

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ  
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ  
СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ  
«БУРЯТСКИЙ РЕСПУБЛИКАНСКИЙ ИНФОРМАЦИОННО-  
ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ» (ГБОУ СПО БРИЭТ)**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ  
для выполнения лабораторных работ  
по профессиональному модулю**

**Организация сетевого администрирования**

**Раздел 1. ПМ.02 Сетевые операционные системы, серверы, службы и протоколы  
Предназначены для обучающихся специальности  
230111 Компьютерные сети  
2 курс**

Составитель:  
Е.А. Тенгайкин

Рассмотрено предметно-цикловой комиссией  
информационных технологий

Протокол № \_\_\_\_ от « \_\_\_\_ » \_\_\_\_\_ 20...г.

Председатель предметной цикловой комиссии  
Никифорова О.С.

Рецензент \_\_\_\_\_

должность, звание, инициалы, фамилия

Настоящие методические указания составлены в соответствии с рабочей программой и предназначены для обучающихся специальности СПО 230111 Компьютерные сети при изучении ПМ.02 Организация сетевого администрирования.

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 230111 Компьютерные сети (начальной профессиональной подготовки) в части освоения основного вида профессиональной деятельности (ВПД): Организация сетевого администрирования и соответствующих профессиональных компетенций (ПК):

1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
2. Администрировать сетевые ресурсы в информационных системах.
3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.
4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в области администрирования компьютерных сетей при наличии среднего (полного) общего образования. Опыт работы не требуется.

## Содержание

<b>Введение</b> .....	5
<b>Лабораторная работа № 1</b> «Применение сетевых утилит для определения работоспособности сети».....	7
<b>Лабораторная работа № 2</b> «Организация функционирования ЛВС на базе ОС Windows Server 2003. Настройка сервера имен» .....	14
<b>Лабораторная работа № 3</b> «Организация функционирования ЛВС на базе ОС Windows Server 2003. Установка и настройка DHCP-сервера» .....	29
<b>Лабораторная работа № 4</b> «Удалённое управление компьютером».....	33
<b>Лабораторная работа № 5</b> «Использование утилиты Backup» .....	38
<b>Лабораторная работа № 6</b> «Управление реестром» .....	45
<b>Лабораторная работа № 7</b> «Установка и настройка web-сервера».....	51

## **Введение**

Методические указания для выполнения лабораторных работ по профессиональному модулю Организация сетевого администрирования составлены в соответствии с рабочей программой междисциплинарного курса МДК 02.01 Программное обеспечение компьютерных сетей: Раздел 1. Сетевые операционные системы, серверы, службы и протоколы.

Актуальность изучения МДК 02.01 Программное обеспечение компьютерных сетей: Раздел 1. Сетевые операционные системы, серверы, службы и протоколы обусловлена тем, что МДК.02.01 Программное обеспечение компьютерных сетей является частью основной профессиональной образовательной программы по специальности СПО 230111 Компьютерные сети (базовой подготовки). Профессиональный модуль Организация сетевого администрирования логически взаимосвязан с профессиональными модулями и учебными дисциплинами специальности СПО 230111 Компьютерные сети (базовой подготовки): основы электротехники, основы теории информации, технологии физического уровня передачи данных, архитектура аппаратных средств, операционные системы, основы программирования и баз данных, проектирование сетевой инфраструктуры, эксплуатация объектов сетевой инфраструктуры.

В этой связи целью выполнения лабораторных работ является овладение указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями и в ходе освоения профессионального модуля должен:

### **иметь практический опыт:**

- настройки сервера и рабочих станций для безопасной передачи информации;
- установки Web – сервера;
- организации доступа к локальным и глобальным сетям;
- сопровождения и контроля использования почтового сервера, SQL – сервера и др.;
- расчета стоимости лицензионного программного обеспечения сетевой инфраструктуры;
- сбора данных для анализа использования и функционирования программно-технических средств компьютерных сетей;

### **уметь:**

- администрировать локальные вычислительные сети;
- принимать меры по устранению возможных сбоев;
- устанавливать информационную систему;
- создавать и конфигурировать учетные записи отдельных пользователей и пользовательских групп;
- регистрировать подключение к домену, вести отчетную документацию;
- рассчитывать стоимость лицензионного программного обеспечения сетевой инфраструктуры;
- устанавливать и конфигурировать антивирусное программное обеспечение, программное обеспечение баз данных, программное обеспечение мониторинга,
- обеспечивать защиту при подключении к Интернет средствами операционной системы;

### **знать:**

- основные направления администрирования компьютерных сетей;
- типы серверов, технологию «клиент-сервер»;
- способы установки и управления сервером;
- утилиты, функции, удаленное управление сервером;
- технологии безопасности, протоколы авторизации, конфиденциальность и безопасность при работе в Web;
- использование кластеров;
- взаимодействие различных операционных систем;

- автоматизацию задач обслуживания;
- мониторинг и настройку производительности;
- технологию ведения отчетной документации;
- классификацию программного обеспечения сетевых технологий, и область его применения;
- лицензирование программного обеспечения;
- оценку стоимости программного обеспечения в зависимости от способа и места его использования.

**Выполнение лабораторных работ способствуют формированию:**

Профессиональных и общих компетенций:

ПК 1.	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев
ПК 2.	Администрировать сетевые ресурсы в информационных системах
ПК 3.	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей
ПК 4.	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности
ОК 10.	Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей)

В результате выполнения лабораторных работ обучающиеся получают практический опыт администрирования компьютерных сетей, устранению различных возможных сбоев. Научатся администрировать сетевые ресурсы в информационных системах. Научатся обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.

**Изучаемая тема:** Сетевые операционные системы.

**Лабораторная работа № 1** «Применение сетевых утилит для определения работоспособности сети»»

**Цель работы:** получить навыки использования стандартных сетевых утилит ОС Windows

В процессе занятия решаются следующие задачи:

1. проанализировать конфигурацию сети на платформе ОС Windows;

### **Краткие теоретические и справочно-информационные материалы по теме занятия.**

Мониторинг и анализ сети представляют собой важные этапы контроля работы сети. Для решения этих задач регулярно производится сбор данных, который дает базу для измерения реакции сети на изменения и перегрузки. Чтобы осуществить сетевую передачу, нужно проверить корректность подключения клиента к сети, наличие у клиента хотя бы одного протокола сервера, знать IP-адрес компьютеров сети и т. д. Поэтому в сетевых операционных системах, и в частности, в Windows, существует множество мощных утилит для пересылки текстовых сообщений, управления общими ресурсами, диагностике сетевых подключений, поиска и обработки ошибок. Утилиты запускаются из сеанса интерпретатора команд Windows XP (Пуск -> Выполнить -> cmd).

#### **1. Сетевые утилиты**

##### **1.1. Утилита *hostname***

Выводит имя локального компьютера (хоста). Она доступна только после установки поддержки протокола TCP/IP. Пример вызова команды *hostname*:

```
C:\Documents and Settings\Администратор>hostname
```

##### **1.2. Утилита *ipconfig***

Выводит диагностическую информацию о конфигурации сети TCP/IP. Эта утилита позволяет просмотреть текущую конфигурацию IP-адресов компьютеров сети. Синтаксис утилиты *ipconfig*:

```
ipconfig [/all | /renew [адаптер] | /release [адаптер]],
```

где *all* - выводит сведения о имени хоста, DNS (Domain Name Service), типе узла, IP-маршрутизации и др. Без этого параметра команда *ipconfig* выводит только IP-адреса, маску подсети и основной шлюз;

*/renew* [адаптер] - обновляет параметры конфигурации DHCP (Dynamic Host Configuration Protocol - автоматическая настройка IP-адресов). Эта возможность доступна только на компьютерах, где запущена служба клиента DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров;

*/release* [адаптер] - очищает текущую конфигурацию DHCP. Эта возможность отключает TCP/IP на локальных компьютерах и доступна только на клиентах DHCP. Для задания адаптера используется имя, выводимое командой *ipconfig* без параметров. Эта команда часто используется перед перемещением компьютера в другую сеть. После использования утилиты *ipconfig /release*, IP-адрес становится доступен для назначения другому компьютеру.

Запущенная без параметров, команда *ipconfig* выводит полную конфигурацию TCP/IP, включая IP адреса и маску подсети.

Пример использования *ipconfig* без параметров:

```
C:\Documents and Settings\Администратор>ipconfig
```

#### **Настройка протокола IP для Windows**

**Подключение по локальной сети - Ethernet адаптер:**

DNS-суффикс этого подключения . . . :  
IP-адрес . . . . . : 10.10.11.70  
Маска подсети . . . . . : 255.255.252.0  
Основной шлюз . . . . . : 10.10.10.1

### 1.3. Утилита *net view*

Просматривает список доменов, компьютеров или общих ресурсов на данном компьютере. Синтаксис утилиты *netview*:

*net view* [*\\компьютер* | */domain[:домен]*]; *net view /network:nw* [*\\компьютер*] - используется в сетях Novell NetWare,

где *\\компьютер* - задает имя компьютера для просмотра общих ресурсов;

*/domain[:домен]* - задает домен (рабочую группу), для которого выводится список компьютеров. Если параметр не указан, выводятся сведения обо всех доменах в сети;

*/network:nw* - выводит все доступные серверы в сети Novell NetWare. Если указано имя компьютера, выводится список его ресурсов в сети NetWare. С помощью этого ключа могут быть просмотрены ресурсы и в других локальных сетях.

Вызванная без параметров, утилита выводит список компьютеров в текущем домене (рабочей группе).

Пример с параметром [\\компьютер](#):

```
C:\Documents and Settings\Администратор>net view \\  
Общие ресурсы на \\  
-----
```

Имя общего ресурса	Тип	Используется как	Комментарий
--------------------	-----	------------------	-------------

NONE (H)	Диск		
----------	------	--	--

Команда выполнена успешно.

### 1.4. Утилита *ping*

Проверяет соединения с удаленным компьютером или компьютерами. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *ping*:

*ping* [*-t*] [*-a*] [*-n счетчик*] [*-l длина*] [*-f*] [*-i ttl*] [*-v мин*] [*-r счетчик*] [*-s число*] [*[-j список комп]* | [*-k список комп*]] [*-w интервал*] список назв,

где *-t* - повторяет запросы к удаленному компьютеру, пока программа не будет остановлена;

*-a* - разрешает имя компьютера в адрес;

*-n счетчик* - передается число пакетов ECHO, заданное параметром. По умолчанию - 4;

*-l длина* - отправляются пакеты типа ECHO, содержащие порцию данных заданной длины. По умолчанию - 32 байта, максимум - 65500; *-f* - отправляет пакеты с флагом запрещения фрагментации (Do not Fragment). Пакеты не будут разрываться при прохождении шлюзов на своем маршруте;

*-i ttl* - устанавливает время жизни пакетов TTL (Time To Live); *-v мин* - устанавливает тип службы (Type Of Service) пакетов; *-r счетчик* - записывает маршрут отправленных и возвращенных пакетов в поле записи маршрута Record Route. Параметр счетчик задает число компьютеров в интервале от 1 до 9;

*-s число* - задает число ретрансляций на маршруте, где делается отметка времени;

*-j список комп* - направляет пакеты по маршруту, задаваемому параметром список\_комп. Компьютеры в списке могут быть разделены промежуточными шлюзами (свободная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;



-*k* список комп - направляет пакеты по маршруту, задаваемому параметром список\_комп. Компьютеры в списке не могут быть разделены промежуточными шлюзами (ограниченная маршрутизация). Максимальное количество, разрешаемое протоколом IP, равно 9;  
-*список назн* - указывает список компьютеров, которым направляются запросы;

Пример использования утилиты ping с параметром *список назн*:

```
C:\Documents and Settings\Администратор>ping 10.10.10.1
```

**Обмен пакетами с 10.10.10.1 по 32 байт:**

**Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128**

**Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128**

**Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128**

**Ответ от 10.10.10.1: число байт=32 время<1мс TTL=128**

**Статистика Ping для 10.10.10.1:**

**Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),**

**Приблизительное время приема-передачи в мс:**

**Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек**

### 1.5. Утилита *netstat*

Выводит статистику протокола и текущих подключений сети TCP/IP. Эта команда доступна только после установки поддержки протокола TCP/IP. Синтаксис утилиты *netstat*:

```
netstat [-a] [-e] [-n] [-s] [-p протокол] [-r] [интервал],
```

где *-a* - выводит все подключения и сетевые порты. Подключения сервера обычно не выводятся;

*-e* - выводит статистику Ethernet. Возможна комбинация с ключом *-s*;

*-n* - выводит адреса и номера портов в шестнадцатеричном формате (а не имена);

*s* - выводит статистику для каждого протокола. По умолчанию выводится статистика для TCP, UDP, ICMP (InternetControl Message Protocol) и IP. Ключ *-p* может быть использован для указания подмножества стандартных протоколов;

*-p протокол* - выводит соединения для протокола, заданного параметром. Параметр может иметь значения *tcp* или *udp*. Если используется с ключом *-s* для вывода статистики по отдельным протоколам, то параметр может принимать значения *tcp*, *udp*, *icmp* или *ip*; *-r* - выводит таблицу маршрутизации;

*интервал* - обновляет выведенную статистику с заданным в секундах интервалом.

Нажатие клавиш CTRL+C останавливает обновление статистики. Если этот параметр пропущен, *netstat* выводит сведения о текущей конфигурации один раз.

### 1.6. Утилита *tracert*

Диагностическая утилита, предназначенная для определения маршрута до точки назначения с помощью посылки эхо-пакетов протокола ICMP с различными значениями срока жизни (TTL, Time-To-Live). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета.

Это делает параметр TTL эффективным счетчиком числа ретрансляций. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP «Time Exceeded». Утилита *tracert* определяет маршрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнуто максимальное допустимое значение TTL. Маршрут определяется проверкой сообщений ICMP «TimeExceeded», полученных от промежуточных маршрутизаторов. Однако некоторые маршрутизаторы сбрасывают пакеты с истекшим временем жизни без отправки соответствующего сообщения. Эти маршрутизаторы невидимы для утилиты *tracert*. Синтаксис утилиты *tracert*:

```
tracert [-d] [-h макс_узл] [-j список компьютеров] [-w интервал] точка назн,
```

где *-d* - отменяет разрешение имен компьютеров в их адреса;

-*h макс\_узел* - задает максимальное количество ретрансляций, используемых при поиске точки назначения;  
-*j список компьютеров* - задает список компьютеров для свободной маршрутизации;  
-*w интервал* - задает интервал в миллисекундах, в течение которого будет ожидать-ся ответ; *точка назн* - указывает имя конечного компьютера.

Пример использования утилиты *tracert*:

```
C:\Documents and Settings\Администратор>tracert 10.10.10.1
```

### Трассировка маршрута к 10.10.10.1 с максимальным числом прыжков 30

```
1 <1 мс <1 мс <1 мс 10.10.10.1
```

Трассировка завершена.

### 1.7. Утилита *net use*

Подключает общие сетевые ресурсы или выводит информацию о подключениях компьютера. Команда также управляет постоянными сетевыми соединениями. Синтаксис утилиты *net use*:

```
net use [устройство | *] [\\компьютер\ресурс[\\том]] [на- роль | *] [/user:[домен]имя пользователя] [[/delete] | /persistent:{yes | no}] net use устройство [home[пароль | *]] [delete: {yes | no}] net use [/persistent:{yes | no}],
```

где *устройство* - задает имя ресурса при подключении/отключении. Существует два типа имен устройств: дисководы (от D: до Z:) и принтеры (от LPT1: до LPT3:). Ввод символа звездочки обеспечит подключение к следующему доступному имени устройства;

*\\компьютер\ресурс* - указывает имя сервера и общего ресурса. Если параметр компьютер содержит пробелы, все имя компьютера от двойной обратной черты (\\) до конца должно быть заключено в кавычки (" "). Имя компьютера может иметь длину от 1 до 15 символов; *том* - задает имя тома системы Novell NetWare. Для подключения к серверам Novell NetWare должна быть запущена служба клиента сети Novell NetWare (для Windows 2000 Professional) или служба шлюза сети Novell NetWare (для Windows 2000 Server);

*пароль* - задает пароль, необходимый для подключения к общему ресурсу;

*\** - выводит приглашение для ввода пароля. При вводе с клавиатуры символы пароля не выводятся на экран;

*/user* - задает другое имя пользователя для подключения к общему ресурсу;

*домен* - задает имя другого домена. Если домен не указан, используется текущий домен;

*имя пользователя* - указывает имя пользователя для подключения;

*/delete* - отменяет указанное сетевое подключение. Если подключение задано с символом звездочки, будут отменены все сетевые подключения;

*/home* - подключает пользователя к его основному каталогу;

*/persistent* - управляет постоянными сетевыми подключениями. По умолчанию берется последнее использованное значение. Подключения без устройства не являются постоянными;

*yes* - сохраняет все существующие соединения и восстанавливает их при следующем подключении;

*no* - не сохраняет выполняемые и последующие подключения. Существующие подключения восстанавливаются при следующем входе в систему. Для удаления постоянных подключений используется ключ */delete*. Вызванная без параметров утилита *net use* извлекает список сетевых подключений.

Пример вызова команды *net use*:

```
C:\Documents and Settings\Администратор>net use
```

### 1.8. Утилита *Net share*

Управление общими ресурсами. При вызове команды *net share* без параметров выводятся сведения обо всех общих ресурсах локального компьютера.

#### Синтаксис

```
net share [имя_ресурса] net share [имя_ресурса=диск:путь [{/users:число|unlimited}]  
[/remark:"текст"]  
[/cache: {manual|automatic|no}]] netshare [имя_ресурса [{/users:число|unlimited}]  
[/remark:"текст"]  
[/cache: {manual|automatic|no}]] net share [{имя_ресурса|диск:путь} /delete]
```

#### Параметры

*имя\_ресурса*- Сетевое имя общего ресурса. Команда **net share** *имя\_ресурса* выводит сведения об отдельном ресурсе.

*диск:путь*- Абсолютный путь к папке, которую требуется сделать общей.

*/users:число*- Максимальное количество пользователей, которым разрешен одновременный доступ к общему ресурсу.

*/unlimited*- Отмена ограничения на число пользователей, которым разрешен одновременный доступ к общему ресурсу.

