве хостов должны выступать виртуальные операционные системы типа Windows с организованной динамической адресацией. DNS-сервер должен использовать статический адрес (согласно лабораторной работе № 2–3). Имена доменов выбрать согласно варианту (см. таблицу). Проверить работу DNS-сервера можно с помощью утилиты ping, как показано в разделе 2.3. Также необходимо отработать использование утилиты ipconfig с соответствующими командами, позволяющими просмотреть DNS-кэш (displaydns) и очистить DNS-кэш (flushdns). Данные операции зачастую необходимы при изменении IP-адресов DNS-имен.

Варианты заданий для лабораторной работы № 4

Номер варианта	Наименование домена
1	ISiT1.by
2	ISiT2.by
3	ISiT3.by
4	ISiT4.by
5	ISiT5.by
6	ISiT6.by
7	ISiT7.by
8	ISiT8.by
9	ISiT9.by
10	ISiT10.by
11	ISiT11.by
12	ISiT12.by
13	ISiT13.by
14	ISiT14.by
15	ISiT15.by

ДОМЕННЫЕ СИСТЕМЫ (СЛУЖБА ACTIVE DIRECTORY)

3.1. Понятие Active Directory. Служба Active Directory

Ранее отмечалось, что в средних и крупных сетях задача настройки параметров протокола TCP/IP является очень сложной для администратора и вручную практически не выполнима. Для решения этой проблемы был разработан протокол DHCP, реализованный посредством службы DHCP.

Однако настройка сетевых параметров – лишь одна из множества задач, встающих перед системным администратором. В частности, в любой сети важнейшей является задача управления ее ресурсами (файлами и устройствами, предоставленными в общий доступ), а также компьютерами и пользователями.

Для решения задач управления ресурсами в сетях под управлением Windows Server применяется служба каталога Active Directory (Активный каталог). Данная служба обеспечивает доступ к базе данных (*каталогу*), в которой хранится информация обо всех объектах сети, и позволяет управлять этими объектами.

Группа компьютеров, имеющая общий каталог и единую политику безопасности, называется *доменом* (*domain*). Под политикой безопасности понимают набор правил по применению средств обеспечения сетевой безопасности: паролей, учетных записей, протоколов аутентификации и защищенной передачи информации, шифрованной файловой системы и т. д.

Каждый домен имеет один или несколько серверов, именуемых *контроллерами домена* (domain controller), на которых хранятся копии каталога.

Основные преимущества, предоставляемые службой каталога Active Directory:

– централизованное управление – если в сети развернута служба Active Directory, системный администратор может выполнять большинство своих задач, используя единственный компьютер – *контроллер домена*;

– простой доступ пользователей к ресурсам – пользователь, зарегистрировавшись в домене на произвольном компьютере, может получить доступ к любому ресурсу сети при условии наличия соответствующих прав;

– обеспечение безопасности – служба Active Directory совместно с подсистемой безопасности Windows Server предоставляет возможность гибкой настройки прав пользователей на доступ к ресурсам сети;

– масштабируемость – это способность системы повышать свои размеры и производительность по мере увеличения требований к ним. При расширении сети организации служба каталога Active Directory способна наращивать свои возможности – увеличивать размер каталога и число контроллеров домена.

Таким образом, служба каталога Active Directory, подобно службе DHCP, существенно облегчает работу системного администратора по управлению сетевыми объектами. Кроме того, пользователи получают возможность использовать ресурсы сети, не заботясь об их месторасположении, так как все запросы обрабатываются службой Active Directory.

3.2. Объекты каталога и их именование

Объект каталога Active Directory – это элемент, содержащийся в базе данных Active Directory и имеющий набор атрибутов (характеристик). Например, объектом является пользователь, а его атрибутами – имя, фамилия и адрес электронной почты.

Некоторые объекты являются контейнерами. Это означает, что данные объекты могут содержать в своем составе другие объекты. Например, объект *домен* является контейнером и может включать пользователей, компьютеры, другие домены и т. д.

Каталог Active Directory содержит следующие основные типы объектов, не являющихся контейнерами:

– пользователь (user);

– группы пользователей (group);

– контакты (contact);

– компьютеры (computer);

– принтеры (printer);

– общедоступные папки (shared folder).

В Active Directory для именования объектов используется несколько способов.

Различающееся имя (Distinguished Name, DN) – состоит из нескольких частей, например для пользователя **Петрова,** принадлежащего к организационному подразделению **Teachers** домена **faculty.ru,** различающееся имя выглядит так:

DC = ru, DC = faculty, OU = teachers, CN = users, CN = petrov.

При этом используются следующие сокращения:

− DC (Domain Component) – домен;

− OU (Organizational Unit) – организационное подразделение;

− CN (Common Name) – общее имя.

Различающиеся имена являются уникальными в пределах всего каталога Active Directory. В целях упрощения именования может использоваться *относительное различающееся имя* (Relative Distinguished Name, RDN). Для приведенного примера это имя **CN = petrov.** Имя RDN должно быть уникально в рамках объекта-контейнера, т. е. в пределах контейнера **CN = users** пользователь **petrov** должен быть единственным.

Основное имя пользователя (User Principal Name, UPN) используется для входа пользователя в систему и состоит из двух частей: имени учетной записи пользователя и имени домена, к которому принадлежит пользователь. Например: petrov@faculty.ru.

Глобальный уникальный идентификатор (Global Unique Identifier, GUID) – это 128-битовое шестнадцатеричное число, которое ассоциируется с объектом в момент его создания и никогда не меняется. В случае перемещения или переименования объекта его GUID остается прежним.

3.3. Иерархия доменов

Домен является основным элементом в логической структуре Active Directory. В рамках домена действуют единые административные полномочия и политика безопасности, применяется общее пространство доменных имен.

Каждый домен имеет по крайней мере один контроллер домена, на котором хранится каталог Active Directory с информацией о домене.

Для организаций со сложной структурой может создаваться иерархия доменов. Первый образованный домен называется *корневым* (root domain). У него могут быть дочерние домены, имеющие общее пространство доменных имен. В свою очередь, у дочерних доменов могут быть свои домены-потомки. Таким образом, создается иерархия доменов, называемая *доменным деревом* (domain tree).

Если требуется в рамках одной организации организовать еще одно пространство имен, то создается отдельное дерево доменов. При этом несколько деревьев, входящих в состав одного каталога Active Directory, образуют *лес доменов* (forest).

Для именования доменов используются правила, принятые в системе доменных имен DNS. Вследствие этого доменная структура организации может при необходимости (и соблюдении требования уникальности имен) встраиваться в доменную структуру Интернета. Кроме того, для разрешения доменных имен становится возможным использование службы DNS.

На рис. 3.1 приведен фрагмент доменной структуры университета.

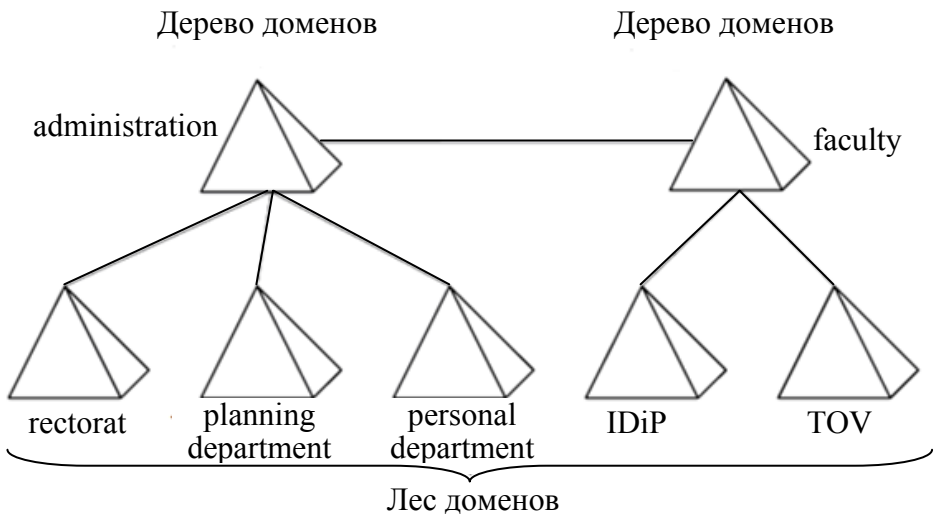

Рис. 3.1. Фрагмент возможной доменной структуры университета

В данном примере лес состоит из двух деревьев – дерева управления университета (домен **administration)** и дерева факультетов (домен **faculty).** Корневой домен головной организации имеет три дочерних домена – **rectorat** (ректорат), planning department (плановый отдел), personal department (отдел кадров). Корневой домен **faculty** является родителем для двух доменов – **IDiP** (ИДиП) и **TOV** (ТОВ).

Следуя правилам DNS, полное имя (FQDN) домена **rectorat** будет иметь следующий вид: **rectorat.administration**, а полное имя домена ИДиП**: IDiP.faculty**.

3.4. Организационные подразделения

Структурирование сетевых ресурсов организации при помощи доменов не всегда бывает оправданно, так как домен подразумевает достаточно крупную часть сети. Часто для администратора возникает необходимость группировки объектов внутри одного домена. В этом случае следует использовать *организационные подразделения* (organizational unit).

Организационные подразделения (ОП) можно использовать в качестве контейнера для следующих объектов:

– пользователей;
– групп пользователей;
– контактов;
– компьютеров;
– принтеров;
– общих папок;
– других организационных подразделений.

Объекты группируются с помощью ОП для следующих целей:

– управление несколькими объектами как одним целым – для этого используются групповые политики;

– делегирование прав администрирования, например начальнику отдела можно делегировать административные права на его отдел, при условии объединения всех объектов отдела в организационную единицу.

В качестве примера структуризации с использованием ОП можно привести возможную структуру домена факультета IDiP (ИДиП) (рис. 3.2).

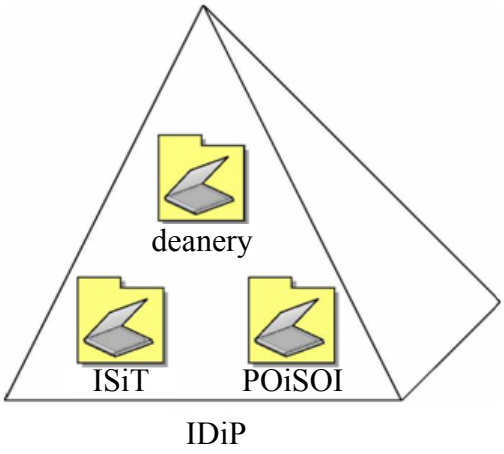

Рис. 3.2. Домен факультета IDiP (ИДиП)

В данной ситуации выделение из домена IDiP дочерних доменов кафедр (ISiT, POiSOI) не имеет смысла, так как факультет слишком мал. С другой стороны, требуется отразить в Active Directory внутреннюю структуру факультета. Решением является структуризация с применением организационных подразделений – в домене создаются ОП deanery (деканат) и кафедр: ISiT (ИСиТ) и POiSOI (ПОиСОИ). При этом для каждого подразделения администратор может назначить собственный набор правил (например, общие требования к паролям).

3.5. Учетные записи пользователей

После реализации спроектированной структуры Active Directory администратор должен добавить в каталог учетные записи всех пользователей системы и назначить каждой из них определенные права. *Учетная запись пользователя* – это набор атрибутов, сопоставленных с определенным пользователем. Самые важные атрибуты следующие:

– имя учетной записи, с помощью которого пользователь осуществляет вход в систему (в пределах домена должно быть уникально);

– полное имя пользователя;

– пароль;

– группы, в которые входит пользователь;

– права пользователя.

Создав все необходимые учетные записи, администратору следует продумать, какими правами должен обладать тот или иной пользователь. *Права пользователя* – это список действий, которые может выполнять пользователь. Права бывают следующих видов:

– *привилегия* (privilege) – право выполнения операций по изменению состояния или параметров системы (например, выключение компьютера или изменение системного времени);

– *право на вход в систему* (logon right);

– *разрешение доступа* (access permission) – право осуществления действий с файлами, папками, принтерами, объектами Active Directory, реестром (при условии, что используется файловая система NTFS).

При условии, что пользователей порядка десяти человек, определить необходимые права можно достаточно просто. Однако гораздо чаще на практике встречаются компьютерные системы с сотнями и тысячами учетных записей. В таких масштабах задача распределения прав отдельным пользователям становится невыполнимой. В этом случае на помощь администратору приходит механизм групп пользователей.

3.6. Группы пользователей

Группа пользователей (группа безопасности, Security Group) – это объединение учетных записей пользователей, которому можно назначать права. С использованием групп распределение прав осуществляется следующим образом. Сначала выбираются такие пользователи, список прав которых должен быть одинаковым. Затем создается группа, членами которой являются выбранные пользователи. Требуемые права назначаются уже не отдельным пользователям, а группе, и эти права автоматически распространяются на всех пользователей группы.

Следует отметить, что группы пользователей и организационные подразделения представляют собой разные механизмы, предназначенные для разных целей. Создание групп безопасности преследует цель распределения прав доступа к ресурсам пользователям сети, в то время как основное назначение организационных подразделений – управление пользователями (а также компьютерами) (рис. 3.3).

Группы пользователей различаются по области действия. Выделяют три области действия:

– *доменную локальную* (domain local scope);

– *глобальную* (global scope);

– *универсальную* (universal scope).

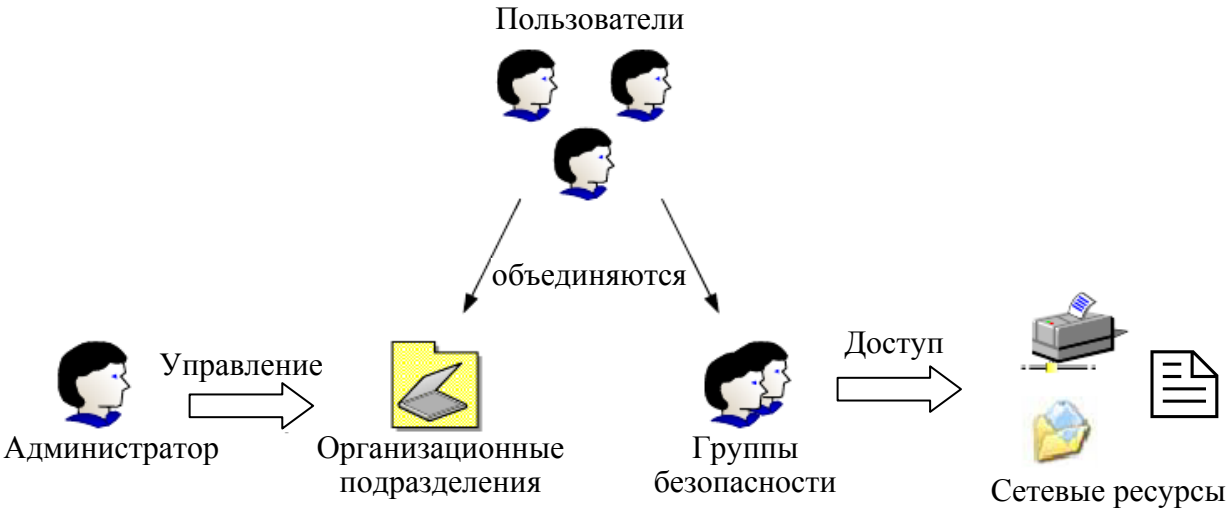

Рис. 3.3. Использование ОП и групп безопасности

Доменные локальные группы действуют в рамках только своего домена. За его пределами указывать локальную доменную группу нельзя. Такие группы обычно применяются для управления доступом к файлам, общим папкам и принтерам.

Глобальные группы могут использоваться в рамках всего леса доменов. Однако глобальная группа принадлежит определенному домену, и в ее состав могут входить только объекты этого домена. Применяются глобальные группы в том случае, если пользователям одного домена нужно получить доступ к ресурсам другого домена.

Универсальные группы привязаны к корневому домену леса, но в их состав могут входить пользователи любого домена. Чаще всего универсальные группы используются для объединения глобальных групп.

3.7. Создание доменов. Создание и настройка пользователей. Распределение ресурсов

3.7.1. Создание домена. Установка роли Active Directory

После настройки сетевой и символьной адресации можно приступить к установке и настройке домена.

1. Щелкните *Start – Server Manager* (*Пуск – Диспетчер сервера*) и выберите *Add roles and features*. Далее нажмите *Next*.

2. Выберите *Role-based or feature-based Installation* (*Установка ролей и компонентов*) и нажмите *Next* (рис. 3.4).

3. Теперь необходимо выбрать сервер, на который устанавливается роль AD, и нажать *Next* (*Select a server from the server pool – Next*) (рис. 3.5).

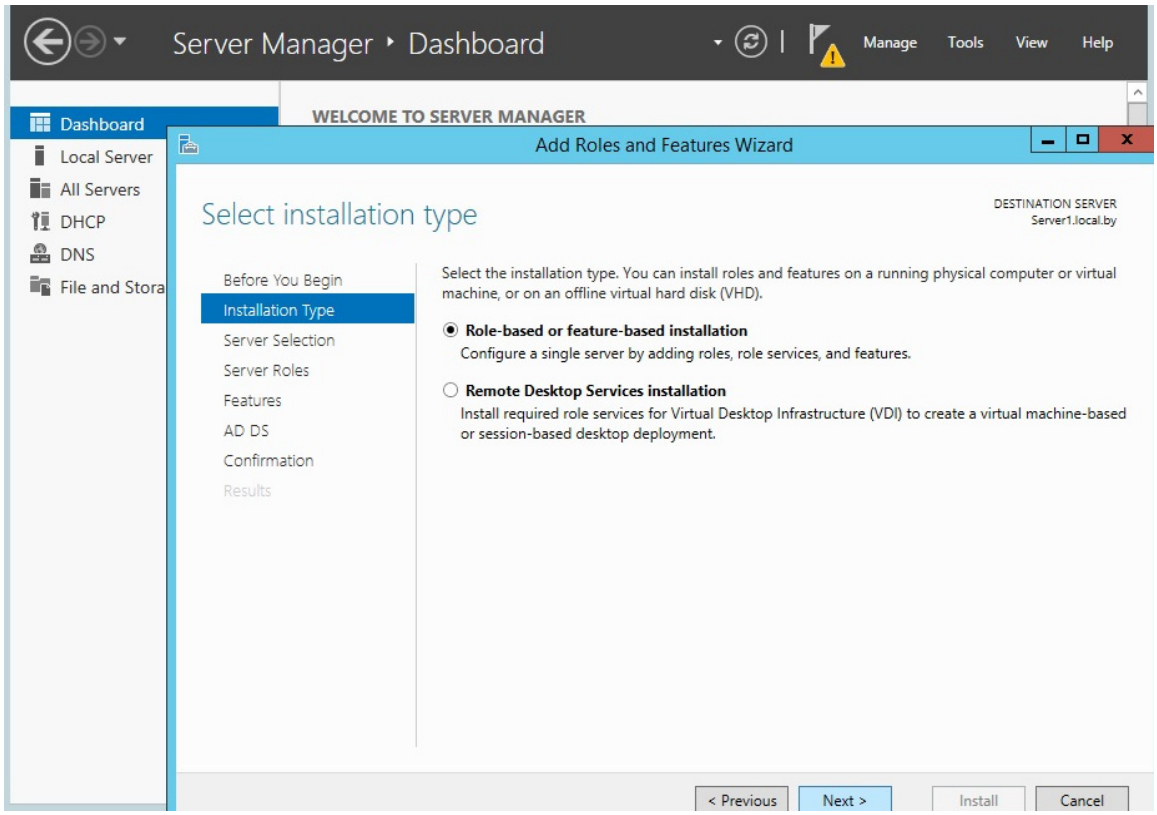

Рис. 3.4. Выбор опции установки ролей и компонент

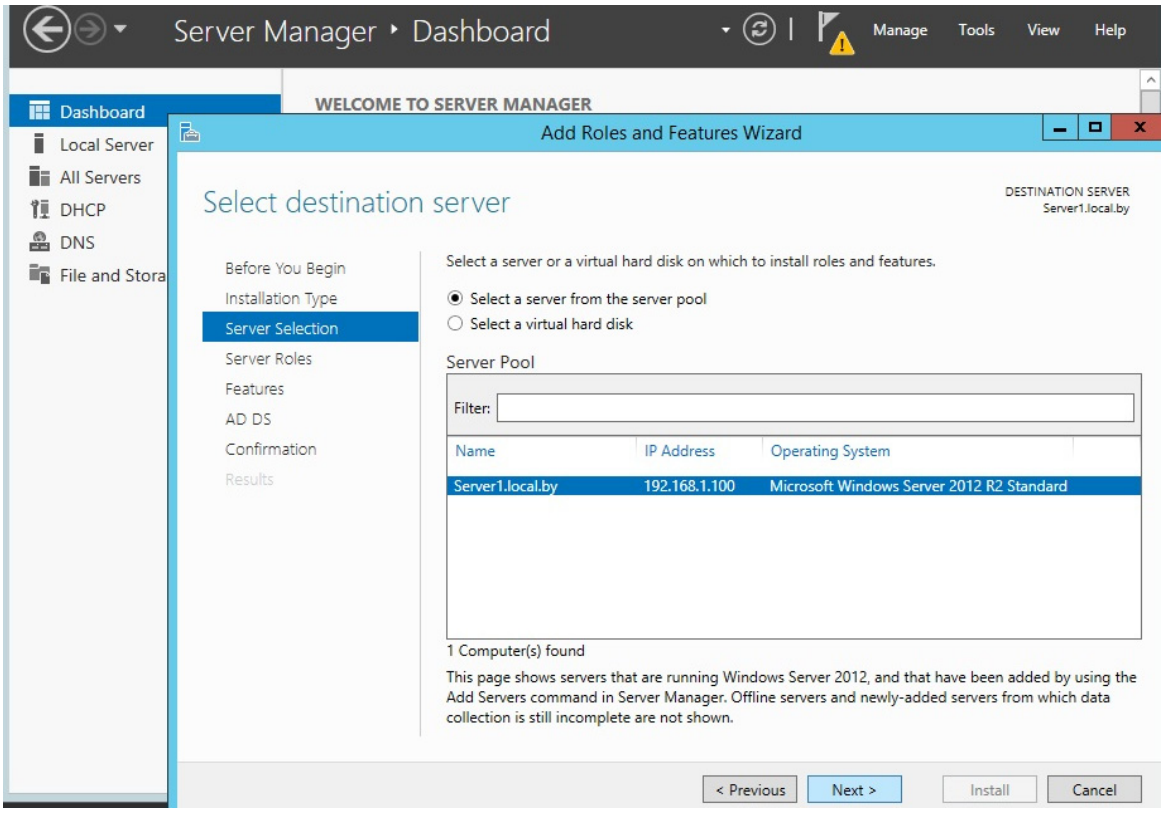

Рис. 3.5. Выбор сервера для установки AD

4. Выбираем роль *Active Directory Domain Services* (*Доменные службы Active Directory*), после чего появляется окно с предложением добавить роли и компоненты, необходимые для установки роли AD. Нажимаем кнопку *Add Features* (рис. 3.6.).

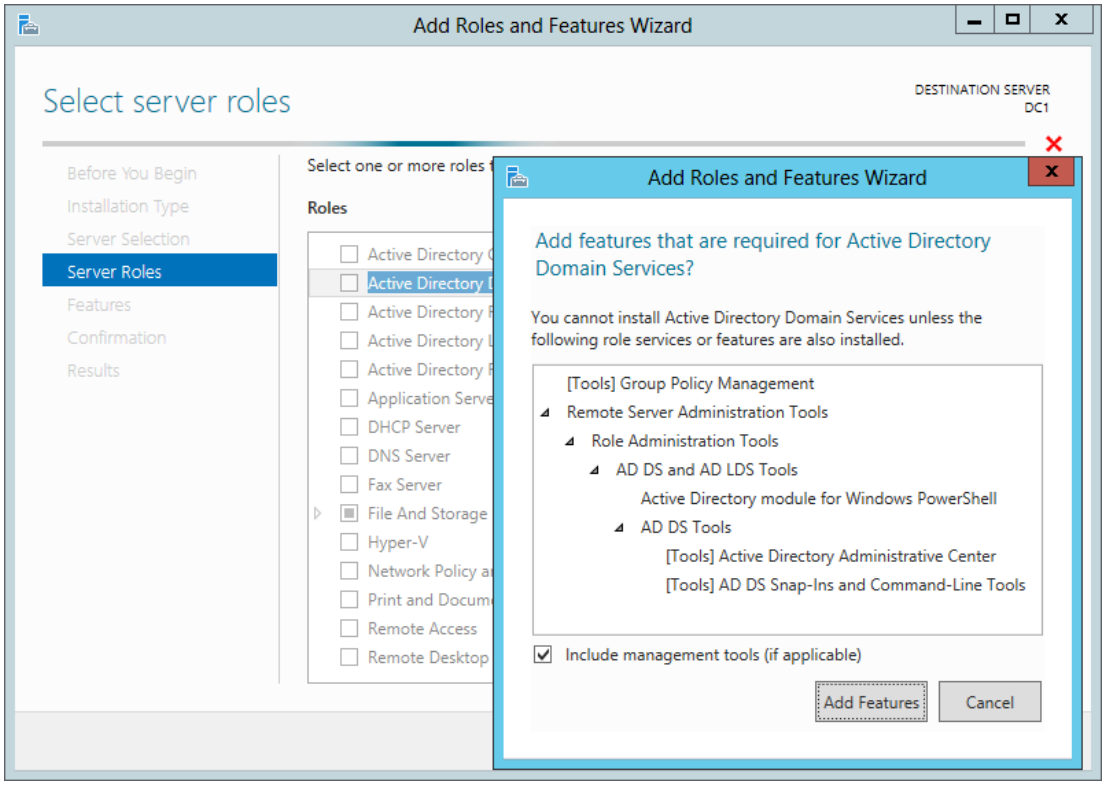

Рис. 3.6. Выбор роли и компонент AD

5. После этого нажимаем каждый раз кнопку *Next* и устанавливаем роль.

6. После установки роли необходимо закрыть окно, нажав *Close*. Теперь необходимо перейти к настройке роли AD. В окне *Server Manager* нажать пиктограмму флага с уведомлением и выбрать *Promote this server to a domain controller (Повысить роль этого сервера до уровня контроллера домена)* на плашке *Post-deploiment Configuration* (рис. 3.7).

7. На следующем этапе необходимо выбрать *Add a new forest (Добавить новый лес)* и ввести название домена, затем нажать *Next (Далее)* (рис. 3.8).

8. На следующей вкладке необходимо выбрать совместимость режима работы леса и корневого домена. По умолчанию устанавливается Windows Server 2012 (рис. 3.9). Так же можно будет отключить *роль DNS Server*, но в нашем случае это нецелесообразно, а поэтому галочку оставляем и вводим пароль для DSRM (Directory Service Restore Mode – режим восстановления службы каталога). Когда все сделано, нажимаем *Next (Далее)*.

