ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Иркутский государственный университет путей сообщения»
Сибирский колледж транспорта и строительства

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ
ПМ.02 ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ

МДК.02.03. ОРГАНИЗАЦИЯ АДМИНИСТРИРОВАНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ

ДЛЯ ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ
(очной формы обучения)
для специальности
09.02.06 Сетевое и системное администрирование

базовая подготовка
среднего профессионального образования

Иркутск 2022

РАССМОТРЕНО:
Цикловой методической
комиссией специальности 09.02.06
Сетевое и системное
администрирование
«08» июня 2022 г.
Председатель: _____/Саквенко Т.В.

СОГЛАСОВАНО:
Заместитель директора по УВР
_____/А.П.Ресельс
«09» июня 2022 г.

Разработчик: Храмова В.К. преподаватель Сибирского колледжа транспорта и строительства ФГБОУ ВО «Иркутский государственный университет путей сообщения».

СОДЕРЖАНИЕ

	Пояснительная записка	5
1	**Практическая работа №1.** Создание общих ресурсов и управление ими	6
2	**Практическая работа №2-3** Настройка конфигурации ЛВС в Windows	14
3	**Практическая работа №4.** Настройка удаленного рабочего стола	23
4	**Практическая работа №5.** Настройка беспроводной сети Wi-Fi	28
5	**Практическая работа №6-7.** Изучение типов серверов, их настройка и конфигурирование	44
6	**Практическая работа №8.** Работа с серверами http и ftp	56
7	**Практическая работа №9.** Изучение стека протоколов TCP/IP	64
8	**Практическая работа №10-11.** Настройка стека протоколов TCP/IP	68
9	**Практическая работа №12-13.** Изучение виртуальных локальных сетей VLAN	77
10	**Практическая работа №14.** Использование сетевых программных утилит Windows	91
11	**Практическая работа №15.** Мониторинг состояния элементов сети	99
12	**Практическая работа №16.** Обеспечение безопасности локальной сети	109
13	**Практическая работа №17** Диагностика IP протокола	123
14	**Практическая работа №18** Программы для работы в сетях LAN и WAN	134
15	**Практическая работа №19** Назначение серверу роли "Контроллер домена"	144
16	**Практическая работа №20** Установка DNS сервера	159
17	**Практическая работа №21** Установка и настройка службы DHCP	171
18	**Практическая работа №22** Создание пользователей домена	182
19	**Практическая работа №23-24** Администрирование сети	195
20	**Практическая работа №25.** Основы работы с Virtual PC 2007. Установка WindowsServer 2008 на виртуальную машину	226
21	**Практическая работа № 26**. Управление загрузкой Windows Server 2008. Добавление ролей. Установка первого контроллера домена	232

22	**Практическая работа № 27.** Основы администрирования домена Windows: добавление компьютера в домен, работа с учетными записями и группами	243
23	**Практическая работа № 28.** Администрирование файлового сервера	247
24	**Практическая работа № 29.** Администрирование файлового сервера (продолжение)	258
25	**Практическая работа №30**. Автономные файлы. Служба DFS	267
26	**Практическая работа № 31**. Настройка DNS и DHCP.	275
27	**Практическая работа № 32.** Службы Internet Information Services (IIS 7.0). Установка и основы администрирования web- и ftp-сервера	288
28	**Практическая работа № 33.** Удаленное управление Windows Server 2008	299
29	**Практическая работа № 34**. Автоматическое обновление операционной системы с использованием службы WSUS	309
30	**Практическая работа № 35**. Резервное копирование в Windows Server 2008	326
31	**Практическая работа №36.** Установка и конфигурирование Windows Server 2012 R2 Essentials	339
32	**Практическая работа №37.** Установка System Center 2012 R2 Virtual Machine Manager	373
33	**Практическая работа №38.** Антивирус Касперского для Microsoft ISA Server. Установка, настройка, управление	395
34	**Практическая работа №39-40.** Антивирус Касперского 5.5 для MS Exchange Server. Установка, настройка, управление	404
35	**Практическая работа №41-42.** Основные признаки присутствия вредоносных программ, и методы по устранению последствий вирусных заражений.	413

Пояснительная записка

Учебно-методическое пособие разработано в соответствии с программой профессионального модуля ПМ.02.«Организация сетевого администрирования» для МДК.02.03. «Организация администрирования компьютерных систем» и предназначено для реализации требований Федерального государственного образовательного стандарта среднего профессионального образования по программам подготовки специалистов среднего звена для специальности 09.02.06 Сетевое и системное администрирование

ПРАКТИЧЕСКАЯ РАБОТА №1.
СОЗДАНИЕ ОБЩИХ РЕСУРСОВ И УПРАВЛЕНИЕ ИМИ
Цель работы:
научиться предоставлять доступ к ресурсам компьютера и использовать сетевые ресурсы в ОС Windows.

Краткие теоретические и учебно-методические материалы по теме практической работы:
Операционная система (ОС) – это совокупность программных средств, осуществляющая управление ресурсами компьютера, запуск прикладных программ и их взаимодействие с внешними устройствами и другими программами, а также обеспечивающая диалог пользователя с ЭВМ. Ресурсом является любой компонент ЭВМ и предоставляемые им возможности: центральный процессор, оперативная и внешняя память, внешнее устройство, программа и т.д. ОС загружается в оперативную память при включении компьютера и предоставляет пользователю удобный способ общения (интерфейс) с вычислительной системой.
Учебная локальная сеть представляет собой обособленный сегмент компьютерной сети УГКР. В структуре сети можно выделить следующие элементы: контроллеры домена, шлюз, рабочие станции.
Учебный сегмент локальной сети УГКР построен на основе клиент-серверной архитектуры с использованием топологии типа звезда.
В упрощенном виде учебный сегмент сети УГКР представлен на рисунке 1.

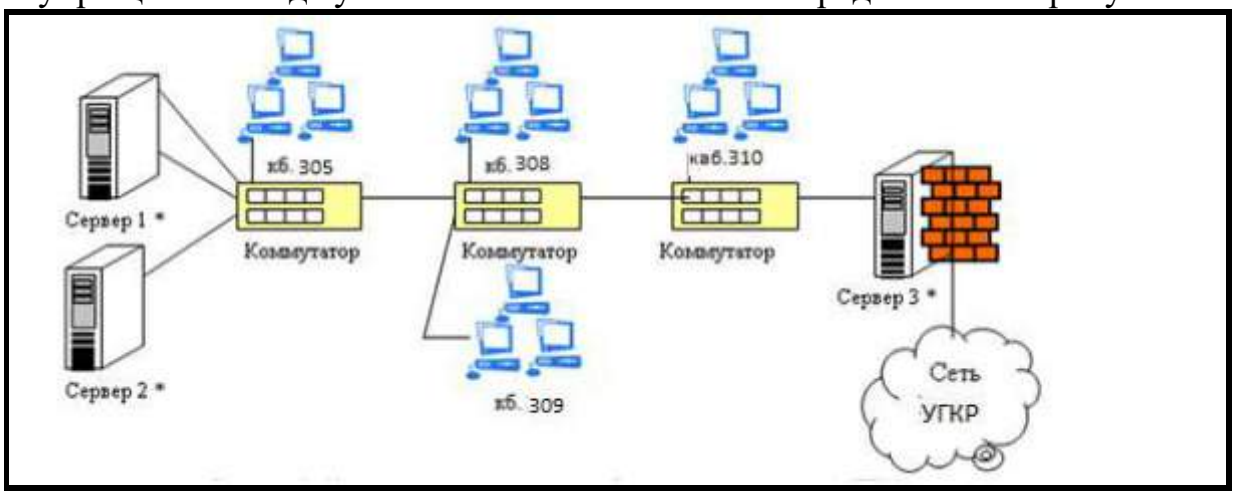


Рисунок 1. Упрощенная структура учебного сегмента сети МГПУ
Здесь Сервер 1 и Сервер 2 – первичный и вторичный контроллеры домена с именами SERVER и TERMINAL соответственно. Сервер 3 (PHOENIX) – это компьютер, выполняющий роль шлюза, прокси-сервера и брандмауэра.
В локальную сеть на базе ОС Windows входят следующие элементы: общие ресурсы, серверы, рабочие станции, группы.
Общий ресурс – это объект (папка, диск, принтер и др.) который могут использовать несколько пользователей одновременно, причем им не

обязательно находится за тем компьютером, на котором физически расположен данный ресурс.

Рабочая станция – это компьютер, подключенный к сети и предназначенный для выполнения задач пользователя.

Сервер – это специализированный компьютер, предоставляющий свои ресурсы в использование клиентам сети (как правило, это рабочие станции) и управляющий сетью.