*/remark:"текст"*-Добавление описательного комментария к ресурсу. Текст следует заключать в кавычки.

*/cache:automatic*- Включение автономного кэширования клиентов с автоматической реинтеграцией.

*/cache>manual*- Включение автономного кэширования клиентов с реинтеграцией вручную.

*/cache:no*- Оповещение клиента о невозможности автономного кэширования.

*/delete*- Отмена общего доступа к ресурсу.

**net help** *команда* -Отображение справки для указанной команды **net**.

#### Заметки

- Чтобы предоставить общий доступ к папке, имя которой содержит пробелы, заключите диск и путь к папке в кавычки (например "**C:\Новая папка**").
- При запросе списка всех общих ресурсов компьютера выводятся: имя общего ресурса, имена устройств или путь, связанный с устройством, а также комментарий к этому ресурсу.
- Когда общий ресурс создается на сервере, его конфигурация сохраняется. После остановки службы «Сервер» все общие ресурсы отключаются, но после следующего запуска службы «Сервер» они будут восстановлены. Имена общих ресурсов, заканчивающиеся знаком \$, не отображаются при обзоре локального компьютера с удаленного компьютера.

#### Примеры

Чтобы вывести сведения об общих ресурсах компьютера, введите: **net share**

Чтобы сделать папку «C:\Данные» общим ресурсом и включить примечание к нему, введите:

```
net share ОбщиеДанные=c:\Данные /remark:"Для отдела 123"
```

Чтобы отменить общий доступ к ресурсу Общие Данные, созданному в предыдущем примере, введите:

```
net share ОбщиеДанные /delete
```

Чтобы сделать папку «C:\Список рисунков» общим ресурсом Список, введите: **net share**  
**Список="c:\Список рисунков"**

### 3. Рекомендации и замечания

На основе рассмотренных сетевых утилит ОС Windows разрабатываются пользовательские приложения, реализующие мониторинг и диагностику локальных сетей. Они позволяют минимизировать усилия по поиску и исправлению ошибок в конфигурации сети и помогают системному администратору контролировать трафик. В настоящее время создано большое количество программ этого направления: Monitor It, Nautilus NetRanger,

CiscoWorks2000, ServiceSentinel и др. Они распространяются через Internet на условиях freeware. Windows NT Server обладает встроенными инструментами мониторинга: Event Viewer, Performance Monitor, Network Monitor.

### Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

**(При выполнении консольных команд сделать скриншот экрана и сохранить в Вашей папке в документе WORD!)**

2. Получите имя своего компьютера;
3. Выведите список доступных сетевых ресурсов своего компьютера;
4. Спросив у соседа слева имя компьютера, просмотрите его общие ресурсы;
5. Получив свой IP адрес, «опросите» его. Сначала с минимальным размером пакета, затем с максимально возможным;
6. Используя ранее полученное от соседа слева имя компьютера, определите его IP адрес;
7. Используя IP адрес полученный в предыдущем пункте, проверьте подключение к нему, используя число ретрансляций на маршруте, где делается отметка времени, равное количеству его общих сетевых ресурсов;
8. Просмотрите список всех сетевых портов на вашем компьютере и сосчитайте количество открытых (прослушиваемых);
9. Определите маршрут до сайта yandex.ru, с максимальным числом прыжков, равным значению полученному в предыдущем пункте;
10. Очистите текущую конфигурацию DHCP, затем обновите её;
11. Изучив утилиту **netsh**, измените с ее помощью свой IP адрес на статический – 192.168.1., маска подсети – 255.255.255.0;
12. Проверьте подключение к IP адресу из п.2.5;
13. Используя **netsh**, верните свой IP адрес на получение по DHCP;
14. Сделайте диск C:\ общим сетевым ресурсом, используя в качестве имени Фамилию, а в качестве комментария строку «Моя первая Шара»;
15. Выведите список общих сетевых ресурсов соседа слева;
16. Подключите созданный соседом ресурс в качестве сетевого диска «Z:»;
17. Выведите список подключений вашего компьютера;
18. Отключите сетевой диск «Z:» ;
19. Сделайте выводы;

**Время выполнения работы** 90 мин;

### Контрольные вопросы

1. Какой протокол необходим для работы с утилитой **ping**? Найти описание и характеристики протокола.
2. Можно ли утилитой **tracert** задать максимальное число ретрансляций?
3. Какой результат выдаст утилита **netstat** с параметрами **-a -s -r**? Поясните полученный результат.
4. Что такое localhost?
5. Найти самостоятельно любую стандартную сетевую утилиту Windows.

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. — 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. — 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
- 4.Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия ]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия ]/Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия ]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.- 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора[электронная версия ]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.— 2-е изд.,-М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия ]/ С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. — Пер. с англ./— СПб: Символ-Плюс, 2009. — 944 с., ил.

**Изучаемая тема:** Сетевые операционные системы.

**Лабораторная работа № 2** «Организация функционирования ЛВС на базе ОС Windows Server 2003. Настройка сервера имен»

**Цель работы:** получить навыки установки ОС Windows Server 2003, сервера имен, добавлять зоны расширения имен, включать автоматическое обновление зон

В процессе занятия решаются следующие задачи:

1. получить базовые навыки настройки сервера имен;
2. получить базовые навыки добавления зон расширения имен;
1. научиться тестировать службу DNS;
2. научиться применять файл HOSTS.

**Краткие теоретические и справочно-информационные материалы по теме занятия.**

Система доменных имен (*DNS*) была исходно определена в документах **RFC (Request for Comments) 1034 и 1035**. Эти документы определяют следующие элементы, общие для всех реализаций программного обеспечения *DNS*.

- Пространство доменных имен *DNS*, которое задает структурированную иерархию доменов, используемую для организации имен.
- Записи ресурсов, сопоставляющие доменные имена *DNS* определенным типам информации о ресурсах, которые используются при регистрации и разрешении имен в пространстве имен.
- *DNS*-серверы, которые сохраняют записи ресурсов и отвечают на запросы клиентов.
- *DNS*-клиенты, которые также называют системами разрешения имен, запрашивающие серверы для поиска и разрешения имен по типам записей ресурсов, указанным в запросе.

Пространство доменных имен *DNS*, как показано на следующем рисунке, базируется на концепции дерева именованных доменов. Каждый уровень дерева может представлять ветвь или лист дерева. Ветвь представляет уровень, на котором используется несколько имен, определяющих семейство именованных ресурсов. Лист представляет единственное имя, которое используется на этом уровне для указания конкретного ресурса.

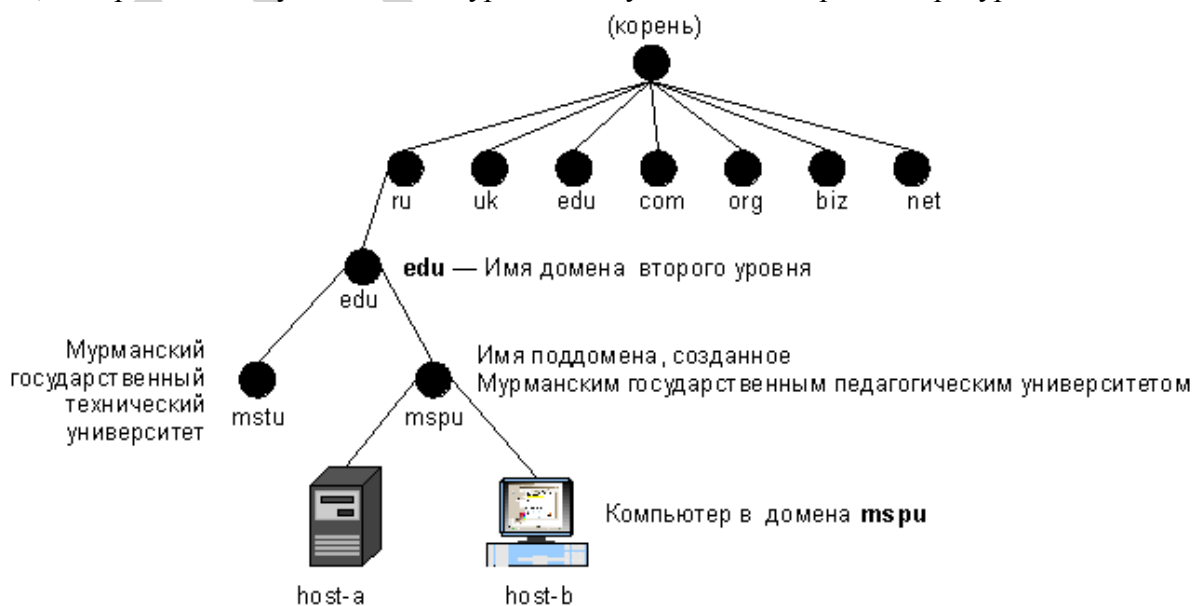


Рисунок 1. Пространство доменных имен.

В процессе разрешения имен существенно, что *DNS*-серверы часто действуют как *DNS*-клиенты, запрашивая другие серверы с целью полного разрешения имени в запросе. Любое доменное имя *DNS* в дереве технически представляет домен. Однако принято считать что имена идентифицируются одним из пяти способов на основании уровня и способа использования имени.

Тип имени	Описание	Пример
Корень доменов	Вершина дерева, представляющая неименованный уровень, иногда обозначается парой прямых кавычек (""), указывающих пустое значение. При использовании в доменном имени <i>DNS</i> для этого применяется завершающая точка (.), свидетельствующая, что имя расположено в корне или на самом верхнем уровне иерархии доменов. В данном случае доменное имя <i>DNS</i> рассматривается как полное и указывает на точное расположение в дереве имен. Имена, установленные таким способом, называют полными доменными именами ( <i>Fully Qualified Domain Name, FQDN</i> ).	Единственная точка (.) или точка, использованная в конце имени, например, « <b>example.microsoft.com.</b> »
Домен верхнего уровня	Имя из двух или трех букв, которое используется, чтобы указать страну/регион или тип организации.	« <b>.ru</b> » указывает имя, зарегистрированное для коммерческого использования в Интернете.
Домен второго уровня	Имена переменной длины, зарегистрированные для индивидуальных пользователей или организаций для использования в Интернете. Эти имена всегда базируются на соответствующем домене верхнего уровня в зависимости от типа организации или географического расположения, в котором используется имя.	« <b>edu.ru.</b> » является именем домена второго уровня, зарегистрированным для образовательных учреждений регистратором доменных имен <i>DNS</i> Интернета.
Поддомен	Дополнительные имена, которые организация может создавать как производные от зарегистрированного имени домена второго уровня. Такие имена обеспечивают рост дерева имен <i>DNS</i> в организации и его распределение по отделам или по географическому расположению.	« <b>mspu.edu.ru.</b> » представляет имя поддомена Мурманского государственного педагогического университета.
Имя узла или ресурса	Имя, представляющее лист в дереве имен <i>DNS</i> , которое определяет конкретный ресурс. Обычно край-	« <b>host-a.mspu.edu.ru.</b> », где первая метка (« <b>host-a</b> ») представляет имя узла <i>DNS</i> для конкретного компьютера в

	<p>няя левая метка в доменном имени <i>DNS</i> определяет конкретный компьютер в сети. Например, имя этого уровня, используемое в записи ресурса узла (A), используется для поиска IP-адреса компьютера по его имени узла.</p>	<p>сети.</p>
--	--	--------------

Например, доменное имя *DNS*, зарегистрированное для образовательных учреждений (**edu.ru.**), представляет домен второго уровня. Это имя состоит из двух частей (называемых метками), показывающих, что оно находится на втором уровне сверху от корня или вершины дерева. Большинство доменных имен *DNS* содержат две или большее число меток, каждая из которых задает новый уровень в дереве. Точки используются в именах для разделения меток.

*DNS* представляет способ интерпретации полного пути к доменному имени *DNS* аналогично способу интерпретации полного пути к файлу или каталогу в окне командной строки. Например, путь в дереве каталогов помогает указать на точное расположение файла, сохраненного на компьютере. Для компьютеров с операционной системой **Windows** обратная косая черта (\) указывает каждый новый каталог, ведущий к точному расположению файла. Эквивалентным символом в *DNS* является точка (.), указывающая каждый новый уровень домена в имени. Для *DNS* примером имени с несколькими уровнями может служить следующее полное доменное имя узла: **host-a.mspu.edu.ru.** В отличие от имен файлов, при чтении полного доменного имени узла *DNS* слева направо осуществляется переход от наиболее конкретной информации (имя *DNS* компьютера «**host-a**») к наиболее общей (завершающая точка (.), которая указывает корень в дереве имен *DNS*). Этот пример демонстрирует четыре уровня доменов *DNS*, которые ведут от конкретного расположения «**host-a**».

1. Домен «**mspu**», в котором зарегистрировано для использования имя компьютера «**host-a**».
2. Домен «**edu**», который соответствует родительскому домену, являющемуся корнем поддомена «**mspu**».
3. Домен «**ru**», который соответствует домену верхнего уровня, предназначенному для использования организациями из России, который является корнем для домена «**edu**».
4. Завершающая точка (.), представляющая стандартный символ разделителя, которая используется, чтобы сделать полным доменное имя *DNS* в дереве пространства имен *DNS*.

### Работа запросов *DNS*

Когда *DNS*-клиенту требуется найти имя, используемое в программе, он запрашивает *DNS*-серверы для сопоставления имени. Каждое сообщение с запросом, отправляемое клиентом, содержит информацию трех типов, определяющую вопрос, на который отвечает сервер:

1. указанное доменное имя *DNS* в виде полного доменного имени узла (**FQDN**);
2. указанный тип запроса, в котором задается либо тип записей ресурсов, либо тип операции запроса;
3. указанный класс доменного имени *DNS*.

Для *DNS*-серверов **Windows** этот класс всегда должен быть указан как класс Интернета (**IN**).

Например, указанное имя может представлять полное доменное имя узла для компьютера, такое как «**host-a.mspu.edu.ru.**», и тип запроса на поиск записей ресурсов адреса (A) для этого имени. Запрос *DNS* можно представить как вопрос клиента, состоящий из двух частей, например «*Имеются ли записи ресурсов A для компьютера с именем*



'*hostname.mspu.edu.ru.*'?» Когда клиент получает ответ от сервера, он читает и интерпретирует содержащуюся в ответе запись ресурса А, узнавая IP-адрес компьютера, запрошенного по имени.

Запросы *DNS* используют несколько способов сопоставления имен. Клиент может иногда ответить на запрос с помощью локальной кэшированной информации, полученной в предыдущем запросе. *DNS*-сервер может использовать собственный кэш информации о записях ресурсов для ответа на запрос. *DNS* -сервер может также запросить или обратиться к другим *DNS*-серверам в интересах запрашивающего клиента для полного сопоставления имени, а затем отправить ответ клиенту. Этот процесс называют *рекурсией*.

В дополнение к этому, клиент может самостоятельно пытаться установить контакт с дополнительными *DNS*-серверами для сопоставления имени. При этом клиент использует отдельные дополнительные запросы, базирующиеся на ссылочных ответах от серверов. Этот процесс называют *итерацией*. В общем случае процесс запроса *DNS* выполняется в две стадии.

1. Запрос к имени начинается на клиентском компьютере и передается в систему сопоставления имен службы *DNS*-клиент.
  2. Когда не удается ответить на запрос на локальном уровне, можно для сопоставления имени запрашивать *DNS*-серверы по мере необходимости.
- Обе стадии процесса подробнее рассматриваются в следующих разделах.

### Локальная система разрешения имен

На начальных этапах процесса в программе на локальном компьютере используется доменное имя *DNS*. Затем запрос передается в службу «*DNS*- клиент» для сопоставления с помощью локальной кэшированной информации. Если удастся разрешить запрошенное имя, поступает ответ на запрос и процесс завершается. Кэш локального сопоставления имен может включать информацию об именах из двух возможных источников.

1. Если имеется локальный файл **Hosts**, все сопоставления имен и адресов из этого файла предварительно загружаются в кэш при запуске службы «*DNS*-клиент».
2. Записи ресурсов, полученные в ответах на запросы из предыдущих запросов *DNS*, добавляются в кэш и сохраняются в нем в течение определенного периода времени.

Если клиент не находит сопоставления в кэше, процесс продолжается с помощью запроса на разрешение имени от клиента к *DNS*-серверу.

### Запрос к *DNS*-серверу

Клиент запрашивает основной *DNS*-сервер. Из глобального списка выбирается сервер, используемый на начальной стадии запроса от клиента к серверу. Когда *DNS*-сервер принимает запрос, он сначала проверяет, можно ли дать удостоверяющий ответ на базе записей ресурсов, содержащихся в локальной зоне в конфигурации сервера. Если запрошенное имя соответствует информации в записи ресурса в локальной зоне, сервер дает удостоверяющий ответ, используя эту информацию для разрешения имени. Если в зоне нет информации для запрошенного имени, сервер проверяет, можно ли разрешить имя, используя информацию предыдущих запросов в локальном кэше. Если здесь обнаруживается совпадение, сервер отвечает с использованием этой информации. И в этом случае, если основной сервер может дать запрашивающему клиенту утвердительный ответ на сопоставление из собственного кэша, запрос завершается. Если на основном сервере не удастся найти запрошенное имя — ни в кэше, ни в зонах — процесс выполнения запроса может продолжаться с использованием рекурсии для полного разрешения имени. При этом другие *DNS*-серверы помогают разрешить имя. Служба «*DNS*-клиент» по умолчанию указывает серверу использовать процесс рекурсии для полного разрешения имен в интересах клиентов перед возвращением ответа. В большинстве случаев *DNS*-серверы по умолчанию настраиваются на поддержку процесса рекурсии, как показано на следующем рисунке.

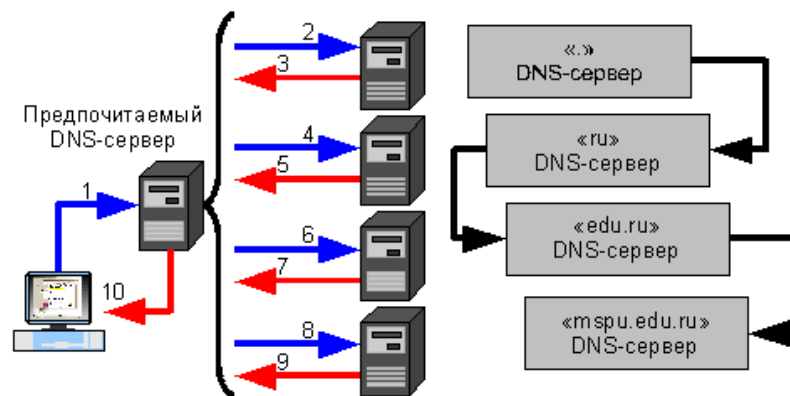


Рисунок 2. Процесс рекурсии при разрешении имени.