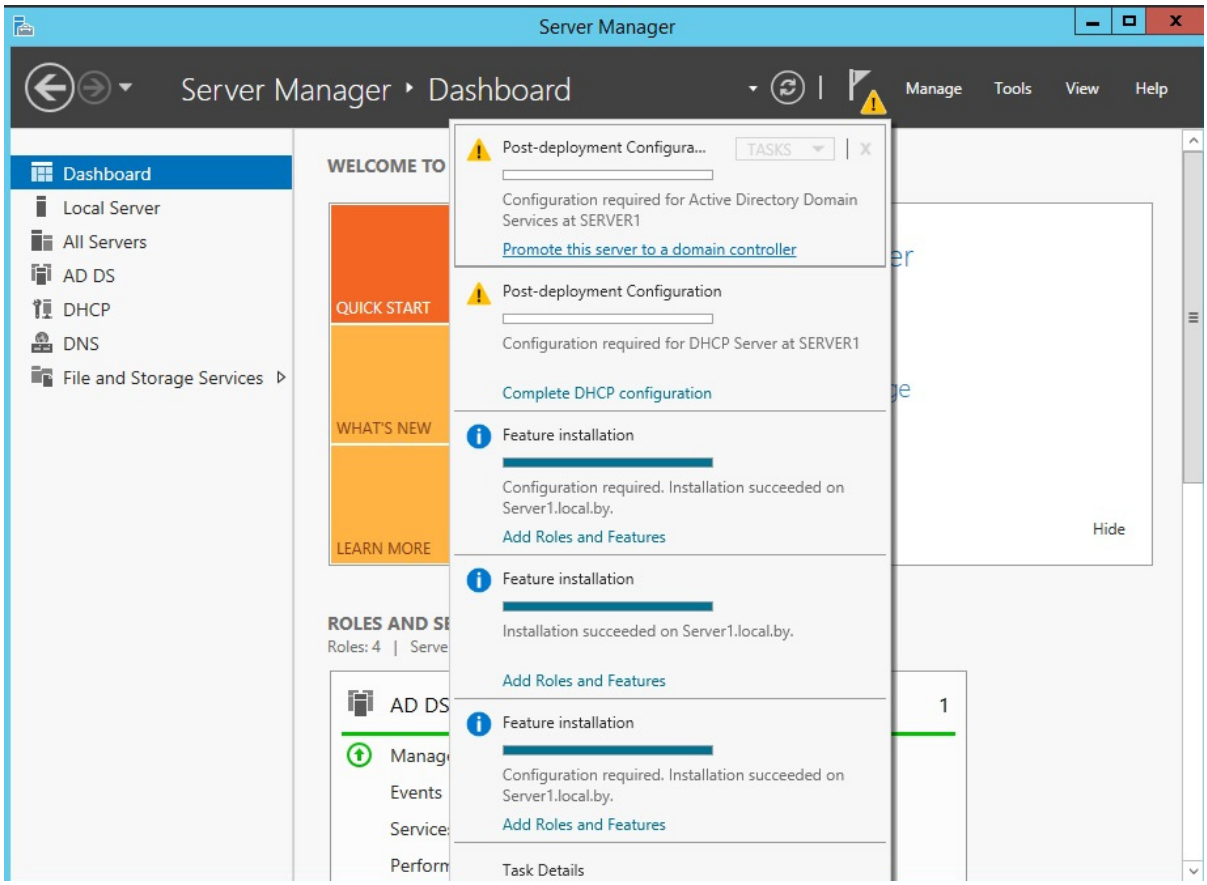

Рис. 3.7. Повышение роли сервера до уровня контроллера домена

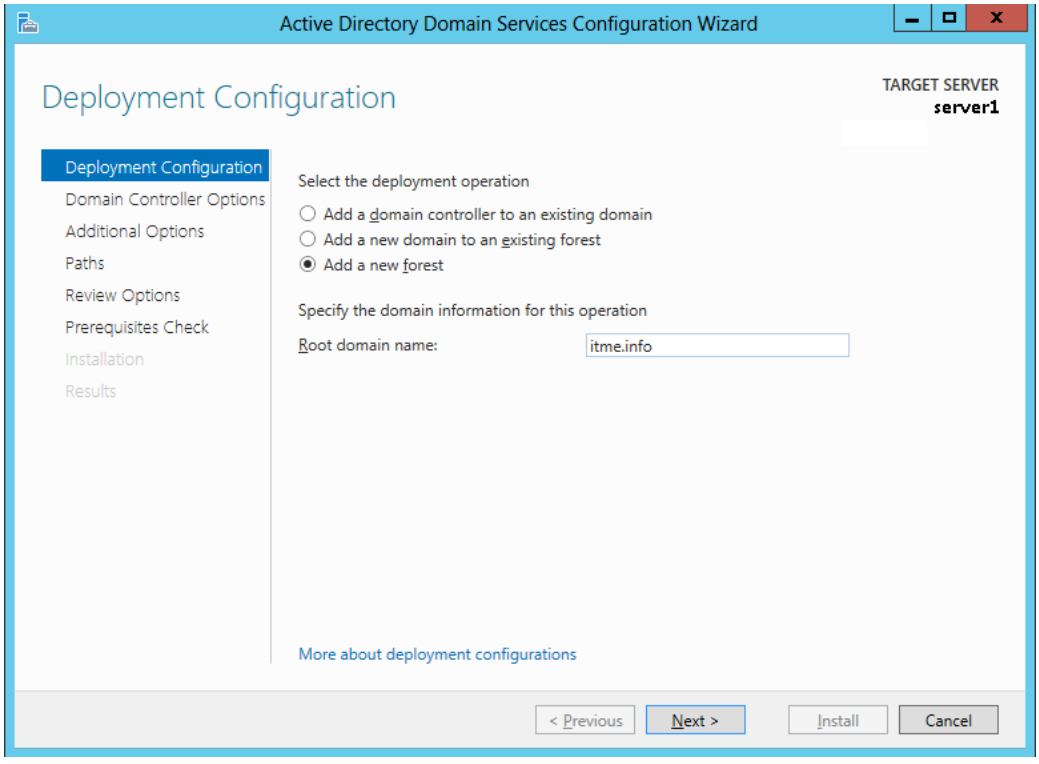

Рис. 3.8. Выбор структуры нового домена

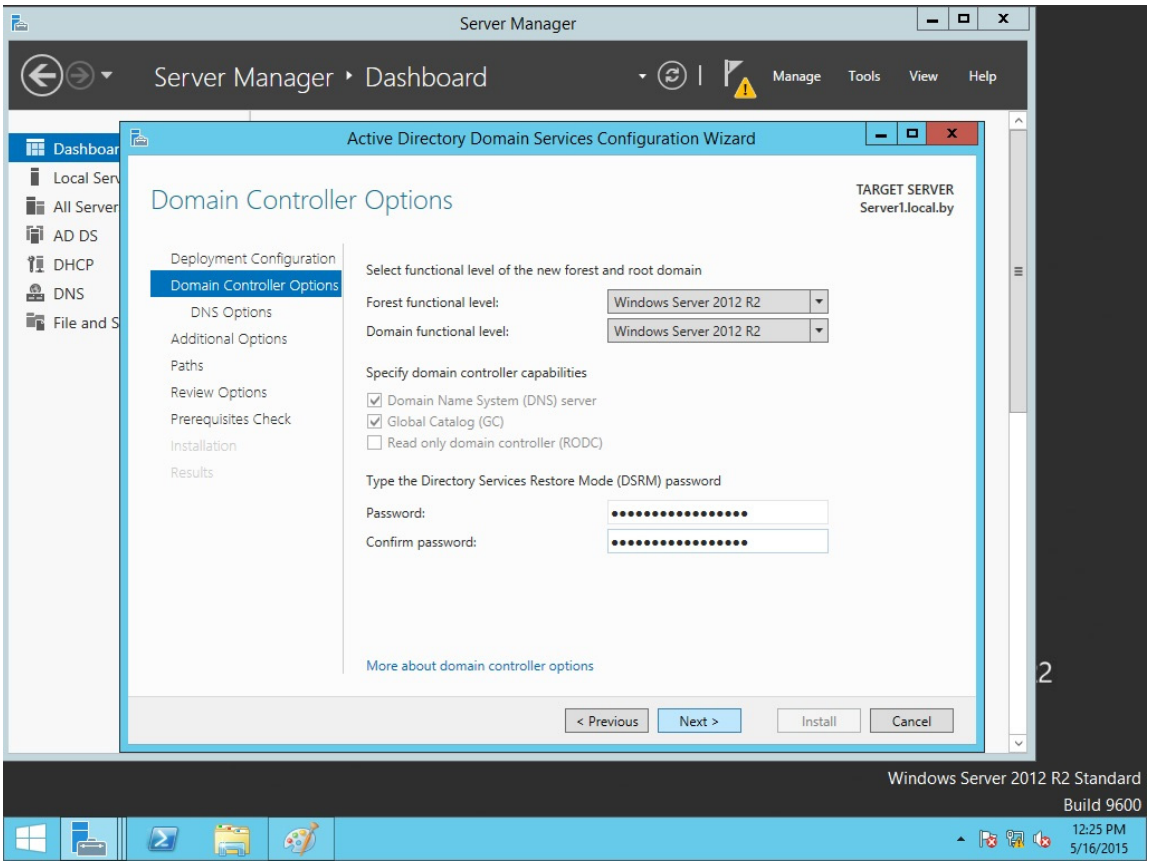

Рис. 3.9. Страница настроек контроллера нового домена

9. На следующем шаге выбирается делегирование полномочий для DNS-сервера (должно быть выбрано по умолчанию) (рис. 3.10).

10. На следующем шаге можно изменить NetBIOS-имя, которое было присвоено домену (рис. 3.11). Необходимо проконтролировать, чтобы имя было в соответствии с планом, а именно *Local*, и нажать *Next (Далее)*.

11. На следующем шаге можно изменить пути к каталогам базы данных AD DS (Active Directory Domain Services – доменная служба Active Directory), файлам журнала, а так же папке Sysvol (рис. 3.12). Отметим, что изменять что-либо нецелесообразно, а поэтому нажимаем кнопку *Next (Далее)*.

12. На следующем шаге отображается сводная информация по настройке (рис. 3.13). Нажав кнопку *View Script*, можно посмотреть Powershell скрипт, который произведет настройку доменных служб Active Directory. Убедившись, что все указано верно, нажимаем на кнопку *Next (Далее)*.

13. На следующем шаге производится проверка, все ли предварительные требования соблюдены (рис. 3.14), после чего нам показывается отчет. Одно из обязательных требований – это установленный пароль локального администратора.

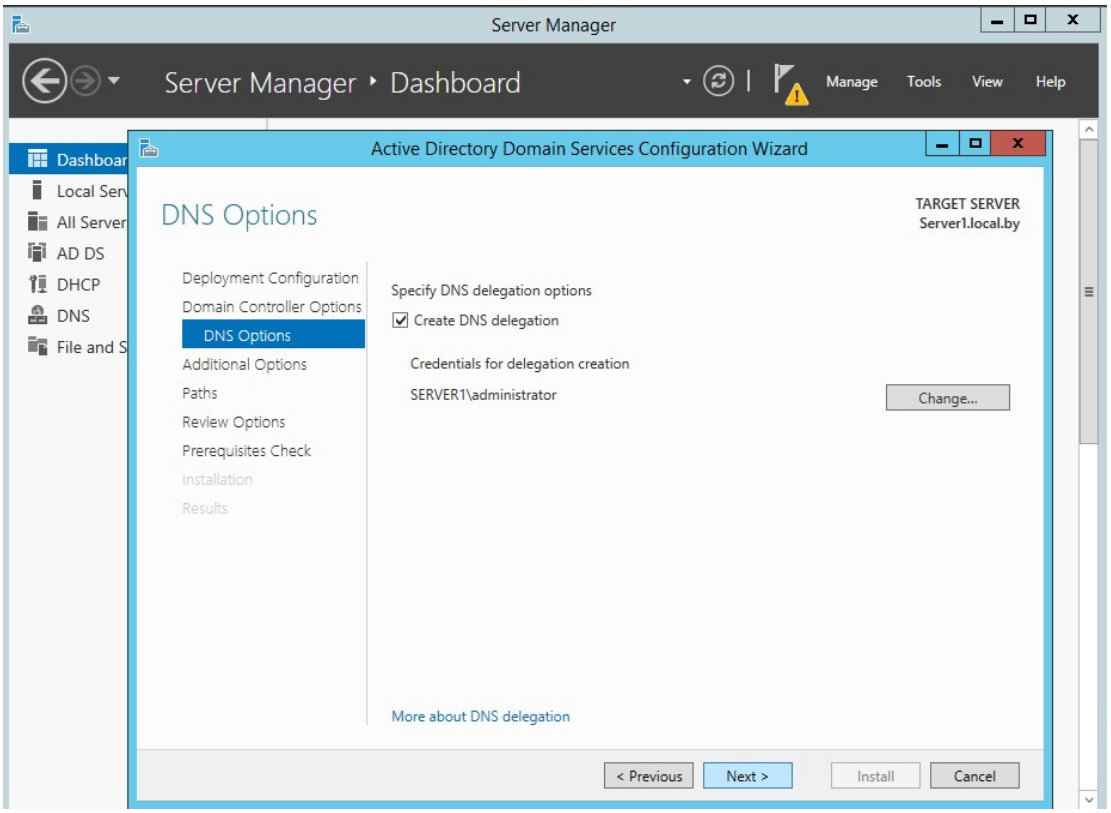

Рис. 3.10. Делегирование полномочий DNS-серверу

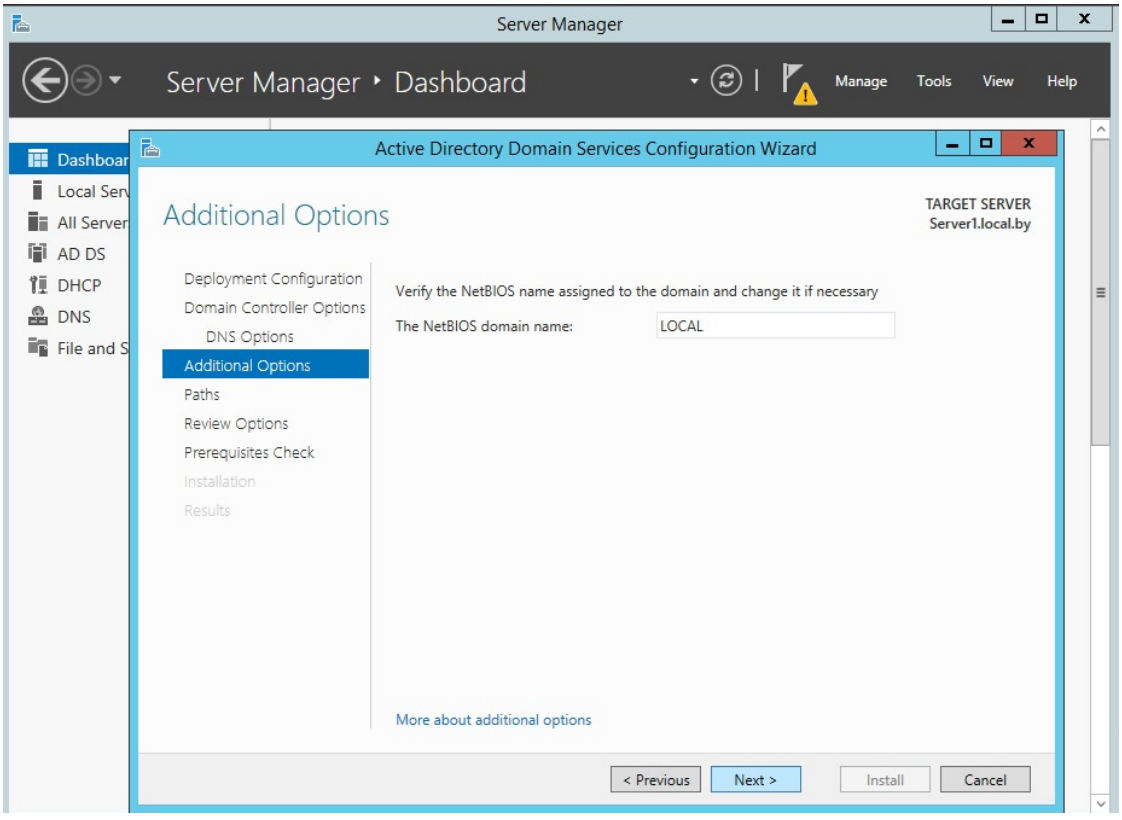

Рис. 3.11. Выбор NetBios-имени контроллера домена

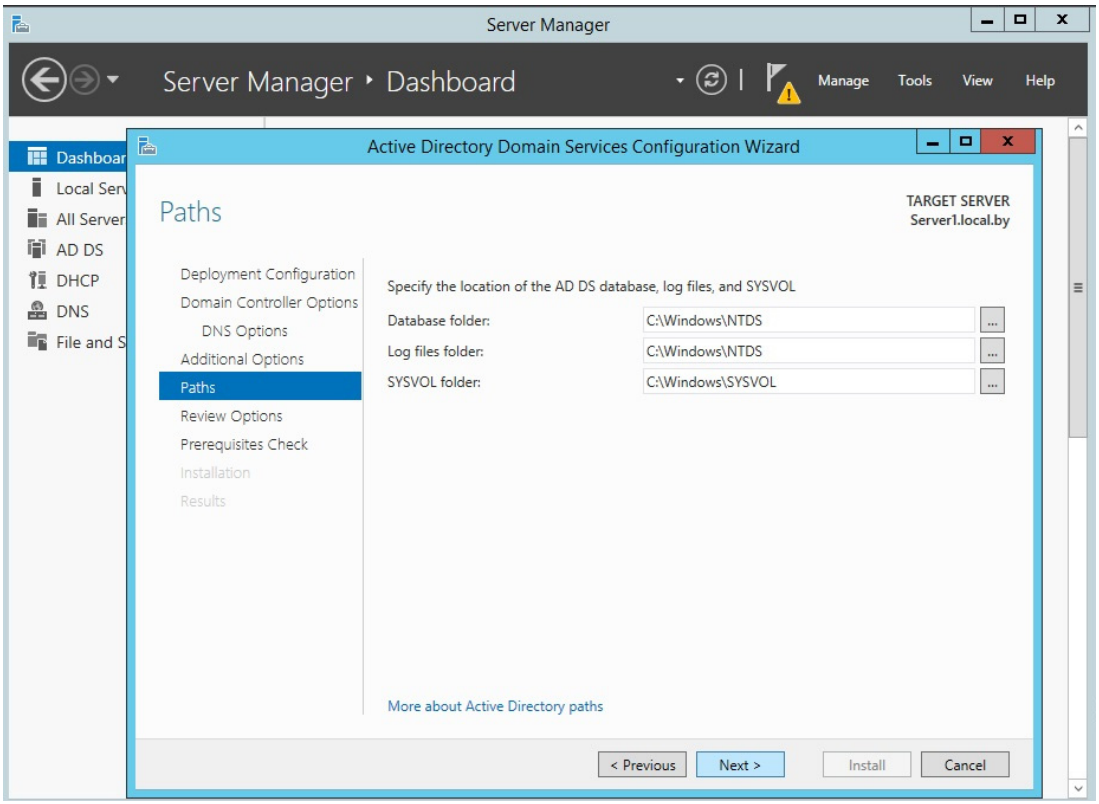

Рис. 3.12. Определение путей к каталогам базы данных, журналам и папке Sysvol создаваемого домена

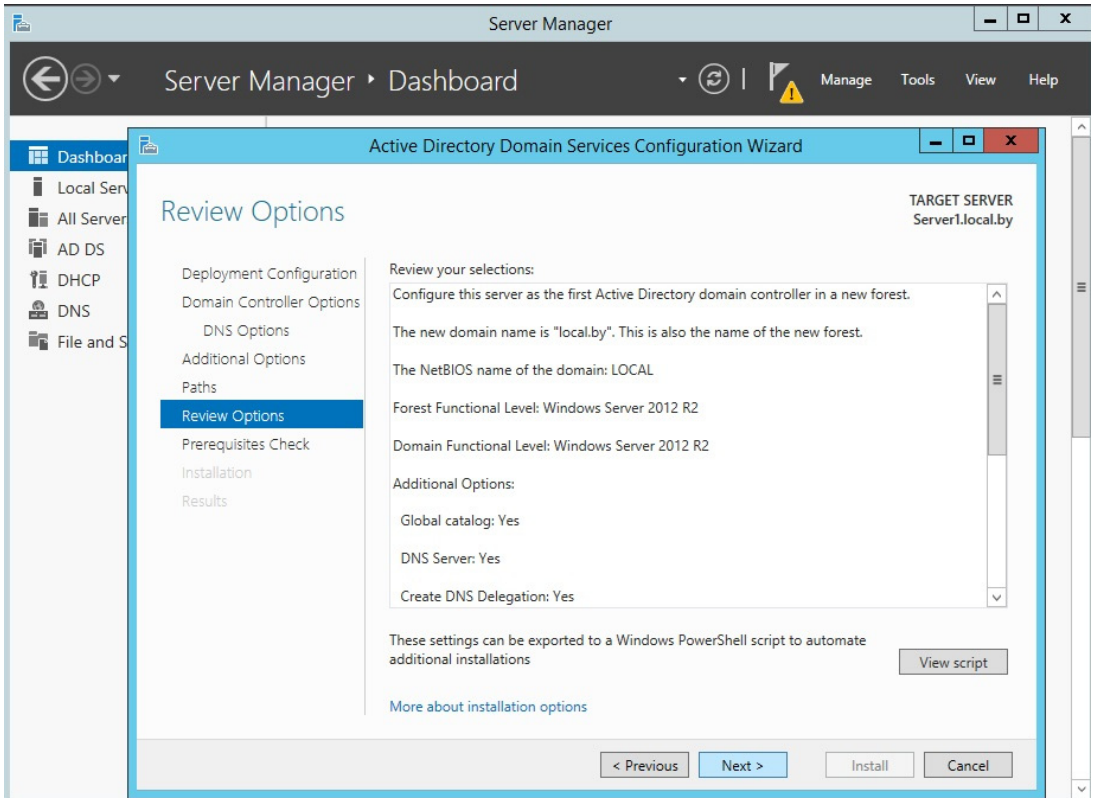

Рис. 3.13. Просмотр сводной информации по настройке домена

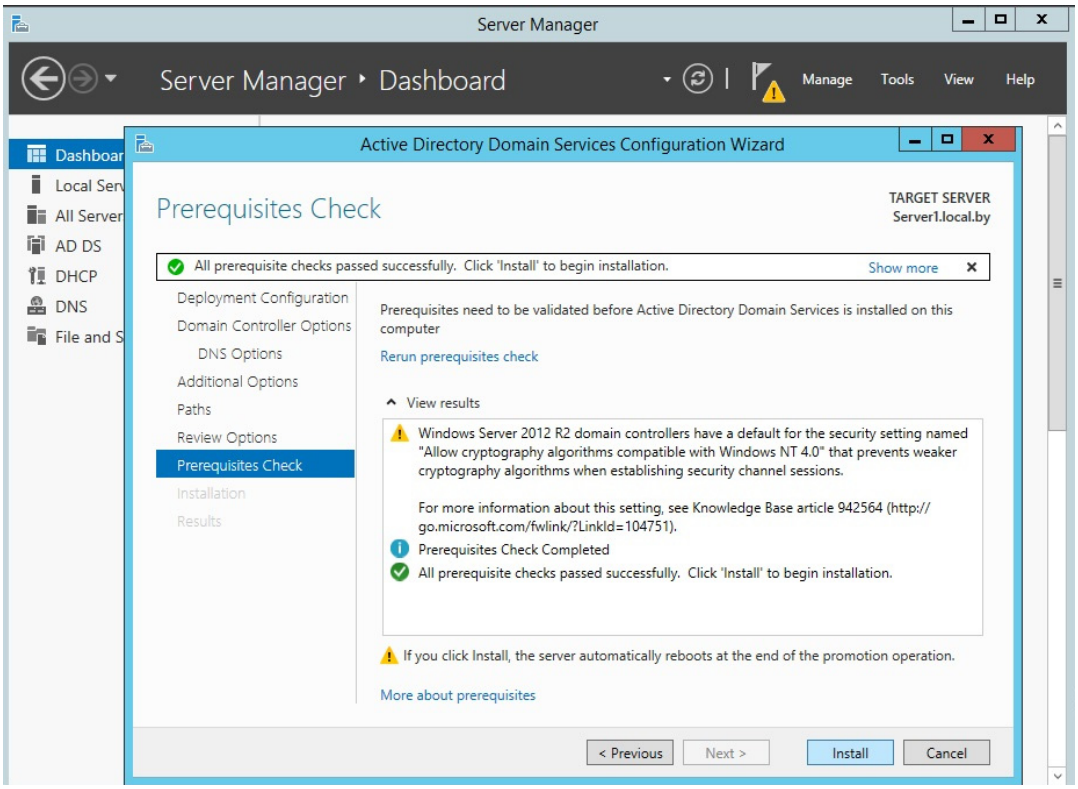

Рис. 3.14. Просмотр отчета о выполнении
всех требований при создании домена

В самом низу можно прочитать предупреждение о том, что после того, как будет нажата кнопка *Install*, уровень сервера будет повышен до контроллера домена и будет произведена автоматическая перезагрузка. После перезагрузки должна появиться надпись *All prerequisite checks are passed successfully. Click «install» to begin installation*.

14. После завершения всех настроек сервер перезагрузится, и вы совершите первый ввод компьютера в ваш домен. Для этого необходимо ввести логин и пароль администратора домена.

На этом базовая настройка служб каталога Active Directory завершена, поэтому нажимаем *Install*. Конечно же, еще предстоит проделать огромный объем работы по созданию подразделений, созданию новых пользователей, настройке групповых политик безопасности.

После завершения операций по установке контроллера домена необходимо выполнить повторную авторизацию DHCP-сервера. Для этого в окне *Server Manager* нажать пиктограмму флага с уведомлением и выбрать *Complete DHCP configuration (Завершить настройку DHCP)* на плашке *Post-deploiment Configuration* (рис. 3.15).

На следующих нескольких шагах фактически необходимо нажимать *Next (Далее)*, тем самым соглашаясь в предложенным вариантом авторизации DHCP-сервера, как показано на рис 3.16–3.18.

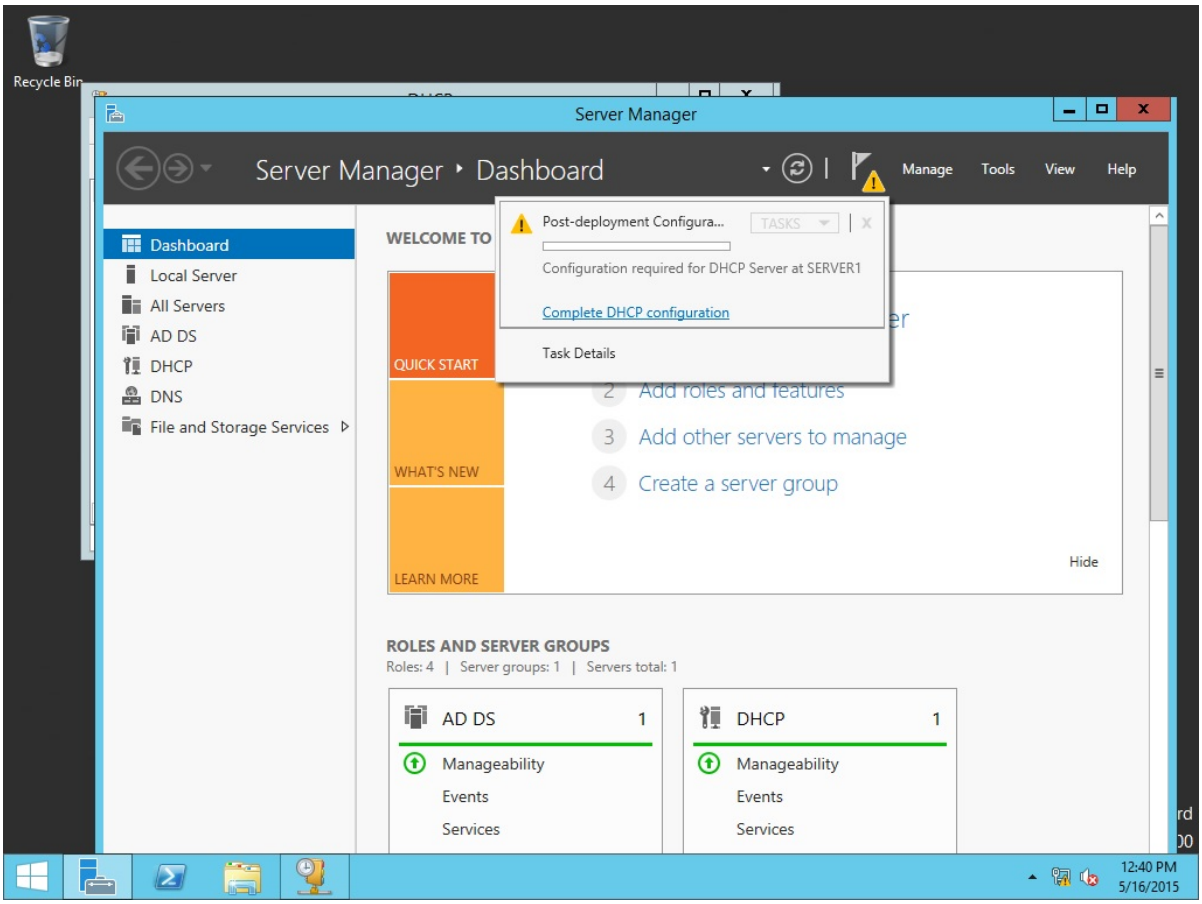

Рис. 3.15. Завершение настройки DHCP (для повторной авторизации)

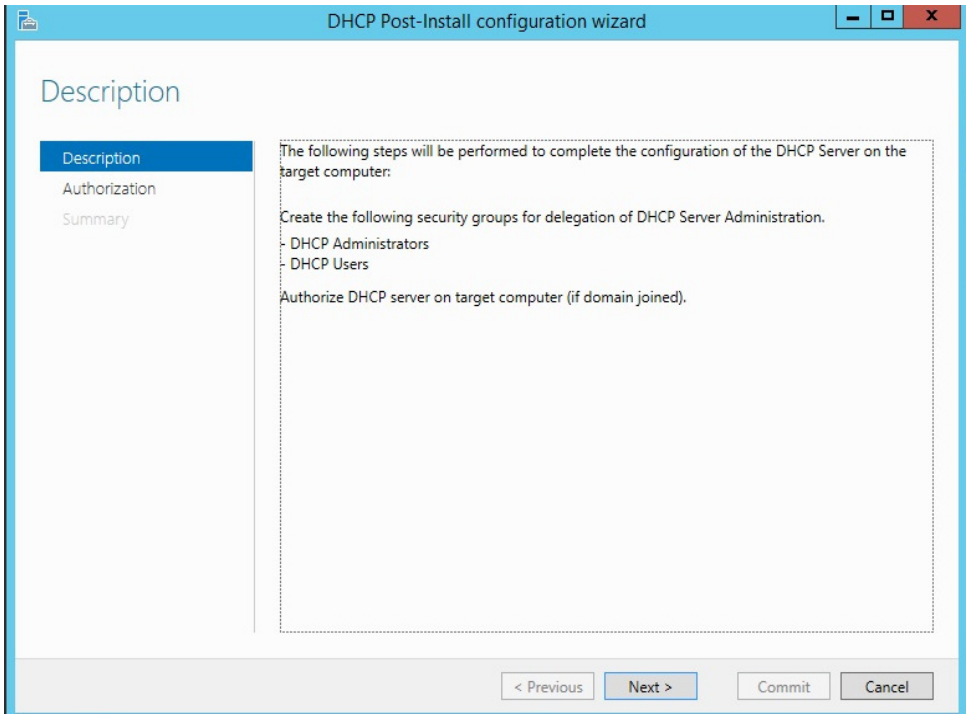

Рис. 3.16. Этап авторизации DHCP-сервера

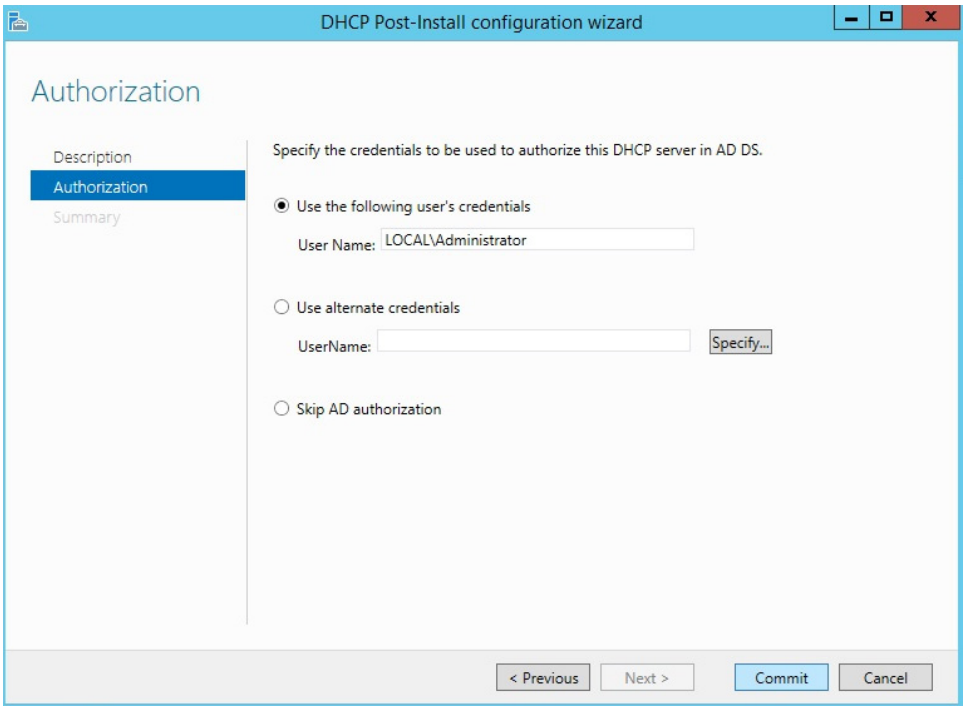

Рис. 3.17. Этап авторизации DHCP-сервера

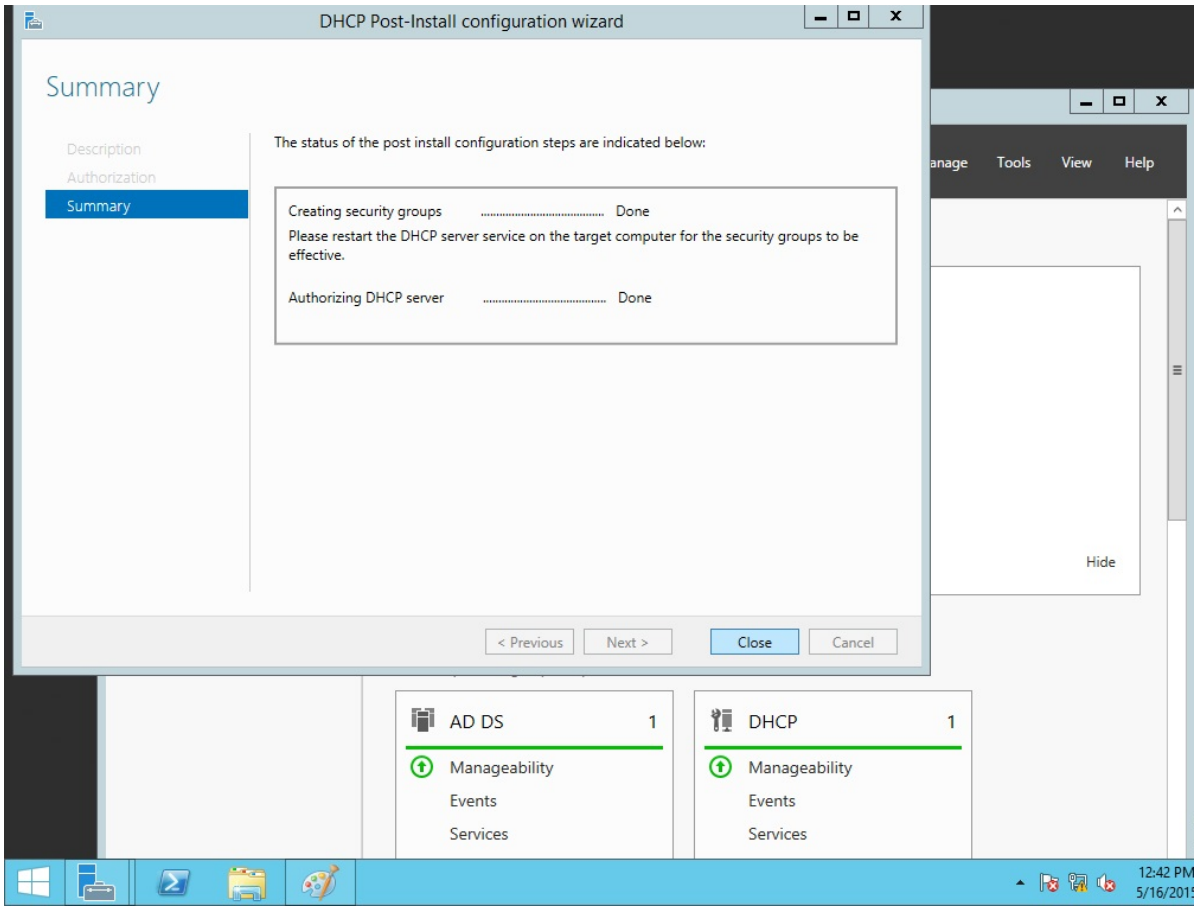

Рис. 3.18. Этап авторизации DHCP-сервера

3.7.2. Присоединение компьютера к домену

Для этого необходим компьютер клиента, имеющий связь с сервером (например, стабильно проходит ping-запрос, и что важно, как по IP-адресу, так и по DNS-имени).