Рабочая группа – логическое объединение компьютеров. Как правило, объединение в группы используется для упрощения администрирования сети. При этом несколько компьютеров выступают как единое целое – группа.

На компьютере с ОС Windows 2000 или Windows XP в общее пользование можно предоставить как любую папку на диске, так и диск целиком. После создания общего ресурса пользователи с соответствующими полномочиями могут получить доступ к нему с любой рабочей станции сети.

Открывая общий доступ к папке, можно ограничить число пользователей, которые могут работать с ней одновременно. Для управления доступом к папке и ее содержимому используются разрешения, назначаемые пользователям и группам. Эти разрешения, а также сетевое имя папки в любой момент можно изменить. При необходимости можно прекратить общий доступ к папке. Если к ней в это время подключены пользователи, на экране появится диалоговое окно с информацией об этом и предложением подтвердить принятое решение.

В Windows 2000 и Windows XP предоставлять папки в общее пользование разрешается членам групп Администраторы, Операторы сервера и Опытные пользователи, причем с некоторыми ограничениями.

Общие ресурсы.

ОС Windows автоматически открывает общий доступ к некоторым ресурсам, необходимым для администрирования компьютера. К их сетевым именам добавляется значок доллара ($), благодаря которому административный общий ресурс скрыт от пользователей, просматривающих содержимое компьютера через сеть.

К числу административных ресурсов относятся: корневые папки каждого тома, корневая системная папка и папки, в которых находятся драйверы принтеров.

Открывая общий доступ к папке, обязательно нужно присвоить ей сетевое имя. Кроме того, при желании можно сопроводить папку описанием, ограничить число пользователей, которые могут пользоваться ею одновременно, и назначить для нее разрешения. Одну и ту же папку можно сделать общей под несколькими сетевыми именами.

Чтобы общий ресурс был доступен клиенту и в автономном режиме, то есть при отсутствии подключения к сети, Windows 2000 или Windows XP может сохранить копии файлов ресурса в специальной области на локальном диске

клиентского компьютера — кэше. По умолчанию размер кэша составляет 10% от доступного дискового пространства, но его можно изменить с помощью вкладки Автономные файлы диалогового окна Свойства папки.

В Windows XP и Windows 2000 входит оснастка Общие папки, позволяющая контролировать доступ к сетевым ресурсам и уведомлять пользователей посредством административных сообщений. Это возможность контролировать доступ к сетевым ресурсам для оценки и управления загруженностью сетевых серверов, а также доступ к общим папкам, чтобы определить, как много пользователей в данный момент подключены к каждой папке.

Возможности раздела Общие ресурсы в оснастке Общие папки позволяют просматривать список всех общих папок на компьютере и определять, сколько пользователей могут обращаться к каждой папке.

Кроме того, можно отслеживать, какие файлы открыты, а также отключать пользователей от одного открытого файла или от всех открытых файлов.

Задания для практического занятия:

Поиск других ПК в сети

Поиск компьютеров и рабочих групп в сети возможен с помощью поисковой системы Windows XP. Зайдите в "Сетевое окружение" и нажмите на клавишу F3, затем заполните поле "Введите имя искомого компьютера или его IP адрес". Мы будем искать, например, второй ПК в рабочей группе 110 (рис. 1).

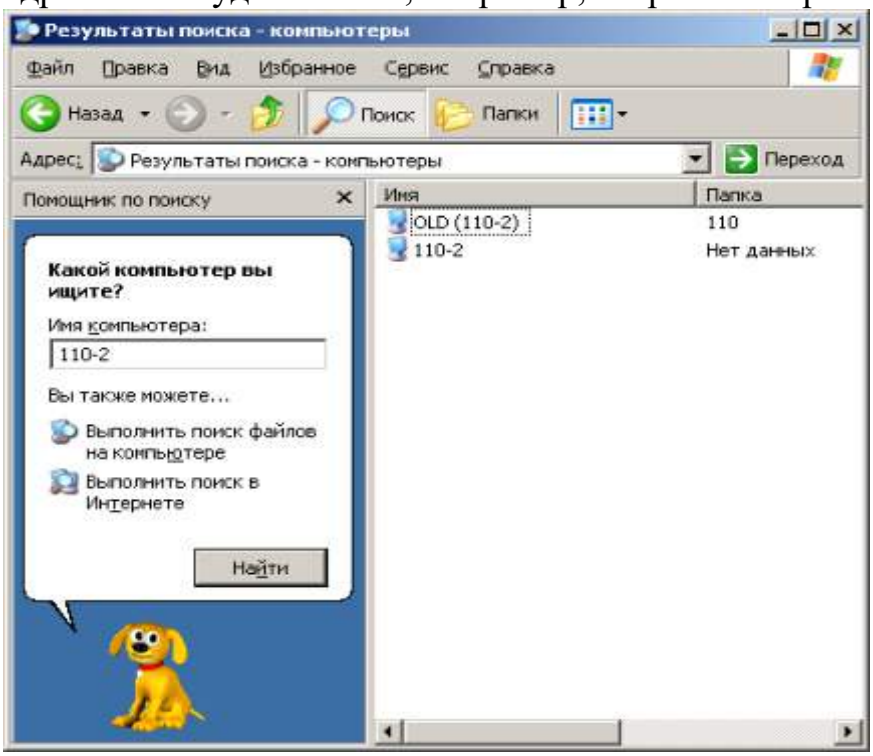


Рис. 1. Поиск компьютера 110-2 в сети

Настройка_11 общего доступа к сетевым ресурсам

В этом примере мы сделаем общей папку Мои документы.

Простой общий доступ к файлам

Правой кнопкой мыши щелкните на папке Мои документы и выполните команду Свойства-Доступ. На вкладке Доступ установите флажки как на рис. 2.

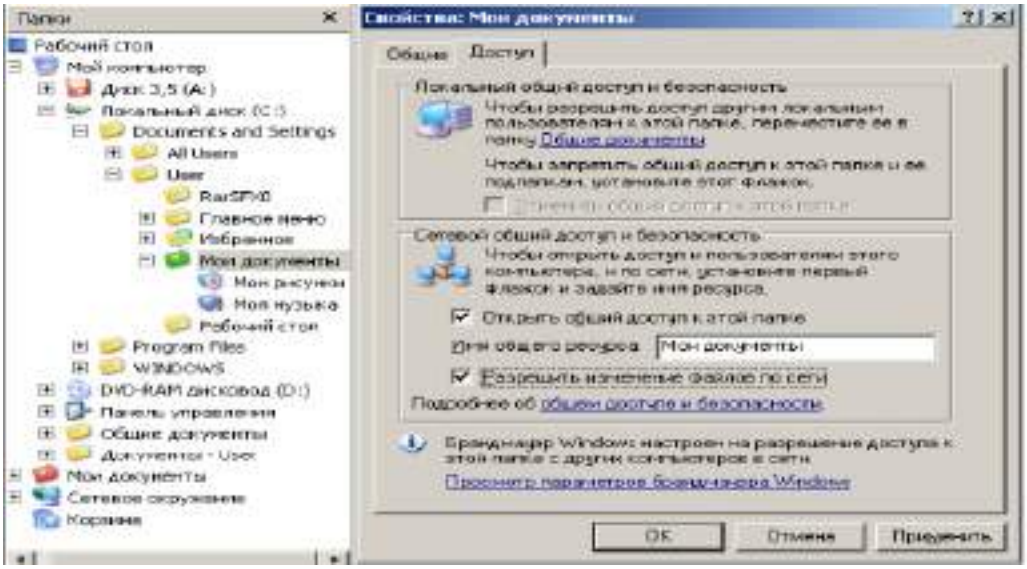


Рис. 2. В окне Мои документы активна вкладка Доступ

После закрытия данного окна с новыми настройками на значке папки Мои документы появиться рука, что означает, что этот ресурс сети – общий.

Расширенный общий доступ к файлам

Обычно достаточно режима "Простой общий доступ к файлам", однако, если требуется более серьёзное разграничение прав пользователей, то необходимо включить "Расширенный общий доступ", для этого, в любом окне нужно выбрать: **Сервис-Свойства** папки-**Вид**, и убрать галочку с параметра "**Использовать простой общий доступ к файлам**" (рис. 3).