Для правильного выполнения рекурсии *DNS*-сервером ему необходимы сведения о контактах с другими *DNS*-серверами в пространстве доменных имен *DNS*. Такая информация обеспечивается в виде корневых ссылок, списка предварительных записей ресурсов, которые могут использоваться службой *DNS* для обнаружения других *DNS*-серверов, которые являются удостоверяющими для корня дерева пространства доменных имен *DNS*. Корневые серверы являются удостоверяющими для корня доменов и доменов верхнего уровня в дереве пространства доменных имен *DNS*.

Ранее отмечалось, что процесс заканчивается возвращением клиенту утвердительного ответа. Однако запросы могут возвращать и другие ответы. Приведем наиболее общие типы таких ответов:

1. удостоверяющий ответ;
2. утвердительный ответ;
3. ссылочный ответ;
4. отрицательный ответ.

*Удостоверяющий ответ* представляет утвердительный ответ, возвращенный клиенту и доставленный с установленным битом полномочий в сообщении *DNS*, указывающим, что ответ получен от сервера, имеющего прямые полномочия для запрашиваемого имени.

*Утвердительный ответ* может содержать запрошенную запись ресурса или список записей ресурсов (который также называют набором записей), соответствующих запрошенному доменному имени *DNS* и типу записи, указанному в сообщении запроса.

*Ссылочный ответ* содержит дополнительные записи ресурсов, не указанные по имени или типу в запросе. Ответ этого типа возвращается клиенту, если процесс рекурсии не поддерживается. Эти записи должны рассматриваться как справочные, которые могут использоваться клиентом для продолжения запроса с помощью итераций. Если клиент способен использовать итерации, он может выполнить дополнительные запросы в попытке полностью разрешить имя самостоятельно.

*Отрицательный ответ* от сервера может указывать на один из двух возможных результатов попытки сервера обработать и рекурсивно полностью и удостоверяющим образом сопоставить имя в запросе:

- Удостоверяющий сервер ответил, что запрошенное имя не существует в пространстве имен *DNS*.
- Удостоверяющий сервер ответил, что запрошенное имя существует, но для этого имени отсутствуют записи указанного типа.

Система сопоставления имен передает результаты запроса в виде утвердительного или отрицательного ответа в запрашивающую программу и кэширует ответ. Итерации представляют тип сопоставления имен, используемый *DNS*-клиентами и серверами при выполнении следующих условий.

- Клиент запрашивает использование рекурсии, но рекурсия отключена на *DNS*-сервере.
- Клиент не запрашивает использование рекурсии при запросе к *DNS*-серверу.

Итерационный запрос от клиента сообщает *DNS*-серверу, что клиент ожидает от *DNS*-сервера наиболее точный ответ немедленно без обращения к другим *DNS*-серверам. Когда используются итерации, *DNS*-сервер отвечает клиенту о запрошенных именах на основании собственной информации о пространстве имен. Например, если *DNS*-сервер в интрасети получает запрос от локального клиента для имени «*www.edu.ru*», он может вернуть ответ из кэша имен. Если в данный момент запрошенное имя не сохраняется в кэше сервера, то сервер может ответить предоставлением ссылки — т.е. списка записей ресурсов других *DNS*-серверов, которые ближе к имени, запрошенному клиентом. Когда предоставляется ссылка, *DNS*-клиент принимает на себя ответственность за продолжение итерационных запросов на сопоставление имени к другим указанным в конфигурации *DNS*-серверам. Например, в наиболее общем случае *DNS*-клиент может расширить область поиска до серверов корневого домена в Интернете в попытках обнаружить удостоверяющие *DNS*-серверы для домена «*ru*». После установления контакта с корневыми серверами Интернета клиент может получить от них дальнейшие итерационные ответы, указывающие на фактические *DNS*-серверы Интернета для домена «*edu.ru*». Когда клиенту предоставляются записи для этих *DNS*-серверов, он может отправить дальнейший итерационный запрос внешним *DNS*-серверам *edu* в Интернете, которые могут дать определенный и удостоверяющий ответ. При использовании итераций *DNS*-сервер может также содействовать в запросе на сопоставление имени, предоставив клиенту собственный наиболее точный ответ. Для большинства итерационных запросов клиент использует локальный список *DNS*-серверов для обращения к другим серверам имен в пространстве имен *DNS*, если его собственный основной *DNS*-сервер не может сопоставить имя в запросе.

По мере того как *DNS*-серверы обрабатывают запросы клиентов с помощью рекурсии или итераций, они находят и накапливают значительный объем информации о пространстве имен *DNS*. Эта информация *кэшируется* сервером. Кэширование дает возможность ускорить сопоставление часто используемых имен *DNS* в последующих запросах и существенно снижает трафик запросов *DNS* в сети. При выполнении рекурсивных запросов *DNS*-серверами для клиентов они временно кэшируют записи ресурсов. Кэшированные записи ресурсов содержат информацию, полученную от *DNS*-серверов, которые являются удостоверяющими для доменных имен *DNS*. Эта информация накапливается при выполнении итерационных запросов в процессе поиска и полного ответа на рекурсивный запрос, выполняемый в интересах клиента. Когда затем другие клиенты размещают новые запросы на информацию, отвечающую кэшированным записям ресурсов, *DNS*-сервер может использовать данные из кэшированных записей ресурсов для ответа. При кэшировании информации значение срока жизни применяется ко всем кэшированным записям ресурсов. Пока не истек срок жизни кэшированной записи ресурса, *DNS*-сервер может продолжать кэшировать и снова использовать запись ресурса при ответах на соответствующие запросы клиентов. Значения срока жизни кэширования, используемые записями ресурсов в большинстве конфигураций зон, назначаются в параметре **Мин. срок жизни TTL (по умолчанию)**, который задается в начальной записи зоны. По умолчанию задается значение минимального срока жизни 3600 секунд (1 час), но это значение может быть изменено; могут также задаваться отдельные значения срока жизни для каждой записи ресурса.

### **Обратный просмотр**

В большинстве операций просмотра *DNS*-клиенты обычно выполняют *прямой просмотр*, т. е. поиск, основанный на имени *DNS* другого компьютера, сохраненного в записи ресурса адреса (A). В этом типе запроса в качестве данных для ответа на запрос ожидается IP-адрес. *DNS* также обеспечивает возможность *обратного просмотра*, в котором клиенты используют известный IP-адрес для поиска имени компьютера по этому адресу. Обратный просмотр фактически является формой вопроса типа «Можете ли вы сказать мне имя *DNS* компьютера, который использует IP-адрес 192.168.1.20?».

Система *DNS* не разрабатывалась изначально для поддержки запросов этого типа. Одной из проблем при поддержке запросов обратного просмотра является различие в способах организации и индексации пространства имен *DNS* и способов назначения IP-адресов. Если бы единственным таким способом был бы поиск во всех доменах пространства имен *DNS*, то для обработки обратного запроса потребовалось бы слишком много времени и такой запрос оказался бы бесполезным.

Чтобы разрешить эту проблему, в стандартах *DNS* был определен и зарезервирован специальный домен в пространстве имен *DNS* Интернета, **in-addr.arpa**, обеспечивающий практичный и надежный способ выполнения обратных запросов. Чтобы создать обратное пространство имен, поддомены в домене **in-addr.arpa** формируются с помощью обратного упорядочения чисел в точечно-десятичной нотации IP-адресов. Такое обратное упорядочение доменов для каждого октета необходимо, поскольку в отличие от имен *DNS*, для которых IP-адреса читаются слева направо, здесь интерпретация выполняется в обратном порядке. Когда IP-адрес читается слева направо, информация анализируется от наиболее общей (IP-адрес сети в левой части адреса) до наиболее конкретной (IP-адрес узла в последнем октете). По этой причине порядок октетов IP-адреса должен быть обращен при построении дерева домена **in-addr.arpa**. IP-адреса дерева *DNS in-addr.arpa* могут делегироваться организациям, которым назначается ограниченный набор IP-адресов в границах определенных для Интернета классов адресов. И, наконец, для дерева домена **in-addr.arpa**, встроенного в *DNS*, требуется определение дополнительного типа записей ресурсов — запись ресурса указателя (**PTR**). Такая запись ресурса используется для сопоставления в зоне обратного просмотра, обычно соответствующего записи ресурса именованного узла (**A**) для имени *DNS* компьютера в зоне прямого просмотра.

Следующий рисунок иллюстрирует обратный запрос, инициируемый *DNS*-клиентом (**host-b**), которому требуется узнать имя другого узла (**host-a**) по его IP-адресу 192.168.1.20.

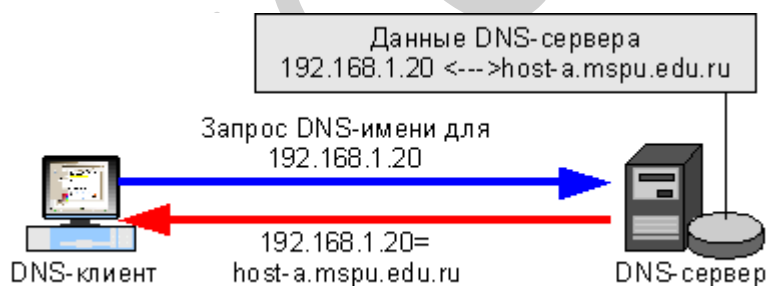


Рисунок 3. Обратный запрос.

Как показано на рисунке, обратный запрос включает следующие этапы.

1. Клиент «**host-b**» запрашивает *DNS*-сервер о записи ресурса указателя (**PTR**), сопоставляющей IP-адрес 192.168.1.20 для имени «**host-a**».

Поскольку запрос относится к записям **PTR**, система сопоставления имен обращает адрес и добавляет имя домена «**in-addr.arpa**» в конец обращенного адреса. В результате образуется полное доменное имя узла («**20.1.168.192.in-addr.arpa**»), для которого будет проводиться поиск в зоне обратного просмотра.

2. После обнаружения имени удостоверяющий *DNS*-сервер для имени «**20.1.168.192.in-addr.arpa**» может вернуть ответ с информацией записи **PTR**. В этой информации содержится доменное имя *DNS* узла «**host-a**», что приводит к завершению процесса обратного просмотра. Необходимо помнить, что если запрошенное обратное имя не может быть возвращено *DNS*-сервером, можно использовать сопоставление имен *DNS* (либо рекурсию, либо итерации) для обнаружения *DNS*-сервера, который является удостоверяющим для зоны обратного просмотра и содержит запраши-

ваемое имя. В этом смысле процесс сопоставления имен при обратном просмотре аналогичен процессу прямого просмотра

### Инвертированные запросы

Инвертированные запросы являются устаревшим средством, которое ранее было предложено как часть стандарта *DNS* для поиска имени узла по его IP-адресу. В них используются нестандартные операции запросов *DNS*, а их применение ограничено ранними версиями программы **Nslookup**, которая является утилитой командной строки для устранения неполадок и тестирования службы *DNS*.

Служба *DNS* распознает и принимает сообщения инвертированных запросов и отвечает на них с имитацией ответа на инвертированный запрос.

### Динамическое обновление

Динамическое обновление позволяет компьютерам *DNS*-клиентов регистрировать и динамически обновлять собственные записи ресурсов с помощью *DNS*-сервера при каждом возникновении изменений. Это снижает необходимость администрирования записей зон вручную, в особенности для клиентов, которые путешествуют или часто меняют расположение и получают IP-адреса через *DHCP*.

Клиентские и серверные службы *DNS* поддерживают использование динамических обновлений, как описано в документе *RFC 2136*, «*Dynamic Updates in the Domain Name System*». Служба *DNS*-сервер поддерживает включение и отключение динамических обновлений отдельно для каждой зоны на каждом сервере, настроенном для загрузки либо стандартной основной зоны, либо зоны, интегрированной в каталоги. Служба *DNS*-клиент будет по умолчанию динамически обновлять свои записи ресурсов узла (A) в *DNS*, когда была выполнена настройка для *TCP/IP*.

Динамические обновления обычно запрашиваются, когда изменяется имя *DNS* или IP-адрес компьютера. Например, предположим, что для клиента с именем «oldhost» в окне **Свойства системы** заданы следующие имена:

Имя компьютера	oldhost
Доменное DNS-имя компьютера	mspu.edu.ru.
Полное имя компьютера	oldhost.mspu.edu.ru

Таблица 2. Старые имена компьютера.

В этом примере в конфигурации компьютера нет доменных имен *DNS*, специфических для подключения. В дальнейшем компьютер переименовывается из «oldhost» в «newhost», в результате чего имена изменяются следующим образом.

Имя компьютера	newhost
Доменное DNS-имя компьютера	mspu.edu.ru.
Полное имя компьютера	newhost.mspu.edu.ru

Таблица 3. Новые имена компьютера.

После изменения имени в окне **Свойства системы** отображается приглашение перезагрузить компьютер. Когда при перезагрузке компьютер запускает ОС, служба *DHCP*-клиент выполняет следующие действия для обновления *DNS*.

1. Служба *DHCP*-клиент отправляет запрос для типа начальной записи зоны (**SOA**) с использованием доменного имени *DNS* компьютера. Клиентский компьютер использует текущее полное доменное имя узла компьютера (в данном случае «newhost.mspu.edu.ru») как имя, указанное в этом запросе.

2. Удостоверяющий *DNS*-сервер зоны, содержащей полное доменное имя узла клиента, отвечает на запрос типа **SOA**.

3. После этого служба *DHCP*-клиент пытается установить контакт с основным *DNS*-сервером.

Клиент обрабатывает ответ на запрос *SOA* для его имени, чтобы определить IP-адрес *DNS*-сервера, удостоверенного как основной сервер, для принятия его имени. Да-

лее он выполняет такую последовательность шагов, необходимых, чтобы установить контакт и динамически обновить его основной сервер.

а. Клиент отправляет запрос на динамическое обновление основному серверу, определенному в ответе на запрос **SOA**.

*Если обновление выполняется успешно, другие действия не предпринимаются.*

б. При отказе на обновление клиент отправляет запрос типа **NS** (о серверах имен) для зоны, имя которой указано в записи **SOA**.

с. Когда клиент получает ответ на этот запрос, он отправляет запрос **SOA** на первый **DNS**-сервер, перечисленный в ответе.

д. После разрешения имен в запросе **SOA** клиент отправляет динамическое обновление серверу, указанному в возвращенной записи **SOA**. *Если обновление выполняется успешно, другие действия не предпринимаются.*

е. При отказе на обновление клиент повторяет запрос **SOA**, отправляя его к следующему **DNS**-серверу, перечисленному в ответе.

4. Как только находится основной сервер, который может выполнить обновление, клиент отправляет запрос на обновление, который обрабатывается сервером.

Содержимое запроса на обновление включает инструкции добавить записи ресурсов **A** (и возможно **PTR**) для имени «**newhost.mspu.edu.ru**» и записи этих типов для ранее зарегистрированного имени «**oldhost.mspu.edu.ru**».

Сервер также выполняет проверку, разрешены ли обновления для запроса клиента. Для стандартных основных зон динамические обновления не являются безопасными, поэтому для клиентов должны выполняться любые попытки обновления. Для зон, интегрированных в службу каталогов **Active Directory**, обновления являются безопасными и выполняются с помощью параметров безопасности, устанавливаемых на основе каталогов.

Динамические обновления отправляются или выполняются периодически. По умолчанию компьютер отправляет обновления каждые 7 дней. Если в результате обновления данные в зоне не изменяются, зона остается в текущей версии и никакие изменения не записываются. Обновления выполняются только при фактических изменениях имен и адресов в зоне или в результате добавочной зонной передачи.

#### **Безопасное динамическое обновление**

Безопасные обновления **DNS** доступны только для зон, интегрированных в службу каталогов **Active Directory**. После преобразования зоны в интегрированную становится возможным использование с консоли **DNS** списков управления доступом. Можно добавлять пользователей и группы в списки или удалять их для указанной зоны или записи ресурса. Параметры безопасного динамического обновления для **DNS**-серверов и клиентов по умолчанию обрабатываются следующим образом.

- **DNS**-клиенты сначала предпринимают попытки выполнить небезопасные динамические обновления. При отказе на небезопасные обновления клиенты пытаются выполнить безопасные обновления.

*Кроме того, клиенты используют политику обновления по умолчанию, которая позволяет им пытаться переписывать ранее зарегистрированную запись ресурса, если она специально не заблокирована условиями безопасности обновления.*

- После интегрирования зоны в службу каталогов **Active Directory DNS**-серверам **Windows Server 2003** по умолчанию разрешаются только безопасные динамические обновления.

*При использовании стандартного сохранения зон настройки по умолчанию службы **DNS**-сервер не разрешают динамические обновления зон. И для зон, интегрированных в каталоги, и для использующих стандартное сохранение в файлах можно изменить параметры зоны и разрешить динамические обновления. Это позволяет принимать любые обновления.*

При развертывании *DNS*-серверов совместно с *Active Directory* необходимо иметь в виду следующее:

- Служба *DNS* требуется для обнаружения контроллеров доменов **Windows Server 2003**. Служба сетевого входа в систему использует новые средства поддержки *DNS*-серверов для обеспечения регистрации контроллеров доменов в пространстве доменных имен *DNS*.

- *DNS*-серверы **Windows Server 2003** могут использовать службу каталогов *Active Directory* для сохранения и репликации зон.

*При интегрировании зон в службу каталогов пользователи получают возможность использовать дополнительные средства *DNS*, такие как безопасные динамические обновления и средства устаревания и очистки записей.*

Способы интеграции *DNS* со службой каталогов *Active Directory*:

- При установке *Active Directory* на сервер выполняется повышение сервера до роли контроллера указанного домена. Когда данный процесс завершается, пользователю выводится приглашение указать доменное имя *DNS* для домена *Active Directory*, для которого выполняется присоединение и повышение сервера.