Дополнительно рекомендуется проверить правильности конфигурации DNS-сервера, чтобы на нем была создана запись ресурса службы (SRV). На втором компьютере DNS должна быть сконфигурирована так, чтобы он мог находить сервер как контроллер домена с именем, выбранным вами, например local.by.

1. Войдите в систему на клиентском компьютере. Чтобы изменять членство этого компьютера в доменах, нужно войти в систему под учетной записью локальной группы Администраторы (Administrators).

2. Откройте вкладку *Имя компьютера (Computer Name)*. Для этого дважды щелкните *Система (System)* в *Панели управления*, в боковом меню выберите *Дополнительные параметры системы (Advanced)* и далее вкладку *Имя компьютера (Computer name)*. На открывшейся вкладке щелкните *Изменить (Change)* (рис. 3.19).

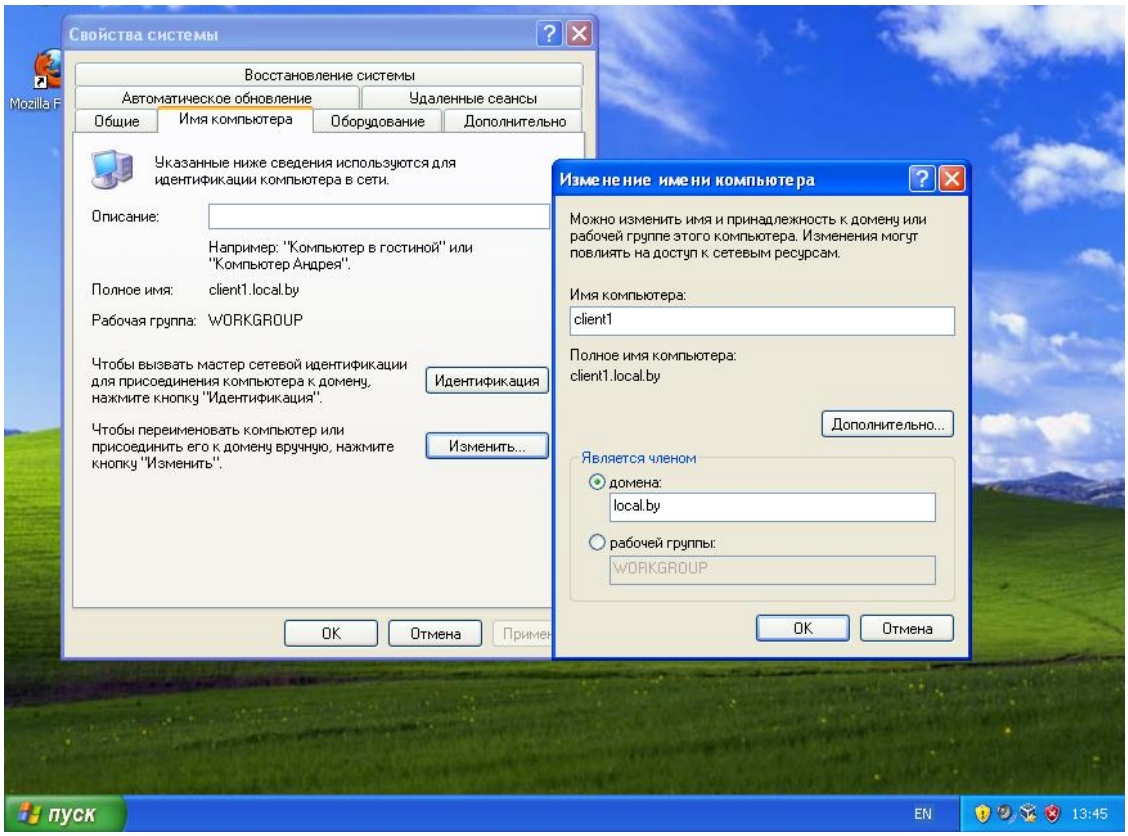

Рис. 3.19. Введение клиента в домен

3. Установите переключатель в положение домена (Domain) и введите DNS-имя домена: в нашем примере это local.by.

Далее щелкните *OK* (рис. 3.19).

4. По запросу введите имя и пароль учетной записи администратора домена local.by (рис. 3.20) и щелкните *OK*.

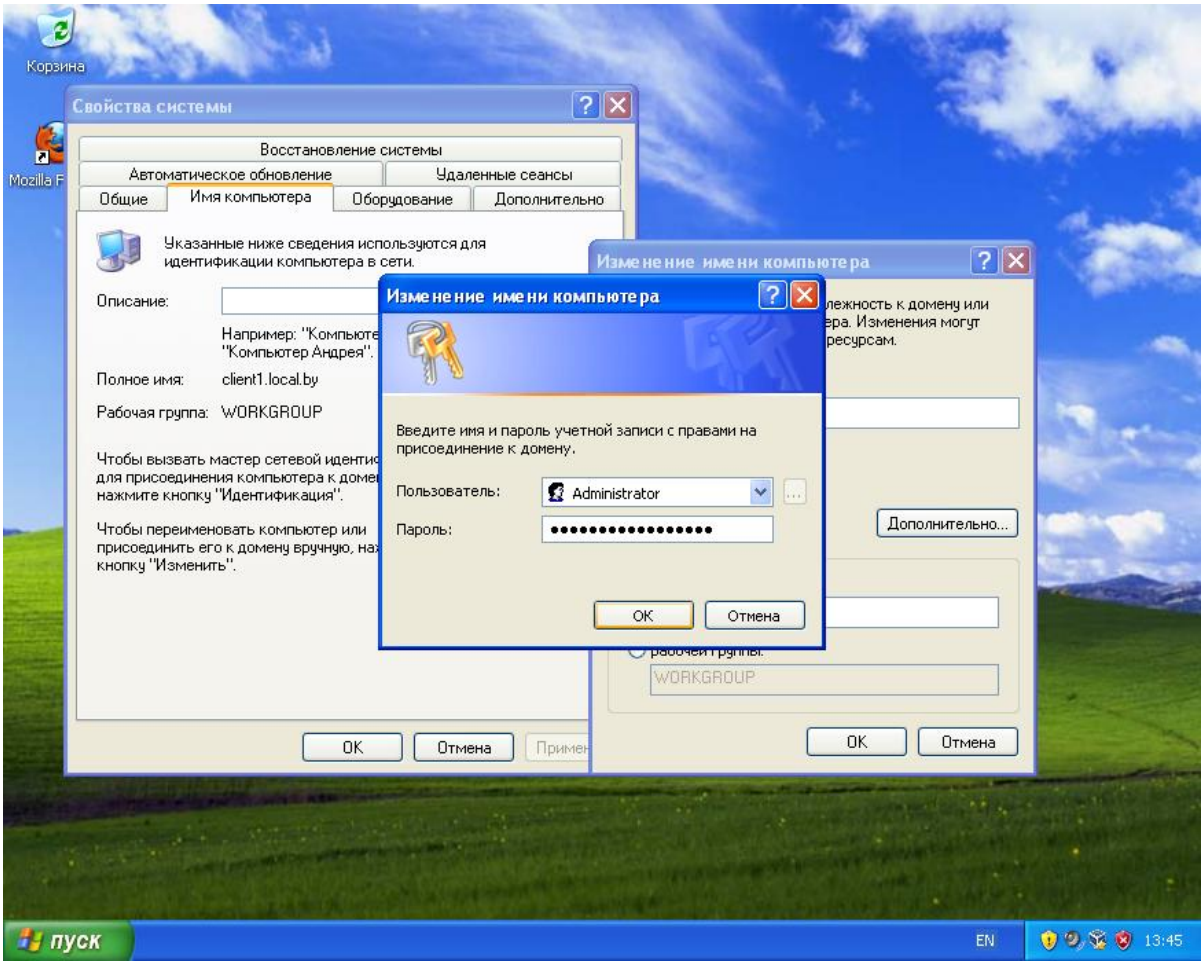

Рис. 3.20. Ввод логина и пароля администратора домена
(для получения права на присоединение к домену)

5. Далее будет получено сообщение о присоединению к домену (рис. 3.21) и предложено перезагрузить систему. Щелкайте *OK* в ответ на все сообщения и закройте все диалоговые окна. Перезагрузите систему. В дальнейшем вы сможете входить в ОС под пользователями домена.

Отметим, что при вводе компьютера в домен для него должна автоматически создаться учетная запись для компьютера с соответствующим именем. Если таковое не будет выполнено, то учетную запись компьютера нужно создать самостоятельно. Для этого откройте консоль *Active Directory – Users and Computers (Active Directory — пользователи и компьютеры)* и, используя контекстное меню, выберите создание учетной записи компьютера (рис. 3.22).

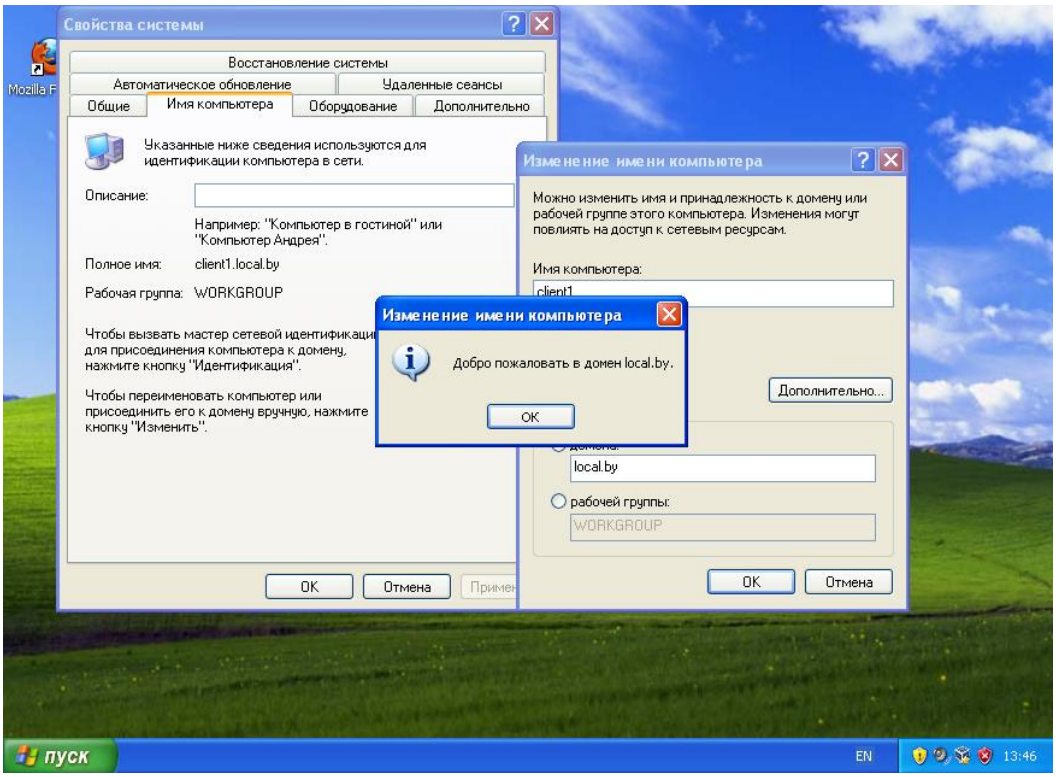

Рис. 3.21. Сообщение о введении компьютера в домен

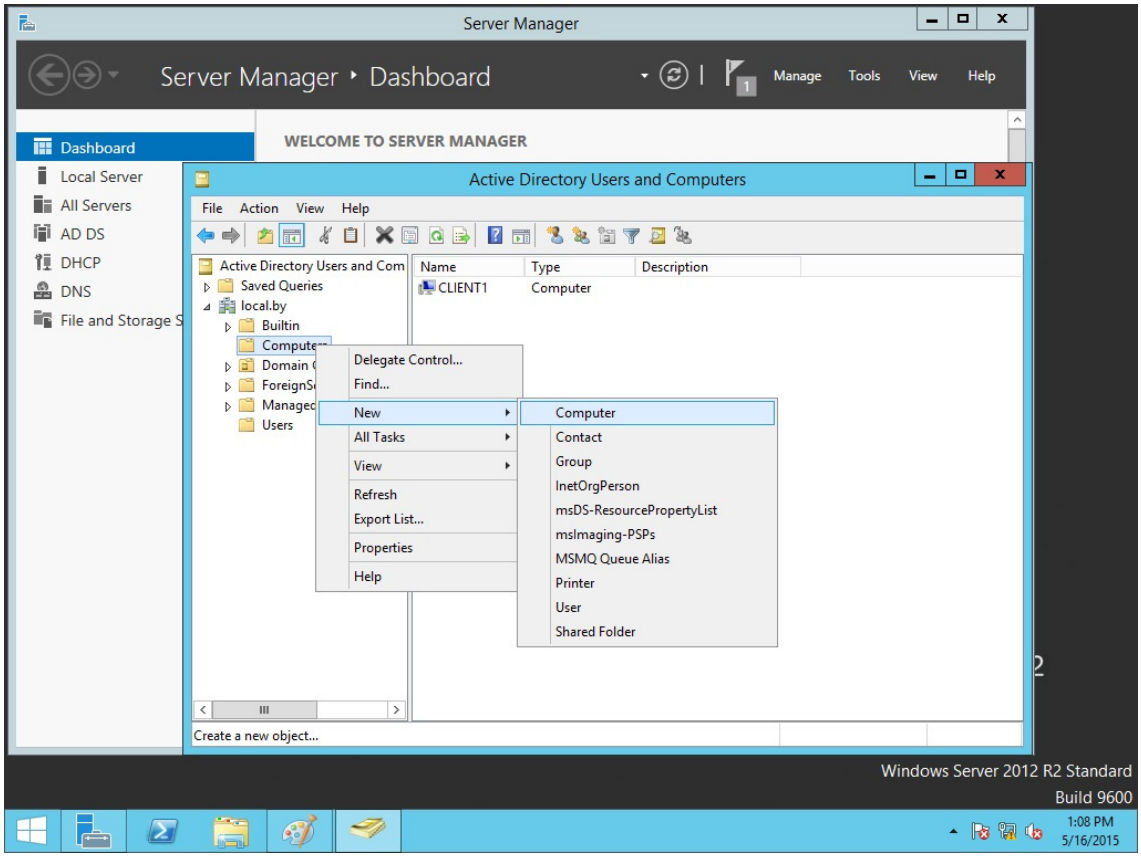

Рис. 3.22. Создание учетной записи компьютера на контроллере домена

3.7.3. Создание учетных записей пользователей. Распределение ресурсов

Создание объектов пользователей

1. Войдите на Serverl как Администратор (Administrator).

2. Откройте консоль *Active Directory Users and Computers (Active Directory пользователи и компьютеры)* (рис. 3.23).

3. Выберите группу *users* и вызовите контекстное меню для создания пользователя (можно также создавать в организационном подразделении – это будет важно при удаленном администрировании с использованием групповых политик) (рис. 3.24).

4. Создайте учетную запись пользователя, причем задайте надежный пароль. Так, при созданном домене обязательным является использование сложных паролей, например содержащих две раскладки клавиатуры либо два разных языка, а также цифры и знаки (рис. 3.25 и 3.26).

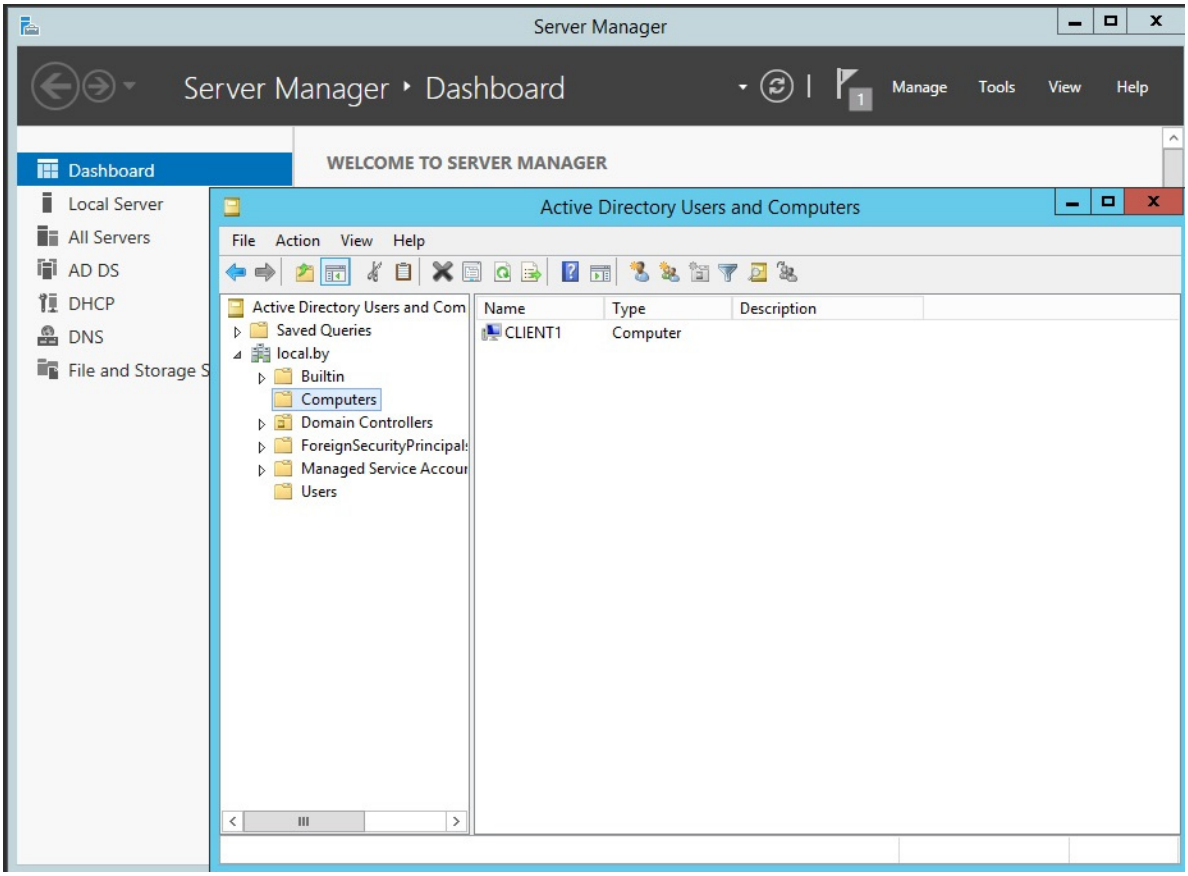

Рис. 3.23. Консоль *Active Directory Users and Computers*

5. Завершите создание пользователя, нажав *Next (Далее)*, а после ввода пароля – *OK*. Также рекомендуется задать подходящие свойства объекта пользователя на вкладках *Общие (General)*, *Адрес (Address)*, *Профиль (Profile)*, *Телефоны (Telephones)* и *Организация (Organization)*.

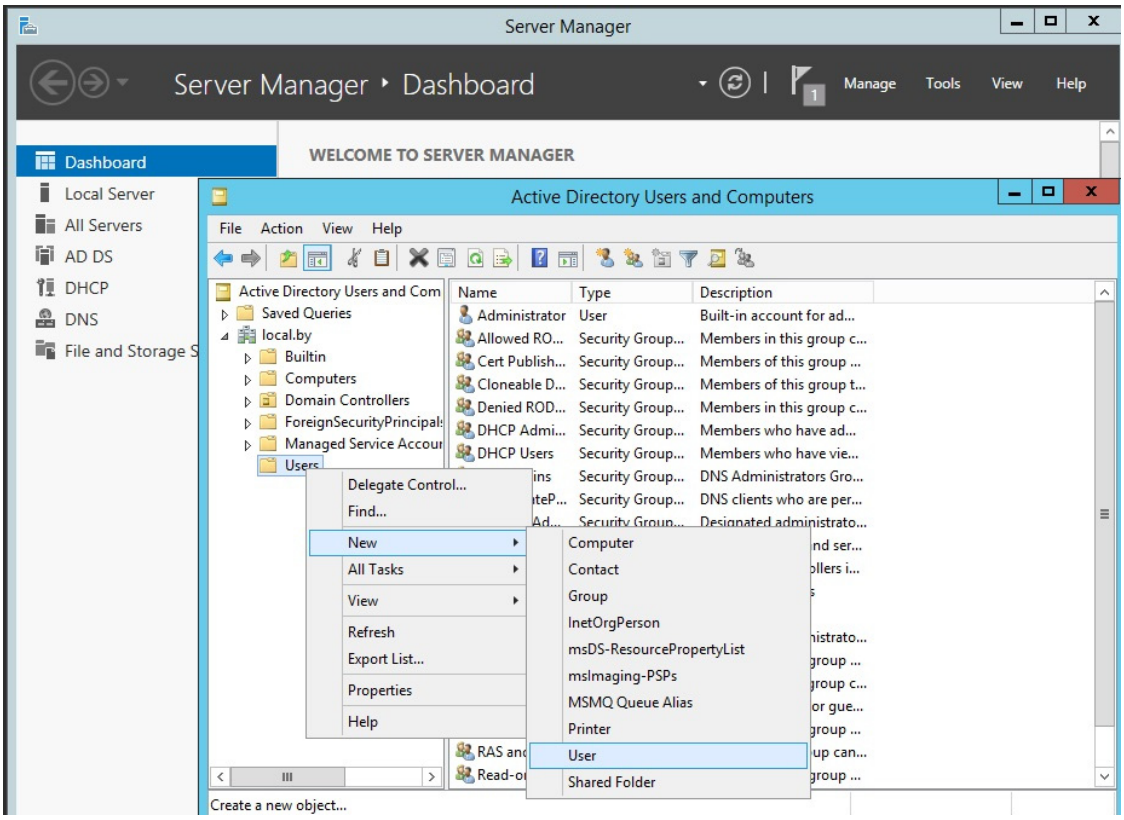

Рис. 3.24. Создание пользователя в консоли *Active Directory Users and Computers*

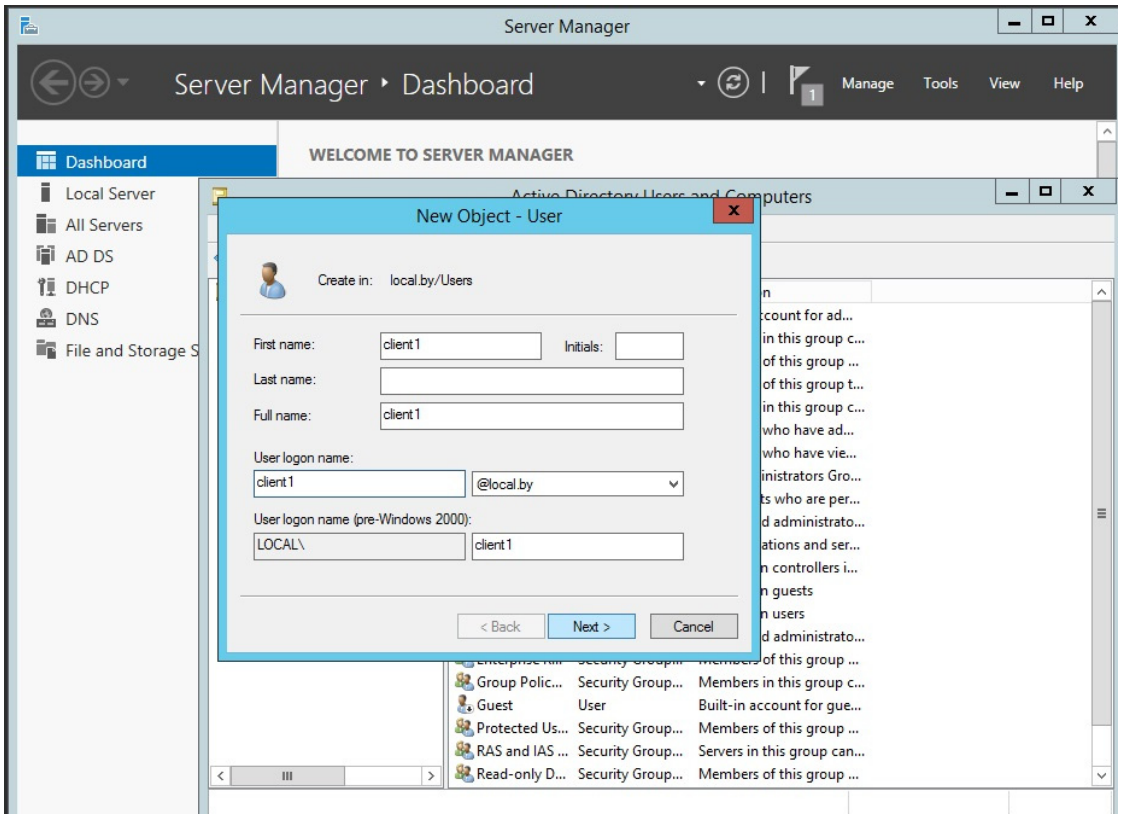

Рис. 3.25. Создание пользователя с заданными параметрами

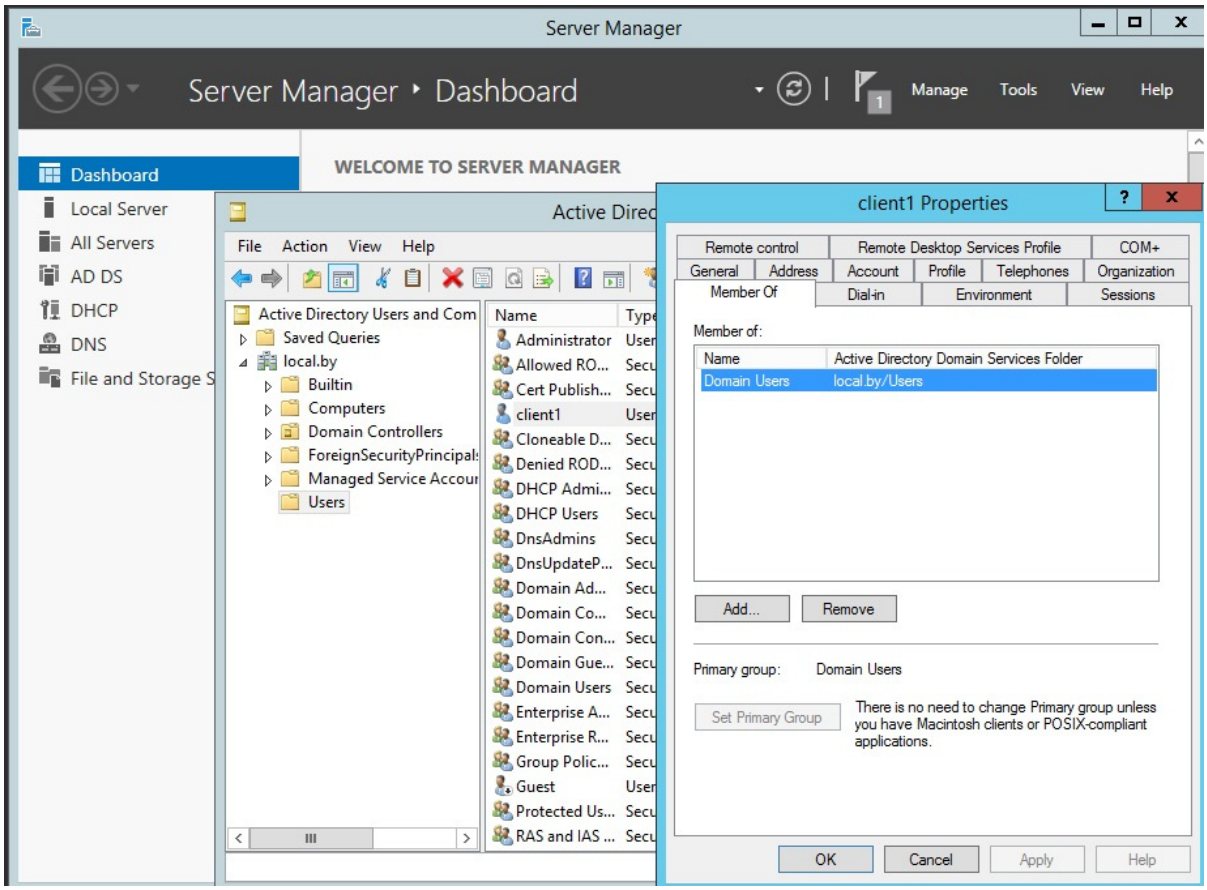

Рис. 3.26. Проверка принадлежности пользователя к группе

Необходимо отметить, что заполнение данных полей не является обязательным, однако при построении реальной системы с большим числом пользователей рекомендуется.