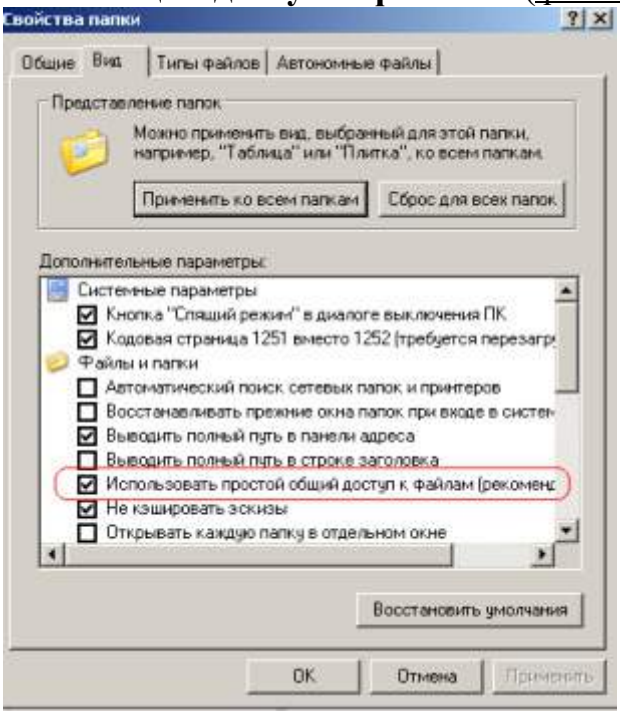


Рис. 3. Задаем Расширенный общий доступ

Снова для папки Мои документы выполняем команду **Свойства – Доступ** (рис. 4).

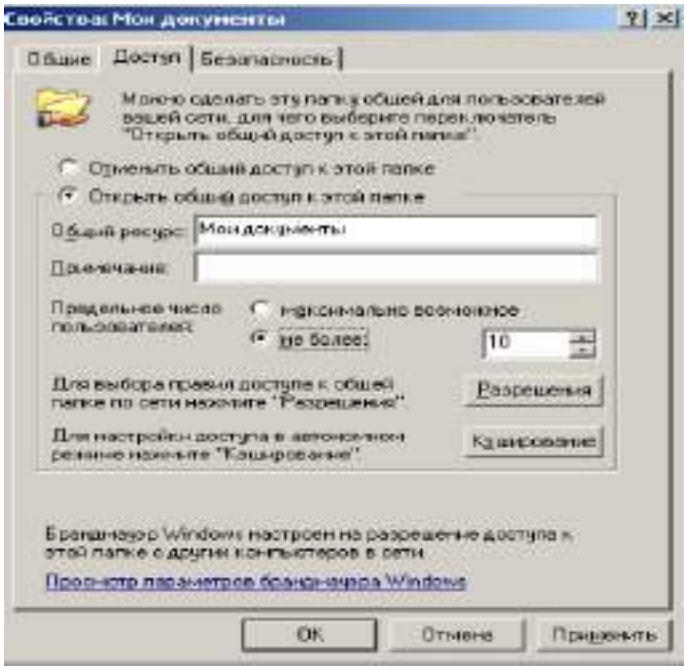


Рис. .4. Активна вкладка Доступ

Теперь мы видим новый элемент - кнопку "Разрешения", которая задает пользователей, которым будет доступна данная папка (рис. 5).

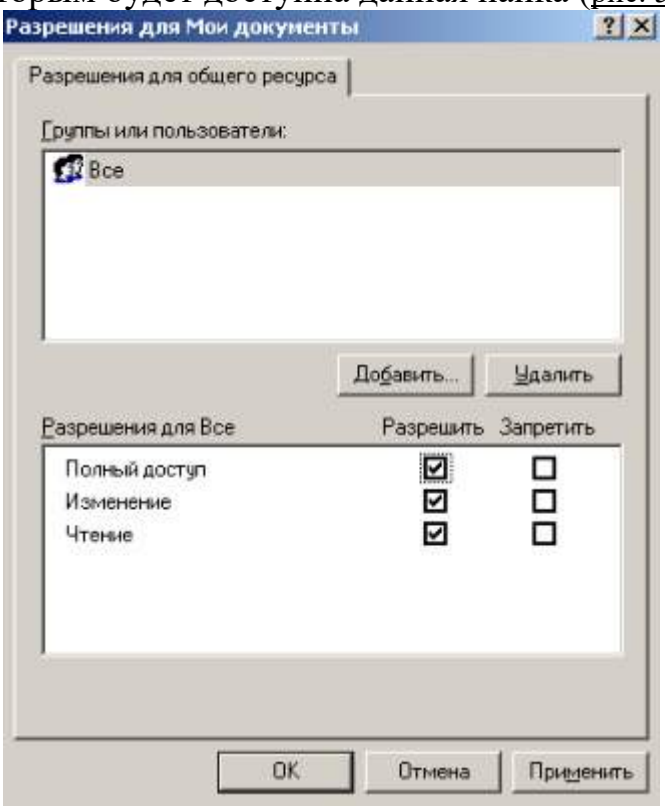


Рис. 5. Разрешено всем все

Возможные проблемы с общим доступом к ресурсам сети

Если создать сетевой доступ к ресурсам не получается, то постарайтесь исправить ситуацию, придерживаясь следующих рекомендаций:

Проверьте правильность сетевых настроек антивируса и брандмауэра.
Не используйте в именах компьютера русские буквы, это может привести к программным ошибкам.
Измените необходимые разрешения прав пользователя на вкладке Безопасность (рис. 6):

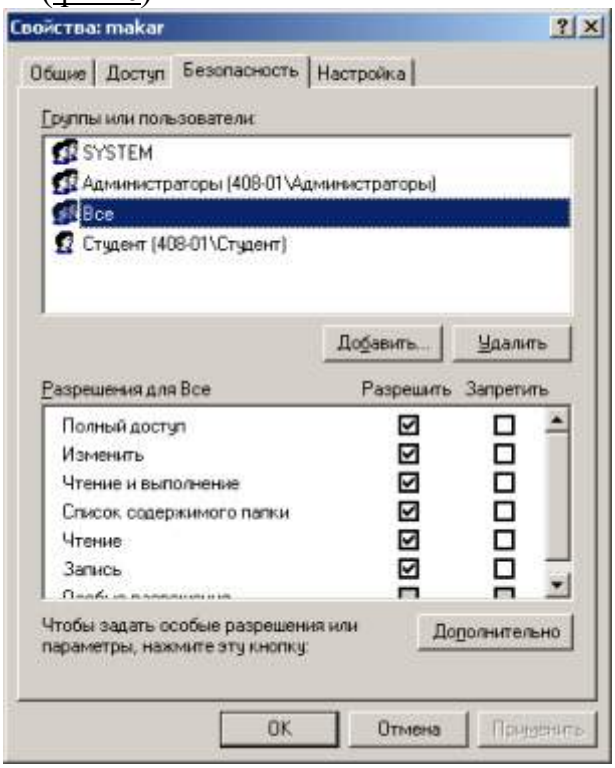


Рис. 6. Всем пользователям даны все права

Вместо задания конкретного IP вручную можно установить переключатель на автоматическое определение IP (рис. 7).

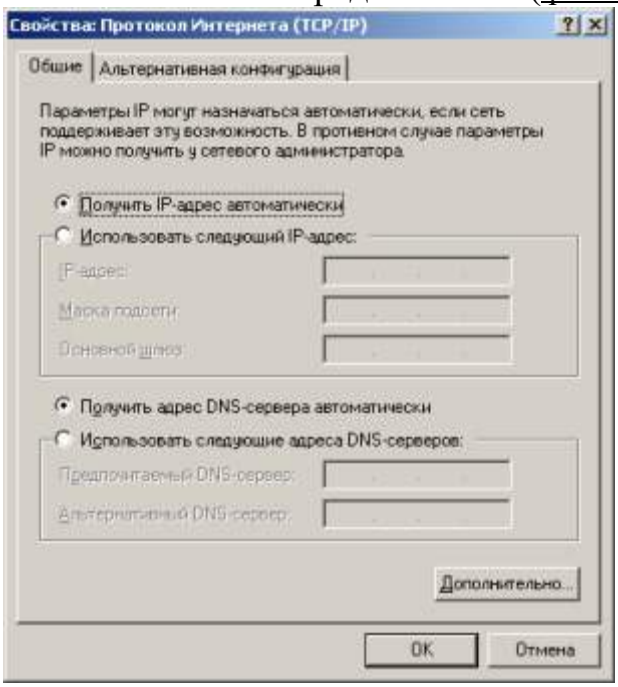


Рис. 7. Переключатель получения IP автоматически

Время и дата на часах всех ПК должны быть одинаковы.
Создаем сетевой диск Z, общий для всех ПК
Каждый раз искать общую папку в Сетевом окружении не очень удобно. Имеет смысл подключить ее к вашему компьютеру в качестве сетевого диска. Он будет отображаться в списке дисков окна Мой компьютер, и вы сможете быстро работать с его содержимым. Чтобы подключить общую папку с другого компьютера как сетевой диск выполните команду Пуск - Мой компьютер - Сетевое окружение, затем выберите компьютер локальной сети и находящуюся на нем общую папку, которую вы хотите подключить на свой ПК в качестве сетевого диска. Щелкните по папке правой кнопкой мыши и выберите Подключить сетевой диск (рис. 8).