- Если в этом процессе удостоверяющий *DNS*-сервер для указанного домена либо не обнаруживается в сети, либо не поддерживает протокол динамического обновления *DNS*, выводится приглашение установить *DNS*-сервер. Такая возможность предоставляется, поскольку *DNS*-серверу необходимо отыскать этот сервер или другие контроллеры домена для рядовых серверов домена *Active Directory*.

После установки *Active Directory* имеются две возможности сохранения и репликации зон при работе с *DNS*-сервером на новом контроллере домена.

- Стандартное сохранение зоны с помощью файла в текстовом формате.

*Зоны, сохраняемые в этом способе, размещаются в файлах с расширением *DNS*, которые сохраняются в папке `systemroot\System32\Dns` на каждом компьютере, на котором выполняется *DNS*-сервер. Имя файла зоны соответствует имени, которое пользователь выбрал для зоны при ее создании, например, `mstu.edu.ru.dns`, если именем зоны является «`mstu.edu.ru.dns`».*

- Сохранение зон, интегрированных в службу каталогов, с помощью базы данных *Active Directory*. Зоны, сохраняемые таким образом, размещаются в дереве *Active Directory* под разделом каталога домена или приложения. Каждая зона, интегрированная в службу каталогов, сохраняется в контейнере `dnsZone`, который идентифицируется по имени, выбранному пользователем при ее создании.

Преимущества интеграции с *Active Directory*

В сетях с развертыванием *DNS* для поддержки службы каталогов *Active Directory* настоятельно рекомендуется использовать основные зоны, интегрированные в службу каталогов, которые предоставляют следующие преимущества.

- Обновление с несколькими главными серверами и расширенные средства безопасности, базирующиеся на возможностях *Active Directory*.

В модели стандартного сохранения зон обновления *DNS* выполняются на основе модели с единственным главным сервером. В такой модели единственный удостоверяющий *DNS*-сервер зоны обозначается как основной источник для зоны. Это сервер содержит главную копию зоны в файле на локальном диске. В этой модели основной сервер зоны представляет единственную фиксированную точку отказа. Если этот сервер недоступен, запросы на обновление зоны от *DNS*-клиентов не обрабатываются. При сохранении зон, интегрированных в службу каталогов, динамические обновления *DNS* выполняются с использованием модели с несколькими главными серверами. В этой модели любой удостоверяющий *DNS*-сервер, например, контроллер домена, выполняющий службу *DNS*-сервер, обозначается как основной источник для зоны. Поскольку главная копия зоны поддерживается в базе данных *Active Directory*, которая полностью

реплицируется на все контроллеры домена, зона может обновляться любыми *DNS*-серверами, выполняющимися на любом контроллере домена.

При использовании модели *Active Directory* с несколькими главными серверами любой из основных серверов для зоны, интегрированной в каталоги, может обрабатывать запросы от *DNS*-клиентов на обновление зоны, пока контроллер домена является доступным по сети. Кроме того, при использовании зон, интегрированных в службу каталогов, можно с помощью списков управления доступом защитить объект-контейнер *dnsZone* в дереве каталогов. Это средство обеспечивает дифференцированный доступ к зоне или к конкретной записи ресурса в зоне. Например, список управления доступом для записи ресурса в зоне можно ограничить так, чтобы разрешить динамические обновления только указанному компьютеру клиента или группе безопасности, например, группе администраторов домена. Это средство безопасности недоступно для стандартных основных зон. Необходимо отметить, что при преобразовании зоны к типу интегрированной в службу каталогов настройка по умолчанию для обновлений зоны изменяется и разрешаются только безопасные обновления. Кроме того, при использовании списков управления доступом на объектах *Active Directory*, относящихся к *DNS*, списки управления доступом могут применяться только к службе *DNS*-клиент.

- Репликация и синхронизация зон с новыми контроллерами домена выполняется автоматически при каждом добавлении нового контроллера в домен *Active Directory*.

Хотя службу *DNS* можно выборочно удалять с контроллеров домена, зоны, интегрированные в службу каталогов, всегда сохраняются на каждом контроллере домена. В результате сохранение и управление зонами не является дополнительным ресурсом. Кроме того, способы синхронизации информации, сохраняемой в службе каталогов, обеспечивают повышение быстродействия по сравнению со стандартными способами сохранения обновлений зон, которые могут потенциально потребовать передачи зоны целиком.

- За счет сохранения баз данных зон *DNS* в *Active Directory* имеется возможность рационализировать репликацию баз данных в сети.

Когда пространство имен *DNS* и домены *Active Directory* сохраняются и реплицируются независимо, необходимо обеспечить планирование и администрирование каждого из них в отдельности. Например, при одновременном использовании стандартного сохранения зон *DNS* и службы каталогов *Active Directory* необходимо обеспечить структуру, реализацию, тестирование и управление для двух различных топологий репликации баз данных. Одна топология требуется для репликации данных из каталогов между контроллерами домена, а другая топология может потребоваться для репликации баз данных зон между *DNS*-серверами.

Это приведет к дополнительным трудностям при планировании и разработке структуры сети с учетом ее естественного роста. За счет интеграции сохранения информации *DNS* появляется возможность унифицировать вопросы управления и репликации для *DNS* и *Active Directory*, объединяя их в единое административное целое.

- Репликация каталогов выполняется быстрее и эффективнее, чем стандартная репликация *DNS*.

Поскольку репликация *Active Directory* выполняется на уровне отдельных свойств, распространяются только необходимые изменения. При этом для зон, интегрированных в службу каталогов, используется и отправляется меньший объем данных.

## Порядок работы

### Средства для выполнения работы:

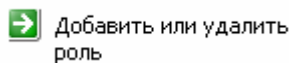
- аппаратные: компьютер с установленной ОС Windows XP.
- программные: приложение VM: VirtualBox; виртуальные машины: VM-1, VM-2; установочные образы ОС: win2003.iso.



1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

### Задание 1. Установка сервера DNS

1. Запустите виртуальную машину VM VM-2.
2. Подключите к виртуальной машине образ установочного диска *win2003.iso*.
3. Откройте диалоговое окно **Управление данным сервером** (**Пуск/Администрирование/Управление Данным Сервером**).
4. Активизируйте установку сервера имен:
  - запустите мастер добавления ролей сервера, кнопкой *Добавить или удалить роль*



- ознакомьтесь с информацией мастера и продолжите установку кнопкой *Далее*;
- укажите тип установки Особая конфигурация и продолжите установку кнопкой *Далее*.
- выберите в списке доступных ролей сервера пункт **DNS-сервер**. Нажмите *Далее*.
- Ознакомьтесь с сводкой выбранных параметров и продолжите установку кнопкой *Далее*. *После завершения установки сервера имен, автоматически запустится Мастер настройки DNS-сервера.*
- 5. Выполните первоначальную настройку **DNS-сервера** с помощью мастера:
  - ознакомьтесь с информацией мастера (*Далее*);
  - ознакомьтесь с предлагаемыми вариантами настройки сервера;
  - выберите создание зоны прямого просмотра для небольших сетей, соответствующей радиокнопкой (*Далее*);
  - укажите ваш **DNS-сервер** в качестве **DNS-сервера**, который будет обслуживать зону прямого просмотра, радиокнопкой *Управление зоной выполняется этим сервером*. Продолжите установку кнопкой *Далее*;

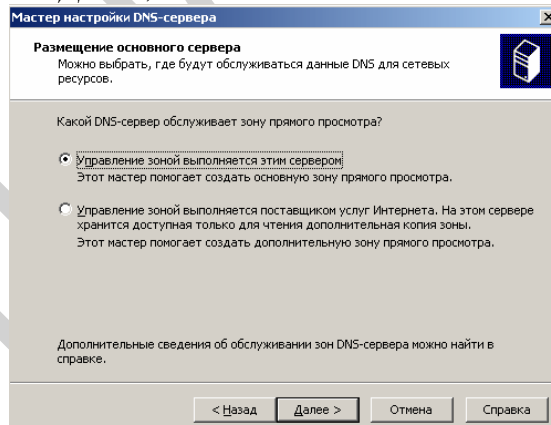


Рисунок 4. Размещение основного сервера

- задайте имя зоны, например **example.edu.ru** и продолжите установку кнопкой *Далее*.
- введите в поле **Создать новый файл** имя файла (например *example.edu.ru.dns*) в котором будет храниться конфигурация зоны. Продолжите установку кнопкой *Далее*;
- запретите динамическое обновление соответствующей радиокнопкой и продолжите настройку кнопкой *Далее*;
- откажитесь от пересылки запросов на другие **DNS-сервера**, выбрав радиокнопку *Нет, не пересылать запросы* (*Далее*);
- ознакомьтесь с информацией о недоступности корневых сертификатов и щелкните **OK**;
- завершите первоначальную настройку **DNS-сервера** кнопкой **Готово**.

### Задание 2. Настройка сервера DNS.

1. Переключитесь в диалоговое окно **Управления данным сервером**.

2. Перейдите в управление *DNS*-сервером, кнопкой *Управление этим DNS-сервером*. Появится окно консоли администрирования, с открытой оснасткой управления *DNS*-сервером

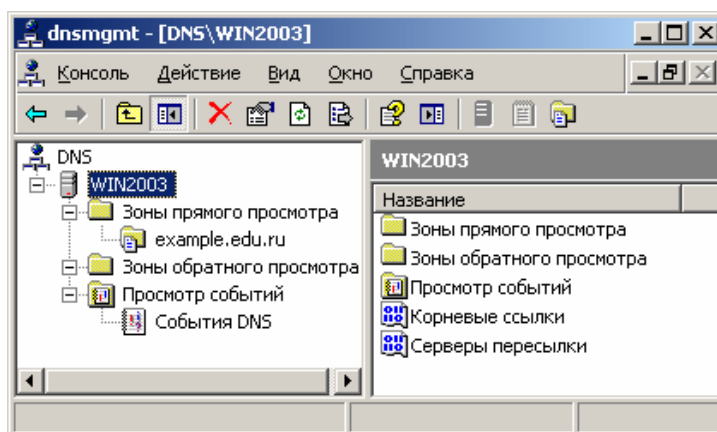


Рисунок 5. Создание зоны прямого просмотра.

3. Настройте зону прямого просмотра:
- откройте диалоговое окно свойств созданной ранее зоны **example.edu.ru** (*контекстное меню/Свойства*)
  - настройте очистку и обновление содержимого *DNS*-сервера:
    - откройте окно очистки, кнопкой **Очистка**;
    - установите флажок *Удалять устаревшие записи ресурсов*;
    - установите **интервал блокирования** - 1 день;
    - установите **интервал обновления** - 7 дней;
    - подтвердите изменения кнопкой **ОК**.
  - установите **срок жизни (TTL) записи** – 2 часа:
    - перейдите на вкладку **Начальная запись зоны (SOA)**;
    - введите в поле **Срок жизни (TTL) записи** – 0: 2: 0: 0;
    - установите **желаемые интервалы для обновления и повтора** - не менее 1 и не более 15 минут.

Завершите настройку кнопкой **ОК**.

4. Создайте запись в *DNS*-сервере соответствующую физическому компьютеру:
- откройте диалоговое окно **добавления новых узлов** (*контекстное меню example.edu.ru/Создать узел (A)*);
  - введите в поле **Имя** - <имя\_физического\_компьютера>;
  - введите в поле **IP-адрес** - 192.168.1.1;
  - завершите добавление кнопкой **Добавить**.
5. Создайте новую основную зону обратного просмотра:
- откройте **мастер создания новых зон** (*контекстное меню Зоны обратного просмотра/Создать новую зону*);
  - ознакомьтесь с информацией мастера и щелкните **Далее**;
  - укажите **тип создаваемой зоны** - *Основная зона (Далее)*;
  - укажите **код сети** – 192.168.1 (*Далее*);

*Поскольку IP-адреса создаваемой сети к сети класса C, то в IP-адресах сети будет меняться только последний разряд адреса.*

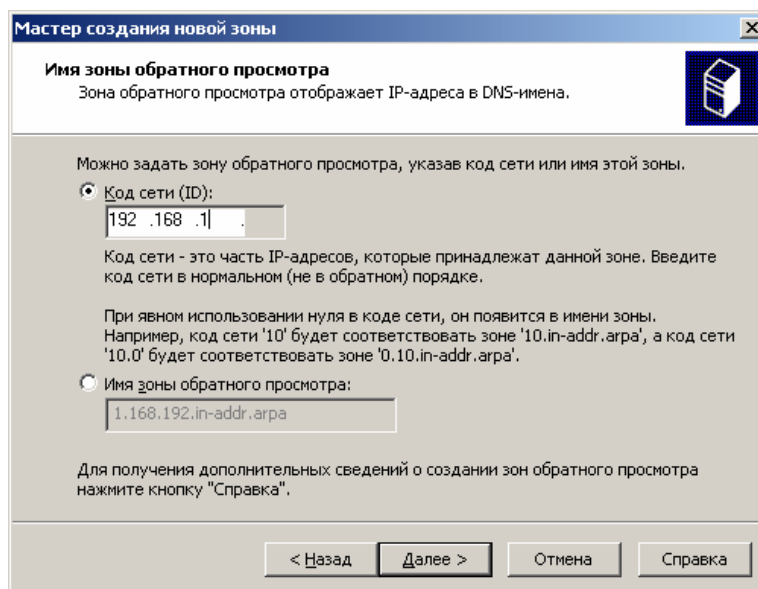


Рисунок 6. Задание кода сети

- укажите имя файла для зоны по умолчанию и продолжите установку кнопкой *Далее*.
- установите запрет динамических обновлений (*Далее*);
- завершите создание зоны кнопкой *Готово*.
- 6. Протестируйте работу *DNS*-сервера:
  - откройте диалоговое окно свойств *DNS*-сервера (*контекстное меню Wind2003/Свойства*);
  - перейдите на вкладку **Наблюдение**;
  - установите флажок *Простой запрос к этому DNS-серверу*;
  - активируйте тестирование кнопкой *Тест*;  
*Результат отобразится в поле Результаты теста.*
  - создайте и сохраните в своей папке снимок экрана с результатами теста;
  - закройте диалоговое окно свойств кнопкой *ОК*.
- 7. Выключите VM.

### Самостоятельная работа

Установите *DNS*-сервер для домена **faculty.ru**. Настройте прямую и обратную зоны, протестируйте сервер с помощью оснастки *DNS*, командной строки и виртуальной машины с Windows XP. Зафиксируйте все шаги установки, настройки и тестирования *DNS*-сервера с помощью скриншотов в отчете.

**Время выполнения работы** 90 мин;

### Контрольные вопросы

1. Для чего предназначены прямые и обратные запросы поиска?
2. Опишите назначение компонентов *DNS*: зона, сервер имен,
3. доменное пространство имен.
4. Назовите основные типы зон и их назначение.
5. Назовите основные правила именования доменов.
6. Какова максимально допустимая длина имени домена?
7. Какова максимально допустимая длина имени FQDN?
8. С какой целью используют несколько серверов имен?
9. Приведите примеры использования утилиты nslookup.
10. Можно ли одному IP-адресу нужно присвоить несколько имен?
11. Перечислите все способы.
12. Для чего используется файл **HOSTS**?
13. В каком порядке нужно располагать записи в файле **HOSTS** – упорядоченными по какому-либо параметру или произвольно?

## **Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М.: Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия ]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия ]/Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия ]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.-736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора[электронная версия ]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия ]/ С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2009. – 944 с., ил.

**Изучаемая тема:** Сетевые операционные системы.

**Лабораторная работа № 3** «Организация функционирования ЛВС на базе ОС Windows Server 2003. Установка и настройка DHCP-сервера»

**Цель работы:** получить навыки работы по установке и удалению DHCP-сервера;

В процессе занятия решаются следующие задачи:

1. формирование навыков настройки области действия DHCP-сервера;
2. формирование навыков резервирования адресов;

**Краткие теоретические и справочно-информационные материалы по теме занятия.**

**DHCP** (англ. *Dynamic Host Configuration Protocol* — протокол динамической настройки узла) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Данный протокол работает по модели «клиент-сервер». Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к так называемому серверу DHCP, и получает от него нужные параметры. Сетевой администратор может задать диапазон адресов, распределяемых сервером среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве сетей TCP/IP.

DHCP является расширением протокола BOOTP, использовавшегося ранее для обеспечения бездисковых рабочих станций IP-адресами при их загрузке. DHCP сохраняет обратную совместимость с BOOTP.

**Порядок работы**

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Значение адреса узла, на котором будет работать DHCP-сервер, равно 192.168.1.1 и зарезервировано, а диапазон динамически выдаваемых адресов 192.168.1.11 – 192.168.1.100

**Задание 1.** Назначить серверу сетевые параметры.

**Указания к выполнению**

1. Запустите виртуальную машину с Microsoft Windows Server 2003. Будем называть эту машину *сервером сети*.
2. Назначьте виртуальной машине IP-адрес 192.168.1.1, маска подсети 255.255.255.0.
3. Проверьте с помощью утилиты IPconfig правильность настройки сетевых параметров.
4. На физическом компьютере проверьте доступность виртуальной машины с помощью утилиты ping.

Поместите скриншоты командной строки для обеих утилит в отчет.

**Задание 2.** Установите DHCP-сервер на виртуальной машине.

**Указания к выполнению**

1. Для установки DHCP-сервера проделайте следующие действия (чтобы установить DHCP-сервер, также можно воспользоваться программой **Manage Your Server (Управление данным сервером)**, выбрав команду **Add or remove a role (Добавить или удалить роль)**.
  - Откройте **Control Panel (Панель управления)**, затем **Add/Remove Programs (Установка и удаление программ)**.
  - На вкладке **Add/Remove Windows Components (Установка компонентов Windows)** найдите **Networking Services (Сетевые службы)** и нажмите **Details (Состав)**.

- Поставьте галочку около **Dynamic Host Configuration Protocol (Протокол Динамической конфигурации хостов)** и подтвердите свой выбор.
- Дождитесь завершения установки сервера.