Организационные подразделения (*Organization Unit*) создаются аналогично другим объектам домена (пользователи, группы пользователей) (рис. 3.27). Они являются объектами контейнерного типа, а значит, в них, равно как и в группах пользователей, можно создавать учетные записи пользователей.

Домашний каталог пользователя

1. Откройте свойства соответствующего пользователя.
2. Перейдите на вкладку *Профиль (Profile)* (рис. 3.28).
3. В поле *Profile Path (Путь к профилю)* введите сетевой путь к подготовленной домашней папке пользователя (ее целесообразно предварительно открыть в сеть с установлением всех необходимых прав через свойства файловой системы NTFS), например \\server1\profiles\%username%.
4. Щелкните *Apply (Применить)*и убедитесь, что вместо переменной %Username% было подставлено имя сервера. Важно, чтобы путь к профилю соответствовал фактическому сетевому пути к папке профиля.
5. Щелкните *OK*.

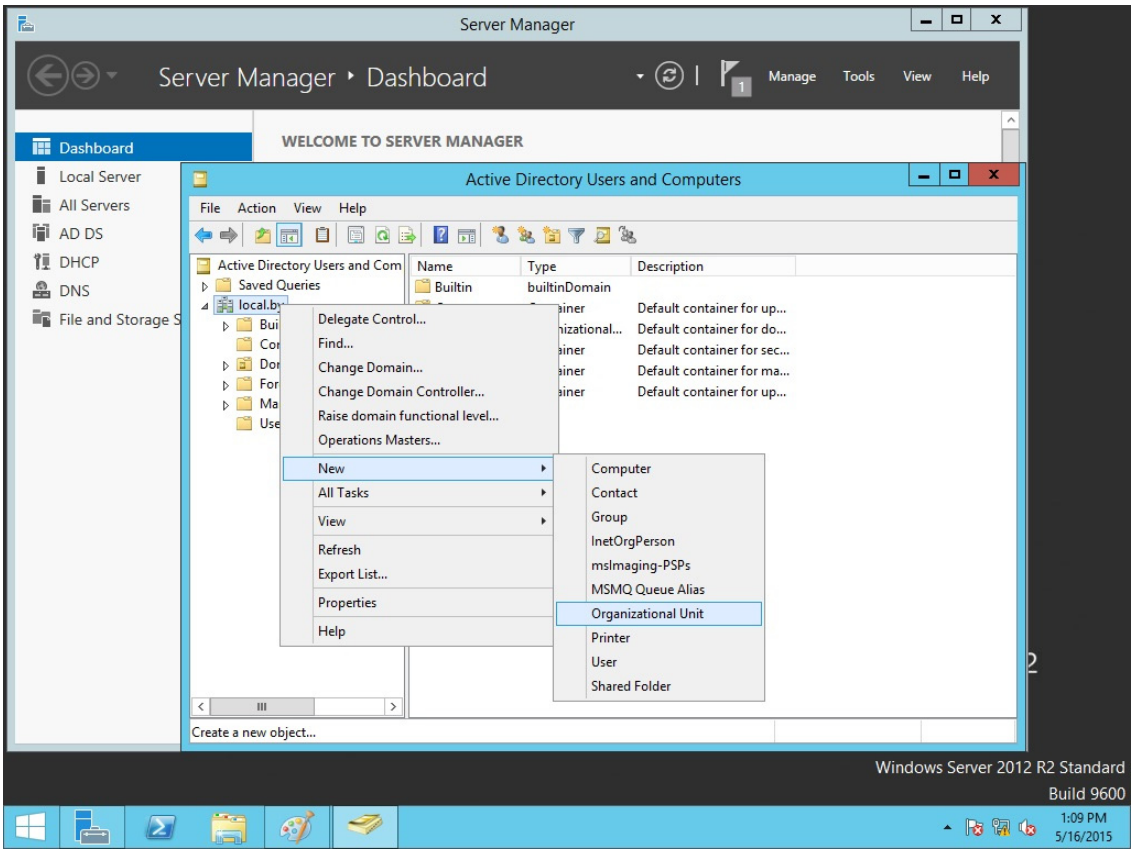

Рис. 3.27. Создание организационного подразделения

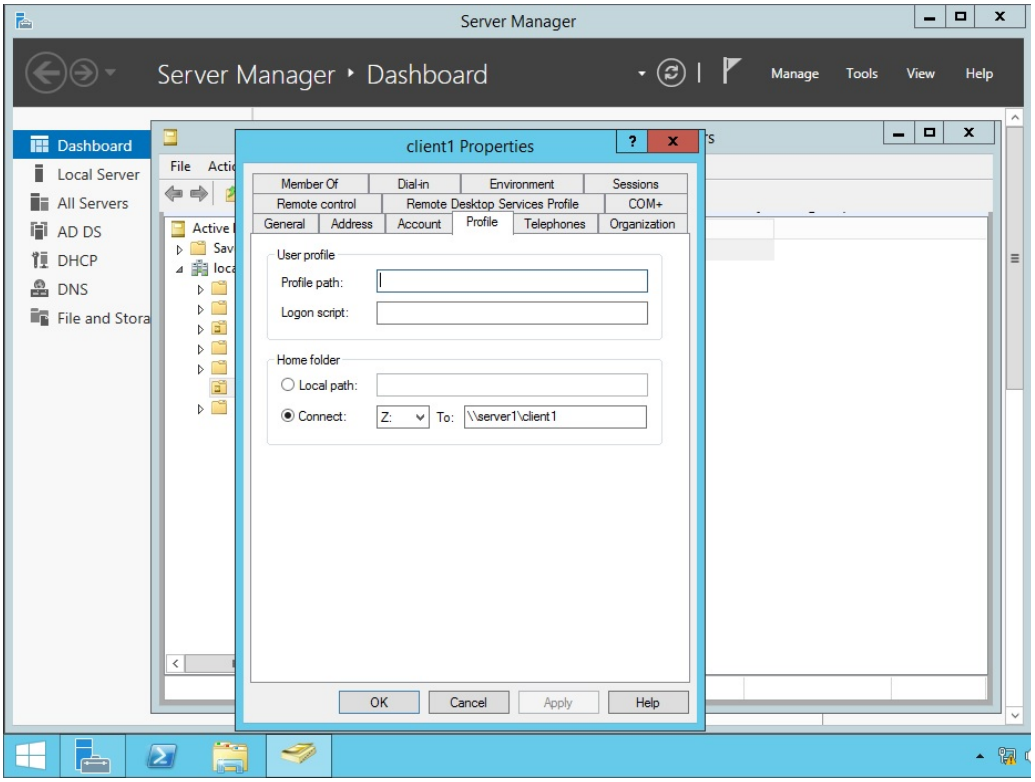

Рис. 3.28. Создание домашней папки пользователя

После входа пользователя на клиентской машине в данном случае ему будет автоматически подключен домашний каталог в виде сетевой папки (рис. 3.29).

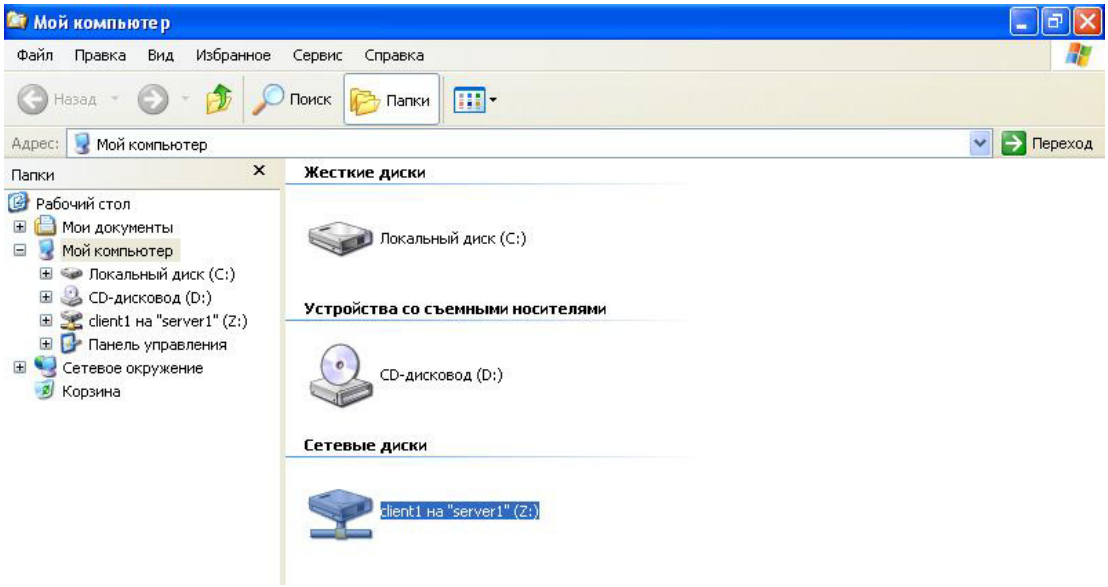

Рис. 3.29. Пример подключенной домашней папки пользователя в виде сетевого диска

Лабораторная работа № 5

Цель: создание и настройка домена, создание пользователей, подключение сетевых ресурсов.

Задание: лабораторная работа состоит из двух частей.

1. Установите на один из серверов службу каталога Active Directory (имя домена целесообразно использовать то же, что и DNS-суффикс, используемый в лабораторной работе № 4). Введите две клиентские машины в домен. Отметим, что в данной лабораторной работе второй сервер использоваться не будет.

2. Создайте двух пользователей (можно сделать так, чтобы они принадлежали разным организационным подразделениям, что будет полезным для следующих работ), а также настройте для каждого из них индивидуальные сетевые ресурсы (отметим, что сетевые папки для каждого из пользователей должны подключаться автоматически при входе пользователя в систему и быть доступны только пользователю).

НАДЕЖНОСТЬ ДОМЕННЫХ СИСТЕМ

4.1. Структура каталога Active Directory

Вся информация об объектах сети содержится в каталоге Active Directory. Физически эта база данных представляет собой файл **Ntds.dit,** который хранится на контроллере домена.

Каталог Active Directory может рассматриваться с двух позиций: с точки зрения логической структуры и с точки зрения физической структуры.

Логическая структура каталога Active Directory представлена на рис. 4.1. Цель такой структуризации – облегчение процесса администрирования.

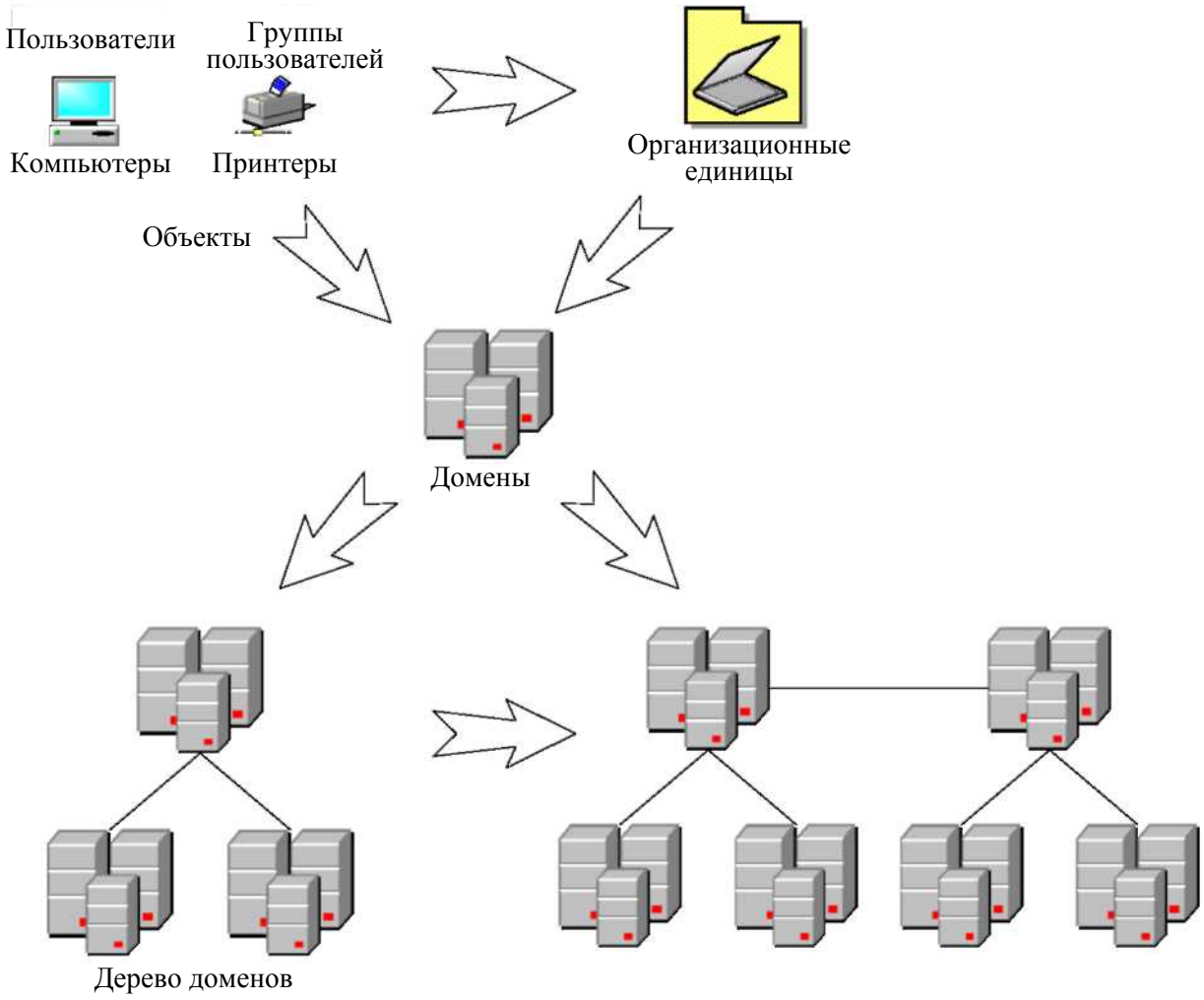

Рис. 4.1. Пример логической структуризации домена

Как говорилось выше, все сетевые объекты (пользователи, группы пользователей, компьютеры, принтеры) объединяются в домен, который является основной структурной единицей каталога. Для удобства управления объекты также могут быть сгруппированы при помощи *организационных подразделений (ОП)*. Несколько иерархически связанных доменов образуют *дерево доменов*. Совокупность деревьев, имеющих общие части каталога Active Directory и общих администраторов, называется *лесом доменов*.

Имея возможность такой логической структуризации, администратор может планировать и выбирать конфигурацию сети в зависимости от своих задач и масштабов организации.

Основной целью *физической структуризации* каталога Active Directory является оптимизация процесса копирования изменений, произведенных на одном из контроллеров домена, на все остальные контроллеры. Этот процесс называется *репликацией* (replication).

Основой физической структуры является *сайт* (site) – это часть сети, все контроллеры домена которой связаны высокоскоростным соединением. Между сайтами, наоборот, установлены более медленные линии связи (рис. 4.2).

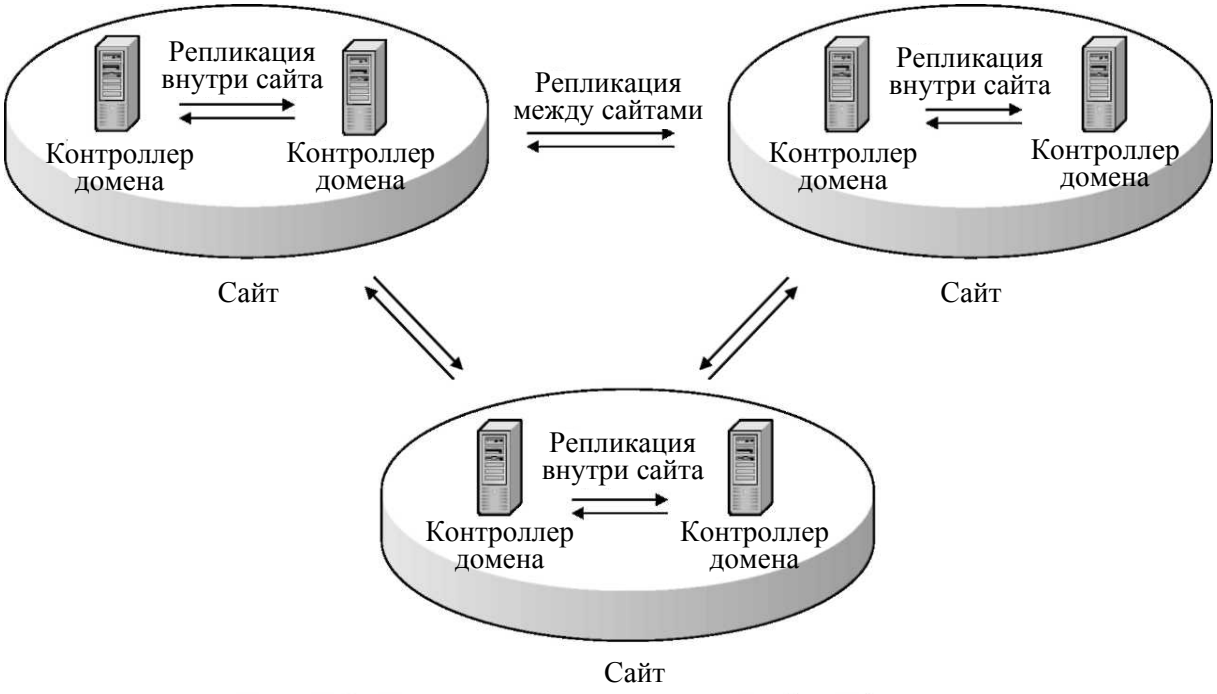

Рис. 4.2. Пример физической структуризации домена

Подобная структура позволяет планировать процесс репликации следующим образом: внутри сайта репликация осуществляется часто и могут передаваться большие объемы информации без сжатия; между сайтами изменения реплицируются редко и данные требуется сжимать.

Логическая и физическая структуры предназначены для решения разных задач и поэтому между собой практически не связаны: в одном домене может быть несколько сайтов, так же как один сайт может содержать несколько доменов. Общим объектом для той и другой структуры является контроллер домена с хранящимся на нем файлом каталога **Ntds.dit**.

В файле каталога Active Directory содержится информация как о логической, так и о физической структурах. Этот файл состоит из нескольких разделов:

− раздел домена (domain partition) – содержатся данные обо всех объектах домена (пользователях, компьютерах, принтерах и т. д.);

− раздел схемы (schema partition) – хранится информация о типах всех объектов, которые могут быть созданы в данном лесе доменов;

− раздел конфигурации (configuration partition) – описывается конфигурация леса доменов – информация о сайтах, соединениях между сайтами и направлениях репликации;

− раздел приложений (application partition) – специальный раздел для хранения данных приложений, не относящихся к службе Active Directory. По умолчанию здесь создается подраздел для службы DNS;

− раздел глобального каталога (global catalog partition). *Глобальный каталог* – это база данных, в которой содержится список всех объектов леса доменов без информации об атрибутах этих объектов. Глобальный каталог необходим для поиска ресурсов леса из любого принадлежащего ему домена.

В зависимости от принадлежности к разделу информация реплицируется между контроллерами доменов следующим образом:

− раздел домена реплицируется между контроллерами одного домена;

− разделы схемы, конфигурации и глобального каталога реплицируются на все контроллеры леса;

− репликацией раздела приложений можно управлять – указывать, какие контроллеры будут получать реплику данного раздела.

4.2. Планирование Active Directory

Успешная работа пользователей сетевых ресурсов, а также служб, реализующих протоколы TCP/IP, зависит от правильного функционирования Active Directory. Поэтому крайне важной становится задача планирования структуры каталога Active Directory. Удачно спроектированный каталог позволит сделать работу сети более эффективной и стабильной, а также намного облегчит труд администратора.

В процессе планирования Active Directory можно выделить два основных этапа (рис. 4.3):

1) планирование логической структуры, включающее проектирование доменов и организационных подразделений, а также проблему именования;

2) планирование физической структуры, состоящее из разделения сети на сайты и размещения контроллеров домена.

4.2.1. Планирование логической структуры

При *планировании доменной структуры* нужно определить количество и способ организации доменов. Возможны три варианта: единственный домен, дерево доменов или лес. Критерии выбора следующие.

1. Размер организации – один домен может содержать до сотен тысяч пользователей – не рекомендуется допускать превышение данного условного предела.

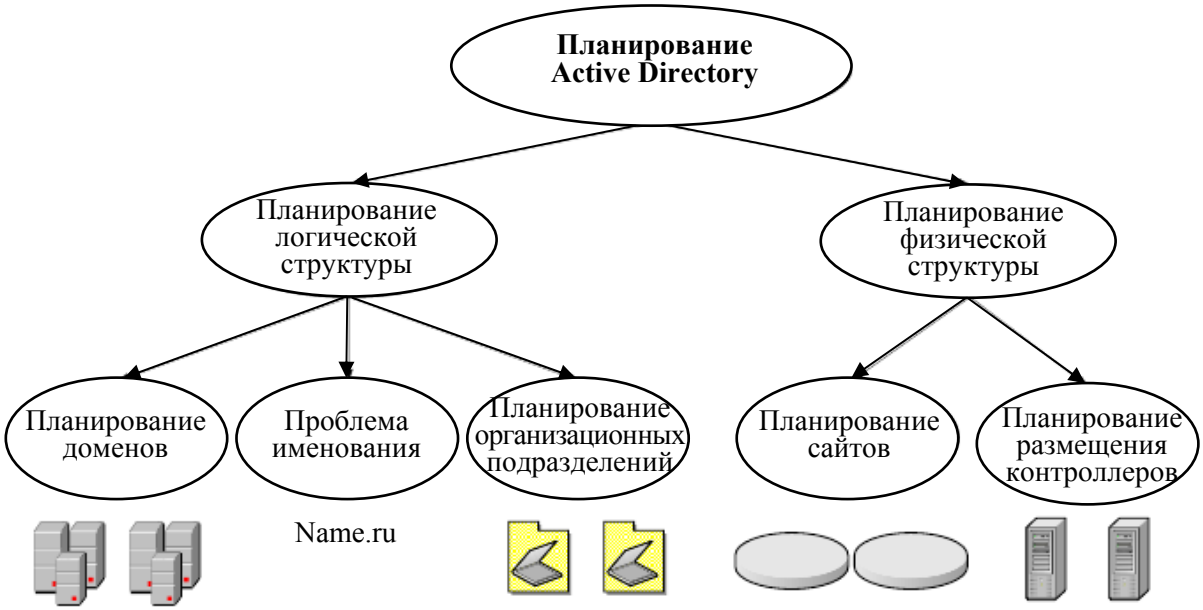

Рис. 4.3. Планирование Active Directory

2. Географическое расположение – имеются ли у организации филиалы или отделы, находящиеся на большом расстоянии и связанные с центральным звеном низкоскоростными каналами связи. Наличие таких филиалов при единственном в организации домене, скорее всего, вызовет перегрузку линий связи из-за трафика репликации.

3. Стабильность организации – насколько высока подвижность кадрового состава, не планируется ли в ближайшее время структурное преобразование организации.

4. Потребности в разных доменных именах – в некоторых случаях в рамках одной организации требуются разные доменные имена. Например, в случае создания единой компьютерной системы двух универси-

тетов каждый из них, вероятно, захочет иметь свое собственное доменное имя.

5. Способ управления сетью – может быть централизованным и децентрализованным. Централизованный способ предполагает сосредоточение всей административной власти у единого коллектива администраторов и наличие однодоменной модели. При децентрализованном способе полномочия делегируются нескольким слабосвязанным удаленным группам администраторов, управляющих доменами дерева или леса.

6. Единство политики безопасности. Чаще всего политика безопасности в одной организации едина для всех отделов и сотрудников, однако бывают исключения.

Исходя из перечисленных критериев, можно выделить те признаки, по которым выбирается вариант с одним доменом:

1) в организации менее сотни тысяч пользователей;

2) отсутствие удаленных филиалов;

3) относительная стабильность структуры организации;

4) отсутствие потребности в разных доменных именах;

5) централизованный способ администрирования;

6) единая политика безопасности.

Отсутствие первых четырех признаков существенно склоняет выбор в пользу многодоменной модели. Последние два признака в меньшей степени должны влиять на выбор, так как задачи делегирования администрирования и разделения политик безопасности можно решить средствами организационных подразделений в рамках одного домена.

При выборе модели с несколькими доменами в большинстве ситуаций нужно использовать дерево доменов. Лес доменов приемлем в том случае, когда две независимые организации хотят иметь общие сетевые ресурсы.

После выбора доменной структуры следует продумать *имена для создаваемых доменов.* Особенно важно имя корневого домена. Правил для выбора доменного имени немного: во-первых, оно должно отражать специфику организации, во-вторых, быть понятным всем пользователям ресурсов домена, а не только администратору, и в-третьих, не должно быть слишком сложным. Для имени очень часто используют аббревиатуры, например bstu и т. д.

Планирование структуры организационных подразделений в каждом домене является важным шагом.

Как отмечалось в предыдущей теме, ОП применяются в том случае, если для задач управления группой объектов или делегирования административных прав образование новых доменов нецелесообразно.

В связи с тем что организационные подразделения можно использовать в качестве контейнеров, допускается строить иерархию ОП с несколькими уровнями вложений.

Иерархию можно строить с помощью двух основных подходов: либо следуя организационной структуре предприятия *(организационный подход)*, либо исходя из задач управления сетевыми объектами *(административный подход)*. Оба способа используются на практике, и задача администратора состоит в том, чтобы выяснить, какой из подходов (или их комбинация) применим в данной ситуации.

4.2.2. Планирование физической структуры

Основная цель планирования физической структуры – оптимизация трафика репликации. Цель достигается путем продуманного расположения сайтов и контроллеров домена.

Основной объем данных репликации присутствует в рамках одного домена, междоменный же трафик репликации существенно ниже внутридоменного. Для оптимизации процесса репликации рекомендуется использовать механизм сайтов.

На начальном этапе следует проанализировать существующую сеть – ее структуру, количество пользователей и компьютеров, пропускную способность, колебания трафика. Все эти данные нужно учитывать при планировании. Чем больше пользователей и компьютеров в сети, тем больше объем передаваемой информации при репликации. Линии с большой пропускной способностью могут быть сильно загружены, и большой трафик репликации внесет существенные проблемы, в то время как низкоскоростные каналы, возможно, практически свободны и выдержат дополнительный объем данных репликации.

Во время анализа следует учитывать возможность расширения сети и увеличения числа пользователей. Считается достаточным принимать коэффициент расширения в пределах 30–50%.

Основной критерий при выделении сайтов – пропускная способность линий связи. Части домена, связанные высокоскоростными линиями, помещаются в один сайт. Если между частями домена имеются каналы с низкой скоростью передачи данных, их следует разместить в разных сайтах. При этом трафик межсайтовой репликации сжимается и его передача происходит во время наименьшей загрузки низкоскоростных линий.

Вопрос о необходимом количестве и размещении контроллеров домена решается тогда, когда известна доменная структура и расположение сайтов. Общее правило таково, что для каждого домена необходимо не менее двух контроллеров (при этом в случае отказа одного из контроллеров второй обеспечит работу сети). Количество контроллеров зависит от числа

пользователей (а следовательно, от числа обращений на контроллеры домена), принадлежащих данному домену или сайту. Например, если домен включает два сайта, связанных модемной линией, и к одному из сайтов принадлежит всего несколько пользователей, то совсем не обязательно в этом сайте располагать отдельный контроллер домена (при условии, что загрузка модемной линии невысока).

4.3. Настройка репликации

Если ранее не был установлен домен (служба Active Directory) на ваш второй сервер, то пункт 4.3.1 можно пропустить.

4.3.1. Удаление Active Directory и установка второго контроллера домена

1. Если на втором сервере уже установлена служба Active Directory, то ее надо удалить. На соответствующем компьютере запустите программу *Server Manager (Управление сервером)* и щелкните по *Manage – Remove role and features*. Далее начнется процесс удаления выбранной роли сервера, по шагам аналогичный процессу установки, поэтому подробно рассматривать его не будем. Запустите удаление домена.

2. После окончания удаления Active Directory откажитесь от немедленной перезагрузки, откройте свойства своего сетевого соединения и укажите в свойствах TCP/IP в поле *Primary DNS Server* IP-адрес первого сервера (отметим, что данная операция, возможно, была уже сделана при настройке вторичного DNS-сервера). Произведите перезагрузку вашего компьютера.

3. После окончания перезагрузки еще раз запустите *Server Manager (Управление сервером)* и запустите установку роли Active Directory, как рассматривалось в разделе 3.7.

4. На экране *Deployment Configuration* установите переключатель в положение *Additional domain controller for an existing domain (Вторичный контроллер домена в существующем лесе)* и нажмите *Next (Далее)* (рис. 4.4).

5. На последующих шагах введите имя пользователя local\Administrator и пароль в соответствующее поле. Также необходимо ввести DNS имя домена (в рассматриваемом примере это Local.by). Остальные предлагаемые параметры можно оставить по умолчанию.

6. На соответствующем шаге (*Directory Services Restore Mode Administrator Password*) введите два раза пароль для режима восстановления Active Directory. Нажмите на кнопку *Next* на этом и следующих экранах и произведите установку Active Directory. По окончании установки перезагрузите компьютер.