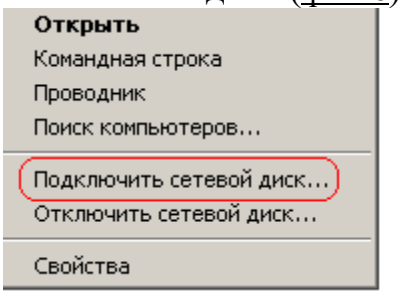


Рис. 8. Контекстное меню подключения сетевого диска

В появившемся окошке выберите букву, под которой сетевой диск будет отображаться в списке дисков вашего компьютера. Также отметьте галочкой пункт "Восстанавливать при входе в систему", чтобы при включении компьютера и загрузке Windows автоматически отображала сетевой диск в списке дисков вашего ПК (рис. 9).

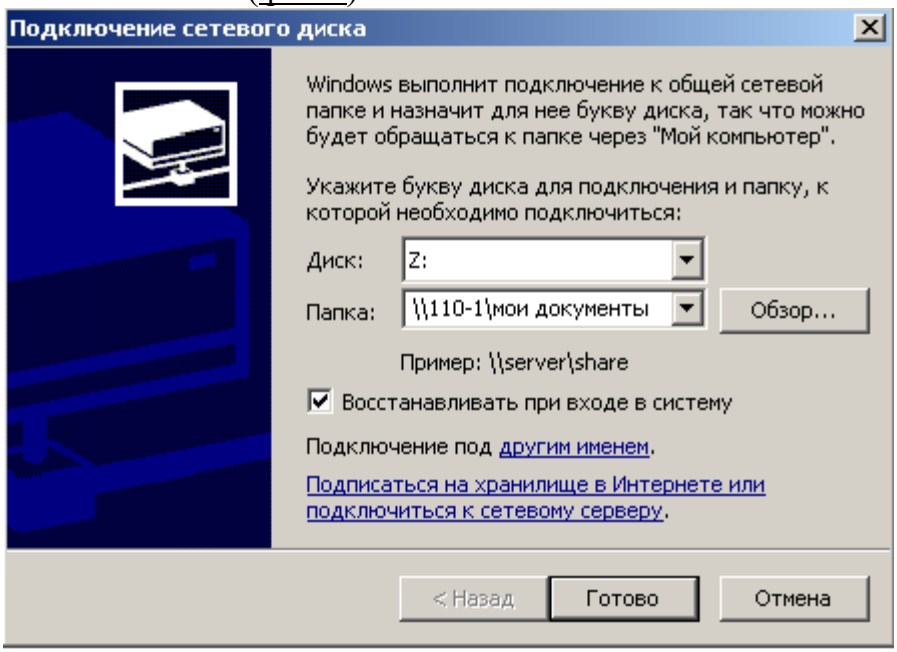


Рис. 9. Назначаем диску букву Z

Теперь можете просто зайти в Мой компьютер, и вы увидите сетевой диск (рис. 10).

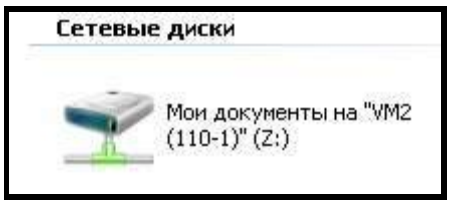


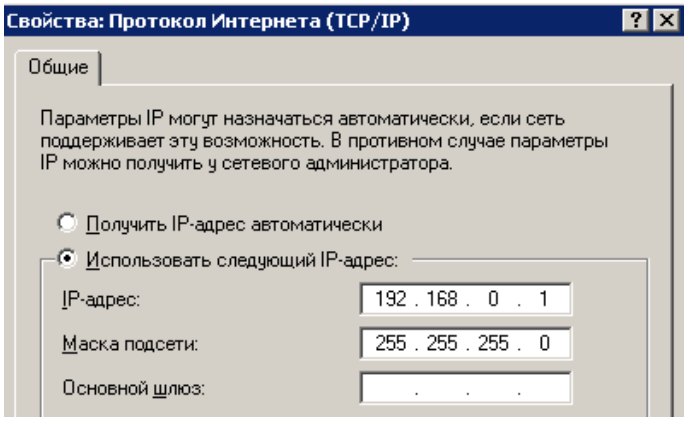
Рис. 10. В качестве сетевого диска будем использовать общую папку Мои документы, размещенную на ПК 110-1.

ПРАКТИЧЕСКАЯ РАБОТА №2-3.
НАСТРОЙКА КОНФИГУРАЦИИ ЛВС В WINDOWS

Цель работы: Научиться настраивать конфигурацию ЛВС в Windows XP

Задание №1. Настроить виртуальный ПК для работы в сети

Запускаем обе, ранее созданные нами виртуальные машины командой **ВМ - Питание Power On**. Для работы в сети настроем сначала первую машину. Для этого в **Панели управления** найдем **Сетевые подключения-Подключение по локальной сети-Свойства**, затем находим свойства **Протокола Интернет (TCP/IP)** и пишем **IP-адрес** и **Маску подсети** как на рис. 1.



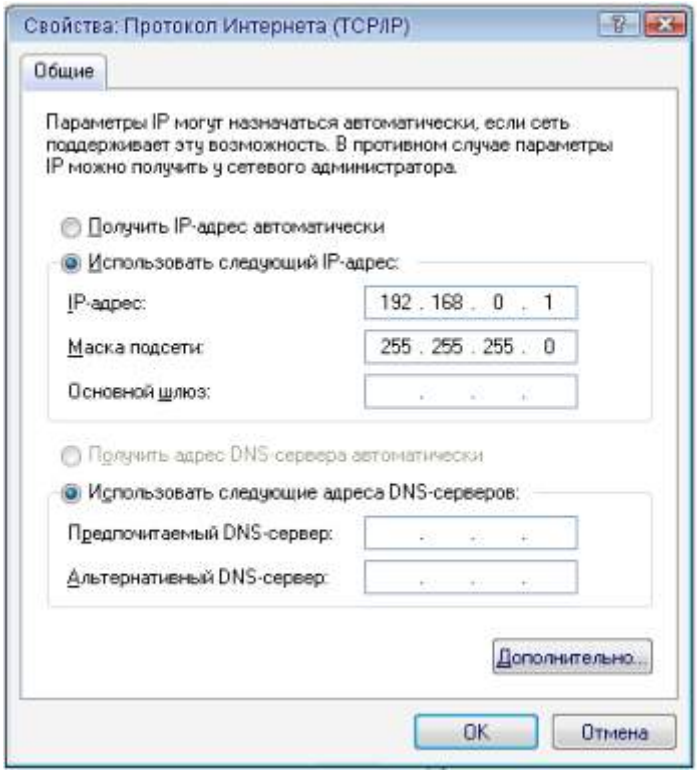


Рис. 1. Настраиваем ВМ-1

Совет

Вам придется периодически переходить от окна физического ПК к окну виртуального ПК. Для этого нажимайте на сочетания клавиш **Ctrl+Alt**

Аналогично включим и настроим вторую машину (рис. 2).

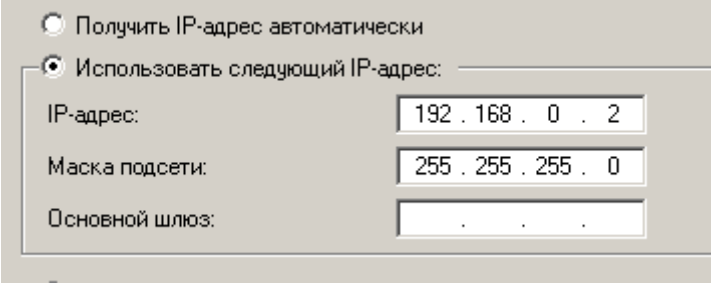


Рис. .2. Настраиваем ВМ-2

Настраиваем виртуальную сеть

Для настройки сети выполним команду **Сетевое окружение-Установить домашнюю или малую сеть** (рис. 3 и 4).