2. Проверьте, что после установки сервера в меню **Administrative Tools (Администрирование)** добавилась новая оснастка – **ДНСП**. Эта оснастка используется для настройки ДНСП-сервера. Если в оснастке **ДНСП** нет вашего сервера, то в меню нужно выбирать команду **Add server (Добавить сервер)**, а затем указать имя ДНСП-сервера или найти его с помощью клавиши **Browse (Обзор)**.

3. Запуск и остановка ДНСП-сервера производятся при помощи пункта контекстного меню ДНСП-сервера **All tasks (Все задачи)**.

4. Заметьте, что перед использованием ДНСП-сервера в сети с установленной службой каталога Active Directory, его нужно авторизовать (для авторизации ДНСП-сервера необходимо запустить оснастку **ДНСП** и в контекстном меню объекта, расположенного в корне пространства имен утилиты, выбрать пункт **Manage authorized servers (Список авторизованными серверами)**). Система покажет список уже авторизованных ДНСП-серверов. Нажмите кнопку **Authorize (Авторизовать)** и укажите имя авторизуемого ДНСП-сервера или его IP-адрес. Выбранный сервер будет немедленно добавлен в список авторизованных серверов.)

Сохраните в отчете скриншот оснастки ДНСП.

**Задание 3.** Создать область действия ДНСП-сервера со следующим диапазоном IP-адресов: 192.168.1.11 – 192.168.1.100.

#### **Указания к выполнению**

1. Запустите оснастку **ДНСП**.
2. В контекстном меню конфигурируемого ДНСП-сервера выберите пункт **New Scope (Создать область)**.
3. В окне **Scope Name (Имя области)** определите имя для создаваемой области действия и дайте ей краткое описание. Используйте понятные имена, которые позволяют легко определить область действия в том случае, если на ДНСП-сервере хранится несколько областей.
4. В окне мастера **IP Address Range (Диапазон адресов)** определите пул IP-адресов, для которых создается область действия. Пул задается путем указания начального (192.168.1.10) и конечного адреса (192.168.1.100) диапазона. Также указывается маска подсети (255.255.255.0).
5. В окне **Add Exclusions (Добавление исключений)** можно определить исключения из только что определенного диапазона, при этом можно исключать как отдельные адреса, так и целые диапазоны. Для исключения одиночного IP-адреса необходимо указать его в поле **Start IP address (Начальный IP-адрес)**. Поле **End IP address (Конечный IP-адрес)** необходимо оставить в этом случае пустым. После нажатия кнопки **Add (Добавить)** введенный адрес будет добавлен в список исключенных из диапазона адресов.
6. В окне **Lease Duration (Время аренды)** определяется время аренды IP-адресов (по умолчанию – 8 дней).
7. На следующей странице мастера будет задан вопрос – требуется ли определить опции ДНСП для создаваемой области действия непосредственно в ходе работы мастера или это будет сделано администратором впоследствии. Определите опции сразу же:
  - **IP address of router (Адрес шлюза по умолчанию)** – поставьте адрес сервера (нажмите клавишу **Add**, чтобы он появился в списке);
  - **DNS server (DNS сервер)** – добавьте адрес сервера;
  - **WINS server** – добавьте адрес сервера или оставьте пустым, если служба WINS в сети не работает.
8. В конце работы мастера необходимо выбрать **Yes, activate scope now (Активизировать область действия сейчас)**

9. Если служба DHCP-сервера функционирует нормально, на значке сервера должна появиться зеленая стрелка. Красная стрелка указывает, что служба не работает, в этом случае следует обновить информацию о сервере (контекстное меню сервера – **Refresh**) или перезапустить службу (контекстное меню сервера – **All Tasks – Restart**).

Поместите в отчете скриншот оснастки DHCP.

**Задание 4.** Проверить работу DHCP-сервера.

**Указания к выполнению**

1. Запустите виртуальную машину с Microsoft Windows XP. Эта машина будет являться DHCP-клиентом, будем называть её *рабочей станцией*.

2. Настройте рабочую станцию на автоматическое получение IP-адреса и имени DNS-сервера.

- Откройте окно свойств **Подключение по локальной сети** и выберите **Протокол Интернета (TCP/IP)**.

- Установите переключатель в положение **Получить IP-адрес автоматически**.

3. Выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила сетевые параметры от DHCP-сервера.

Поместите в отчете скриншот командной строки.

**Задание 5.** Резервируйте для рабочей станции постоянный IP-адрес 192.168.1.20.

**Указания к выполнению**

1. Запустите оснастку **DHCP**.

2. Для просмотра текущих аренд откройте раздел **Address Leases (Аренды адресов)** и найдите аренду для рабочей станции.

3. Определите MAC-адрес станции (столбец **Unique ID**) и запишите его.

4. В контекстном меню раздела **Reservations (Резервирования)** выбираем **New reservation...** и вводим параметры – имя резервирования, необходимый IP-адрес (192.168.1.20), MAC-адрес станции.

Поместите в отчет скриншот окна.

5. На рабочей станции выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила зарезервированный IP-адрес от DHCP-сервера.

Поместите в отчете скриншот командной строки.

**Задание 6.** Резервируйте для рабочей станции адрес вне текущей области действия DHCP-сервера.

**Указания к выполнению**

1. Выполните резервирование для рабочей станции IP-адреса вне области действия DHCP-сервера, например, 192.168.1.200.

2. Проверьте на рабочей станции, получила ли она новые параметры.

Поместите в отчете скриншоты выполненных действий.

**1. Задание 7.** Настройте мониторинг DHCP-сервера.

**Указания к выполнению**

1. Служба DHCP-сервера ведет мониторинг своих действий, записывая их в журнал (**audit logging**). Этот журнал можно использовать при решении проблем с DHCP-сервером.

2. Чтобы включить журнал, откройте окно свойств DHCP-сервера (контекстное меню сервера – **Properties**). На вкладке **General (Общие)** выберите пункт **Enable DHCP audit logging (Разрешить мониторинг DHCP)**.

3. Файлы журнала находится в следующем каталоге:

**C:\Windows\system32\dhcp**. Файлы создаются ежедневно и называются по следующему принципу: к постоянному имени **DhcpSrvLog** добавляется обозначение дня недели, например, журнал понедельника называется **DhcpSrvLog-Mon.log**.

4. Просмотрите файл журнала за текущий день. В начале журнала приводятся значения кодов событий. Затем указывается точное время и краткое описание события.

5. Найдите в журнале записи, соответствующие вашим действиям в этой лабораторной работе.

Сохраните в отчете текст файла журнала.

### Самостоятельная работа

Сохраняйте в отчете скриншоты каждого действия.

Установите диапазон адресов для DHCP-сервера 172.16.0.1 – 172.16.0.10, маска подсети 255.240.0.0. Проверьте работу DHCP-сервера. Установите зарезервированный за рабочей станцией IP-адрес 172.16.0.20. Проверьте получение станцией адреса. Используйте вкладку альтернативной конфигурации рабочей станции на случай отключения службы DHCP. Протестируйте полученные настройки. Что такое автоматические частные адреса? Протестируйте их получение и работу сети в случае, если DHCP-сервер оказывается недоступным.

**Время выполнения работы 90 мин;**

### Контрольные вопросы

1. Для чего предназначена служба DHCP?
2. Что означает термин «аренда адреса»?
3. Для каких компьютеров сети следует применять резервирование адреса?
4. Какой IP-адрес шлюза по умолчанию определяют для подсети DHCP-сервера?
5. Какой IP-адрес вы дадите шлюзу по умолчанию для компьютера-арендатора адреса, находящегося в другой подсети (маска 255.255.240.0), если IP-адрес DHCP-сервера 201.212.96.1, а маска подсети 255.255.240.0?
6. Какой IP-адрес шлюза по умолчанию вы определите для подсети DHCP-сервера, IP-адрес которого 201.212.96.1, а маска подсети 255.255.240.0?
7. Установите соответствия между протоколами и выполняемыми ими функциями:

Протоколы	Функции протоколов
1. DHCP	а. Отображение IP-адресов на MAC-адреса.
2. DNS	б. Присвоение IP-адресов клиентским компьютерам.
3. ARP	в. Отображение доменных имен на IP-адреса.

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### Критерии оценки:

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.



4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов [электронная версия] / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора [электронная версия] / Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 [электронная версия] / Пер. с англ. - М.: ООО «И.Д.Вильямс», 2011. - 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора [электронная версия] / Ч. Рассел, Ш. Кроуфорд, Дж. Джеренд., пер. с англ. — 2-е изд., - М.: Русская Редакция, 2007. - 656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия] / С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия] / Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия] / Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. - М.: ООО «И.Д. Вильямс», 2011. - 1456 с.: ил. - Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство [электронная версия] / Т. Лимончелли, К. Хоган, С. Чейлап - 2-е издание. — Пер. с англ. / - СПб: Символ-Плюс, 2009. — 944 с., ил.

**Изучаемая тема:** Программное обеспечение для управления сетевыми операционными системами.

#### Лабораторная работа № 4 «Удалённое управление компьютером»

**Цель работы:** получить практические навыки удаленного администрирования компьютеров;

В процессе занятия решаются следующие задачи:

1. формирование навыков удаленного администрирования серверов, рабочих станций;

#### **Краткие теоретические и справочно-информационные материалы по теме занятия.**

Для выполнения административных задач на компьютерах сети часто используется специальное программное обеспечение удаленного управления.

##### **Удаленный рабочий стол**

*Подключение к удаленному рабочему столу* — это технология, позволяющая пользователю, работающему за своим компьютером, связываться с удаленным компьютером, находящимся в другом месте. Например, можно подключиться к рабочему компьютеру из домашнего компьютера и получить доступ ко всем программам, файлам и сетевым ресурсам (как если бы вы работали за рабочим компьютером). Можно оставить программы выполняться на рабочем компьютере, а дома вывести на экран рабочий стол рабочего компьютера и продолжить работу с выполняющимися программами.

Удаленный рабочий стол работает по протоколу **RDP** (англ. *Remote Desktop Protocol*, протокол удалённого рабочего стола) — протокол прикладного уровня, использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений. Клиенты существуют практически для всех версий **Windows** (включая **Windows CE** и **Mobile**), **Linux**, **Free BSD**, **Mac OS X**. По умолчанию используется порт **TCP 3389**. Официальное название **Майкрософт** для клиентского программного обеспечения - **Remote Desktop Connection** или **Terminal Services Client (TSC)**, в частности, клиент в **Windows XP/2003/vista** называется *mstsc.exe*.

## Virtual Network Computing (VNC)

VNC система удалённого доступа к рабочему столу компьютера, использующая протокол [RFB](#) (*Remote FrameBuffer*). Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть.

Система VNC платформонезависима: VNC-клиент, называемый *VNC viewer*, запущенный на одной операционной системе, может подключаться к VNC-серверу, работающему любой другой ОС. Существуют реализации клиентской и серверной части практически для всех операционных систем, в том числе и для Java. К одному VNC-серверу одновременно могут подключаться множественные клиенты. Наиболее популярные способы использования VNC — удалённая техническая поддержка и доступ к рабочему компьютеру из дома.

VNC была разработана компанией [AT&T](#). Оригинальные исходные коды доступны на условиях лицензии [GNU General Public License](#), как и многие варианты VNC, существующие на данный момент.

VNC состоит из двух частей: *клиента* и *сервера*. *Сервер* — программа, предоставляющая доступ к экрану компьютера, на котором она запущена. *Клиент* (или *viewer*) — программа, получающая изображение экрана с сервера и взаимодействующая с ним.

VNC — очень простой протокол, основанный на графических примитивах: «Положить прямоугольник пиксельных данных на заданную координатами позицию». *Сервер* посылает небольшие прямоугольники *клиенту*. Такая схема в своей примитивной форме потребляет большую часть пропускной возможности канала. Для снижения нагрузки на канал используются различные методы. Существуют различные кодировки — методы определения наиболее эффективного способа передачи этих прямоугольников. Протокол VNC позволяет клиенту и серверу «договориться» о том, какая кодировка будет использована. Самый простой метод кодирования, поддерживаемый всеми клиентами и серверами — «raw encoding», при котором пиксели передаются в порядке слева-направо, сверху-вниз, и после передачи первоначального состояния экрана передаются только изменившиеся пиксели. Этот метод работает очень хорошо при незначительных изменениях изображения на экране (движения указателя мыши по рабочему столу, набор текста под курсором), но загрузка канала становится очень высокой при одновременном изменении большого количества пикселей, например, при просмотре видео в полноэкранном режиме.

По умолчанию VNC использует диапазон портов с **5900** до **5906**. Каждый порт представляет собой соответствующий экран [X-сервера](#) (порты с **5900** по **5906** ассоциированы с экранами с **:0** по **:6**). Java-клиенты, доступные во многих реализациях, использующих встроенный web-сервер для этой цели, например, в **RealVNC**, связаны с экранами таким же образом, но на диапазоне портов с **5800** до **5806**. Порты могут быть изменены. Многие компьютеры под управлением ОС **Windows** могут использовать лишь один порт из-за отсутствия многопользовательских свойств, присущих UNIX-системам. Для **Windows**-систем экран по умолчанию — **:0**, что соответствует порту **5900**.

Сегодня существует большое количество программ удаленного управления рабочим столом, основанных на VNC. Перечислим некоторые из них: [TightVNC](#), [RealVNC](#), [UltraVNC](#), [TridiaVNC](#), [Radmin](#)

### Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

### Задание 1. Установите на виртуальный компьютер программу *UltraVNC*.

В задании используется ВМ *VM-1*.

1. Запустите виртуальную машину **VM-1** и загрузите ОС **Windows XP**.
2. Подготовьте **VM-1** для удаленного управления:
  - переключитесь в **VM-1**;

- разрешите удаленные подключения к компьютеру:
    - откройте диалоговое окно **Свойства системы (Пуск/Панель управления/Система)**;
    - активизируйте вкладку **Удаленные сеансы**;
    - установите флажок *Разрешить удаленный доступ к этому компьютеру*;
    - добавьте пользователя, которому разрешено удаленное подключение:
      - откройте диалоговое окно добавления пользователей кнопкой **Выбрать удаленных пользователей**;
      - щелкните по кнопке **Добавить**;
      - введите **имя пользователя - администратор**;
      - подтвердите выбор кнопкой **ОК**;
      - закройте диалоговое окно добавления пользователей кнопкой **ОК**;
    - закройте окно **Свойства системы** кнопкой **ОК**;
  - подключите к виртуальному компьютеру образ диска **CD-For-LAB.iso**.
3. Подключитесь к виртуальному компьютеру с помощью **Удаленного рабочего стола**:
- подключитесь к виртуальному компьютеру **VM-1** с помощью удаленного рабочего стола:
    - запустите **приложение удаленного рабочего стола (Пуск/Программы/Стандартные/Связь/Подключение к удаленному рабочему столу)**;
    - введите в поле **Компьютер** - *<имя удаленного компьютера>* (например, **VM-1**);

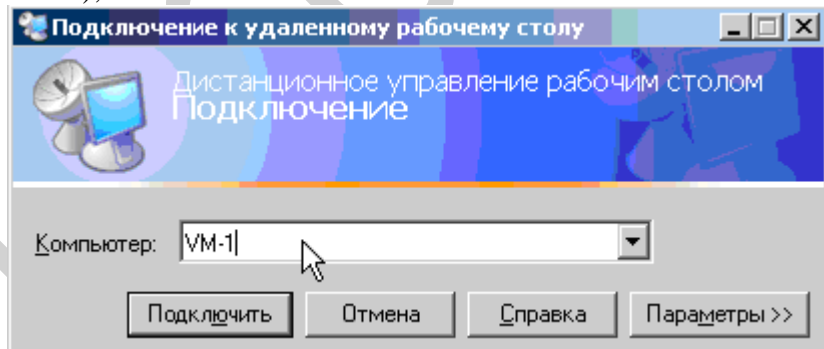


Рисунок 1. Окно подключения к удаленному рабочему столу

- настройте подключение через медленный канал связи:
    - отобразите параметры **Подключения к удаленному рабочему столу** кнопкой **Параметры**;
    - перейдите на вкладку **Дополнительно**;
    - выберите в раскрывающемся списке *Модем (28,8 Кбит/с)*;
  - выполните подключение кнопкой **Подключить**.
4. Установите приложение **UltraVNC** на виртуальный компьютер:
- перейдите в каталог с устанавливаемой программой;
  - запустите процесс установки (**UltraVNC-1.0.4-RC6-Setup.exe**);
  - ознакомьтесь с информацией установщика и щелкните **Next**;
  - ознакомьтесь с лицензионным соглашением и согласитесь с ним *I accept the agreement* и щелкните **Next**;
  - ознакомьтесь с информацией о версии устанавливаемого программного обеспечения и щелкните **Next**;
  - укажите **каталог установки** - **C:\Program Files\UltraVNC** и щелкните **Next**;
  - укажите **тип установки** – **Full Installation** и щелкните **Next**;

- введите **имя желаемой папки** в меню **Пуск** (например *UltraVNC*) и подтвердите кнопкой *Next*;
  - сбросьте флажок *Download Vista addons files now* (Скачать дополнительные файлы для **Windows Vista**) и щелкните *Next*;
  - сбросьте флажок *Download and Install the mirror driver* (Загрузить и установить драйвер **mirror**) и щелкните *Next*;
  - выполните дополнительные задачи по установке, установите следующие флажки:
    - *Register UltraVNC as a system Service* (Зарегистрировать *UltraVNC* как сервис);
    - *Start or restart UltraVNC service* (Запустить или остановить сервис *UltraVNC*);
    - *Create UltraVNC desktop icon* (создать ярлык на рабочем столе);
    - *Associate UltraVNC Viewr with the .vnc file extension* (Ассоциировать *UltraVNC Viewr* с файлами *.vnc*);
    - подтвердите изменения кнопкой *Next*;
  - инициализируйте установку кнопкой *Install*;  
*на заднем фоне появится диалоговое окно свойств сервера UltraVNC*
  - ознакомьтесь с послеустановочной информацией и щелкните *Next*;
  - завершите установку кнопкой *Finish*.
5. Выполните настройку *UltraVNC*:
- задайте пароль в поле **VNC Password** - *qwerasdf*;
  - задайте действие при множественных подключениях к серверу – *Keep existing connections* (удерживать существующие соединения);
  - подтвердите изменения кнопкой *OK*.