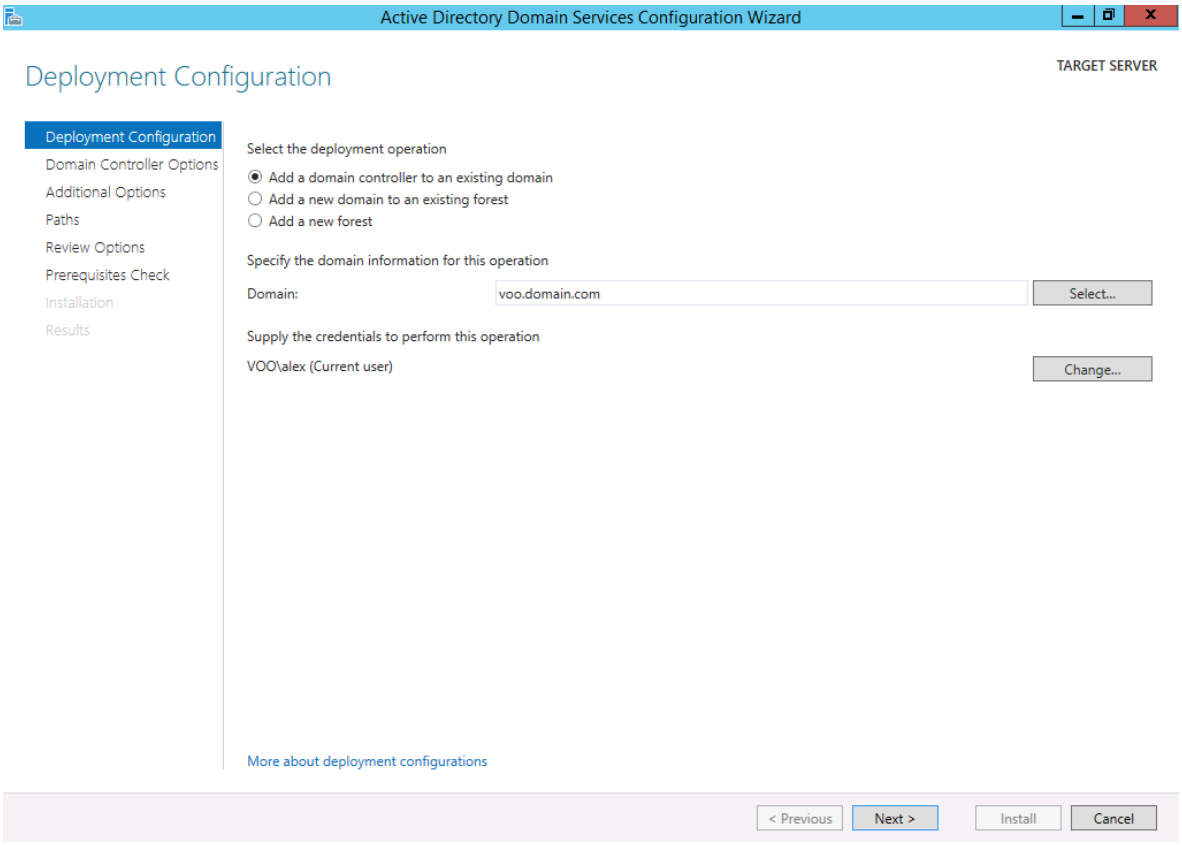

Рис. 4.4. Выбор создания вторичного контроллера домена

Таким образом был создан второй контроллер домена, которые будет вторичным к основному. Между ними будут реплицироваться любые изменения, происходящие на любом из контроллеров, например создание либо удаление пользователей и т. д.

4.3.2. Создание системы сайтов Active Directory и настройка расписания репликации

Пусть необходимо создать в вашем лесу второй сайт, который будет называться Site2, и поместить в него второй контроллер домена. Настройте расписание репликации между сайтами таким образом, чтобы оно выполнялось только в определенный (удобный для вас) промежуток времени.

1. Откройте консоль *Active Directory Sites and Services*. Щелкните правой кнопкой мыши по контейнеру *Sites* и в контекстном меню выберите *New Site*. Введите имя создаваемого сайта – Site2, в списке соединений – Site Link выберите единственный имеющееся соединение – DEFAULTSITELINK и нажмите *OK*.

2. Раскройте узел *Sites – Default First Site Name – Servers*, щелкните правой кнопкой мыши по объекту второго контроллера домена, в контекстном меню выберите *Move*, в списке *Site Name* выберите Site2 и нажмите *OK*.

3. Раскройте узел *Inter-Site Transports*, раскройте узел IP, щелкните правой кнопкой мыши по объекту DEFAULTIPSITELINK в правой части экрана и в контекстном меню выберите *Properties*.

4. На вкладке *General* свойств DEFAULTIPSITELINK нажмите на кнопку *Change Schedule*, выделите весь прямоугольник и установите переключатель в положение *Replication Not Available*. Затем выделите столбец, соответствующий времени репликации, и установите для него переключатель в положение *Replication Available*. Нажмите на кнопку *OK* два раза и закройте консоль *Active Directory Sites and Services*.

Лабораторная работа № 6

Цель: изучение методов обеспечения надежного функционирования доменной системы (путем настройки репликации контроллеров доменов).

Задание: выполнить настройку репликации контроллеров доменов двумя способами (с использованием вторичных контроллеров, т. е. внутридоменная репликация и репликация между сайтами).

Тема 5

УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ

5.1. Групповые политики

С увеличением парка компьютеров в сети все более остро встает вопрос о стоимости его управления и содержания. Ручная настройка компьютеров отнимает немало времени у администраторов и персонала и заставляет с увеличением количества компьютеров увеличивать штат обслуживающего их персонала. К тому же при большом количестве машин следить за соблюдением принятых на предприятии стандартов настройки становится все труднее. Групповые политики (Group Policy) являются комплексным инструментом централизованного управления компьютерами с ОС Windows Server в домене Active Directory. К компьютерам под управлением устаревших ОС Windows типа 95, 98, ME групповые политики не применяются: они управляются системными политиками (System Policy), которые в рамках данного раздела рассматриваться не будут.

5.1.1. Объекты групповых политик

Групповые политики (*Group Policy*) – это способ автоматизации работы по настройке рабочих столов пользователей и параметров компьютеров. Групповые политики представляют собой наборы правил конфигурирования, применяемых к компьютеру или пользователю. Каждый такой набор правил называется *объектом групповой политики* (*Group Policy Object, GPO*).

Один или несколько объектов групповой политики могут применяться к трем видам объединений:

− сайтам;

− доменам;

− организационным подразделениям.

Кроме того, для каждого компьютера может быть определен *объект локальной групповой политики* (*Local Group Policy Object, LGPO*).

Объекты групповых политик являются наследуемыми. Это означает, например, что GPO, применяемый к домену, наследуется всеми его организационными подразделениями. В том случае если правила одного объекта групповой политики конфликтуют с правилами другого, наибольший приоритет имеет GPO организационного подразделения, ниже по уровню GPO домена, затем следует GPO сайта, наименьший приоритет у LGPO.

Приведем краткий обзор возможностей, предоставляемых групповыми политиками (рис. 5.1).

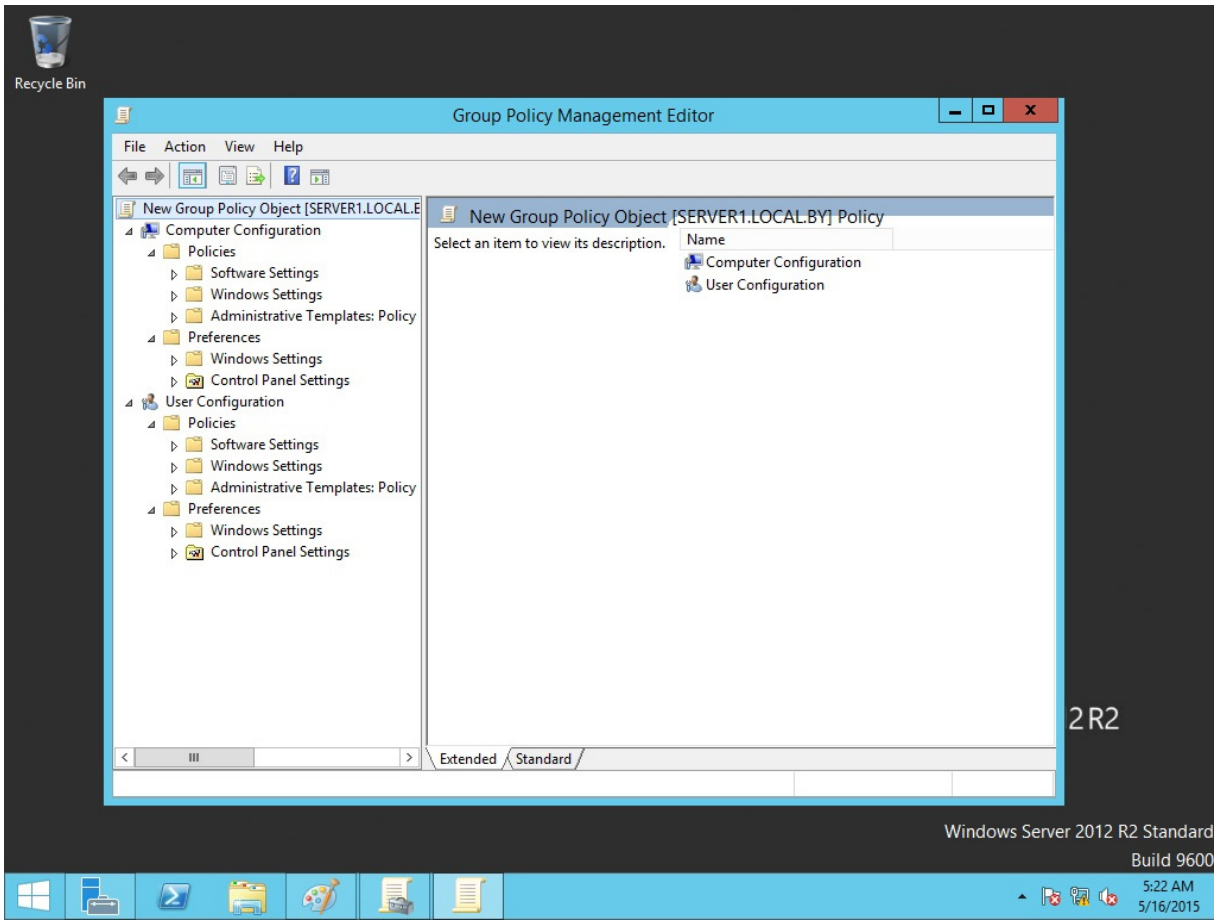

Рис. 5.1. Пример консоли для настройки объекта групповой политики

Объект групповой политики содержит две основные части:

− *Конфигурация компьютера (Computer Configuration)*;

− *Конфигурация пользователя (User Configuration)*.

Каждая из частей включает три раздела:

− *Настройки приложений (Software Settings)*;

− *Настройки Windows (Windows Settings)*;

− *Административные шаблоны (Administrative Templates)*.

В разделе *Настройки приложений* находится подраздел *Установка приложений* (*Software Installation*), позволяющий автоматически устанавливать выбранные программы на компьютеры пользователей.

Правила, создаваемые в разделе *Настройки Windows*, позволяют:

– выполнять задаваемые сценарии (*Scripts*) при включении-выключении компьютера, при входе пользователя в систему и выходе из нее;

– настраивать параметры безопасности (*Security Settings*) компьютера и пользователя (требования к паролям, доступ к реестру, политику аудита событий);

– конфигурировать Internet Explorer (*Internet Explorer Maintenance*);

– изменять места расположения папок пользователей (*Folder Redirection*).

Раздел *Административные шаблоны* предназначен для настройки рабочего стола пользователя, ограничения доступа к системным компонентам и компонентам приложений.

Таким образом, Windows Server предоставляет мощный набор инструментов администрирования, способствующий эффективному управлению сети любой организации.

5.1.2. Создание объекта групповой политики

Для того чтобы создать политику (т. е. фактически создать новый объект групповой политики), открываем соответствующую консоль управления (в коммандной строке набираем gpmc.msc (рис. 5.2)) и выбираем созданное ранее организационное подразделение (в нашем примере это user_group1, либо создаем новое с добавлением туда нужных пользователей), для которого создаем новый объект GPO (Group Policy Object) (рис. 5.3), также задаем ему название (можно оставить дефолтное) (рис. 5.4). Создавать и привязывать объект групповой политики можно только к объекту сайта, домена или организационному подразделению.

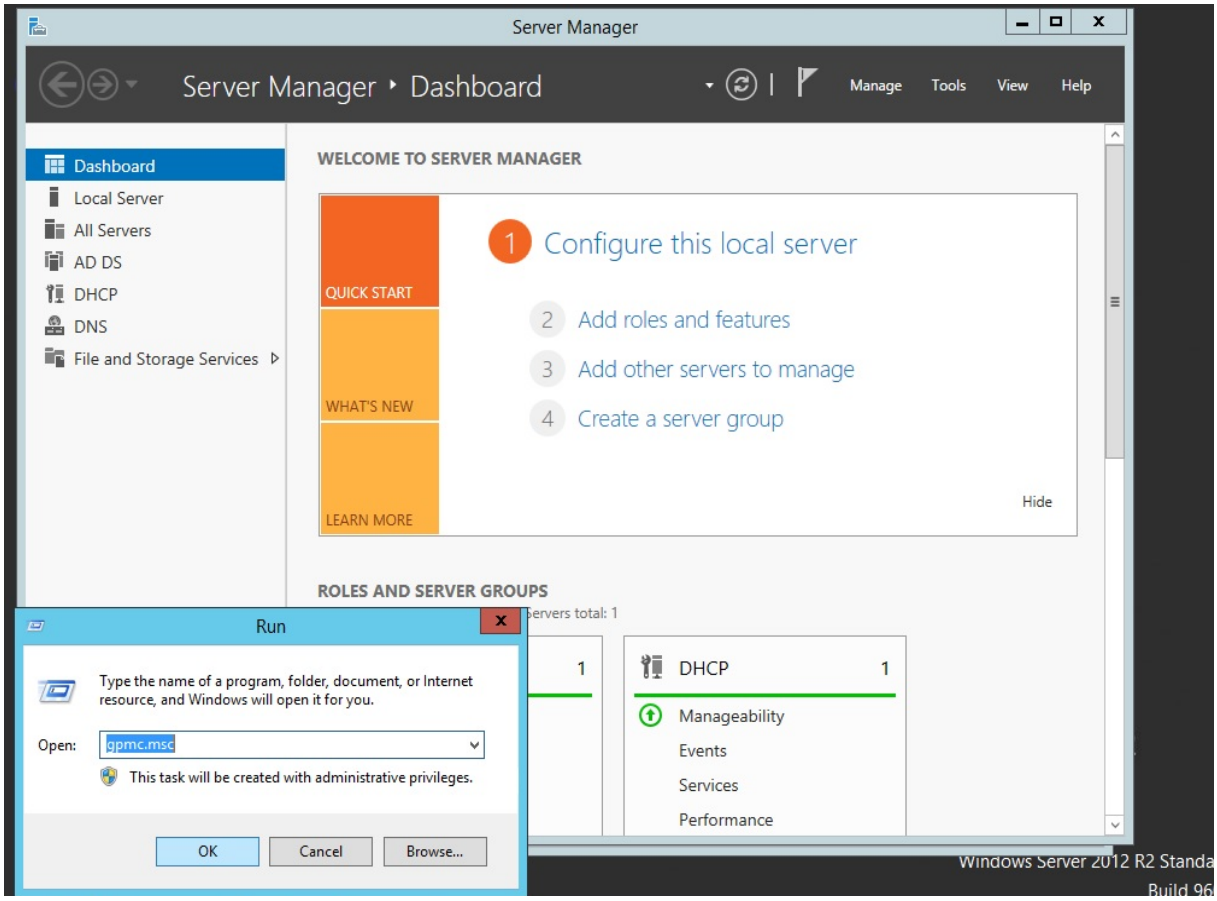

Рис. 5.2. Вызов консоли настройки групповой политики

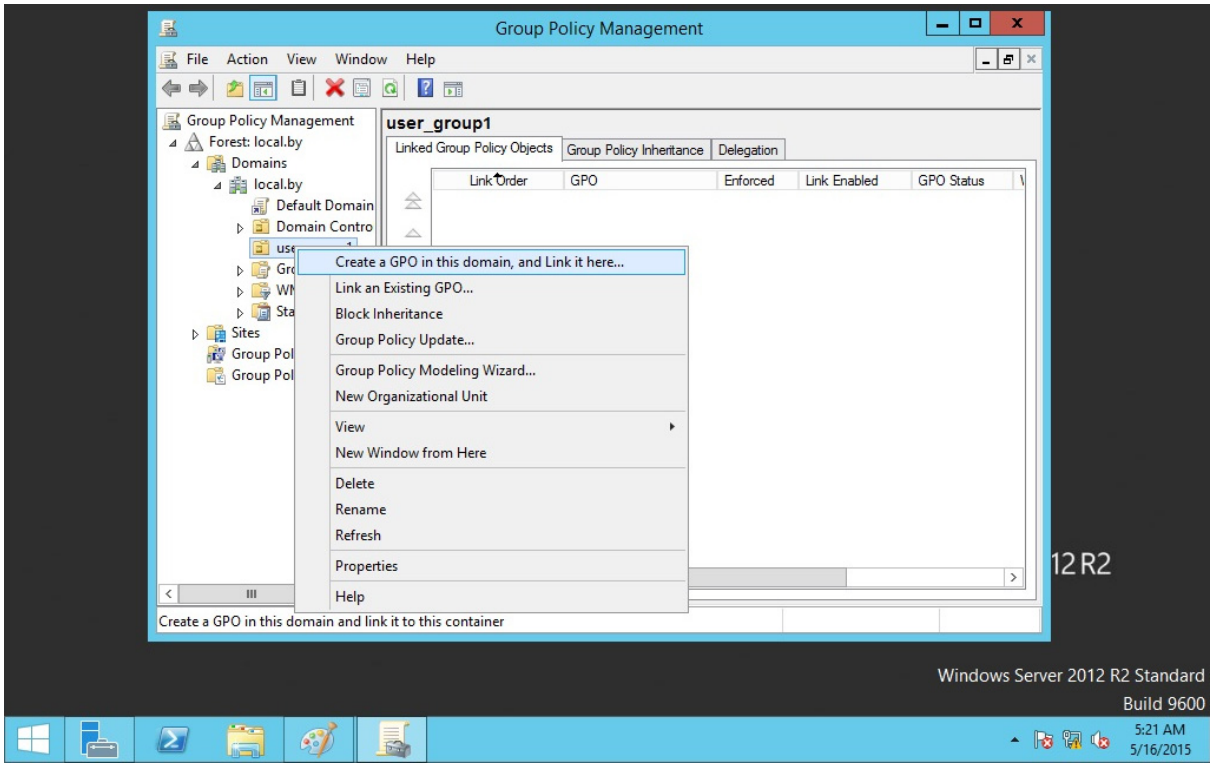

Рис. 5.3. Создание объекта групповой политики
для организационного подразделения

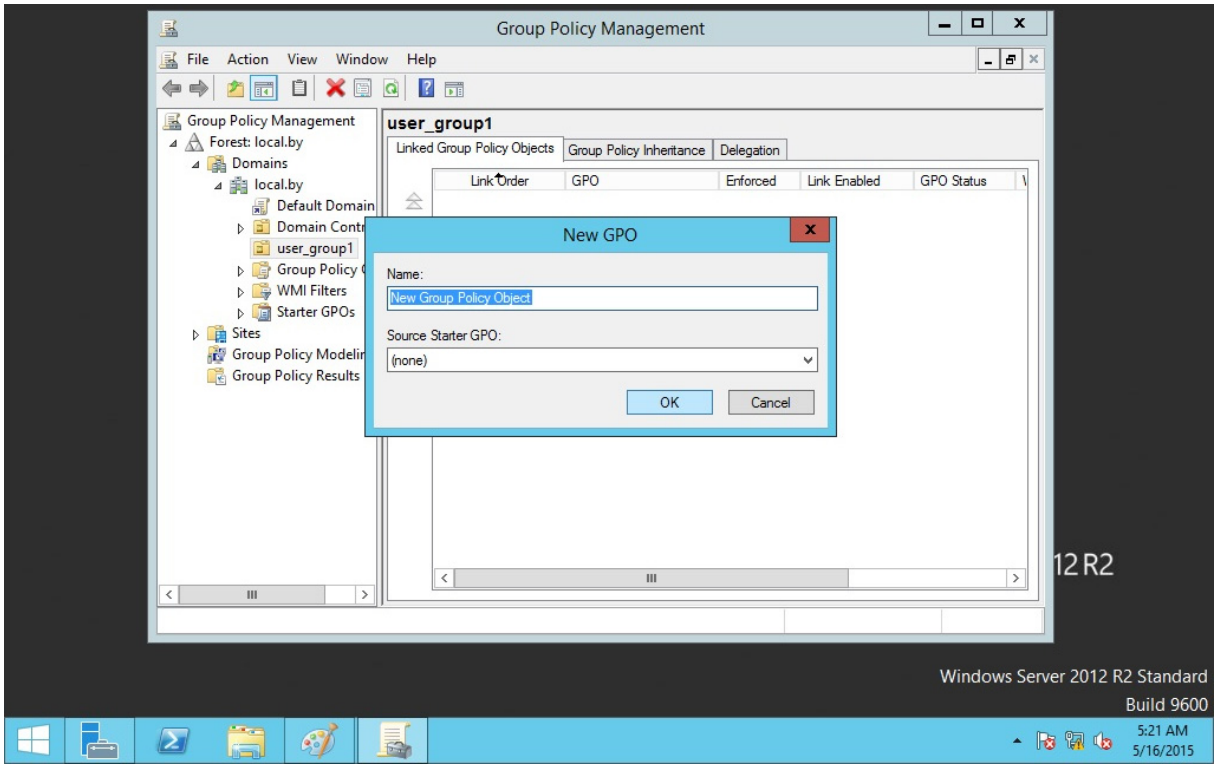

Рис. 5.4. Название объекта групповой политики

Далее фактически необходимо отредактировать (настроить) созданный объект групповой политики (рис. 5.5).

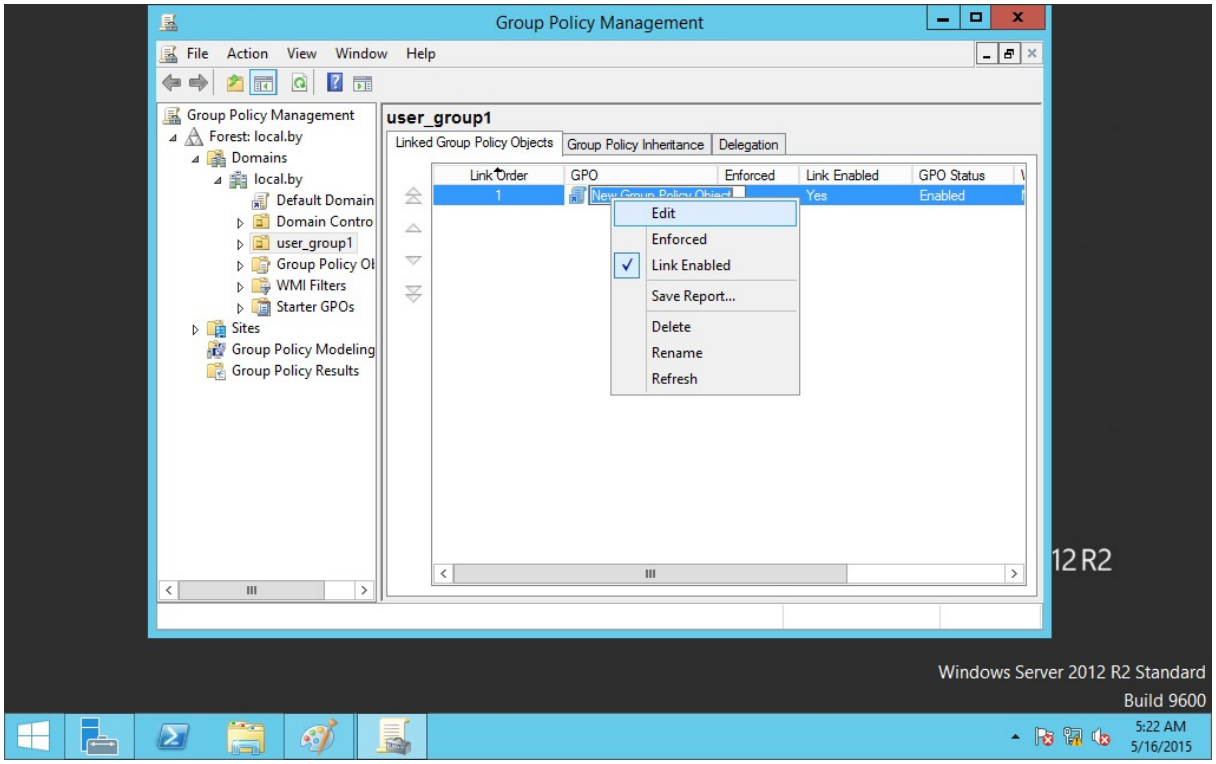

Рис. 5.5. Редактирование (настройка) объекта групповой политики

При выборе команды *Edit* из контекстного меню откроется окно редактора GPO, где вы можете настроить конкретные параметры объекта (рис. 5.6). Отметим, что целесообразно выполнять настройки конфигурации пользователя (user configuration). В таком случае пользователь независимо от места входа в домен (независимо от компьютера) будет получать всегда одни и те же настройки, права, ограничения.

Большинство основных настроек интуитивно понятны (к тому же имеют описание, если открыть соответствующую вкладку), и поэтому не будем подробно останавливаться на каждой. Приведем лишь один пример. Пусть необходимо воспользоваться «белым списком» для запрета запуска всех приложений, кроме тех, что находятся в списке разрешенных. Для этого воспользуемся политикой, показанной на рис. 5.7. При этом данную политику нужно включить и настроить соответствующим образом. На рис. 5.8 приведена настройка запрета запуска всех приложений, кроме mspaint.exe и iexplorer.exe. Корректность настроек можно проверить, войдя под соответствующим пользователем в домен на клиентской машине и попробовав запустить различные приложения.

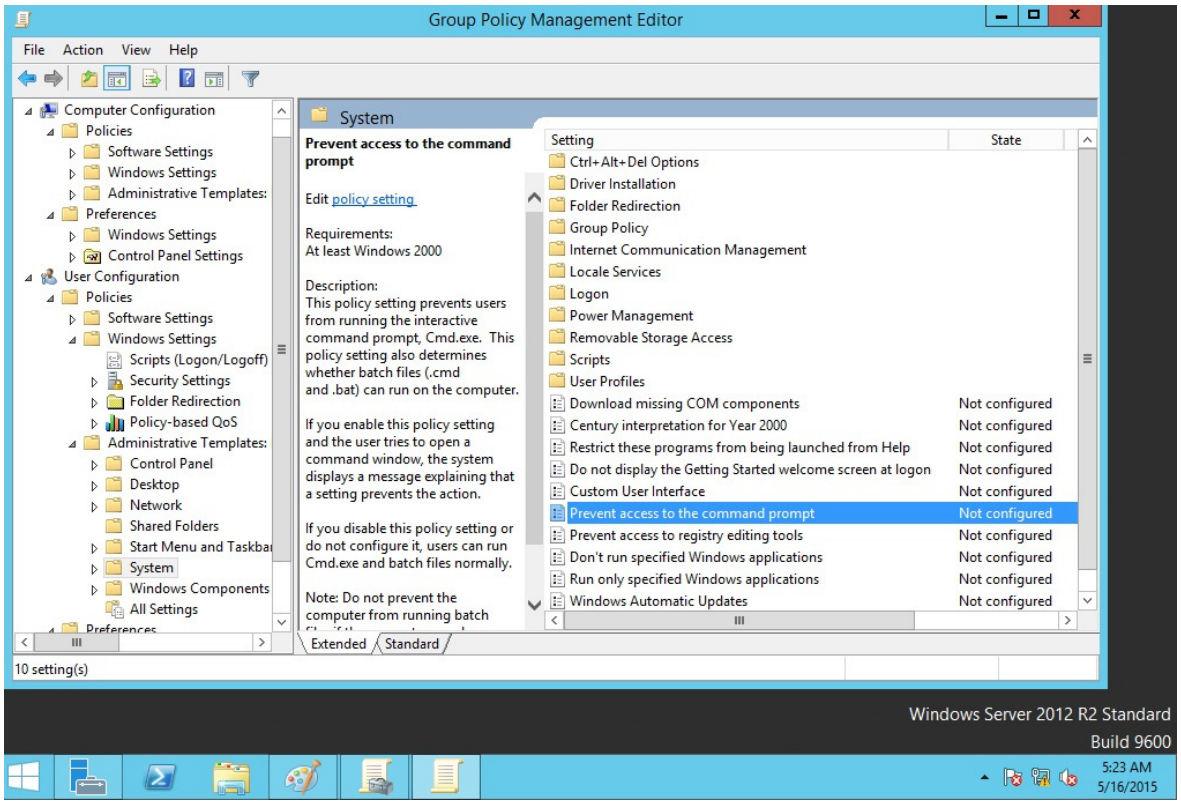

Рис. 5.6. Настройка объекта групповой политики

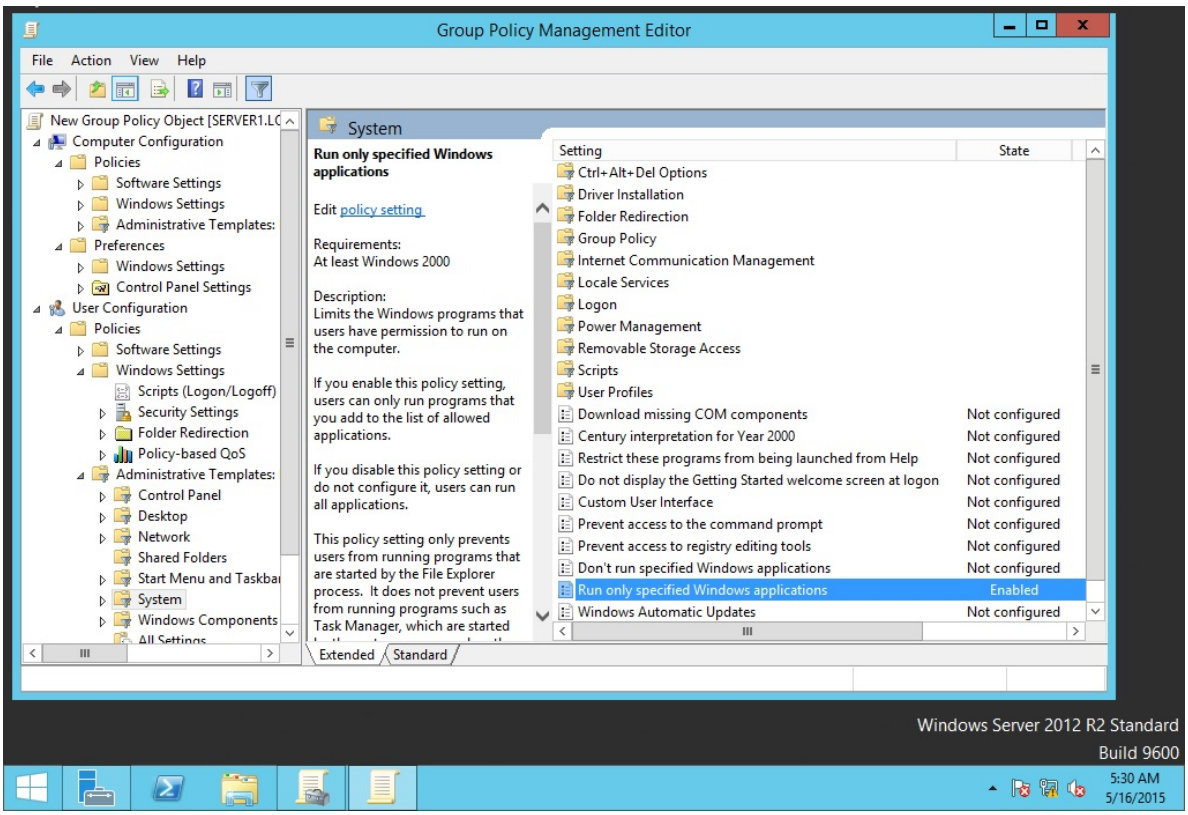

Рис. 5.7. Запрет запуска приложений с помощью GPO

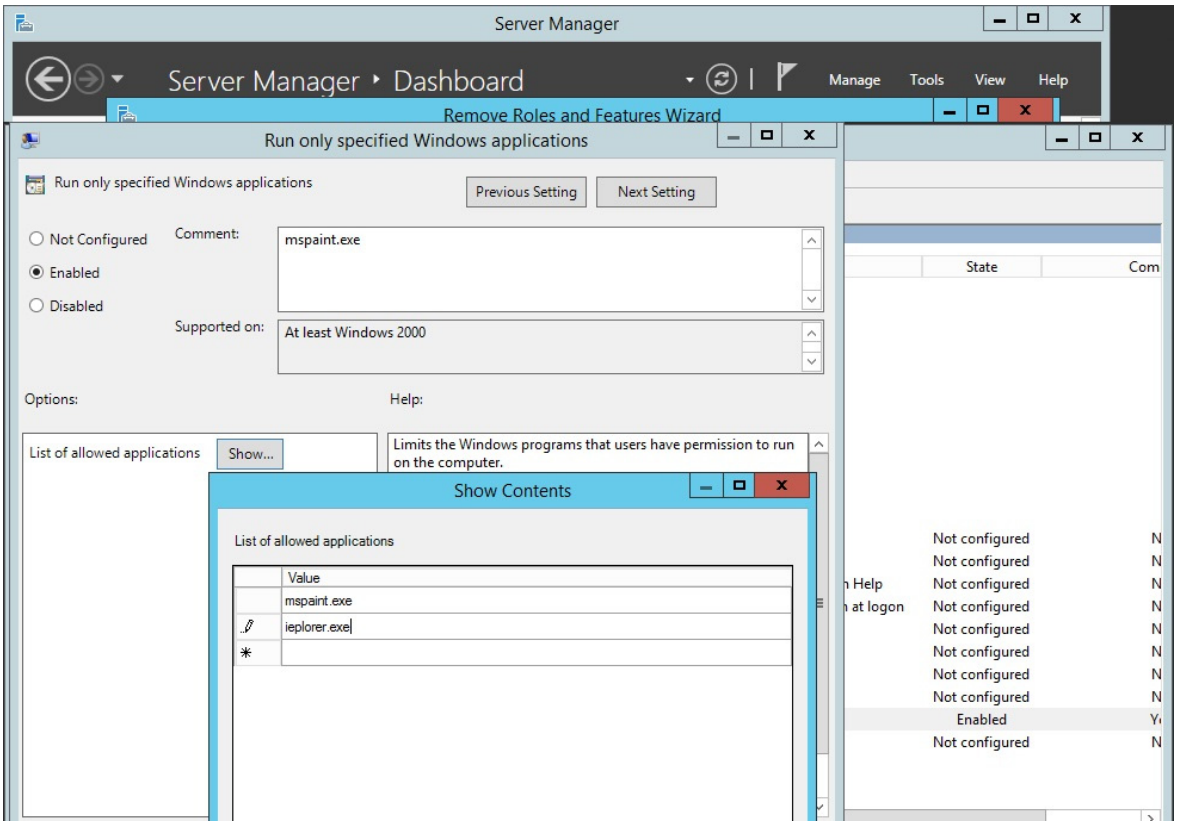

Рис. 5.8. Настройка политики запуска приложений

5.1.3. Порядок применения объектов групповой политики

Когда компьютер запускается, происходят следующие действия:

1) читается реестр и определяется, к какому сайту принадлежит компьютер. Делается запрос серверу DNS с целью получения IP-адресов контроллеров домена, расположенных в этом сайте;

2) получив адреса, компьютер соединяется с контроллером домена;

3) клиент запрашивает список объектов GP у контроллера домена и применяет их. Последний присылает список объектов GP в том порядке, в котором они должны применяться;

4) когда пользователь входит в систему, компьютер снова запрашивает список объектов GP, которые необходимо применить к пользователю, извлекает и применяет их.