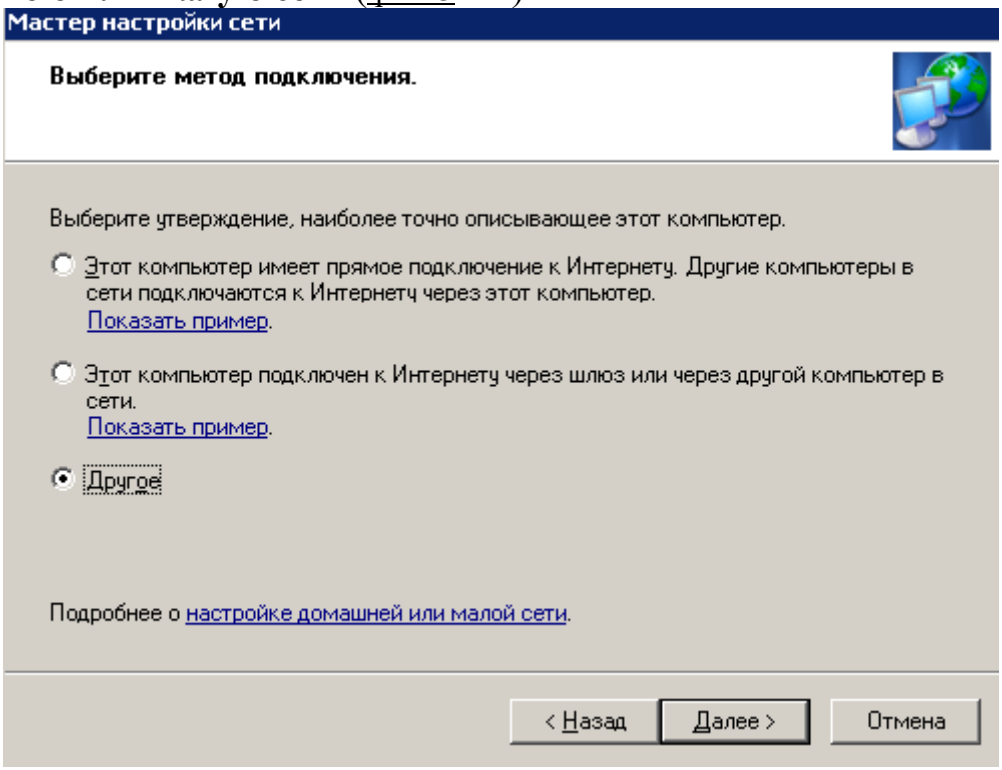


Рис. 3. Выбираем переключатель Другое

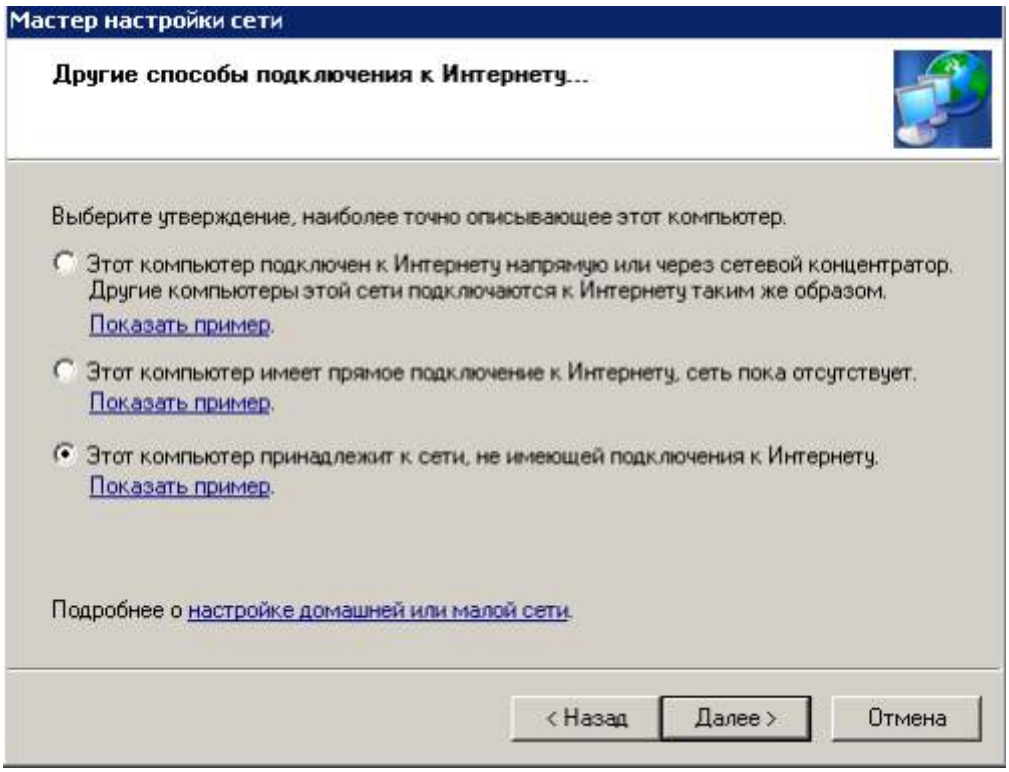


Рис. 4. Установим третий переключатель сверху

Присвоим машине сетевое имя (рис. 5).

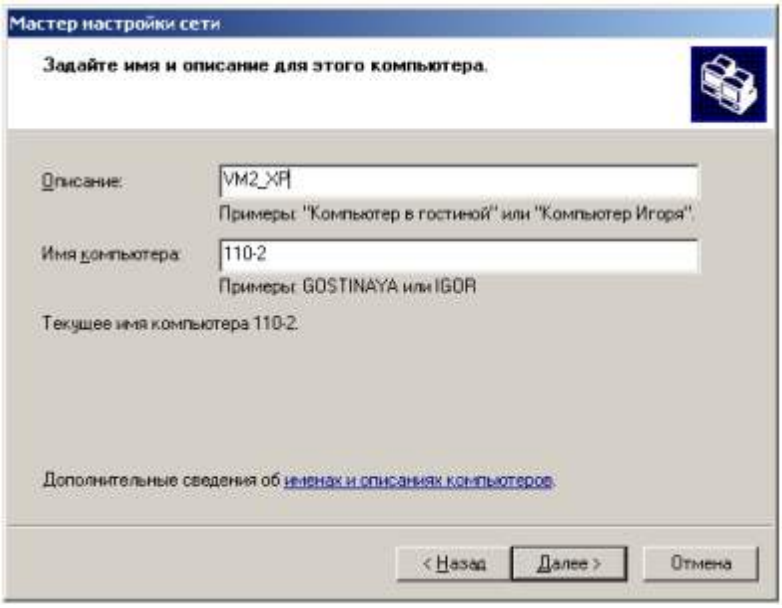


Рис. 5. Даем машине имя и описание

На следующем шаге (нажав **Далее**) создадим рабочую группу 110 (рис. 15.6).

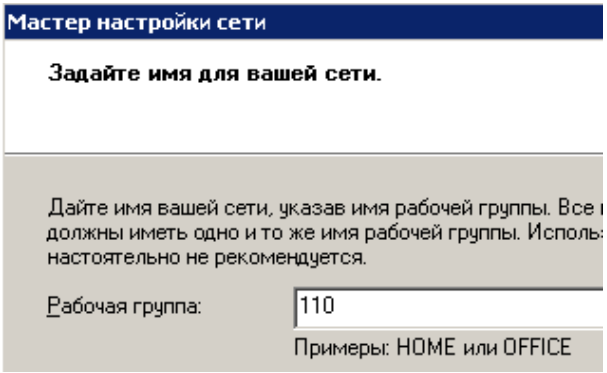


Рис. 6. Задаем имя для локальной сети

Снова **Далее** и включим общий доступ (рис. 7).

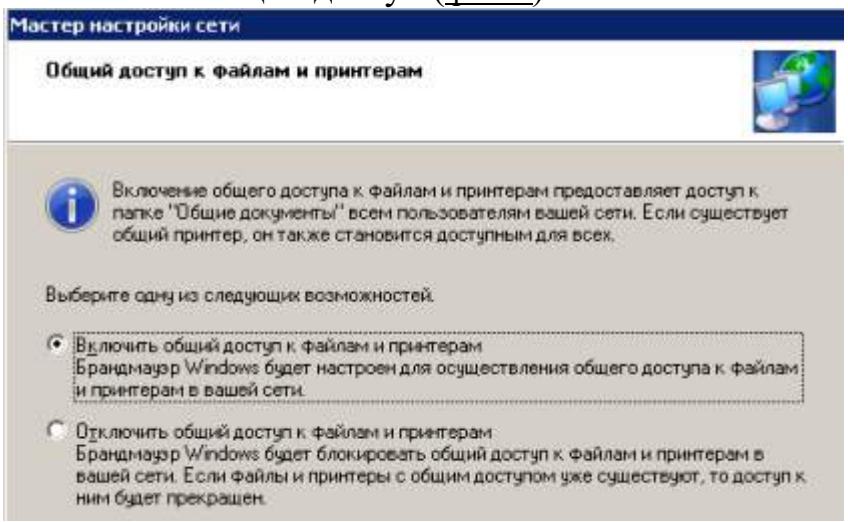


Рис. 7. Установим верхний переключатель

Работу мастера завершаем (рис. 8).