## Задание 2. Установите удаленно на виртуальный компьютер браузер *Opera*.

1. Подключитесь к виртуальному компьютеру **VM-1** с помощью *UltraVNC Viewer*:
  - запустите с диска к лабораторным работам *UltraVNC Viewer (vncviewer.exe)*;
  - введите в поле **VNC Server** - *<имя удаленного компьютера> (VM-1)*;
  - установите режим подключения для просмотра (флажок *View only*);
  - активируйте подключение кнопкой *Connect*;
  - введите пароль для подключения - *qwerasdf*;
2. Переключитесь из режима просмотра в нормальный (*контекстное меню окна UltraVNC Viewer/View only*);
3. Установите браузер *Opera*:
  - перейдите в каталог с устанавливаемой программой;
  - запустите процесс установки (*Opera\_9.24\_International\_Setup.exe*);
  - укажите желаемый язык установки - *Русский (OK)*;
  - активизируйте процесс установки кнопкой *Установить*;
  - ознакомьтесь с лицензионным соглашением и согласитесь с ним кнопкой *Принимаю*;
  - укажите тип установки – *Стандартная* и щелкните *Далее*;
  - установите приложение кнопкой *Установить*;
  - завершите процесс установки кнопкой *Готово*.
4. Создайте и сохраните в своей домашней папке снимок экрана виртуального компьютера с запущенным браузером *Opera*.

**Время выполнения работы** 90 мин;

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. — 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. — 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
- 4.Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия ]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия ]/Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия ]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.- 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора[электронная версия ]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.— 2-е изд.,-М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия ]/ С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. — Пер. с англ./– СПб: Символ-Плюс, 2009. — 944 с., ил.

**Изучаемая тема:** Программное обеспечения для управления сетевыми операционными системами.

## Лабораторная работа № 5 «Использование утилиты Backup»

**Цель работы:** получить практический опыт архивирования данных и научиться пользоваться службой восстановления системы.

В процессе занятия решаются следующие задачи:

1. формирование навыков создания резервных копий;
2. Получить навыки архивирования и восстановления системы, используя стандартные утилиты Windows Server 2003.
3. Решить задачи сетевого администратора связанные с сохранением, архивированием информации, и ее последующим восстановлением

### Краткие теоретические и справочно-информационные материалы по теме занятия.

#### Архивация и восстановление

**Мастер архивации и восстановления (*Backup or Restore Wizard*)** создает копию файлов и папок на указанном пользователем носителе информации. В случае потери или повреждения пользовательских данных их можно восстановить из файла резервной копии. Специалисты рекомендуют выполнять регулярное создание резервных копий важных файлов и папок. Частота архивации (*резервного копирования*) зависит от частоты изменений файлов, так как в случае потери данных придется повторно создать то, что было сделано после последней архивации. По этой причине многие компании создают резервные копии важных файлов ежедневно. Пользователь может выбирать различные типы архивации в зависимости от его требований.

- Для типа *Обычная (Normal)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, и каждый файл маркируется как прошедший архивацию (имеющий резервную копию).
- Для типа *Копирование (Copy)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, но файлы не маркируются как прошедшие архивацию.
- Для типа *Добавочная (Incremental)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, и каждый файл маркируется как прошедший архивацию.
- Для типа *Разностная (Differential)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, но файлы не маркируются.
- Для типа *Ежедневная (Daily)* происходит архивация только тех файлов, которые были созданы или изменены в данный день, но файлы не маркируются.

Тип архивации, который применяется, определяет, насколько сложным будет процесс восстановления. Для восстановления после нескольких добавочных или разностных архиваций необходимо выполнить восстановление из последней обычной резервной копии и из всех добавочных или разностных копий, полученных после обычной архивации и вплоть до настоящего момента.

Выполняя архивацию данных, пользователь указывает имя и место для файла резервной копии. По умолчанию файлы резервных копий сохраняются с расширением *.bkf*. Файлы архивации можно сохранять на жестком диске, на гибком диске или на любом другом типе съемного носителя. При выборе места для резервной копии нужно учитывать размер файла архивации, типы имеющихся носителей, а также возможное требование того, что файлы резервных копий нужно хранить отдельно от компьютера на случай катастрофы.

### **Функция восстановления системы**

Восстановление системы позволяет выполнить откат состояния операционной системы к одной из точек восстановления, фиксирующих состояние на момент, когда система стабильно работала. Преимуществом данной функции заключается в том, что она предоставляет возможность быстрого восстановления ("отката" состояния системы к с остоянию, в котором она находилась в один из предыдущих моментов во времени) без переустановки системы, а также не подвергает риску случайного перезаписывания рабочих файлов пользователей. Возможно выполнение отката к любому из следующих типов контрольных точек и точек восстановления.

- *Начальная контрольная точка (initial system checkpoint)* системы создается при первом запуске компьютера с вновь установленной ОС.
- Точки восстановления для автоматических обновлений (*Automatic update restore points*) создаются, когда инсталлируются обновления, которые загружаются с помощью **Windows Update**.
- Точки восстановления при восстановлении с резервной копии (*Backup recovery restore points*) создаются, когда пользователь использует мастер архивации или восстановления (**Backup or Restore Wizard**).
- Пользователь может создавать свои собственные точки восстановления вручную (*"ручные" контрольные точки - manual checkpoints*) в любой момент с помощью мастера восстановления системы (**System Restore Wizard**).
- Точки восстановления при инсталляции программ (*Program name installation restore points*) создаются, при установке программного обеспечения.
- Точки восстановления для операции восстановления (*Restore operation restore points*) создаются каждый раз, когда пользователь осуществляет какое-либо восстановление.
- *Системные контрольные точки (System checkpoints)* - это запланированные точки восстановления, которые создаются компьютером регулярно, даже если пользователь не вносил никаких изменений в систему.
- Точки восстановления для неопознанного устройства (*Unsigned device driver restore points*) создаются, когда устанавливается драйвер устройства, который не был опознан или сертифицирован.

Средство **Восстановление системы (System Restore)** обычно сохраняет набор контрольных точек восстановления за период от одной до трех недель. Количество контрольных точек восстановления, доступных в любой заданный момент времени, ограничено объемом пространства, которое выделено пользователем для работы системы восстановления. Максимальный размер пространства, которое можно выделить, составляет приблизительно 12 процентов.

В ходе процедуры восстановления происходит восстановление ОС и программ, инсталлированных на компьютере, к состоянию, в котором они находились на момент выбранной контрольной точки восстановления. Этот процесс не затрагивает личные файлы пользователя (включая сохраненные документы, сообщения электронной почты, адресную книгу, список **Избранные (Favorites)** и список **Журнал (History) Интернет Explorer**).

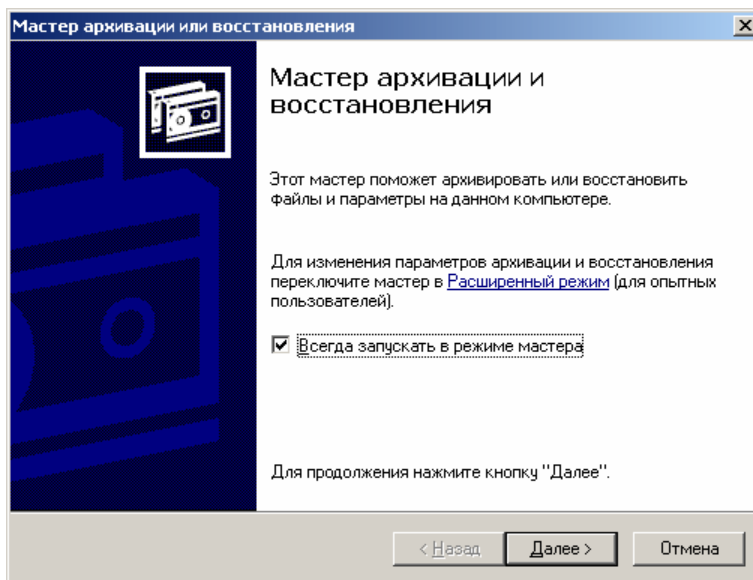
Все изменения, внесенные утилитой **Восстановление системы (System Restore)**, полностью обратимы, и если пользователя не удовлетворяют результаты, то можно восстановить предыдущие настройки и выполнить все снова.

### **Порядок работы**

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

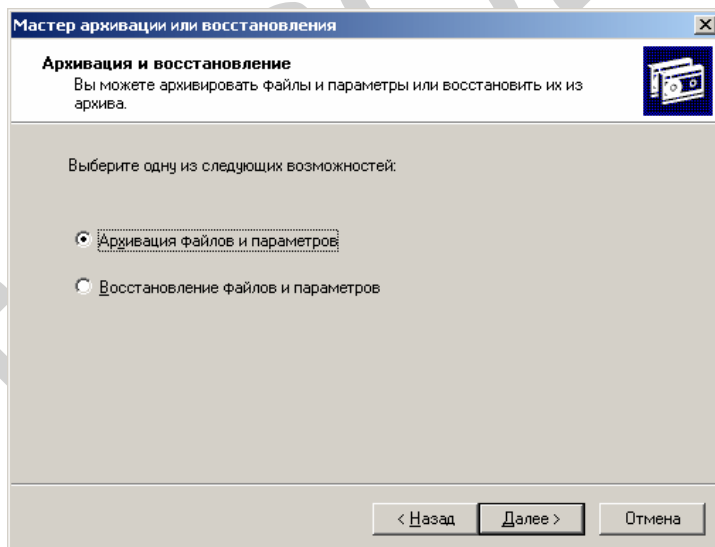
**Задание 1. Выполните резервное копирование системных конфигурационных файлов.**

1. Запустите виртуальную машину VM-1 и загрузите ОС Windows.
2. Запустите **Мастер Архивации (Пуск/Программы/Стандартные/ Службные/Архивация данных)**.
3. Ознакомьтесь с информацией мастера и щелкните *Далее*.



*Рисунок 1. Мастер Архивации данных.*

4. Выберите возможность мастера – **Архивация файлов и параметров** и щелкните *Далее*.



*Рисунок 2. Выбор архивации или восстановления.*

5. Укажите выбор элементов архивирования в самостоятельном режиме – *Предоставить возможность выбора объектов для архивации* и щелкните *Далее*.



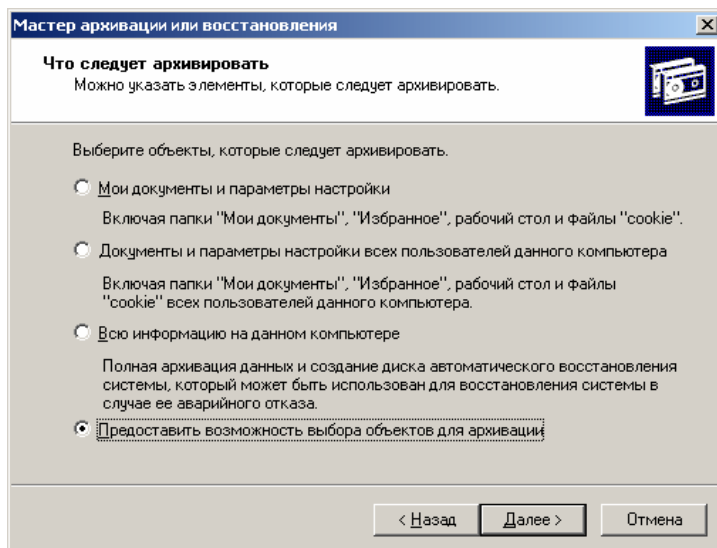


Рисунок 3. Выбор способа указания объектов архивирования.

6. Укажите элементы для архивации – папки *Documents and Settings* и *Program Files* и щелкните *Далее*.

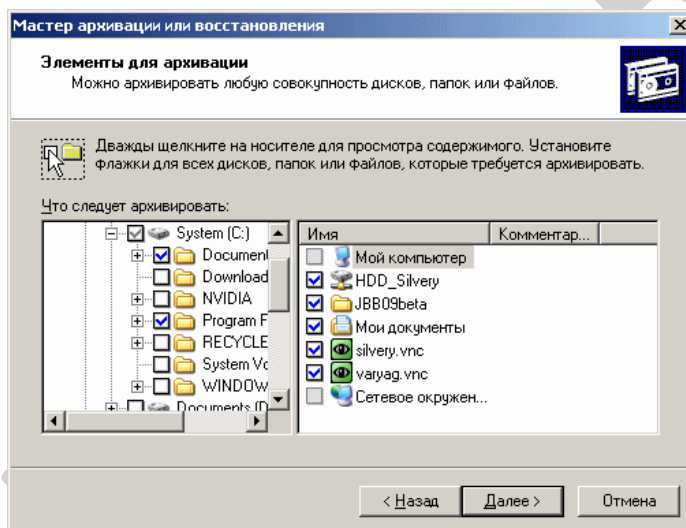


Рисунок 4. Выбор объектов архивирования.

7. Укажите место хранения архива:
- откройте диалоговое окно **Сохранить** как кнопкой *Обзор*;

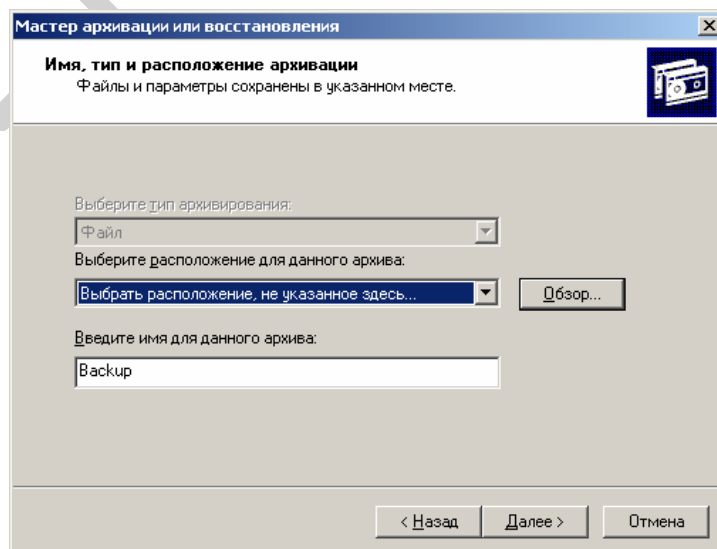


Рисунок 5. Выбор места хранения архива.

- перейдите в корневой каталог диска C;
  - введите в поле **Имя Файла** – имя сохраняемого файла - *Резервная Копия*;
  - сохраните файл кнопкой **Сохранить**;
  - подтвердите введенные данные кнопкой **Далее**.
8. Настройте дополнительные параметры архивации:
- откройте диалоговое окно дополнительных параметров кнопкой **Дополнительно**;
  - выберите в раскрывающемся списке **тип архивации** – *Обычный* и щелкните **Далее**;
  - установите флажок *Проверять данные после архивации* (**Далее**);
  - укажите **способ добавления архива** – *Добавить этот архив к существующему* (**Далее**);
  - укажите **время архивации**:
    1. установите радиокнопку *Позднее*;
    2. введите имя задания в соответствующее поле;

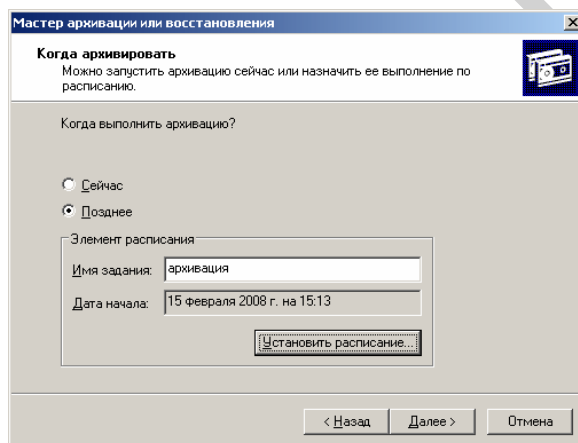


Рисунок 6. Указание имени и времени выполнения архивирования.

3. откройте диалоговое окно **Запланированное задание** кнопкой **Расписание**;

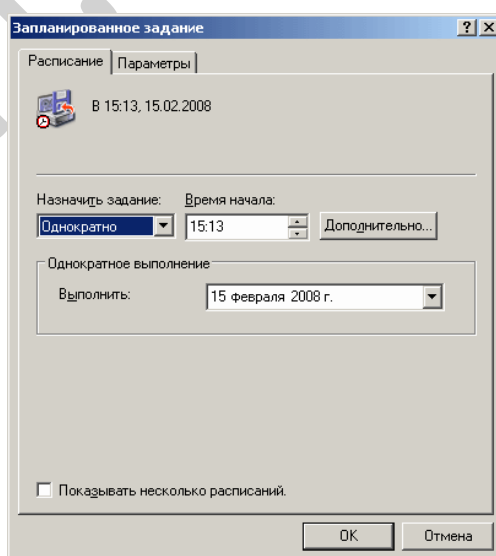


Рисунок 7. Указание точного времени начала выполнения архивирования.

4. введите в поле **Время начала** время на 2 минуты позже текущего (например, если сейчас 12.40, то вам необходимо ввести 12.42);

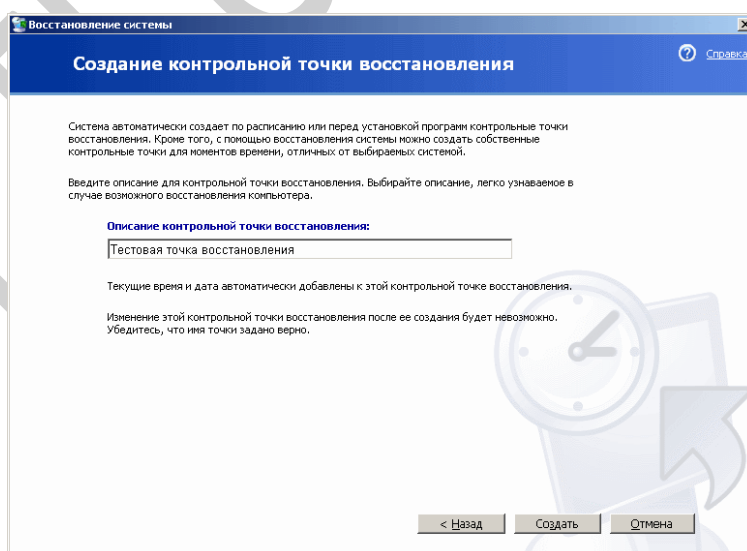
5. подтвердите введенные параметры кнопкой **ОК**;
- завершите ввод времени выполнения архивации кнопкой **Далее**;
- введите данные пользователя от имени которого будет выполняться архивирование:
  1. введите в поле **Пользователь** имя пользователя на компьютере - **USER**;
  2. введите в поля **Пароль** и **Подтверждение пароля** для пользователя **USER**;
  3. подтвердите ввод данных кнопкой **ОК**;
9. завершите работу мастера кнопкой **Готово**.