Групповые политики применяются при загрузке ОС и при входе пользователя в систему. Затем они применяются каждые 90 минут с вариацией в 30 минут для исключения перегрузки контроллера домена в случае одновременного запроса большого количества клиентов. Для контроллеров домена интервал обновления составляет 15 минут. Изменить это поведение можно в разделе *Computer Configuration – Administrative Templates – System Group Policy*. Объект групповой политики может действовать только на объекты «компьютер» и «пользователь». Политика действует только на

объекты, находящиеся в объекте каталога (сайт, домен, организационное подразделение), с которым связан GPO и ниже по «дереву» (если не запрещено наследование).

GPO применяются в следующем порядке: локальные политики, политики уровня сайта, политики уровня домена, политики уровня OU.

Групповые политики применяются с некоторыми ОС Windows асинхронно, а с некоторыми синхронно, т. е. пользовательский экран входа появляется только после применения всех политик компьютера, а политики пользователя применяются до того, как появился рабочий стол. Асинхронное применение политик означает, что пользовательский экран входа появляется раньше, чем успевают примениться все политики компьютера, а рабочий стол – раньше, чем применятся все пользовательские политики, что приводит к ускорению загрузки и входа пользователя.

Описанное выше поведение изменяется в двух случаях. Первый – компьютер клиента обнаружил медленное сетевое подключение. Тогда по умолчанию применяются только параметры настройки защиты и административные шаблоны. Медленным считается подключение с пропускной способностью менее 500 Кб/сек. Изменить это значение можно в *Computer Configuration – Administrative Templates – System Group Policy – Group Policy slow link detection*. Также в разделе *Computer Configuration – Administrative Templates – System Group Policy* можно настроить некоторые другие параметры политик так, чтобы и они обрабатывались по медленному соединению. Второй способ изменения порядка применения политик – опция *User Group policy loopback processing*. Эта опция изменяет порядок применения политик по умолчанию, при котором пользовательские политики применяются после компьютерных и перезаписывают последние. Вы можете установить опцию loopback, чтобы политики компьютера применялись после пользовательских политик и перезаписывали все пользовательские политики, противоречащие политикам компьютера.

У параметра loopback есть 2 режима.

1. Merge (соединить) – сначала применяется компьютерная политика, затем пользовательская и снова компьютерная. При этом компьютерная политика заменяет противоречащие ей параметры пользовательской политики своими.

2. Replace (заменить) – пользовательская политика не обрабатывается.

Пояснить применение параметра *User Group policy loopback processing* можно, например, на общедоступном компьютере, на котором необходимо иметь одни и те же ограниченные настройки независимо от того, какой пользователь им пользуется.

5.1.4. Приоритетность, наследование и разрешение конфликтов

Как было уже отмечено, на всех уровнях объекты групповой политики содержат одинаковые параметры настройки, и один и тот же параметр может быть определен на нескольких уровнях по-разному. В таком случае действующим значением будет применившееся последним (о порядке применения объектов групповой политики говорилось выше). Это правило распространяется на все параметры, кроме определенных как not configured. Для этих параметров Windows не предпринимает никаких действий. Но есть одно исключение: все параметры настройки учетных записей и паролей могут быть определены только на уровне домена, на остальных уровнях эти настройки будут проигнорированы.

Если на одном уровне расположены несколько GPO, то они применяются «снизу вверх» по списку. Изменяя положение объекта политик в списке (стрелочками Up и Down), можно выбрать необходимый порядок применения (рис. 5.9).

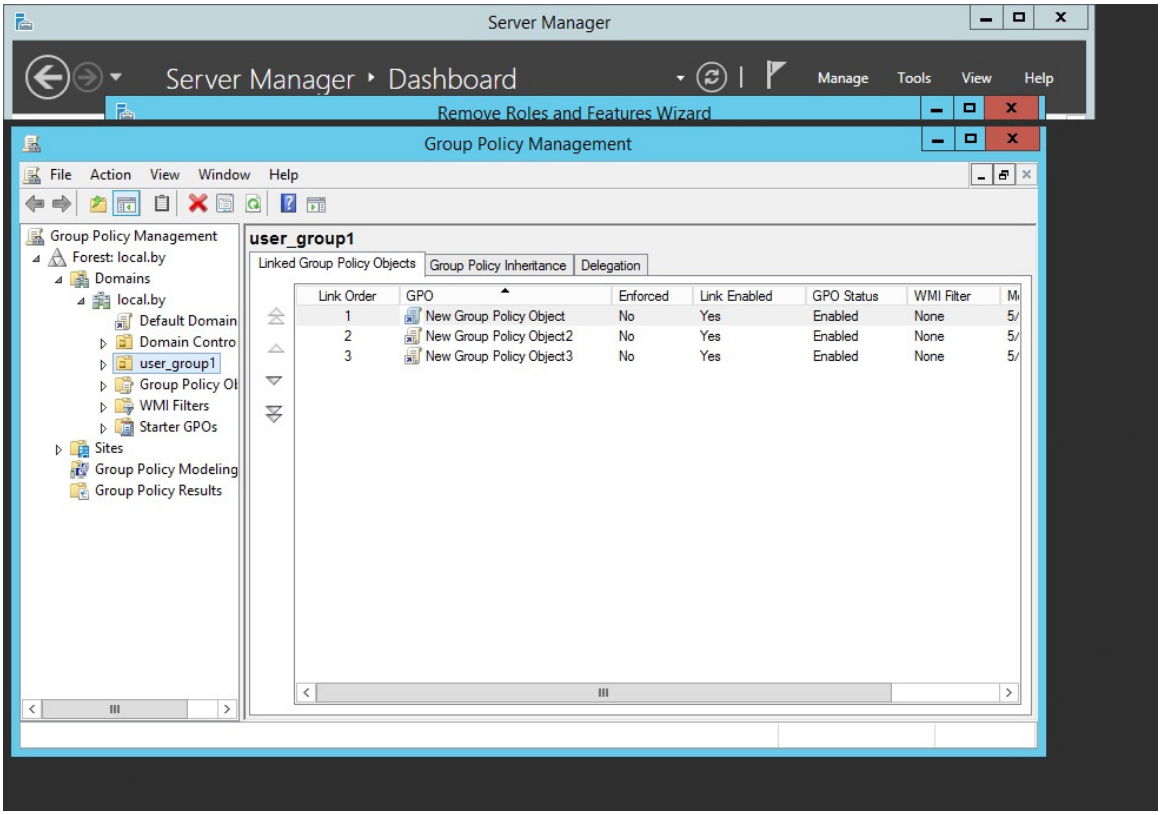

Рис. 5.9. Порядок применения политик

Отметим, что при помощи дополнительных параметров GPO можно сделать так, чтобы определенное OU не получало параметры политик от GPO, связанных с вышестоящими контейнерами. Фактически необходимо заблокировать наследование политик. При этом будут блокироваться все

наследуемые параметры политик, и нет способа блокировать отдельные параметры. Параметры настройки уровня домена, определяющие политику паролей и политику учетных записей, не могут быть заблокированы.

Лабораторная работа № 7

Цель: изучение методов удаленного администрирования с использованием групповых политик.

Задание: используя возможности Active Directory и групповых политик, выполнить создание двух организационных подразделений в рамках домена.

1. Первому организационному подразделению (с названием, например, power_users) запрещено:

– изменять конфигурацию IP-протокола;

– создавать, удалять и изменять настройки пользователей (например, пароль);

– устанавливать/удалять приложения;

– редактировать реестр.

2. Второму организационному подразделению (с названием, например, limited_users) запрещено:

– изменять конфигурацию IP-протокола;

– запускать диспетчер задач;

– запускать управление компьютером (computer managment);

– запускать апплеты панели управления;

– изменять настройки Internet Explorer;

– изменять настройки рабочего стола;

– использовать командную строку;

– создавать, удалять и изменять настройки пользователей (например, пароль);

– устанавливать/удалять приложения;

– редактировать реестр;

– запускать какие-либо приложения кроме тех, что в списке (список придумать самостоятельно и согласовать с преподавателем, например проводник, Internet Explorer), т. е. запрет в данном случае необходимо организовать по принципу «белого списка».

По желанию можно выполнить настройку и иных запретов/разрешений, например скрыть системные (локальные) диски клиентской ОС и т. д.

Отметим, что ограничения могут быть выполнены как за счет применения групповых политик, так и за счет принадлежности пользователя в определенной группе пользователей.

5.2. Удаленный рабочий стол

Подключение к удаленному рабочему столу

Подключение к удаленному рабочему столу (*Remote Desktop Connection*) – это клиентское приложение, используемое для подключения к серверу в контексте режима *Дистанционное управление рабочим столом* (Remote Desktop) или *Сервер терминалов* (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и старше, а также Windows Server программа *Подключение к удаленному рабочему столу* установлена по умолчанию, но «спрятана»: *Пуск* (*Start*) \ *Все программы* (*All Programms*) \ *Стандартные* (*Accessories*) \ *Связь* (*Communications*) \ *Подключение к удаленному рабочему столу* (*Remote Desktop Connection*).

На других платформах программу *Подключение к удаленному рабочему столу* можно установить с компакт-диска Windows Server либо из установочной папки клиента (% Systemroot %\ System32\Clients\Tsclient\ Win32) на любом из компьютеров под управлением Windows Server. Установочный пакет msi можно распространять на системы Windows с помощью групповой политики (будет рассмотрено в разделе 5.3).

На рис. 5.10 показан клиент программы *Дистанционное подключение к рабочему столу*, настроенный для подключения под пользователем client2 к серверу с именем Server1 (имя вашего компьютера может быть другим) в домене local.by (имя домена также может быть другим).

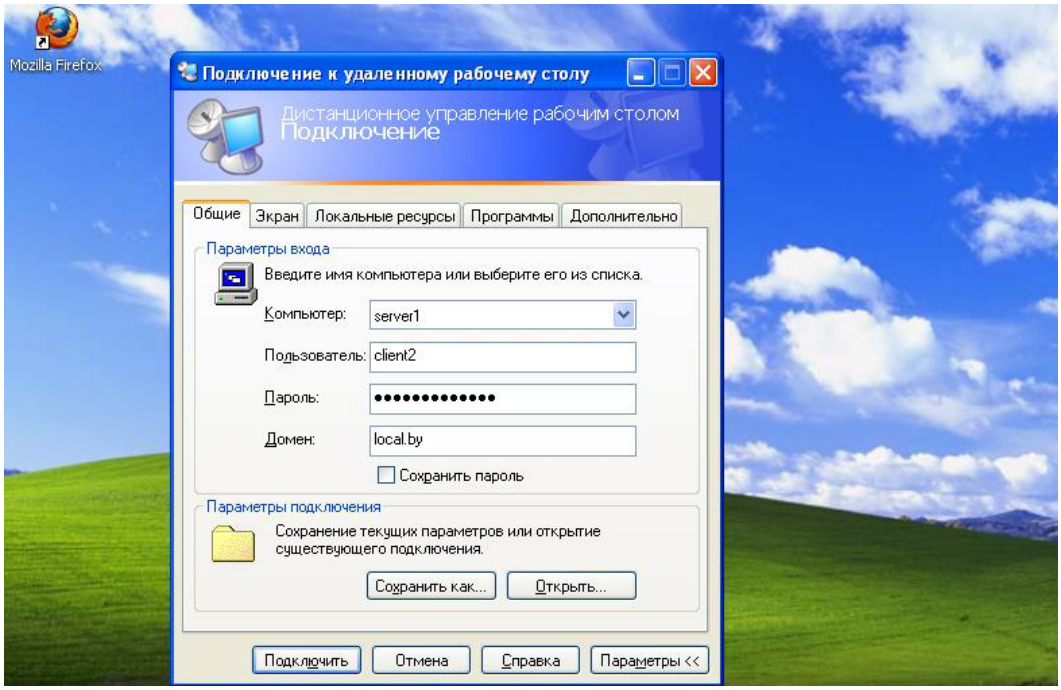

Рис. 5.10. Подключение к удаленному рабочему столу

Отметим, что до подключения на стороне сервера должны быть разрешены подобные операции, а также определены пользователи, кому можно выполнять удаленное подключение (рис. 5.11).

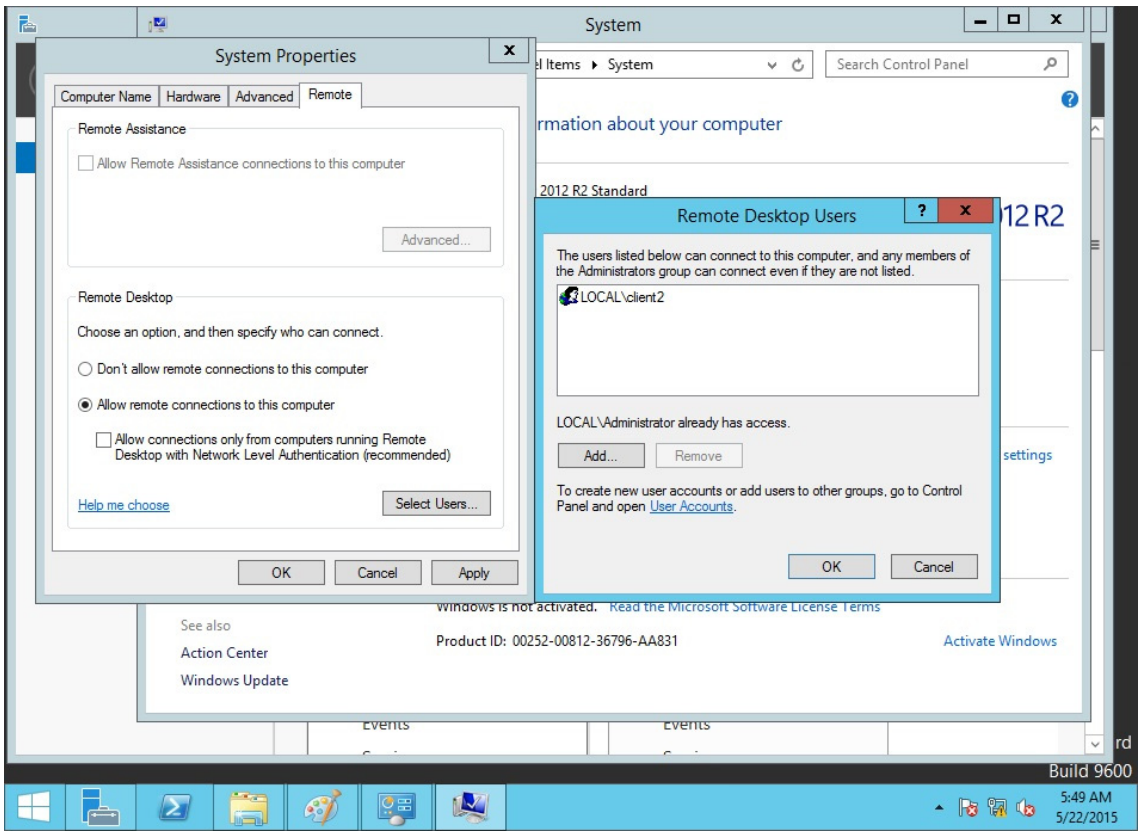

Рис. 5.11. Настройки, разрешающие подключение по удаленному рабочему столу

Настроив клиента удаленного подключения к рабочему столу и сервер, вы сможете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В следующей таблице перечислены конфигурационные параметры и их назначение.

Параметры программы
Удаленное подключение к рабочему столу

Параметры	Назначение
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться, настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задает размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме

Окончание таблицы

Параметры	Назначение
Локальные ресурсы (Local Resources)	Параметры передачи звуковых событий на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows (например, Alt + Tab), и доступны ли в сеансе удаленного доступа такие устройства, как локальные диски, принтеры и последовательные порты
Программы (Programs)	Задает путь и папки расположения для любых программ, которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании, визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом
Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой *Подключение к удаленному рабочему столу*
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом *Подключение к удаленному рабочему столу*, и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента *Дистанционное управление рабочим столом*
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network Adapters)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования
Общие (General)	Задает уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов

При использовании программы *Удаленный рабочий стол для администрирования* (*Remote Desktop for Administration*) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

1. Сбои сети. Ошибки в работе стандартной TCP/IP-сети могут вызывать сбои или разрывы подключений *Дистанционное подключение к рабочему столу* (*Remote Desktop*). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт *Служб терминалов* (*Terminal Services*) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.

2. Реквизиты входа. Для успешного подключения к серверу средствами программы *Удаленный рабочий стол для администрирования* пользователи должны быть включены в группу *Администраторы* (*Administrators*) или *Пользователи удаленного рабочего стола* (*Remote Desktop Users*).

3. Политика. Только администраторам разрешено подключаться средствами программы *Дистанционное подключение к рабочему столу* (*Remote Desktop*) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

4. Слишком много параллельных подключений. Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя. Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Управление настройками удаленного подключения осуществляется через консоль службы терминалов, которая устанавливается как роль сервера (*Remote Desktop Services* – компонент *Remote Desktop Licensing*) (рис. 5.12).

Наиболее интересным является настройка следующих параметров подключения к рабочему столу.

1. На вкладке *Сетевой адаптер* (*Network Adapter*) установите значение параметра *Максимальное число подключений* (*Maximum Connections*) равным 1.

2. На вкладке *Сеансы* (*Sessions*) установите оба флажка *Заменить параметры пользователя* (*Override User Settings*) и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия:

− завершение отключенного сеанса (End a disconnected session): 15 минут;

− ограничение активного сеанса (Active session limit): никогда (never);

− ограничение пассивного сеанса (Passive session limit): 15 минут;

− при превышении ограничений или разрыве подключения (When session limit is reached or connection is broken): Отключить сеанс (Disconnect from session).

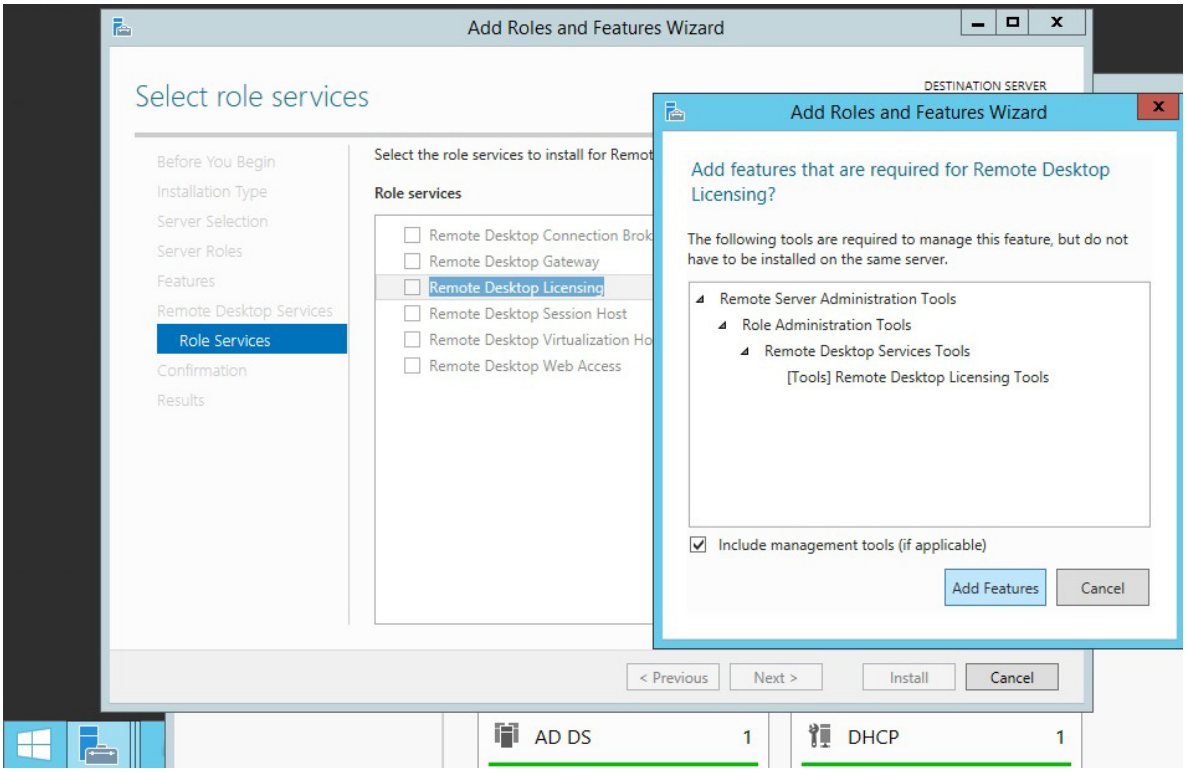

Рис. 5.12. Установка службы терминалов

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы *Удаленный рабочий стол для администрирования* (*Remote Desktop for Administration*).

Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На другом удаленном компьютере (виртуальной машине) в группе *Стандартные\Связь* (*Accessories\Communications*) щелкните *Подключение к удаленному рабочему столу* (*Remote Desktop Connection*), подключитесь к Server1 и войдите в его систему.

2. На сервере Server1 откройте консоль tscc.msc: *Администрирование* (*Administrative tools*)*Настройка служб терминалов* (*Terminal Services Configuration*). В открывшейся консоли выберите *Подключения* (*Connections*). Вы должны увидеть сведения о сеансе удаленного подключения к Server01.

3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы *Удаленное подключение к рабочему столу* (Remote Desktop), не завершив сеанс *Сервера терминалов* (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к Server1 удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Лабораторная работа № 8

Цель: изучение методов удаленного администрирования с помощью подключения к удаленному рабочему столу.

Задание: настроить удаленное подключение к рабочему столу и выполнить подключение к серверу с помощью клиентской виртуальной машины либо другого сервера. Изучить параметры подключения (число подключений, время отключения при бездействии пользователя). Выполнить подключение к компьютеру с правами администратора (т. е. с полным доступом) и с правами пользователя (т. е. с ограниченным доступом). Ограничения определить самостоятельно.

5.3. Удаленная установка программного обеспечения

В Active Directory групповые политики позволяют вам распространять программное обеспечение пользователям и компьютерам, используя переупаковывающий файловый формат – msi. Когда приложение распространяется через групповую политику, пользователю не требуется специальных прав, так как приложение устанавливается при повышенных привилегиях самой политики. Если производитель не предоставляет файл msi для своего приложения, вы можете использовать специальную переупаковывающую программу для его создания. Второй важный момент при распространении программ через групповые политики – это то, как мы его распространяем. Есть две возможности – либо *Assign* (назначить), либо *Publish* (опубликовать) их. Программы могут быть как опубликованы, так и назначены пользователям. В случае их назначения приложение начинает «следовать» за пользователем независимо от того, на каком компьютере он входит в сеть. Иконка программы появляется в стартовом меню, но программа не устанавливается до тех пор, пока пользователь не «кликнет» по иконке. Когда программа назначается компьютеру, она устанавливается на компьютер при его следующей перезагрузке, и становится доступной всем пользователям этого компьютера. Когда программа публикуется (что может быть сделано только для пользователей, но не для компьютеров), она становится доступной для установки при помощи программы *Add/Remove programs* или при обращении к соответствующему документу (когда пользователь «кликнет» по до-

кументу, формат которого ассоциируется с этой программой). Опубликование программы делает ее доступной для пользователей, но у вас не должно создаться иллюзии, что оно уже является установленным.

Приложение может быть также опубликовано с использованием файла с расширением .zap, если нет файла .msi или его невозможно создать. Заметьте, однако, что при использовании файла .zap у пользователя должен быть соответствующий уровень привилегий, достаточный для установки приложения. Также заметьте, что внедрение программного обеспечения через групповые политики доступно только для систем с OS Windows XP и старше.

Раздел *Software Setting* (*Установка программного обеспечения*) групповой политики, где и производится назначение или опубликование программ, показано на рис. 5.13. Когда приложение внедряется через групповую политику, важно сам дистрибутив расположить в сетевой папке и в процессе настройки указать именно сетевой путь (рис. 5.14). Также должна быть выбрана следующая опция – будет ли ваше приложение опубликовано (*Published*) или назначено (*Assigned*) (рис. 5.15).

Дополнительные свойства для внедрения программного обеспечения могут быть настроены, если вы выбираете опцию *Advanced published or assigned* (*Дополнительные настройки опубликования или назначения*), или позднее, изменяя свойства внедряемого пакета.