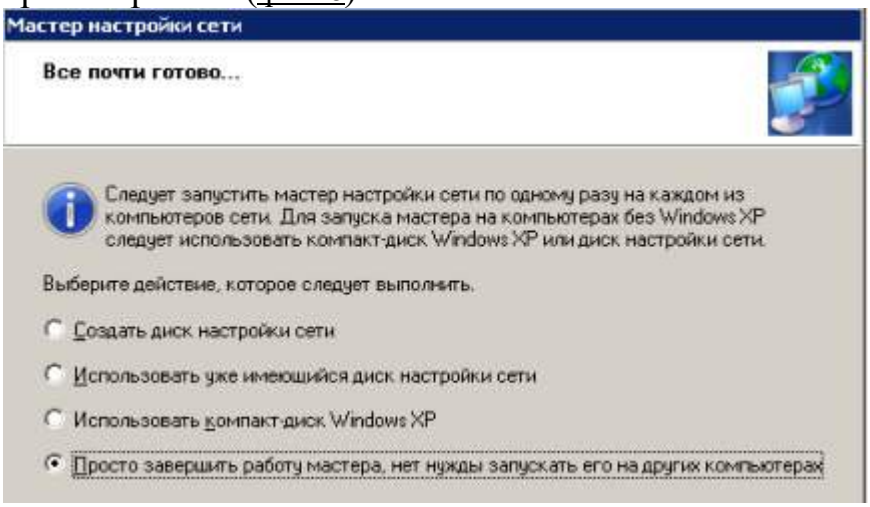


Рис. 8. Устанавливаем первый переключатель снизу

Эта машина настроена для работы в сети, перезагружаем ее и аналогично настроим другой виртуальный ПК, также включив его в рабочую группу 110. Перезагружаем. Сетевая настройка обоих машин завершена.

Проверяем работу виртуальных машин в сети

Попробуем зайти с первой машины на вторую и наоборот. Для этого войдем в **Сетевое окружение** и выполним команду **Отобразить компьютеры рабочей группы.** Если все нормально, то в рабочей группе 110 мы увидим машину 1 и машину 2 (рис. 9).

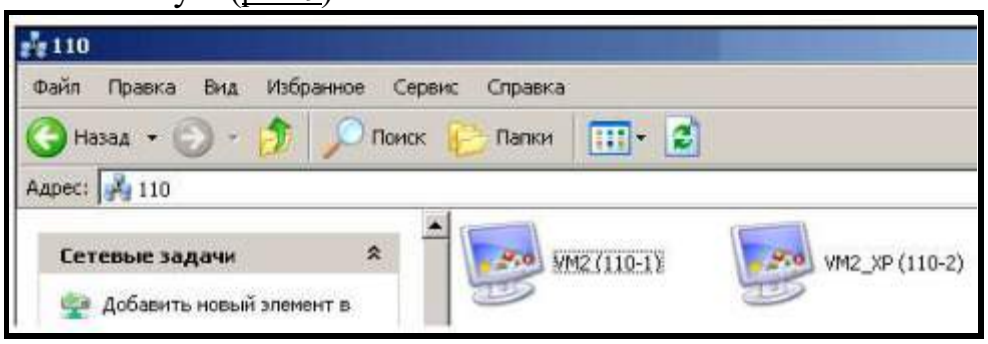


Рис. 9. Локальная виртуальная сеть настроена

Далее мы можем работать с такой сетью, как с обычной. Например, создать папки с общим доступом. Однако, может выйти и такое сообщение (рис. 10).

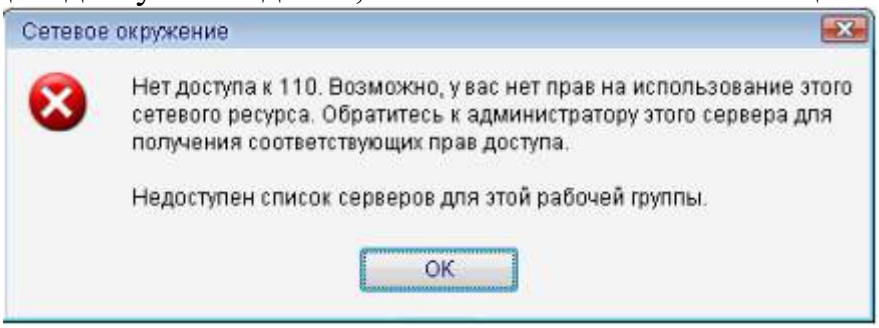


Рис. 10. Нет доступа к рабочей группе 110

Примечание

Одной из причин конфликтов в локальной сети (отсутствие общего доступа между ресурсами) может быть установка разного времени на рабочих станциях, т.е. для обеих машин таймер времени должен быть синхронным. Еще причина – использование нелицензионной операционной системы. Другие причины мы изучим позднее.

Установка средств Wmware

Чтобы получить доступ из виртуальной машины к файлам на физическом ПК потребуется команда **ВМ-Установка средств Wmware** (рис. 11).

Рис. 11. Окно начала установки средств Wmware

После инсталляции средств и перезагрузки виртуальной машины на рабочем столе Windows XP появится соответствующий значок . Далее выполним команду **ВМ-Настройки** и откроем вкладку **Опции** (**Options)** и встанем курсором на строчку папок с общим доступом (рис. 12).

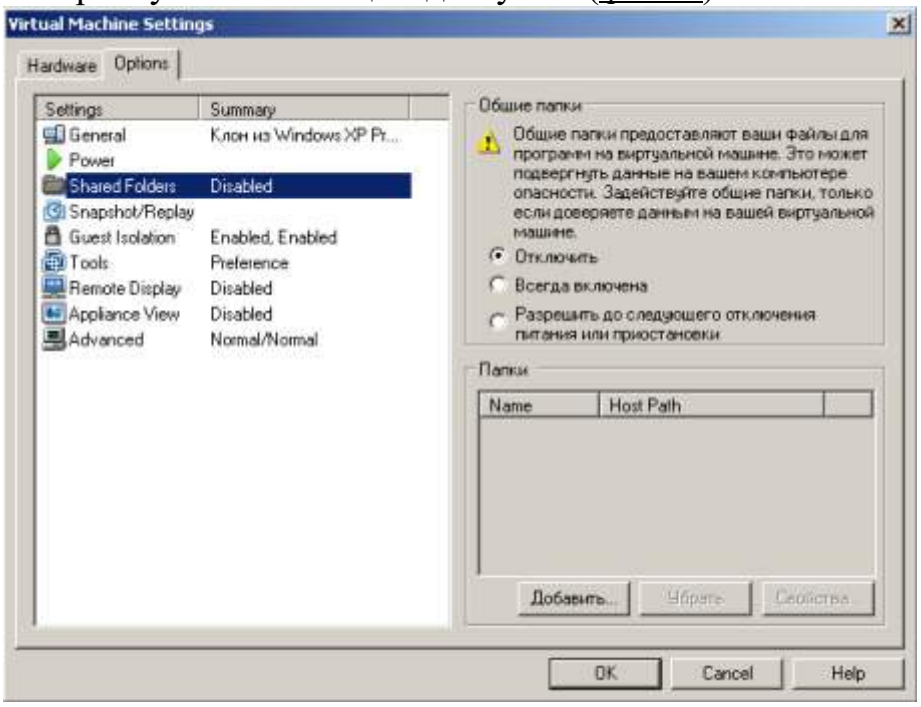


Рис. 12. Папки с общим доступом пока недоступны и пусты

Нажимаем на кнопку **Добавить**, дадим этой папке имя и укажем диск для нее (рис. 13).