**Задание 2. Выполните восстановление системных конфигурационных файлов.**

1. Запустите **Мастер Архивации** (**Пуск/Программы/Стандартные/Служебные/Архивация данных**).
2. Ознакомьтесь с информацией мастера и щелкните **Далее**.
3. Выберите возможность мастера – **Восстановление файлов и параметров** и щелкните **Далее**.
4. Выберите для восстановления в левом списке с содержимым архива, папку **Мои рисунки** (**Далее**);
5. Ознакомьтесь с выбранными параметрами и активизируйте восстановление кнопкой **Готово**.
6. Откройте отчет кнопкой **Отчет** и просмотрите его.
7. Закройте диалоговое окно **Ход восстановления** кнопкой **Закреть**.

**Задание 3. Создайте точку восстановления.**

1. Запустите мастер **Восстановление системы** (**Пуск/Программы/Стандартные/Служебные**).
2. Ознакомьтесь с информацией мастера.
3. Создайте точку восстановления:
  - Установите радиокнопку **Создать точку восстановления** (**Далее**);
  - введите в текстовое поле **Описание контрольной точки восстановления** - **Тестовая точка восстановления**;



*Рисунок 8. Восстановление системы.*

- создайте точку восстановления кнопкой **Создать**.
4. Завершите работу мастера кнопкой **Закреть**.  
Продемонстрируйте результаты выполнения работы преподавателю.
- Задание для самостоятельной работы**
1. Создайте план резервного копирования

2. Выполните резервное копирование различного типа с помощью программы Backup Utility (**Start**(Пуск) - **Programs** (Программы) - **Accessories** (Стандартные) - **System Tools** (Служебные) - **Backup** (Архивация данных)):
  - Полное
  - Инкрементное
  - Ежедневное
3. Проанализируйте журнал резервного копирования. Сделайте выводы на основании анализа.

**Время выполнения работы 90 мин;**

### **Контрольные вопросы**

1. Какие причины резервирования данных?
2. Какие существуют типы резервного копирования?
3. Какие преимущества дает механизм теневых копий?
4. Какие типы резервного копирования Вы знаете? В чем их особенности?
5. Кто планирует какие данные нужно резервировать?
6. Какие недостатки имеет архивирование, сделанное в данной лабораторной работе?
7. Какие данные необходимо резервировать?

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
- 4.Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия ]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия ]/Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия ]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.- 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора[электронная версия ]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия ]/ С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил

9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. – Пер. с англ./– СПб: Символ-Плюс, 2009. – 944 с., ил.

**Изучаемая тема:** Программное обеспечения для управления сетевыми операционными системами.

### **Лабораторная работа № 6 «Управление реестром»**

**Цель работы:** познакомиться с понятием реестра и, научиться производить удаленную конфигурацию, резервировать и восстанавливать реестр.

В процессе занятия решаются следующие задачи:

1. Формирование навыков удаленного конфигурирования, резервирования и восстановления реестра;

### **Краткие теоретические и справочно-информационные материалы по теме занятия.**

Начиная с Windows 95, реестр является центральной базой данных для персонального пользователя и конфигурации данных ЭВМ. Говоря в общем, это большая база данных, в которой содержится вся информация о конфигурации Windows 2003: установки учетных записей пользователя, настройки программ и аппаратной части. Здесь находится абсолютно все, начиная от установок пользователя (фоновый цвет, хранители экрана и т.д.), и заканчивая зашифрованной локальной учетной записью пользователя.

Реестр был изобретен взамен устаревших файлов с расширением .INI, которые сохраняли параметры конфигурации в редактируемых файлах с расширением txt. Файлы .INI были довольно удобными в силу краткости и легкости в редактировании. Тем не менее, они имели веские ограничения своего применения: ограничение размеров файла, отсутствие поддержки для нескольких пользователей. На смену им пришел реестр, позволивший нам снять эти ограничения, облегчивший задачу восстановления параметров после системных ошибок, упростивший контрольный доступ и слежение за изменениями в системе. Реестр игнорирует ошибки: так, если Вы устанавливаете приложение, которое записывает новый ключевой набор к реестру, и вдруг происходит отключение электричества, то все остается неповрежденным—Вы можете начать установку приложения снова после восстановления системы.

### **Внимание:**

Некоторые приложения продолжают использовать файлы с расширением INI для сохранения параметров обычного пользователя или языков для обычного пользовательского интерфейса.

Большая часть информации в реестре размещается там автоматически системой Windows при установке самой операционной системы. Остальная часть данных размещается из утилит и приложений во время выполнения их установки. Также возможно редактировать реестр вручную, регулируя, активируя и сохраняя точные установки.

### **Заключение**

Знание того, как устроен реестр, как его резервировать и восстанавливать, будет полезным для всех. Как администратор сети вы увидите, что редактирование реестра в не-

которых случаях является единственным ответом на многие проблемы. Никто не любит возиться с реестром, но подчас не остается иного выхода. Не бойтесь вносить изменения, просто будьте осторожны и четко осознавайте, что Вы делаете!

## Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

### ПРЕДУПРЕЖДЕНИЕ!

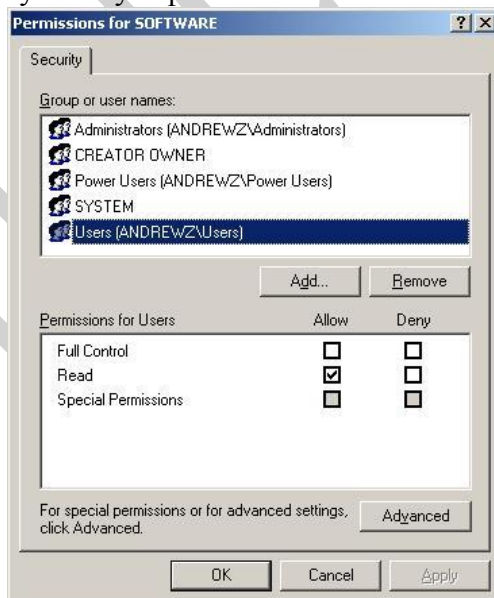
Все изменения, вносимые Вами в реестр с помощью Редактора реестров **Registry Editor**, являются неизменяемыми, поскольку здесь отсутствует кнопка отмены. Поэтому будьте очень осторожны перед внесением изменений в реестр. Нужно очень хорошо понимать, что вы делаете. В противном случае последствия могут быть ужасными. В крайнем случае, Вам придется переустанавливать систему Windows с нуля. Редактируя реестр всегда делайте резервную копию текущих параметров.

Ниже приведен рисунок, на котором показана структура реестра, включающего пять поддеревьев. Вы можете выделить ключ слева, и его данные будут отображены в окне справа. Для открытия Редактора Реестра нажмите на **Start (Пуск) > Run (Выполнить)**, а затем введите “**regedit.exe**”.

### Право на установочные параметры

Вы можете произвольно устанавливать права на установочные параметры к определенным поддеревьям или ключам, разрешая или запрещая доступ к ним пользователям или приложений. По умолчанию пользователи имеют право на чтение, а администраторы на чтение и написание большинства ключей.

Для установки прав доступа откройте **regedit.exe**, нажмите на ключ справа и выберите опцию “**Permissions...**” (*Разрешения*). Таким образом, Вы вызовете *Список контроля доступа* для данного ключа, что позволит Вам вносить изменения в права на установочные параметры к настоящему ключу в файле или папке NTFS.



**Рисунок 1:** Список контроля доступа по правам на установочные параметры к ключу программного обеспечения SOFTWARE

Будьте осторожны касательно того, кому и на что Вы даете или ограничиваете права доступа.

### Пять поддеревьев реестра

Следующие пять секций реестра содержат логически сгруппированную информацию и называются поддеревьями. Поддеревья являются пятью важнейшими частями реестра и содержат набор подключей. При внесении изменений вы наверняка будете выполнять большую часть работы в поддеревьях **\_MACHINE** и **\_USER**.

Поддереву	Описание
HKEY_CLASSES_ROOT	HKEY_CLASSES_ROOT содержит данные, ассоциирующие разные типы файлов с приложениями и конфигурацией для объектов COM
HKEY_LOCAL_USER	Объединяется общей аббревиатурой HKCU. HKEY_LOCAL_USER содержит текущие установки пользователя зарегистрированные в системе. Данные установки являются динамическими и уникальны для каждого отдельного пользователя.
HKEY_LOCAL_MACHINE	Объединяется общей аббревиатурой HKLM. HKEY_LOCAL_MACHINE содержит информацию об установленных в текущий момент аппаратных средствах, а также установках системы ЭВМ. Данные установки статичны для всех пользователей до внесения в них изменений.
HKEY_USERS	Данное поддерево содержит ссылку на HKEY_LOCAL_USER и на профиль пользователя по умолчанию DEFAULT (трафарет, используемый при внесении профиля нового пользователя).
HKEY_CURRENT_CONFIG	Данное поддерево сохраняет конфигурацию данных текущего профиля аппаратных средств и ссылается на HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles

### Типы файлов, распознаваемые реестром

С правой стороны в Редакторе реестра Вы можете заметить различные типы файлов и их значения.

Типы	Описание
REG_SZ	Простая строка данных. Обычно содержит URL, путь или номер порта.
REG_BINARY	Необработанные двоичные данные в шестнадцатеричном формате.
REG_DWORD	Еще один тип REG_BINARY, но размером в 4 байта.
REG_MULTI_SZ	Знаковая строка различного размера, позволяющая Вам осуществлять ввод однозначных параметров.
REG_EXPAND_SZ	Знаковая строка различного размера, содержащая динамическую информацию, изменяющуюся с запуском. Например, «имя пользователя» username, которое имеет разный размер, в зависимости от конкретного пользователя.

### Конфигурация удаленного реестра

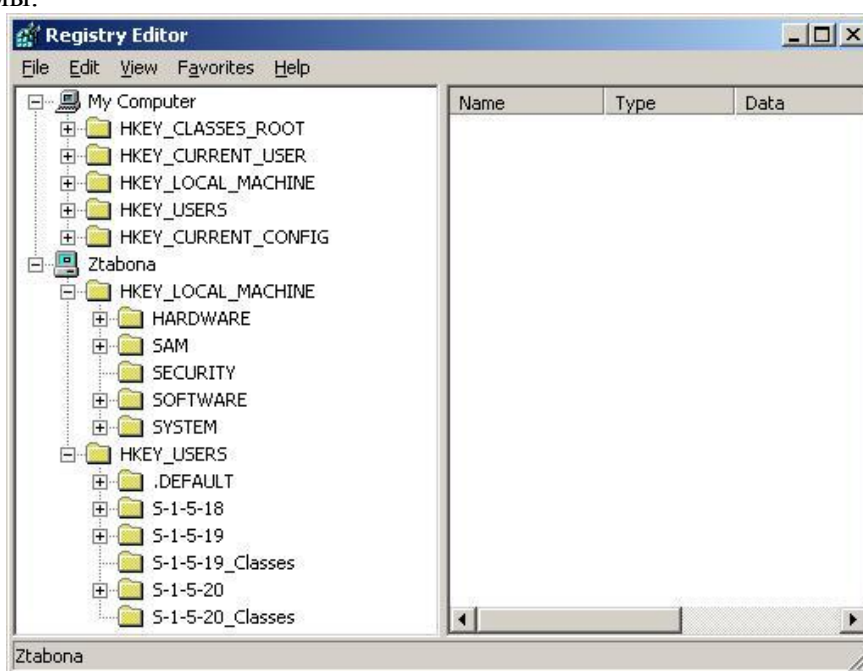
Regedit.exe позволяет Вам быстро и легко производить удаленную конфигурацию реестра на другом компьютере. Все, что Вам нужно — это администраторские права на подобные действия.

**Подсказка:** Убедитесь в том, что установки сетевых пользователей позволяют производить удаленное конфигурирование реестра.

Откройте **regedit.exe** и выберите в опции **File (Файл)** пункт меню “**Connect Network Registry...**” (*Подключить сетевой реестр*). Наберите на клавиатуре имя компьютера, или нажмите на [Advanced...] (*Дополнительно*) и выберите нужный Вам компьютер и затем нажмите **ОК**. После ввода правильных мандатов, реестр удаленного компьютера будет загружен в консоль так, как будто он находится на локальной машине.

После завершения внесения изменений выберите опцию “**Disconnect Network Registry...**” (*Отключить сетевой реестр*) из меню **File (Файл)**, и **regedit.exe** разорвет соединение.

Еще раз запомните, что все изменения, вносимые Вами, будут введены в действие на соответствующем компьютере немедленно или, в некоторых случаях, после перезагрузки системы.



**Рисунок 2:** Показывает соединение с удаленным реестром

Когда Вы соединяетесь с удаленным реестром, вы можете редактировать только ключи **HKEY\_LOCAL\_MACHINE** и **HKEY\_USERS**.

На рисунке 2 изображено соединение локальной машины с другим сервером под названием ZTABONA. Теперь можно вносить необходимые изменения в указанные выше ключи.

### **Резервирование и восстановление реестра**

Существуют три метода резервирования реестра или его части в Windows 2003. Вы можете зарезервировать/восстановить весь реестр, используя утилиту **Windows Backup**; импортировать/экспортировать необходимые поддеревья или ключи из **regedit.exe**; либо, использовать такой инструмент, как **reg.exe**, в командной строке. Все они расписаны более подробно ниже.

### **Утилита резервирования и восстановления («Мастер»)**

Из стартового меню выберите пункты «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки («Пуск» — «Выполнить» — «ntbackup» — кнопка «ОК»). Так вы запустите Мастер резервирования и восстановления, либо непосредственно перейдете к соответствующей утилите (в зависимости от выбранных Вами до этого

### **Импортирование/Экспортирование файлов реестра**

Если вы экспортируете часть реестра, то она сохраняется как файл с расширением **.reg**. При активации, данные, содержащиеся в нем, будут помещены обратно в реестр. Это обычно используется тогда, когда распространитель программного обеспечения, к примеру, заинтересован в том, чтобы клиент нуждался в «наладке программы».

Для экспортирования файла реестра выберите желаемый ключ в левой части **regedit.exe**, нажмите правую кнопку мыши и выберите опцию **Export (Экспортировать)**. Выберите директорию, в которую Вы хотите сохранить файл **.reg** и нажмите на **Save (Сохранить)**. После экспорта файла вы можете редактировать его, используя **Блокнот** или любой текстовый редактор.

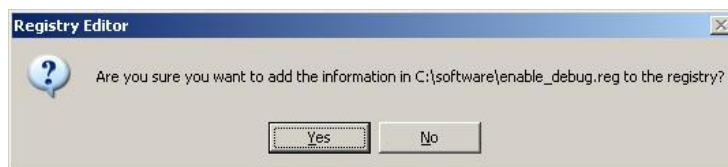
Пример файла с расширением **.reg**:

*Windows Registry Editor Version 5.00*



```
[HKEY_CURRENT_USER\Control Panel\Accessibility\MouseKeys]
«Flags»=»62"
«MaximumSpeed»=»80"
«TimeToMaximumSpeed»=»3000"
```

Для импортирования файла **.reg**, нажмите на нем два раза мышью для вызова диалогового окна и нажмите на кнопку подтверждения **Yes (Да)**. Информация будет добавлена в реестр.



**Рисунок 4:** Окно подтверждения Редактора реестра

Импортируйте информацию в реестр только тогда, когда вы знаете, что содержится в ключах.

**Внимание:** Вы можете также импортировать/экспортировать файлы в реестр, используя инструмент **reg.exe** из командной строки.

### Использование командной строки

Используя **reg.exe** вы можете резервировать и восстанавливать части реестра несколькими простыми командами. Данный инструмент позволит Вам сразу резервировать целое поддерево при работе всей системы.

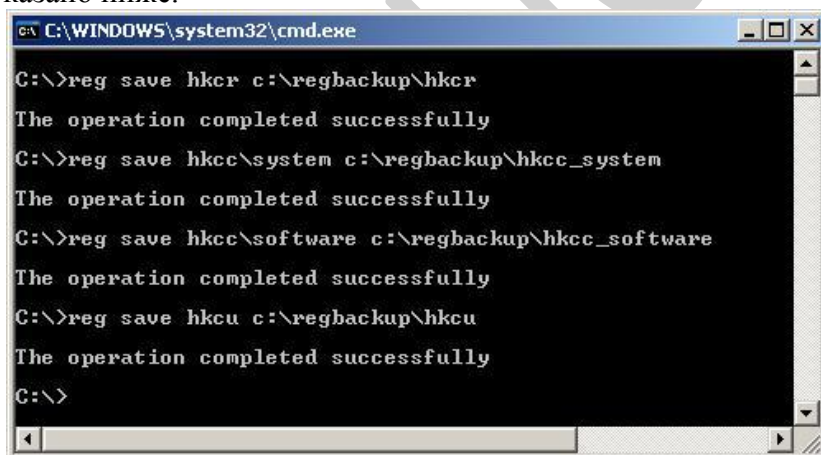
Пример использования **REG SAVE** и **REG RESTORE**.