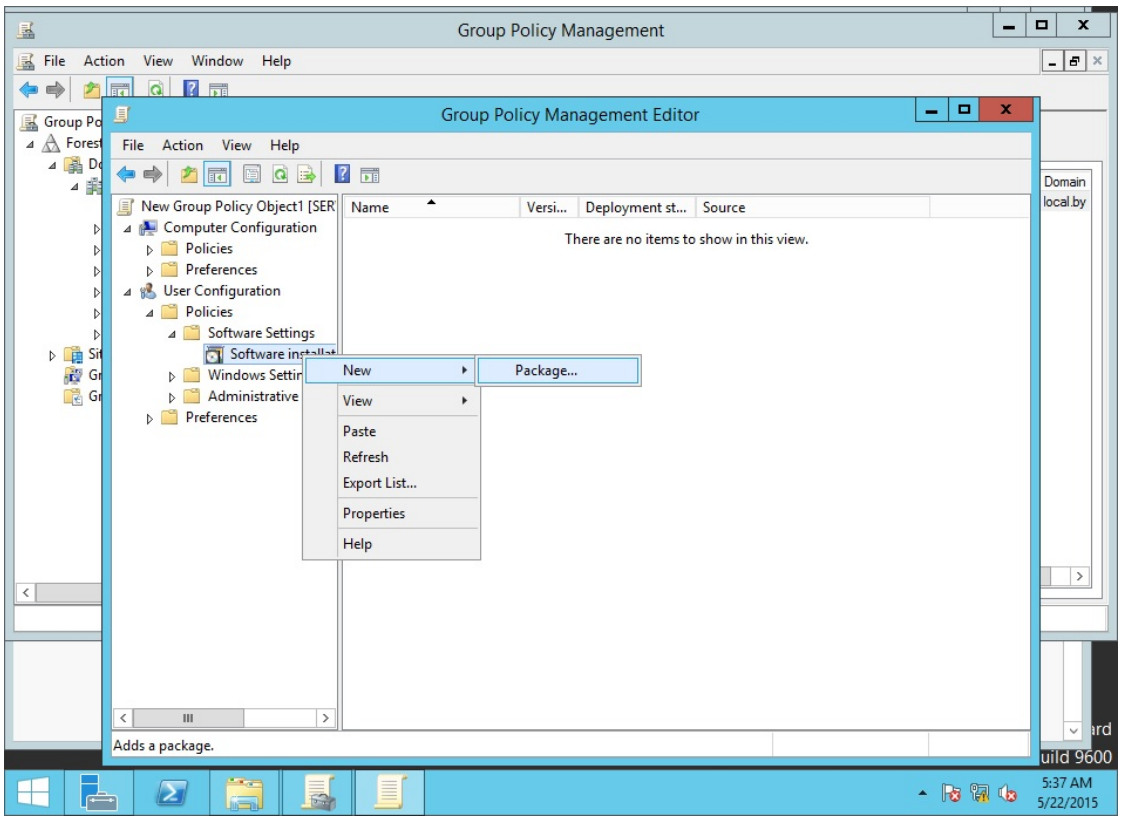

Рис. 5.13. Интерфейс консоли для организации удаленной установки ПО

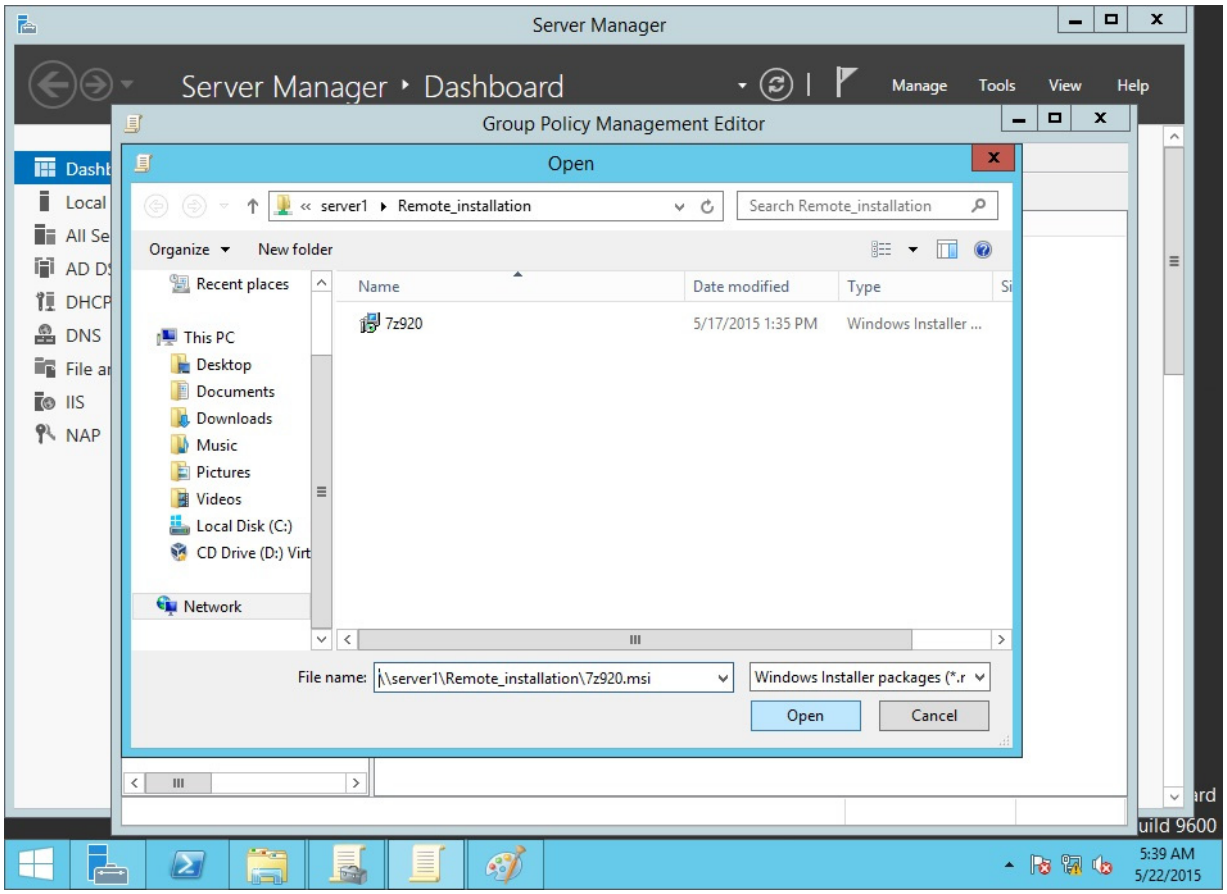

Рис. 5.14. Определение сетевого пути к папке с дистрибутивом устанавливаемого приложения

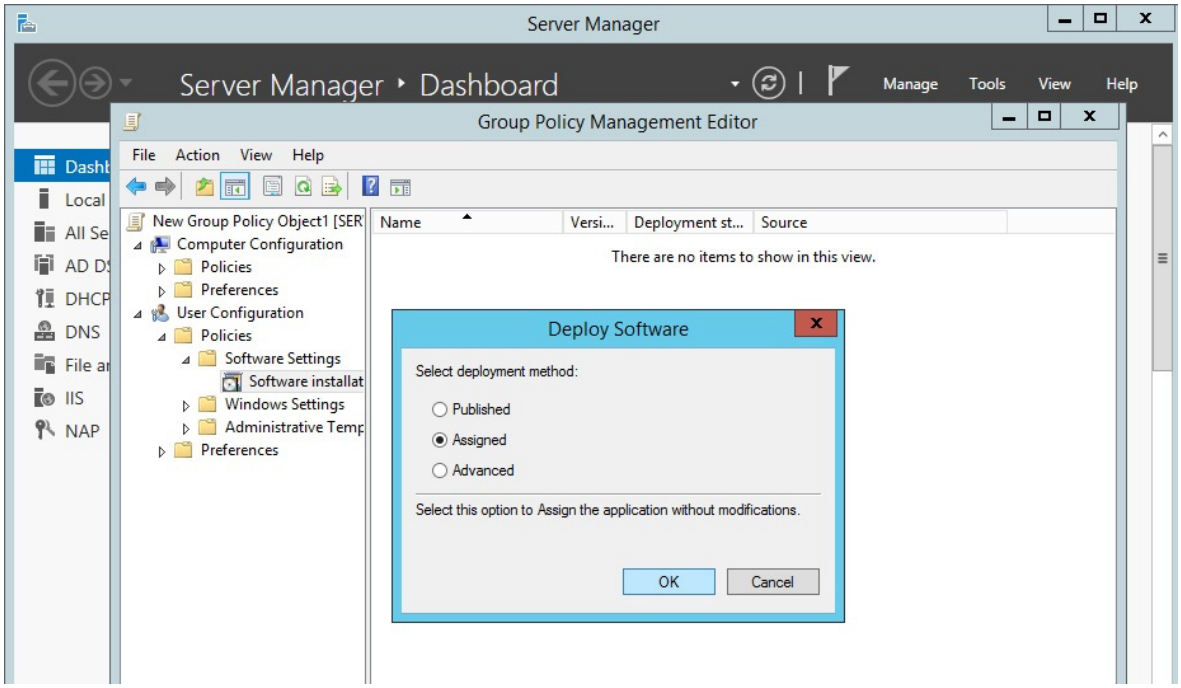

Рис. 5.15. Выбор типа публикации приложения

Дополнительные свойства позволяют вам контролировать многие параметры, имеющие отношение к распространяемому приложению, включая такие, как добавление обновлений и патчей, модификация, а также удаление пакетов.

Есть шесть вкладок дополнительных свойств внедряемого приложения, и вы должны быть хорошо знакомы с ними. Вкладка *General* (*Общая*) содержит основную информацию об объекте (такую как номер версии и т. д.) (рис. 5.16), в то время как вкладка *Security* (*Безопасность*) содержит ACL объекта (рис. 5.17). Вкладка *Deployment* (*Внедрение*) (рис. 5.18) контролирует, было ли приложение опубликовано или назначено (эта настройка может быть изменена). Если опубликовано, вы можете контролировать, будет или нет приложение устанавливаться при обращении к файлам, ассоциирующимся с данным приложением (эта опция будет «залита» серым, если вы выбрали *Назначить приложение*).

Заметьте, что существует опция *Uninstall the application when it falls out of the scope of management* (*Удалять приложение, если оно выходит из сферы управления*). Если она выбрана и групповая политика, которая установила это приложение, больше не применяется (например, если объекты «пользователь» или «компьютер» были перемещены), тогда приложение будет автоматически удалено.

Опция *Installation user interface options* (*Установка опций пользовательского интерфейса*) позволяет вам контролировать, как много взаимодействий пользователь будет иметь в процессе установки.

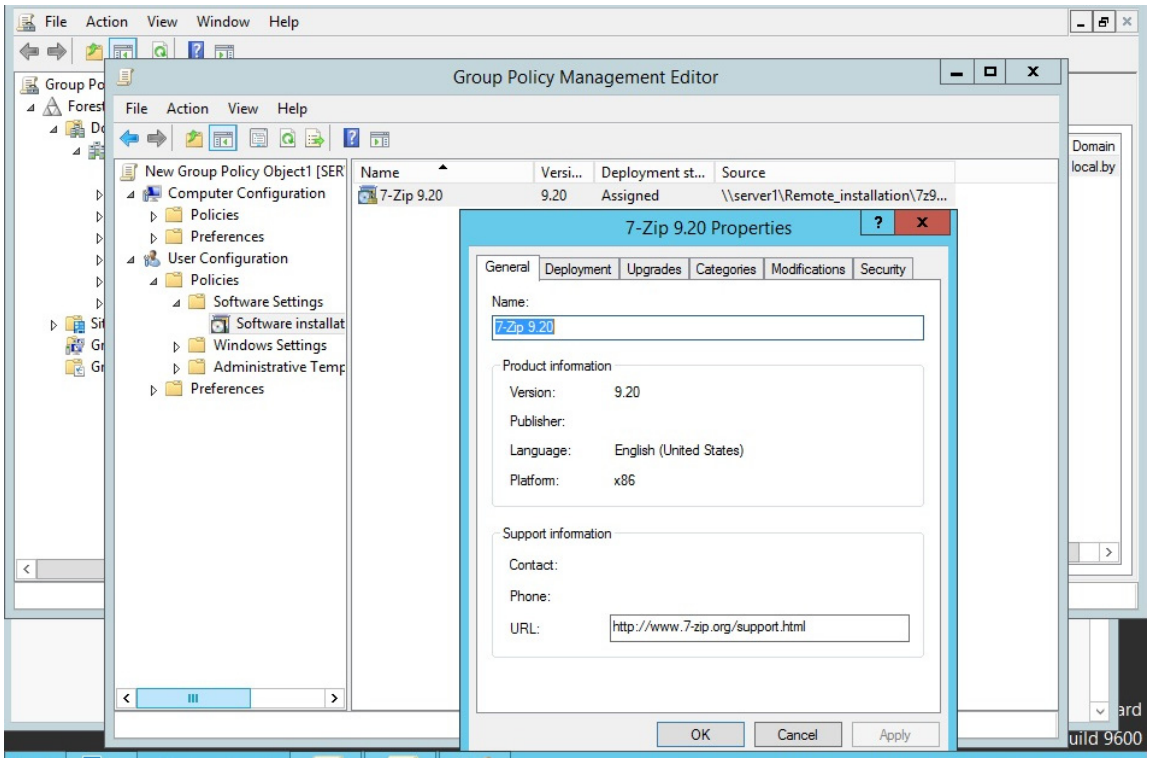

Рис. 5.16. Вкладка *General* в опциях удаленной установки ПО

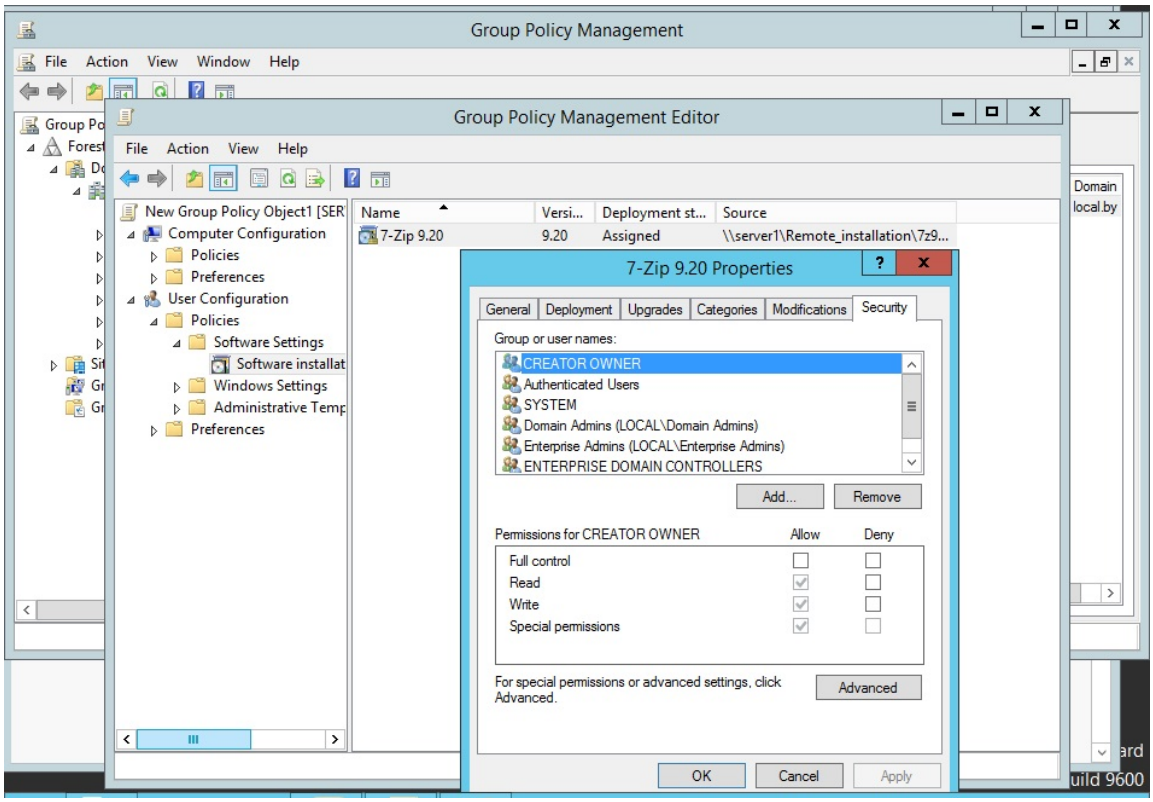

Рис. 5.17. Вкладка *Security* в опциях удаленной установки ПО

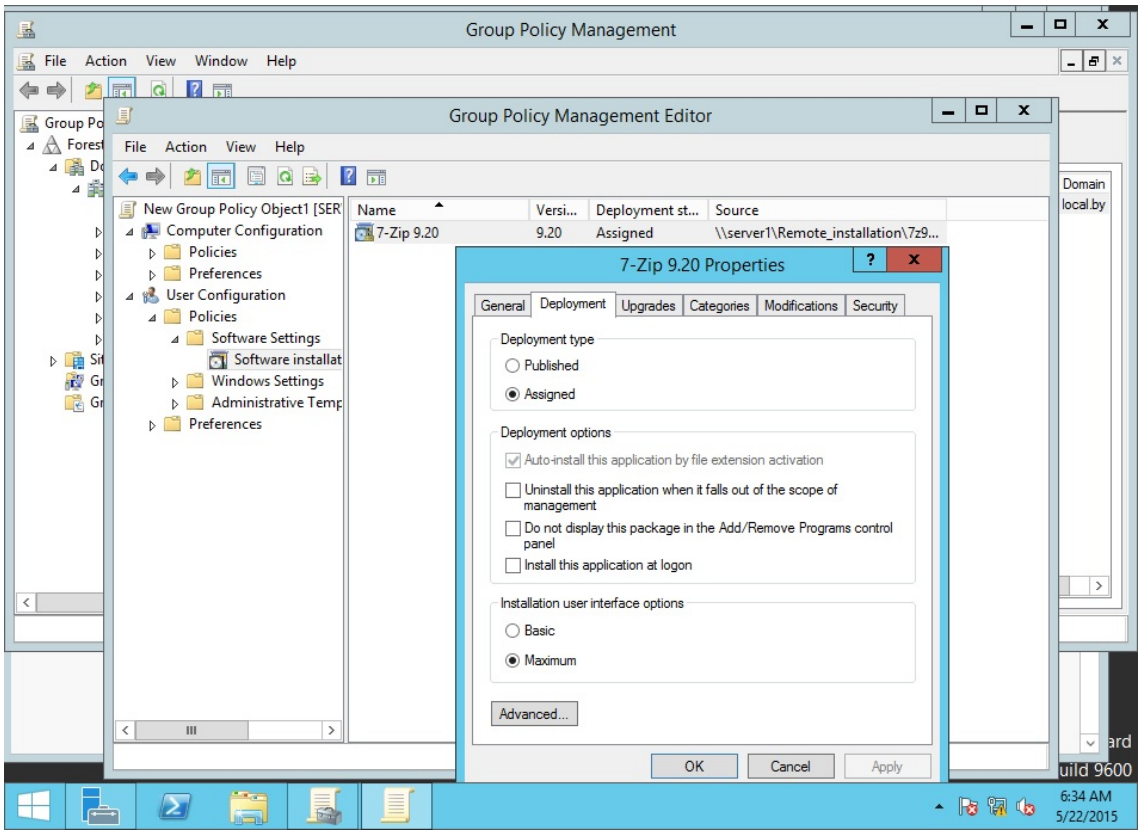

Рис. 5.18. Вкладка *Deployment* в опциях удаленной установки ПО

Вкладка *Upgrades* (*Обновления*), изображенная на рис. 5.19, позволяет вам автоматизировать установку патчей и обновлений (таких как новейшие версии) в приложения, которые уже внедрены через групповую политику. Если обновление должно выполняться в обязательном порядке, выбирается опция *Required* (*Обязательный*), и тогда обновление внедряется сразу и пользователь сможет использовать только новую версию приложения. Если это не обязательное требование, тогда пользователь может использовать как старую, так и новую версию. Это может быть потенциально полезным, если новое приложение не имеет обратной совместимости (не работает с документами, созданными в старой версии программы).

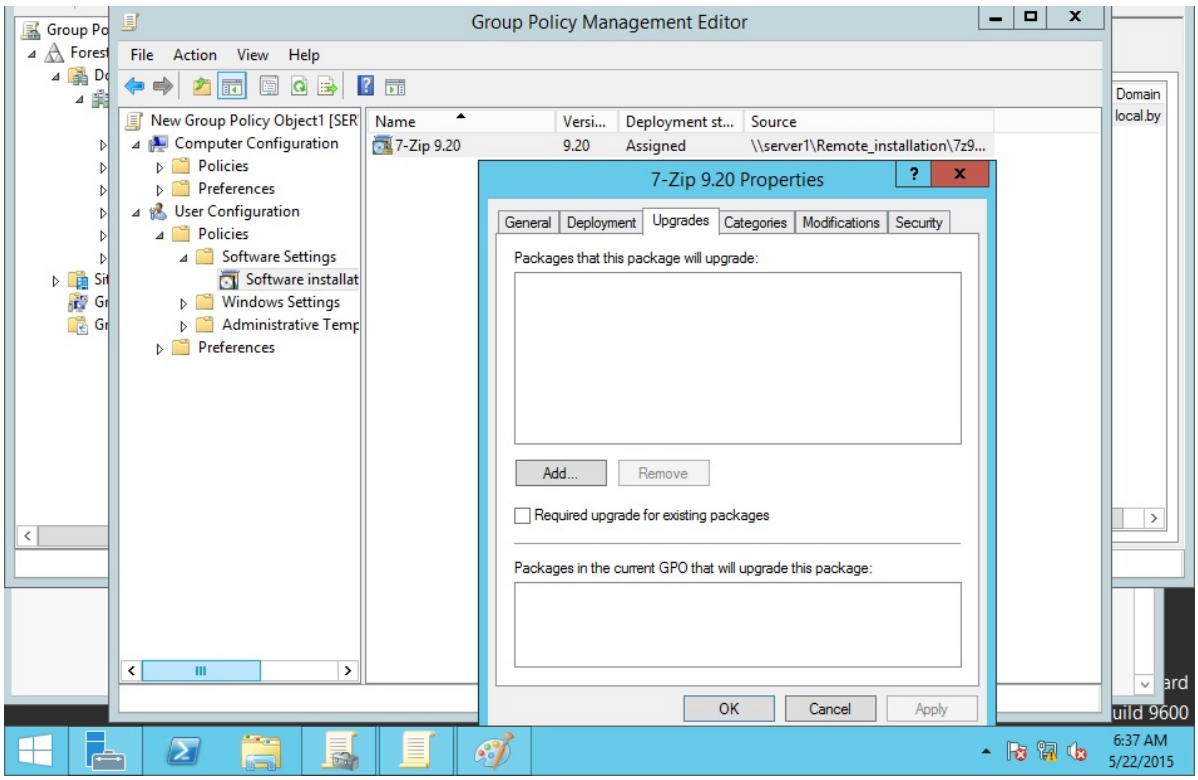

Рис. 5.19. Вкладка *Upgrades* в опциях удаленной установки ПО

Вкладка *Categories* (*Категории*) позволяет вам контролировать то, каким образом приложение будет представлено в программе *Add*/*Remove* (рис. 5.20). Например, вы можете создать категории для каждого типа приложений, таких как графические приложения, программы для работы с текстом и т. д. Эта вкладка позволит вам группировать вновь публикуемые приложения в эти категории для того, чтобы упростить пользователю процесс выбора необходимых ему программ.

И, наконец, вкладка *Modifications* (*Изменения*) позволяет выполнять дальнейшую настройку пакета для пользователей со специфическими потребностями (рис. 5.21).

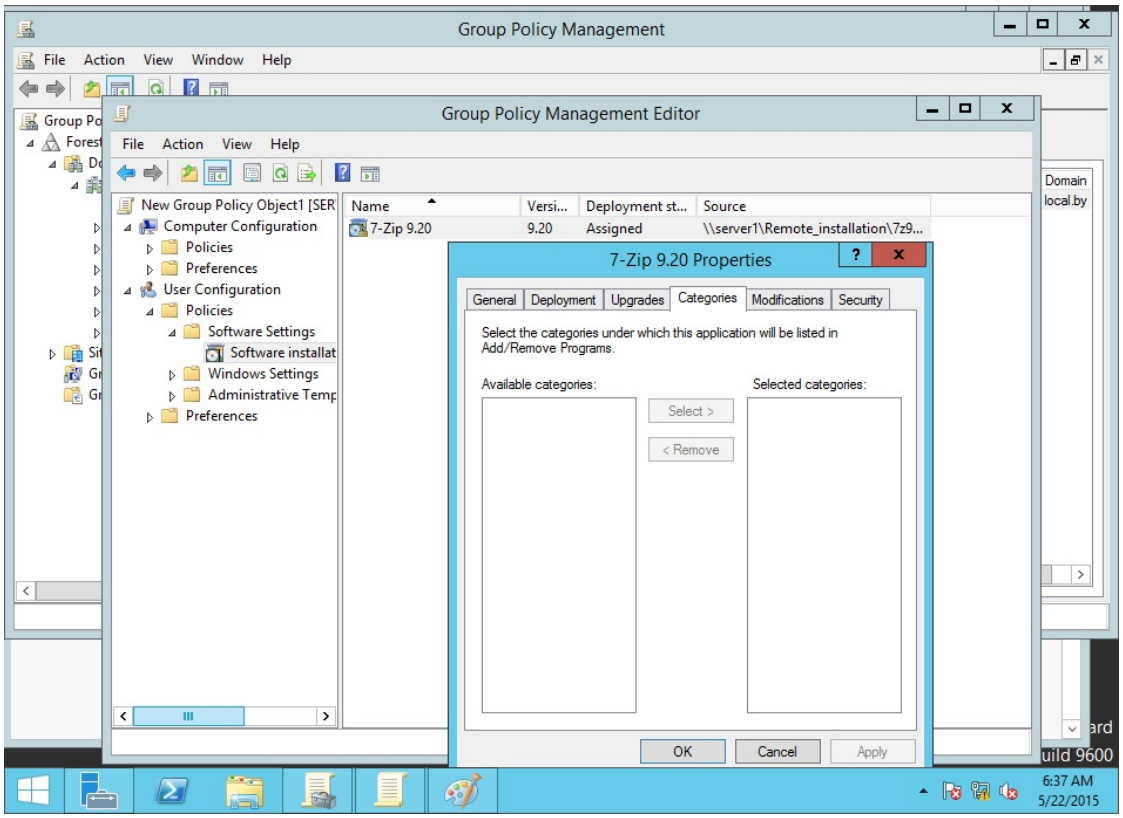

Рис. 5.20. Вкладка *Categories* в опциях удаленной установки ПО

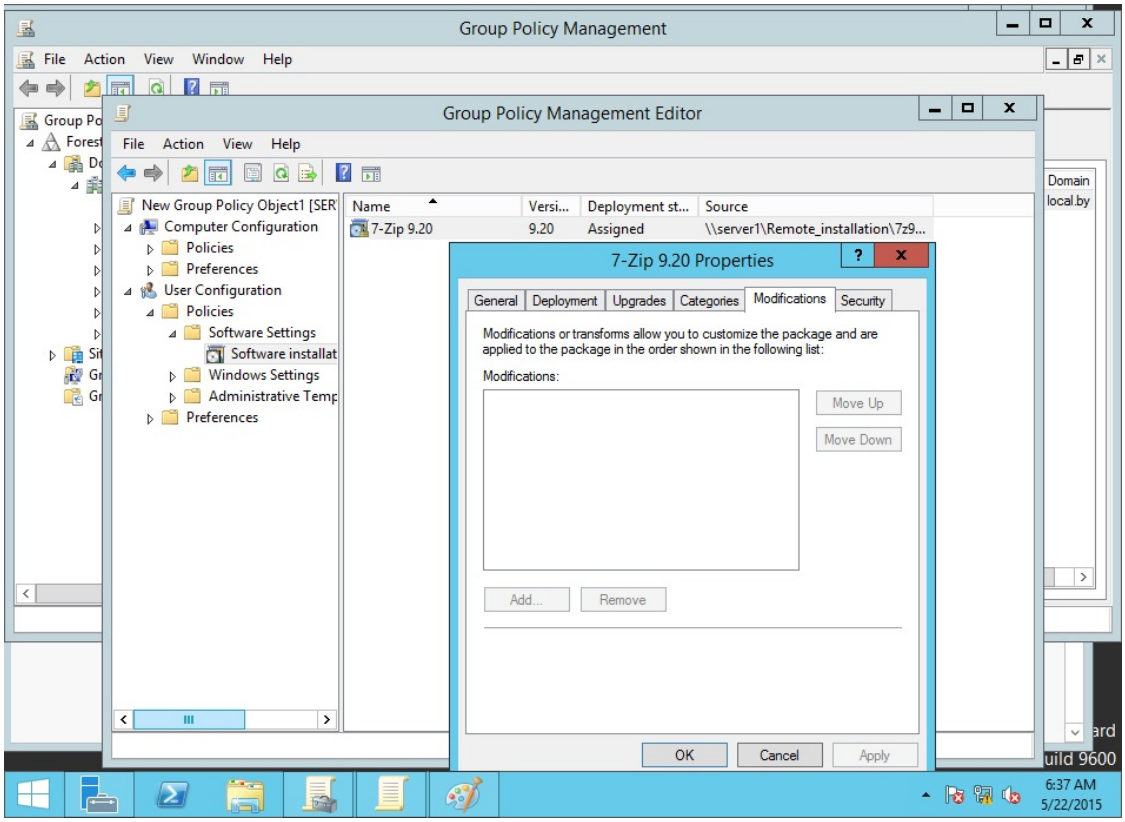

Рис. 5.21. Вкладка *Modifications* в опциях удаленной установки ПО

Например, вы хотите внедрить различающиеся по языку словари для пользователей в разных офисах и применяете модифицирование пакета. Модифицирование выполняется в виде файла с расширением .mst (также известном, как файл трансформации). Есть специальная утилита для создания файлов .mst, которая содержится в resource kit (наборе инструментов) Microsoft Office.

Необходимо отметить, что дистрибутив устанавливаемого приложения должен находится в папке, открытой для доступа по сети для соответствующего пользователя.

Лабораторная работа № 9

Цель: изучение методов удаленного администрирования (удаленная установка программного обеспечения).

Задание: удаленно (с помощью групповых политик) установить клиенту программное обеспечение (например, skype, the bat и т. д.). Операции выполнить таким образом, чтобы при первой загрузке пользователя приложение было автоматически доустановлено и, соответственно, пользователь смог им воспользоваться. Установленное приложение необходимо занести в список разрешенных приложений, сделанный в лабораторной работе № 7 (удаленное администрирование с помощью групповых политик).

Тема 6

БЕЗОПАСНОСТЬ ДОМЕННЫХ СИСТЕМ

6.1. Мониторинг и устранение неполадок подключений TCP/IP. Прослушивание сетевого траффика

В данном разделе рассказывается о популярных инструментах устранения неполадок протокола IP. Вы узнаете о *Сетевом мониторе* (*Network Monitor*), анализаторе протоколов, служащим для покадрового анализа сетевого трафика. Сетевые администраторы применяют анализаторы протоколов для выяснения, почему не работает механизм разрешения имен или почему сбоят подключения к сетевым ресурсам. Иначе говоря, без такого анализатора протокола, как сетевой монитор, очень сложно узнать, что в действительности происходит с сетью.

Также здесь рассматриваются инструментальные средства, чаще всего используемые для устранения неполадок связи в сети. Некоторыми из этих средств (такими как *Ipconfig* и *Ping*) администраторы пользуются ежедневно, если не ежечасно. Другие инструментальные средства, например *Диагностика сети* (*Network Diagnostics*), предоставляют больше информации и позволяют более основательно подходить к устранению неполадок связи сети.

6.1.1. Анализ сетевого трафика средствами Сетевого монитора

Для наблюдения за сетевым трафиком используется анализатор протоколов, например *Сетевой монитор* (*Network Monitor*). В версиях Windows 2003 и 2008 он устанавливается с помощью Мастера компонентов Windows (Windows Components Wizard), который запускают из окна приветствия Microsoft Windows Server 2003 или из утилиты Установка и удаление программ (Add or Remove Programs) в Панели управления. Для Windows Server 2012 его необходимо скачивать с сайта www.microsoft.com. В Windows Server 2012 используется версия 3.4.

Сетевой монитор (Network Monitor) – это программный анализатор трафика, позволяющий:

– перехватывать кадры прямо из сети;

– отображать и фильтровать перехваченные кадры как во время сбора данных, так и после;

– редактировать перехваченные кадры и пересылать их по сети (только в полной версии);

– перехватывать кадры с удаленного компьютера (только в полной версии).

В частности, *Сетевой монитор* применяют для диагностики неполадок оборудования и ПО, когда сервер не в состоянии подключиться к другим компьютерам. Перехваченные кадры можно сохранять в файле или просматривать и анализировать непосредственно в окне *Сетевого монитора*. Разработчики сетевого ПО также применяют *Сетевой монитор* для мониторинга и отладки разрабатываемых сетевых прикладных программ.

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

Есть две версии *Сетевого монитора*. В составе Windows Server (бесплатно скачивается с сайта) поставляется базовая версия, а полная входит в Microsoft Systems Management Server.

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

6.1.2. Компоненты Сетевого монитора. Порядок работы Сетевого монитора

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

Сетевой монитор отслеживает сетевой поток данных, который состоит из всей информации, пересылаемой по сети на данный момент времени. Перед пересылкой сетевое ПО разбивает данные на небольшие порции, или кадры, каждая из которых содержит следующую информацию:

– адрес компьютера – отправителя сообщения;

– адрес компьютера-адресата (который принял кадр);

– заголовочная информация всех протоколов, использованных при пересылке кадра;

– данные (или их часть), посылаемые на компьютер-адресат.