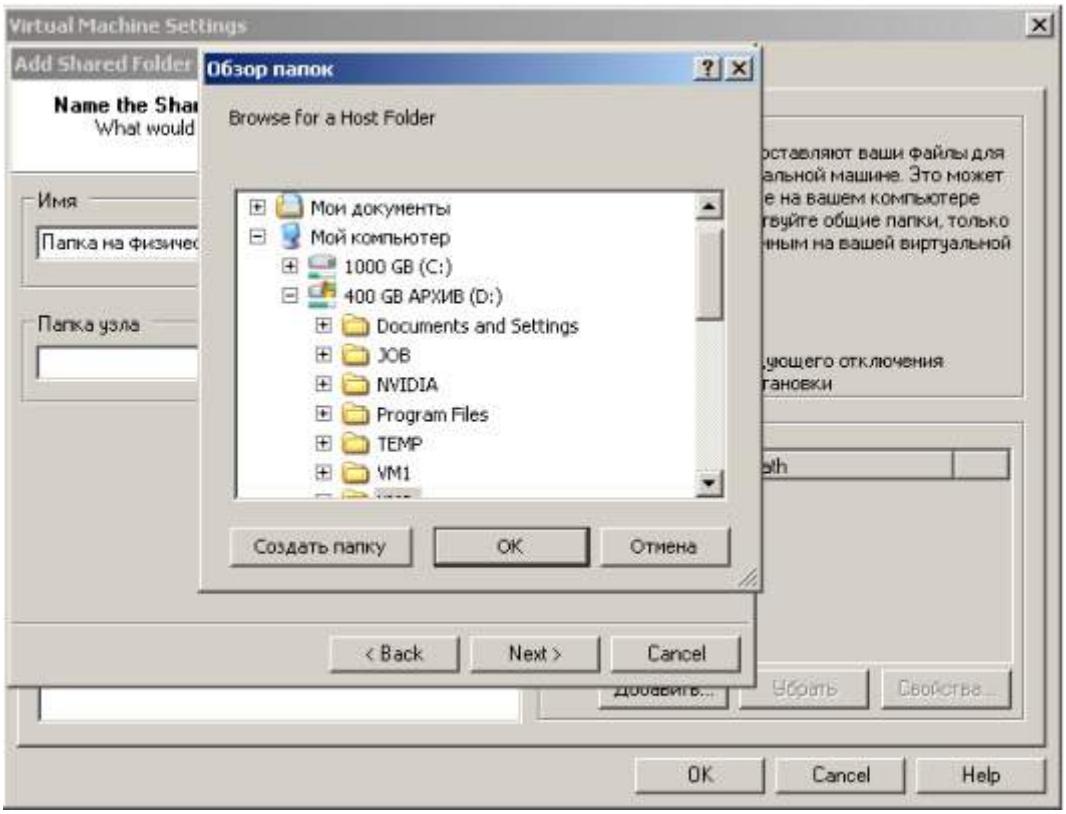


Рис. 13. Задаем параметры для папки с общим доступом

Далее активируем атрибуты папки (рис. 14).

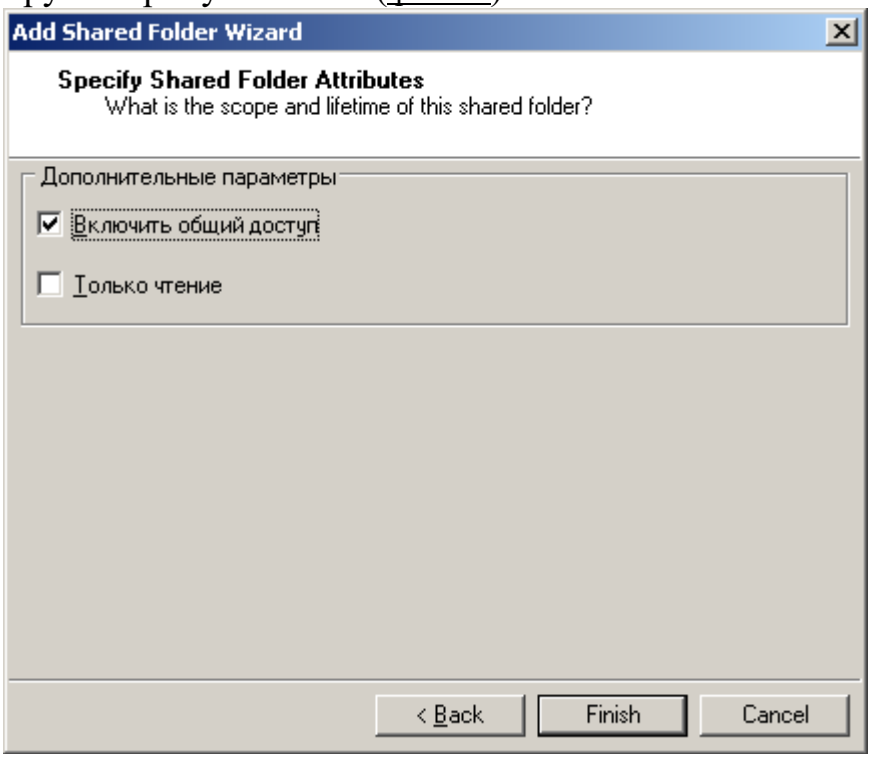


Рис. 14. В этом окне нам нужны оба флажка

В следующем окне устанавливаем переключатель **Всегда включена** (рис. 15).

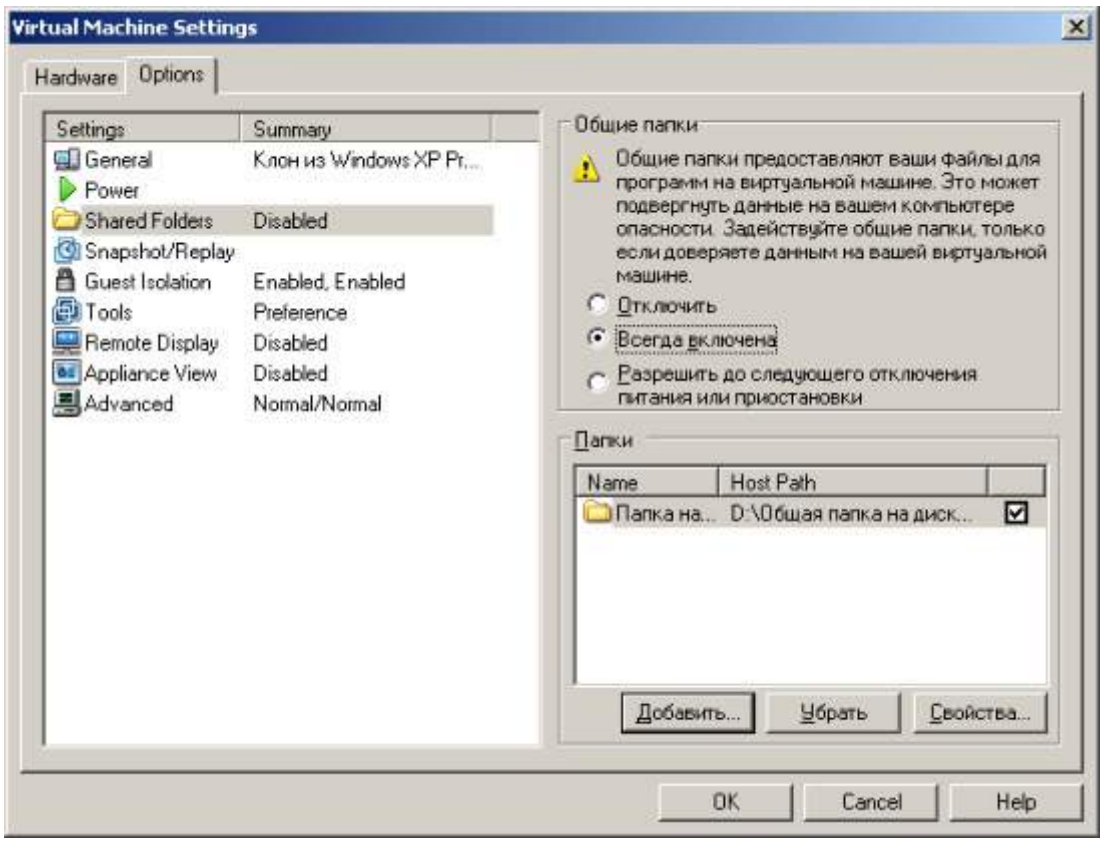
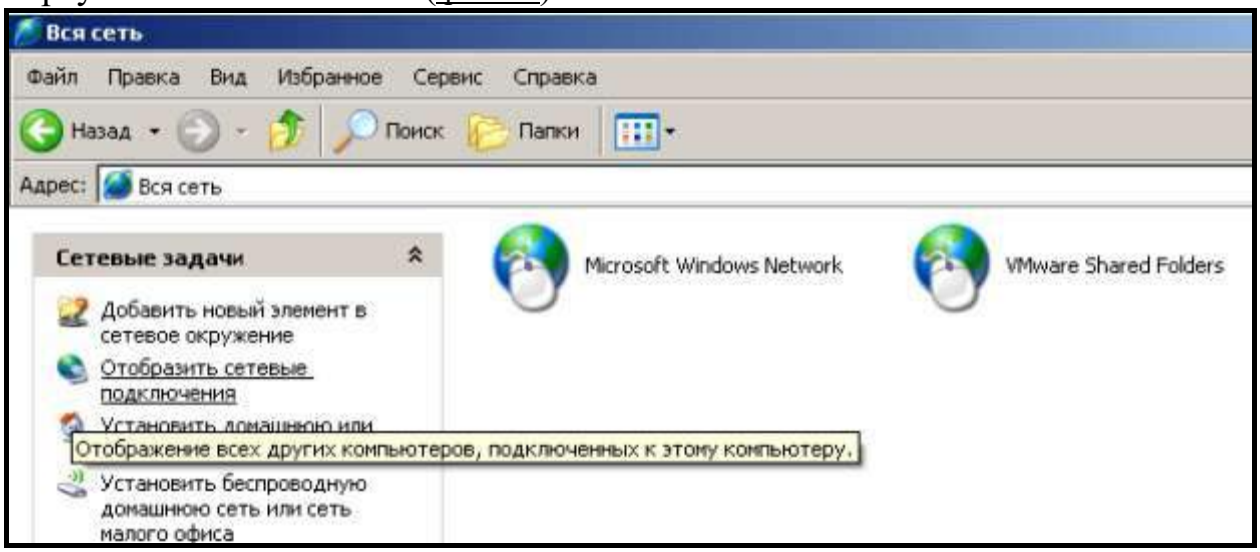


Рис. 15. Активируем этот переключатель

Теперь при просмотре всей сети мы увидим папку на нашем физическом ПК, т.е. через значок **VMware Shared Folders** у нас есть связь физического ПК с виртуальными машинами (рис. 16).