### REG save

Использование команды **REG save** для сохранения корневых ключей с целью последующего восстановления. Синтаксис команды следующий:

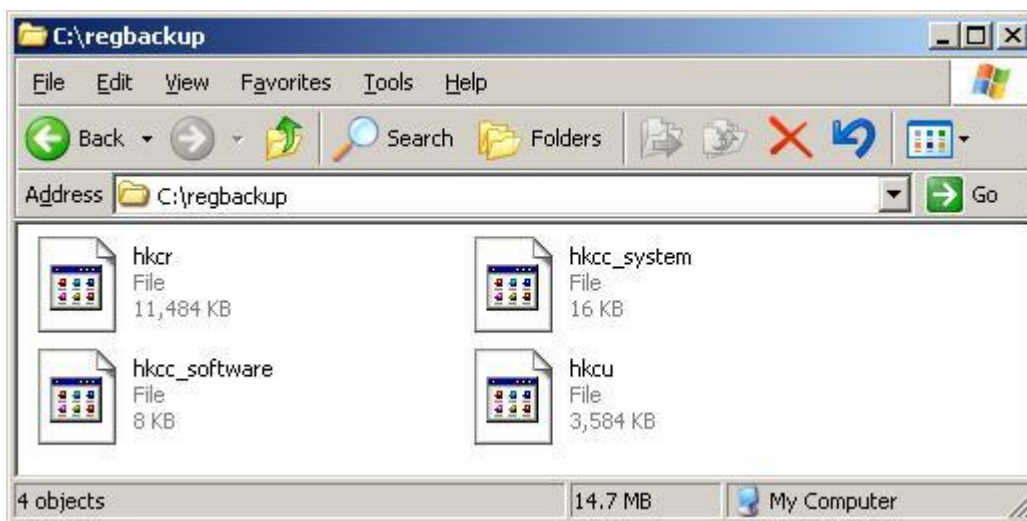
```
reg save <root_subtree> <save_location>
```

В данном примере, используя указанный выше синтаксис, сохраняются разделы **HKEY\_CLASSES\_ROOT**, **HKEY\_CLASSES\_CONFIG** и **HKEY\_CLASSES\_USER**, как показано ниже.



**Рисунок 5:** Использование инструмента **reg.exe** из командной строки для сохранения реестровых ключей

Реестровые файлы будут сохранены в специальную директорию, как показано на рисунке ниже.



**Рисунок 6:** Папка для сохранения реестровых ключей

### **REG restore**

Используя команду **reg restore**, Вы можете восстанавливать ранее сохраненные с помощью команды **reg save** ключи. В примере выше, если бы Вы захотели восстановить **HKEY\_CLASSES\_ROOT**, то необходимо ввести команду:

```
Reg restore hkcr c:\regbackup\hkcr
```

И так далее для остальных ключей.

**Время выполнения работы** 90 мин;

### **Контрольные вопросы**

1. Что такое системный реестр Windows?
2. Расскажите о структуре реестра.
3. Поясните особенности «троянских программ».
4. Почему профилактика «троянских программ» связана с системным реестром?
5. Какие разделы и ключи являются потенциальными местами записей «троянских программ»?

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.

4. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов [электронная версия] / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора [электронная версия] / Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 [электронная версия] / Пер. с англ. - М.: ООО «И.Д.Вильямс», 2011. - 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора [электронная версия] / Ч. Рассел, Ш. Кроуфорд, Дж. Джеренд., пер. с англ. - 2-е изд., - М.: Русская Редакция, 2007. - 656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия] / С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия] / Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия] / Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. - М.: ООО «И.Д. Вильямс», 2011. - 1456 с.: ил. - Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство [электронная версия] / Т. Лимончелли, К. Хоган, С. Чейлап - 2-е издание. - Пер. с англ. / - СПб: Символ-Плюс, 2009. - 944 с., ил.

**Изучаемая тема:** Программное обеспечения для управления сетевыми операционными системами.

#### **Лабораторная работа № 7 «Установка и настройка web-сервера»**

**Цель работы:** получить практический опыт установки и настройки web-сервера операционной системы Windows Server 2003.

В процессе занятия решаются следующие задачи:

1. формирование навыков по установке веб-сервера, изменению его настроек и проведению мониторинга работы сервера. ;

#### **Краткие теоретические и справочно-информационные материалы по теме занятия.**

**Internet Information Services (IIS) 6.0** – полнофункциональный веб-сервер, обеспечивающий основу для систем семейства **Windows Server 2003**, а также существующих веб-приложений и веб-служб XML. В IIS 6.0 предусмотрен выделенный режим, обеспечивающий выполнение кода приложений в изолированной среде. IIS 6.0 также поддерживает технологию Web Gardens (веб-сады), в рамках которой запросы, обычно адресуемые отдельному процессу, распределяются по набору эквивалентных процессов, что обеспечивает повышенную масштабируемость в многопроцессорной среде.

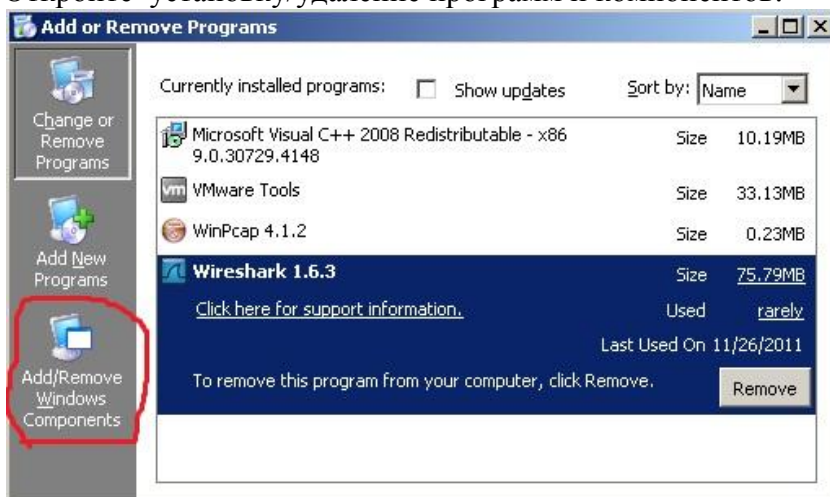
В составе Microsoft Windows Server 2003 имеются службы, обеспечивающие поддержку со стороны сервера наиболее употребительных протоколов Интернета прикладного уровня, благодаря чему сервер Windows Server 2003 может выполнять следующие роли:

- Web-сервер;
- FTP-сервер;
- SMTP-сервер;
- NNTP-сервер.

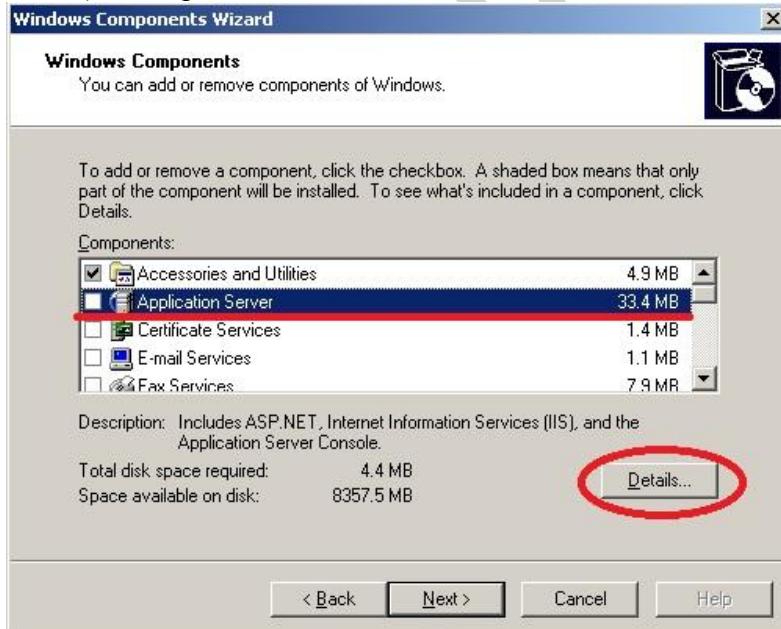
Все эти функции реализуются компонентом Internet Information Services (IIS), являющимся преемником компонента Internet Information Server, входившего в состав NT Option Pack для Windows NT 4.0.

## Порядок работы

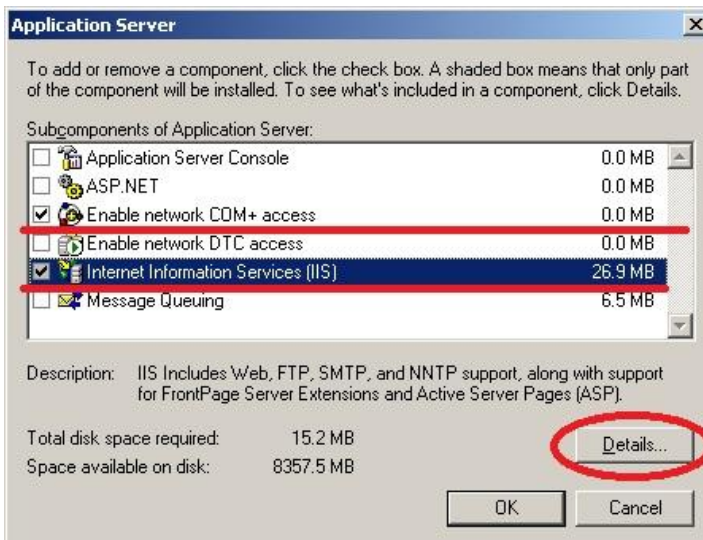
1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. **Устанавливаем IIS**  
Серверная ОС Windows Server 2003, состав которой уже бесплатно входит Web-сервер от Microsoft, уже установлена.  
Откройте установку/удаление программ и компонентов:



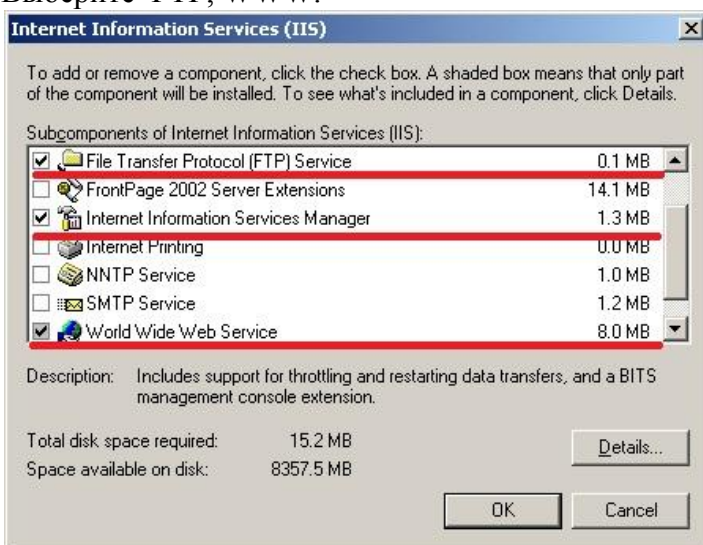
Выберите "Компоненты Windows". Нас интересует сервер приложений (Application Server). Отобразите дополнительные компоненты кнопкой "Detail".



Установите галочки напротив IIS, COM+. На IIS нажмите "Detail".

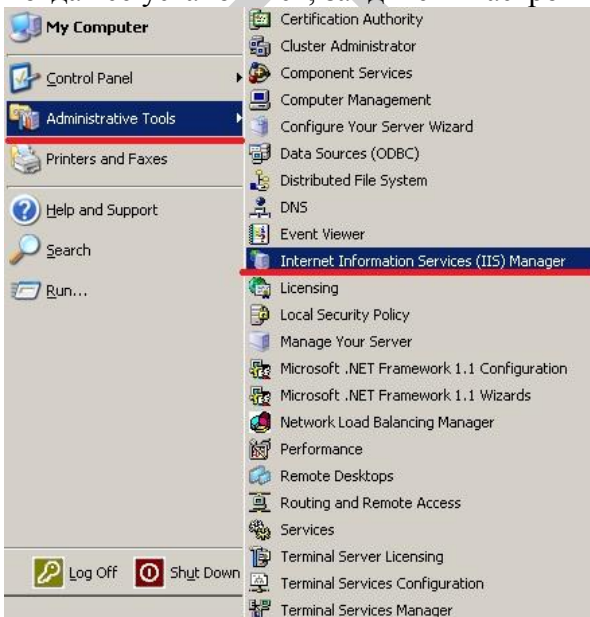


Выберите FTP, WWW.



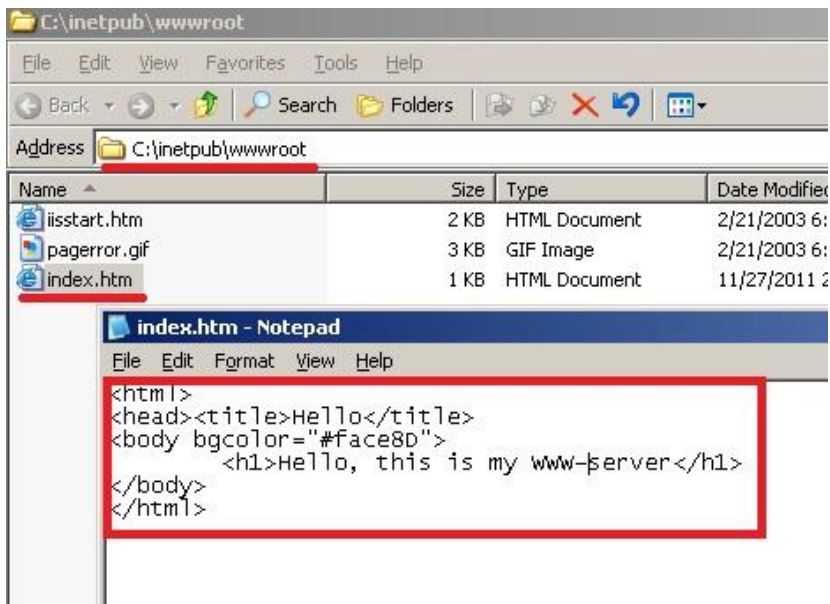
### 3. Начальная настройка IIS.

Когда всё установится, зайдите в настройки IIS в консоли администрирования.



Откройте директорию **C:\inetpub\wwwroot\** (это по-умолчанию, можно изменить путь потом). Создайте файл **index.htm**

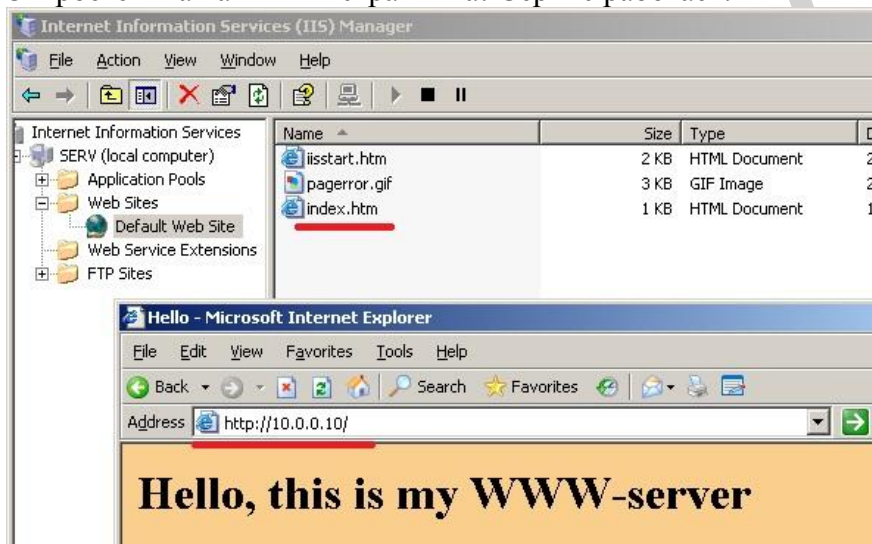
Наберите следующий текст для создания HTML-странички.



В консоли управления IIS-сервером появится наш файл в разделе **Web Sites \ Default Web Site**

Откройте в браузере адрес локального компьютера (127.0.0.1)

Откроется наша HTML-страничка! Сервис работает!



Продемонстрируйте результаты установки и настройки преподавателю.

**Время выполнения работы 180мин;**

### **Контрольные вопросы**

1. Чем отличается Web – сервер от FTP – сервера
2. Чем отличается Анонимный доступ к серверу от Административного
3. Перечислите основные настройки Web – сервера
4. Как определить IP- адрес сервера
5. Назовите и объясните два вида адресации, используемой в работе с сетями.

**Составьте отчет о проделанной работе в тетради для самостоятельных работ.**

### **Критерии оценки:**

1. Работа оценивается на «пять баллов», если все части задания выполнены верно и выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если не выполнена одна часть задания ,выводы сделаны правильно
3. Работа оценивается на «три балла» если не выполнены 2 части задания, выводы сделаны правильно

### **Рекомендуемая литература**

1. Новожилов, Е.О. Компьютерные сети : учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.
2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия ]/ Н.В.Максимов, И.И.Попов. — 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. — 437 с.
3. Кузин, А. В. Компьютерные сети: учебное пособие [электронная версия ]/А. В. Кузин. - 3-е изд., перераб. и доп .- М.: ФОРУМ: ИНФРА-М, 2011.- 192 с.
- 4.Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов[электронная версия ]/В.Г. Олифер, Н.А. Олифер.- СПб.: Питер, 2010.
5. Microsoft Windows Server 2003. Справочник администратора[электронная версия ]/Пер. с англ. — М.: Русская Редакция, 2004. - 640 с.
6. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2[электронная версия ]/ Пер. с англ.-М.:ООО «И.Д.Вильямс»,2011.- 736 с.
7. Рассел, Ч. Microsoft Windows Server 2003: Справочник администратора[электронная версия ]/Ч.Рассел, Ш.Кроуфорд, Дж.Джеренд., пер. с англ.– 2-е изд.,-М.: Русская Редакция, 2007.-656 с.
8. Бормотов, С. В. Системное администрирование на 100 % [электронная версия ]/ С. В. Бормотов — СПб.: Питер, 2006. — 256 с: ил
9. Учебный курс Основы сетевой инфраструктуры Windows Server 2008 [электронная версия]/ Academy, Softline- 139 с.
10. Моримото, Microsoft Windows Server 2008 R2. Полное руководство. Пер. с англ. [электронная версия]/ Ноэл, Майкл, Драуби, Омар, Мистри, Росс, Амарис, Крис Рэнд. -М.: ООО «И.Д. Вильямс», 2011.-1456 с.: ил.- Парал.тит.англ
11. Лимончелли, Т. Системное и сетевое администрирование. Практическое руководство[электронная версия]/ Т.Лимончелли, К. Хоган, С. Чейлап- 2-е издание. — Пер. с англ./– СПб: Символ-Плюс, 2009. — 944 с., ил.