Сетевой монитор из состава Windows Server копирует в буфер кадры, исходящие или входящие на локальный компьютер, этот процесс называется записью данных (data capture). Объем информации, собираемой *Сетевым монитором*, ограничен лишь объемом памяти, однако обычно нужно собирать только небольшую часть всего потока кадров. Подмножество собираемых кадров задается фильтрами, работа которых напоминает запрос базы данных: они выделяют из общего потока лишь нужную информацию. Фильтрованные кадры можно отсортировать на основе адресов источника и целевого узла, уровня протоколов: сетевого интерфейса, межсетевого и транспортного, а также на основе свойств протокола и при отклонении структуры кадров от заданного шаблона.

Установка и настройка сетевого монитора будет рассмотрена далее.

Анализ записанных данных

При включении просмотра собранных данных открывается окно просмотра кадров со сводной информацией о кадрах в порядке их поступления (рис. 6.1).

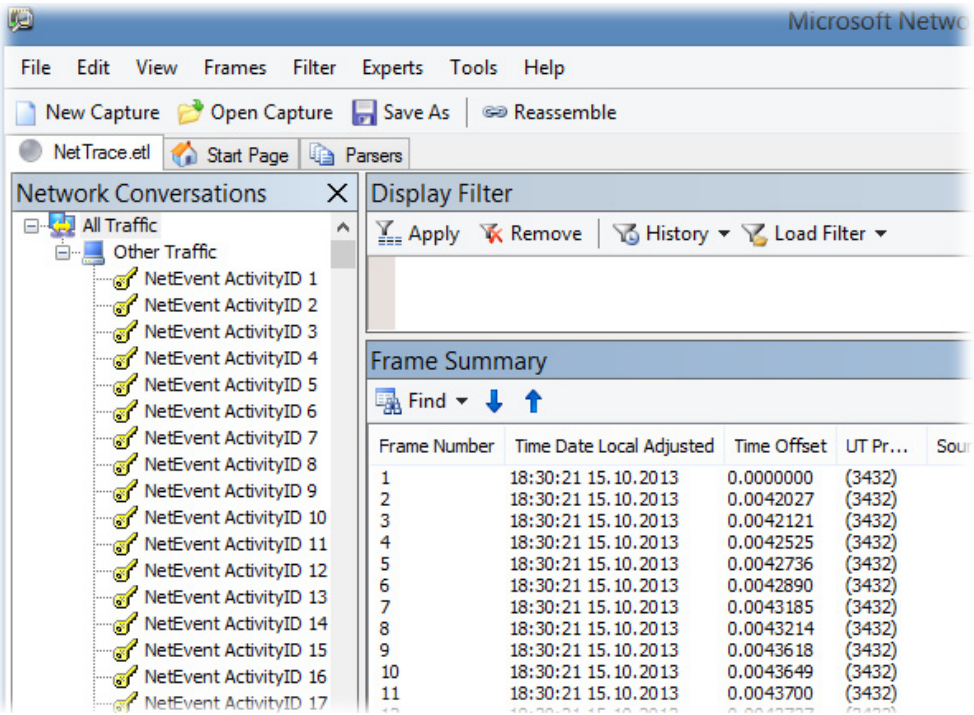

Рис. 6.1. Интерфейс сетевого монитора

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

Панель Сводка. Содержит перечень всех кадров, отображаемых в текущем представлении. При выборе кадра информация о нем отображается в панелях *Сведения* и *Шестнадцатеричный*.

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

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

Анализ кадров

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

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

+ Frame: Base frame properties
+ ETHERNET: EType = Internet IP (IPv4)
+ IP: Protocol = UDP - User Datagram; Packet ID = 1576;
Total IP Length = 236; Options = No Options
+UDP: Src Port: NETBIOS Datagram Service (138):
Dst Port: NETBIOS Datagram Service (138); Length = 216 (0xD8)
+ NBT: DS: Type = 17 (DIRECT GROUP)
+ SMB: C transact, File = \MAILSL0T\BR0 WSE
+ Browser: Workgroup Announcement [0x0c] WORKGROUP

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

Добавление парсеров Сетевого монитора

Процесс чтения, анализа и описания содержимого кадров называется разбором (parsing) и выполняется специальными модулями, или парсерами

(parser). В *Сетевом мониторе* это DLL-файлы, отвечающие за разбор и чтение сообщений различных протоколов. По умолчанию *Сетевой монитор* содержит более 20 парсеров, обеспечивающих разбор свыше 90 протоколов.

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

Добавление записей в файл Parser.ini на первый взгляд может показаться сложным, но на самом деле все записи одинаковы. Во-первых, в разделе parsers надо добавить следующую запись:

<имя_парсера>.dll = 0: <имя_протокола>

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

Необходимо отметить, что для выполнения операций по прослушиванию сетевого трафика можно также воспользоваться альтернативными сниферами, например Wireshark.

6.1.3. Использование Сетевого монитора

Запись данных средствами Сетевого монитора

Записывается и просматривается информацию о трафике с помощью *Сетевого монитора* следующим образом.

1. Войдите в систему как Администратор (Administrator) и в *Сетевой монитор*.

2. Далее откроется окно *Сетевой монитор* (*Network Monitor*) с сообщением о необходимости выбрать сеть (рис. 6.2). Щелкните *OK*.

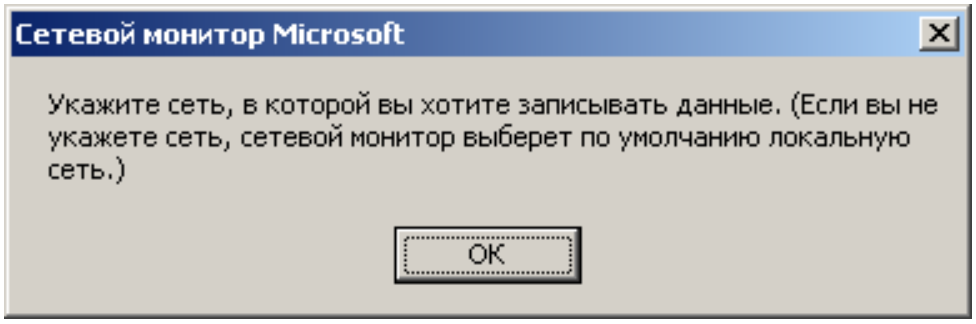

Рис. 6.2. Окно с сообщением о необходимости выбора сети

3. Разверните узел *Локальный компьютер* (*Local Computer*) в левой панели окна *Выбор сети* (*Select a network*), чтобы открыть список сетевых адаптеров на локальном компьютере. Подключения по телефонной линии объединены в узел *Подключение удаленного доступа или VPN* (*Dial-up Connection or VPN*) (рис. 6.3).

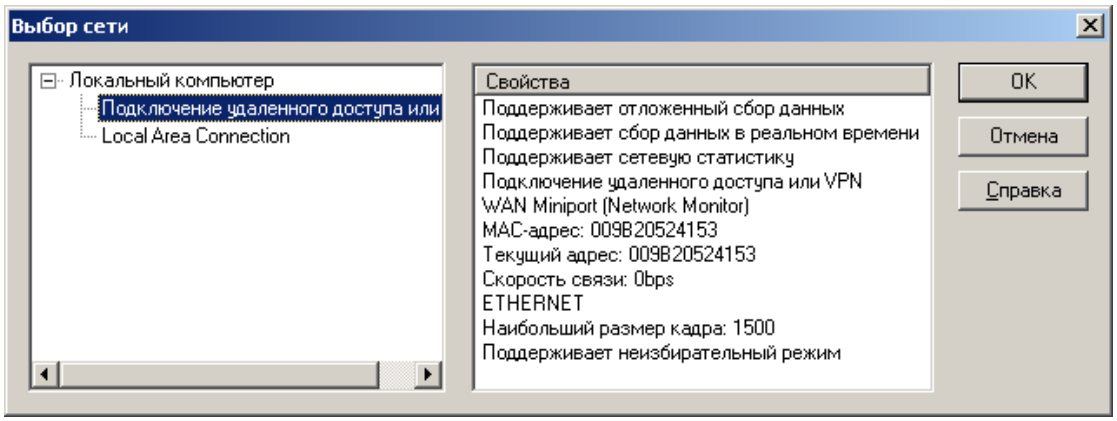

Рис. 6.3. Окно выбора подключения

4. Выберите *Подключение к локальной сети* (*Local Area Connection*) и щелкните *OK*. Откроется окно *Сетевого монитора* с окном *Запись* (*Capture*) для выбранного сетевого адаптера (рис. 6.4).

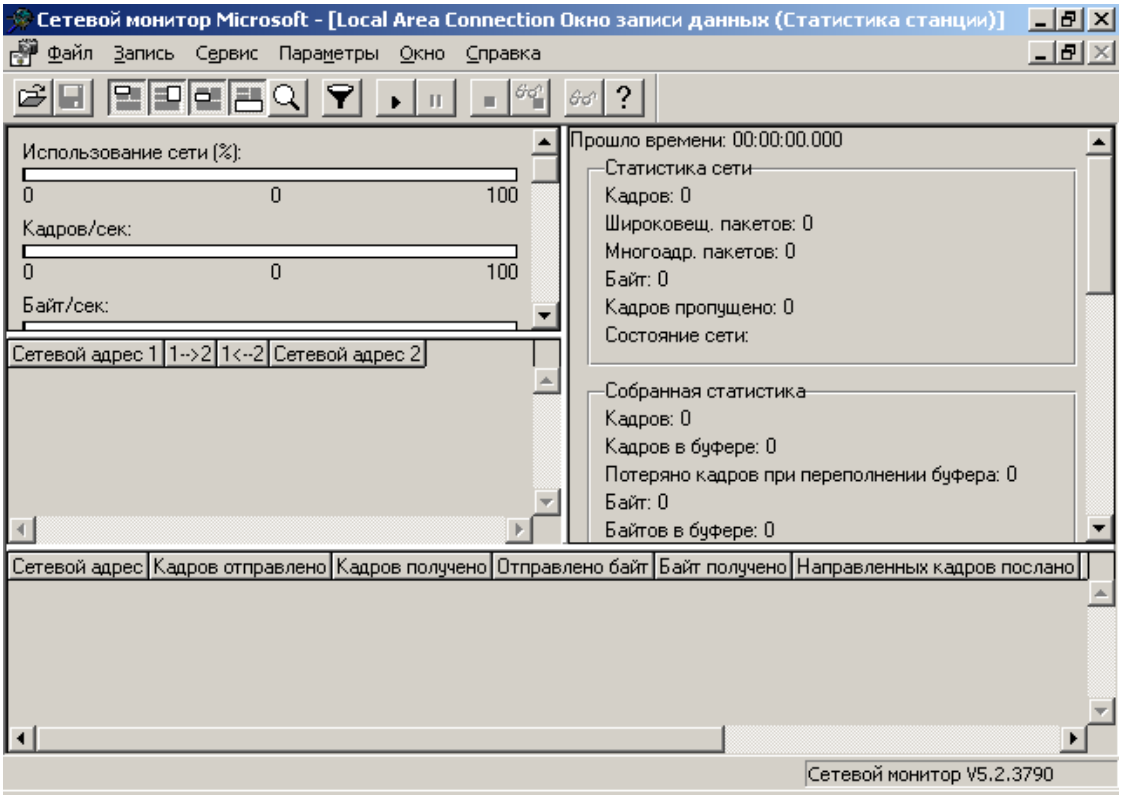

Рис. 6.4. Основное окно *Сетевого монитора*

5. На панели инструментов окна *Запись* щелкните кнопку *Начать запись данных* (*Start Capture*) (рис. 6.5).

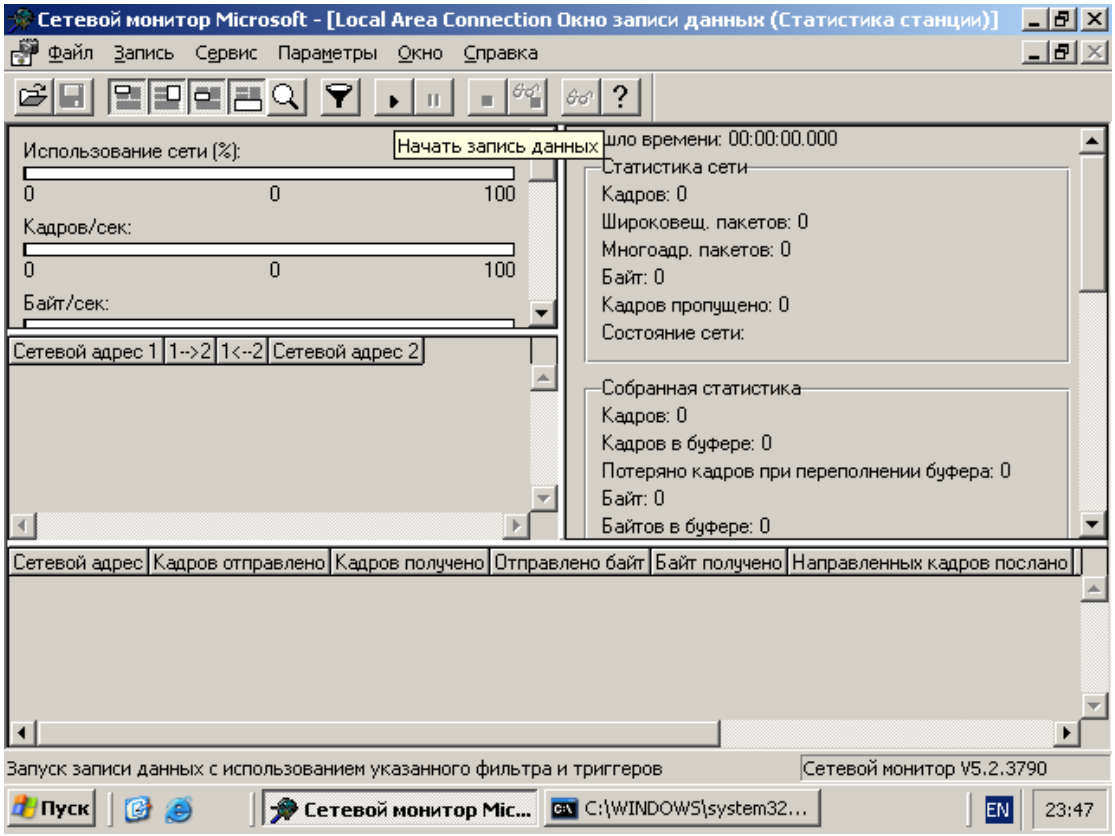

Рис. 6.5. Окно *Сетевого монитора*, выполняющего запись передаваемой информации

6. Из командной строки исполните следующую команду: ping 127.0.0.1. Это нужно для проверки сетевых подключений.

7. По завершении работы команды *Ping* на панели инструментов щелкните кнопку *Закончить запись и просмотреть данные* (*Stop and View Capture*) или нажмите Shift+F11.

Откроется окно записи данных с заголовком *Запись данных*: 1 (*Capture*: 1). В скобках отображается слово *Сводка* (*Summary*), указывающее на то, что панель сводных данных является активной и единственной видимой панелью окна. Здесь перечисляются все записанные кадры.

8. Дважды щелкните любой из кадров, указанных в панели *Сводка*. В окне записи данных откроются две дополнительных панели: *Сведения* (*Details*) и *Шестнадцатеричный* (*Hexadecimal*), содержащие подробную информацию о выбранном кадре.

9. Снова дважды щелкните кадр в панели *Сводка*. Панели *Сведения* и *Шестнадцатеричный* скроются – так переключаются между двумя представлениями окна *Запись*.

10. Выберите *Файл* (*File*)/*Сохранить как* (*Save As*), чтобы открыть окно *Сохранить как* (*Save As*).

11. В поле *Имя файла* (*File Name*) введите *Ping Capture* и щелкните *Сохранить* (*Save*). Файл Ping Capture.cap сохранится в папке *\Рабочий стол\Мои документы\Мои записи* (*\Desktop\My Documents\My Captures*).

12. Выберите *Файл* (*File*)*\Закрыть* (*Close*). Окно записи данных закроется, а в консоли *Сетевой монитор* снова появится окно *Запись*.

Сохранение кадров в текстовом файле

Копирование информации пакета в текстовый файл выполняется в окне *Сетевой монитор* (*Network Monitor*) под учетной записью Администратор (Administrator).

1. Выберите *Файл* (*File*)/*Открыть* (*Open*). Откроется окно *Открыть* (*Open*) с файлом Ping Capture.cap в папке Мои записи (My Captures).

2. Выберите файл Ping Capture.cap и щелкните *Открыть* (*Open*), чтобы открыть его в окне записи данных.

3. В панели *Сводка* (*Summary*) найдите и выберите кадр со словом ICMP в столбце *Протокол* (*Protocol*).

4. Нажмите Ctrl+C, чтобы скопировать кадр.

5. Откройте *Блокнот* (*Notepad*) и нажмите Ctrl+V, чтобы вставить информацию о кадре в новый текстовый файл. В текстовый файл вставляются все данные записанного кадра. Обратите внимание, первая строка содержит все поля и в той же последовательности, что и в панели *Сводка* окна сбора данных. Кроме того, большая часть данных – около 40 строк – соответствуют информации, отображаемой в панели *Сведения* (*Details*). Но здесь информация представлена в развернутом виде. В конце текста размешены шестнадцатеричные значения из панели *Шестнадцатеричный* (*Hexadecimal*).

6. В *Блокноте* нажмите Ctrl+S, чтобы сохранить файл. Откроется окно *Сохранить как* (*Save As*). Выберите пайку *\Рабочий стол\Мои документы\Мои записи* (*\Desktop Documents\My Captures*), но пока не сохраняйте файл.

7. В поле со списком *Кодировка* (*Encoding*) выберите Юникод (Unicode).

8. В поле *Имя файла* (*File Name*) замените введите ICMP frame и щелкните *Сохранить* (*Save*).

9. Закройте окно ICMP Frame.txt – Блокнот (ICMI Frame.txt – Notepad).

10. Закройте окно *Сетевой монитор*, выбрав *Файл* (*File*)*\Выход* (*Exit*). На предложение сохранить адрес в базе данных ответьте *Нет* (*No*).

11. Выйдите из системы.

6.2. Протокол IPsec

Протокол Kerberos применяется для аутентификации участников соединения. Но и после этапа аутентификации данные, передаваемые по се-

ти, следует защищать. Стандартные протоколы стека TCP/IP, такие как IP, TCP, UDP, не обладают встроенными средствами защиты. На эту проблему в 1994 г. обратил внимание Совет по архитектуре Интернета (Internet Architecture Board, IAB), издав RFC 1636 (Report of IAB Workshop on Security in the Internet Architectures («Отчет семинара IAB по безопасности в архитектуре Интернета»)). Инициированная этим сообщением работа привела к появлению протокола IPsec (IP security – безопасность IP), описанного в нескольких стандартах RFC (в частности, в RFC 2401-2412). Новая технология безопасности является необходимой частью протокола IPv6, а также может применяется и в сетях IPv4.

Протокол IPsec действует на сетевом уровне модели OSI и может применяться независимо от протоколов верхнего уровня, т. е. прикладной протокол может использовать IPsec, считая, что работает с обычным протоколом IP. При этом данные протоколов верхних уровней упаковываются в пакеты IPsec, которые, в свою очередь, помещаются в пакеты протокола IP.

6.2.1. Функции протокола IPsec

Протокол IPsec обеспечивает наличие следующих функций:

− аутентификация – приемник пакетов в состоянии проверить подлинность их источника;

− целостность – осуществляется контроль того, что данные дойдут до получателя в неизменном виде;

− конфиденциальность – шифрование данных обеспечивает их недоступность для несанкционированного просмотра;

− распределение секретных ключей – для правильной работы протокола IPsec необходимо автоматически обеспечивать источник и приемник пакетов секретными ключами для шифрования и расшифрования данных.

Для реализации представленных функций используются три основных протокола:

− AH (Authentication Header – заголовок аутентификации) обеспечивает целостность и аутентичность;

− ESP (Encapsulating Security Payload – инкапсуляция зашифрованных данных) предоставляет функции целостности, аутентичности и конфиденциальности;

− IKE (Internet Key Exchange – обмен ключами Интернета) генерирует и распределяет секретные ключи.

Можно заметить, что протокол ESP имеет схожие функции с протоколом AH. Пересечение функций вызвано тем, что на применение протоколов шифрования во многих странах накладываются определенные ограничения. В связи с этим оба протокола могут применяться независимо, хотя наивысший уровень защиты достигается при их совместном использовании.

На рис. 6.6 представлена структура протокола IPsec и взаимосвязь основных протоколов, входящих в его состав.

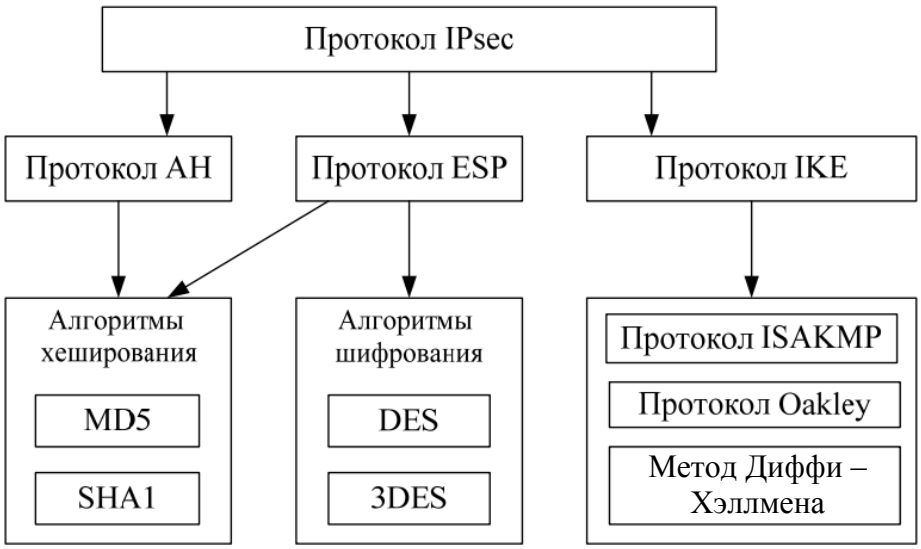

Рис. 6.6. Структура протокола IPsec

6.2.2. Протоколы AH и ESP

Протокол AH (описан в RFC 2402) снабжает пакет IPsec своим незашифрованным заголовком, который обеспечивает:

− аутентификацию исходных данных;

− целостность данных;

− защиту от дублирования уже полученных данных.

Первые две функции протокола AH реализуются путем применения алгоритмов хеширования (MD5 (Алгоритм MD5 (Message Digest – алгоритм формирования профиля сообщения) разработан Рональдом Ривестом (Ronald Rivest). См. RFC 2403) или SHA1 (Алгоритм SHA1 (Secure Hash Algorithm – алгоритм безопасного хеша) разработан Национальным институтом стандартов и технологий (NIST, National Institute of Standards and Technology), является более стойким по сравнению с MD5 (описан в RFC 2404)). Процедура хеширования осуществляется источником с помощью секретного ключа, который был выдан источнику и приемнику пакета с использованием протокола IKE. Полученное значение хеша помещается в специальное поле заголовка AH. Приемник также осуществляет процедуру хеширования, применяя тот же секретный ключ. В том случае если вычисленный хеш совпадает с хешем, извлеченным из пакета, данные считаются аутентифицированными и целостными. Иначе пакет в процессе передачи подвергся каким-либо изменениям и не является правильным.

Функция защиты от дублирования уже полученных пакетов осуществляется с помощью поля номера пакета в заголовке AH. В это поле прием-

ник заносит значение счетчика, увеличивающееся при отправке каждого пакета на единицу. Приемник отслеживает номера получаемых пакетов, и если такой номер совпадает с недавно полученным, пакет отбрасывается.

Протокол ESP (описан в RFC 2406) решает задачи, подобные протоколу AH, – обеспечение аутентификации и целостности исходных данных, а также защиту от дублирования пакетов. Кроме того, протокол ESP предоставляет средства обеспечения конфиденциальности данных при помощи алгоритмов шифрования.

Задачи аутентификации, целостности и защиты от дублирования решаются теми же методами, что и в протоколе AH. Передаваемый пакет, за исключением нескольких служебных полей, шифруется с применением алгоритмов шифрования DES и 3DES (DES с тремя ключами).

6.2.3. Протокол IKE

Управление секретными ключами в протоколе IPsec осуществляется при помощи протокола IKE (описан в RFC 2409). Данный протокол основан на двух протоколах: ISAKMP (Internet Security Association and Key Management Protocol – протокол межсетевой ассоциации защиты и управления ключами) и протоколе определения ключей Оакли (Oakley Key Determination Protocol).

Протокол IKE устанавливает соединение между двумя узлами сети, называемое *безопасной ассоциацией* (Security Association, SA). Безопасная ассоциация обеспечивает передачу защищенных данных только в одну сторону, поэтому для установки двустороннего соединения требуется определить две безопасные ассоциации. Для аутентификации узлов безопасной ассоциации, согласования между ними методов хеширования и шифрования IKE использует протокол ISAKMP (описан в RFC 2408).

Для генерации и обмена секретными ключами IKE использует протокол определения ключей Оакли (описан в RFC 2412), разработанный на основе метода обмена ключами Диффи – Хэллмена (Diffie – Hellman). В этом методе секретный ключ генерируется на двух узлах путем обмена двумя числами через открытую сеть. При этом перехват чисел не даст информации о ключах.

6.3. Настройка протокола IPSecurity

Для выполнения шифрования сетевого трафика необходимо выполнить настройку политики безопасности (оснастку) на обоих компьютерах с операционной системой Windows Server. Далее будет рассмотрен пример настройки одной из ОС.

1. В командной строке выполните команду MMC. Откроется оболочка *Microsot Management Console*. В меню *File* выберите *Add*/*Remove Snap-In* и

добавьте две консоли*: IP Security Policy Managment* (*для локального компьютера*) и *IP Security Monitor*. Нажмите на кнопку *Add*, а затем *OK*, чтобы вернуться в основное окно консоли. Для удобства созданную вами консоль можно сохранить, например на рабочем столе под именем IPSec.msc.

2. В созданной вами консоли раскройте узел *IP Security Policies on Local Computer*, щелкните по этому узлу правой кнопкой мыши и в контекстном меню выберите *Create IP Security Policy*. Запустится мастер создания политики IPSecurity.

3. На первом экране мастера введите имя политики (например, TestPolicy) и нажмите *Next*.

4. На втором экране (*Requests for Secure Communication*) снимите флажок *Activate the default response rule* и нажмите *Next*.

5. На последнем экране мастера убедитесь, что флажок *Edit Properties установлен* и нажмите *Finish*. Откроется экран свойств вашей политики. Нажмите в нем на кнопку *Add*, чтобы добавить новое правило для вашей политики. На первом экране мастера создания правил нажмите *Next*.

6. На втором экране мастера (*Tunnel Endpoint*) убедитесь, что переключатель стоит в положении *This rule does not specify a tunnel* и нажмите *Next*.

7. На экране *Network Type* оставьте переключатель в положении *All network connections* и нажмите *Next*.

8. На экране *IP Filter list* нажмите на кнопку *Add*. Откроется окно создания нового фильтра. В этом окне введите название фильтра (например, имя компьютера партнера_filter) и нажмите *Add*. Откроется еще один мастер – создания фильтров. На его первых двух экранах нажмите *Next*.

9. На экране *IP Traffic Source* оставьте в качестве адреса источника *My IP Address* и нажмите *Next*.

10. На экране *IP Traffic Destination* выберите в списке адресов назначения *A specific IP address* и укажите IP-адрес вашего партнера. На остальных экранах этого мастера оставьте значения по умолчанию. Вы опять вернетесь в окно *IP Filter List*, в котором будет присутствовать созданный вами фильтр. Нажмите в нем *OK* и в окне *Security Rule Wizard* на экране *IP Filter List* установите переключатель напротив созданного вами фильтра. Нажмите *Next*.

11. На следующем экране (*Filter Action*) установите переключатель в положение *Require Security* и нажмите *Next*.

12. На следующем экране (*Authentification Method*) установите переключатель в положение *Use this string to protect the key exchange* (*preshared key*) и в поле внизу введите текстовое значение, например TEST. Это значение должно совпадать с тем значением, которое ввел у себя партнер. Нажмите *Next*, на последнем экране снимите флажок *Edit Properties* и нажмите *Finish*. Затем в окне консоли MMC щелкните правой кнопкой

мыши по созданной вами политике и в контекстном меню выберите *Assign*. Дождитесь, пока партнер завершит выполнение аналогичных действий на своем компьютере.

13. Раскройте узел *IP Security Monitor – имя вашего компьютера – Active Policy* и просмотрите информацию о назначенной вами политике и о статистике взаимодействия по IPSec (под Main Mode).

14. Запустите *Network Monitor* (либо другой снифер) и настройте в нем фильтр для перехвата трафика между ОС системами Windows Server. В качестве сетевого траффика может выступать отправленный ping-запрос или подключение по ftp, http, telnet и т. д. *Network Monitor* покажет служебную информацию протокола ESP (а не какого-либо другого в зависимости от типа сетевого траффика). Необходимо обратить внимание, что для успешного шифрования сетевого траффика настроить оснастки необходимо на обеих машинах с ОС Windows Server.

Лабораторная работа № 10–11

Цель: изучение методов прослушивания и шифрования сетевого трафика между операционными системами типа Windows.

Задание: выполнить настройку политик безопасности (оснастки) для шифрования сетевого траффика с помощью протокола IPSecurity на обеих виртуальных машинах с ОС Windows Server. Проверить обеспечение безопасности (шифрования данных) путем прослушивания сетевого траффика при помощи программы-снифера, например *Network monitor*.

ЛИТЕРАТУРА

1. Урбанович, П. П. Компьютерные сети: учеб. пособие для студентов высших учебных заведений по техническим специальностям / П. П. Урбанович, Д. М. Романенко, Е. В. Кабак. – Минск: БГТУ, 2011. – 400 с.

2. Романенко, Д. М. Компьютерные сети. Лабораторный практикум / Д. М. Романенко, Н. В. Пацей. – Минск: БГТУ, 2011. – 133 с.

3. Танненбаум, Э. Компьютерные сети / Э. Танненбаум, Д. Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб.: Питер, 2010. – 944 с.

5. Линн, С. Администрирование Windows Server 2012 / С. Линн. – СПб.: Питер, 2013. – 304 с.

6. Windows Server 2012. Полное руководство / Р. Моримото [и др.]. – Вильямс, 2013. – 1456 с.

7. Котельников, Е. В. Сетевое администрирование на основе Microsoft Windows Server 2003. Курс лекций / Е. В. Котельников. – М.: МТУ, 2007. – 103 с.

8. Полак-Брагинский, А. Администрирование сети на примерах / А. Полак-Брагинский. – СПБ.: БВХ-Санкт-Петербург, 2005. – 320 с.

ОГЛАВЛЕНИЕ

Учебное издание

Романенко Дмитрий Михайлович

ОСНОВЫ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ

Лабораторный практикум

Редактор *О. П. Приходько*
Компьютерная верстка *О. П. Приходько*
Корректор *О. П. Приходько*

Издатель:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/227 от 20.03.2014.
Ул. Свердлова, 13а, 220006, г. Минск.