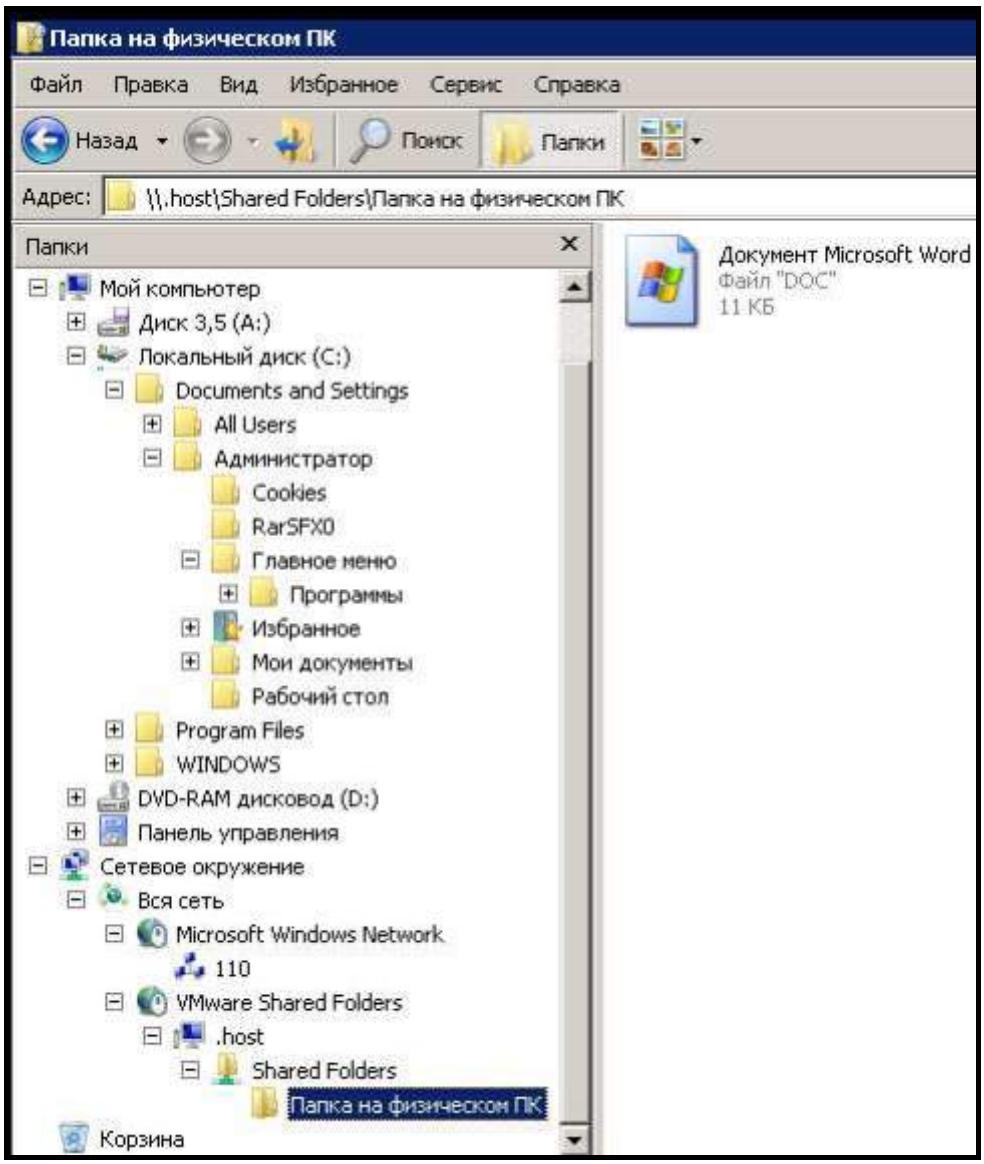


Рис. 16. Связь физической машины с виртуальной установлена

Теперь на виртуальную машину мы можем устанавливать любой soft.

Примечание

Обратите внимание на то, что установка средств Wmware решает сразу и другие проблемы, например, настройку драйверов устройств на виртуальном ПК.

Если общая папка на физическом ПК не видна, то в **Сетевом окружении** вы ее можете добавить, используя команду **Добавить новый элемент в сетевом окружении** (рис. 17).

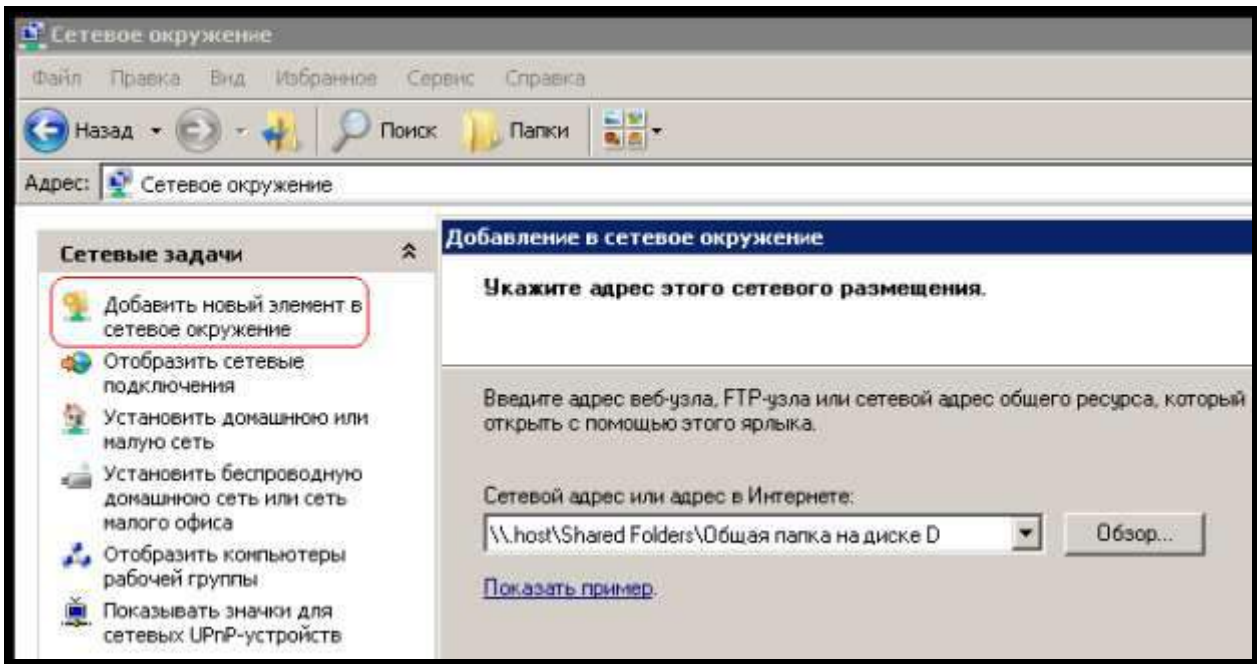


Рис. 17. Красным отмечена команда Добавить новый элемент в сетевом окружении

ПРАКТИЧЕСКАЯ РАБОТА №4.
НАСТРОЙКА УДАЛЕННОГО РАБОЧЕГО СТОЛА

Цель работы: **научиться выполнять удаленное администрирование компьютеров.**

Краткие теоретические и учебно-методические материалы по теме практической работы:

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. Офицальное 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 платформо-независима: 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 изменения 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

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

В задании используется ВМ VM-1.
Запустите виртуальную машину VM-1 и загрузите ОС Windows XP.
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.
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);

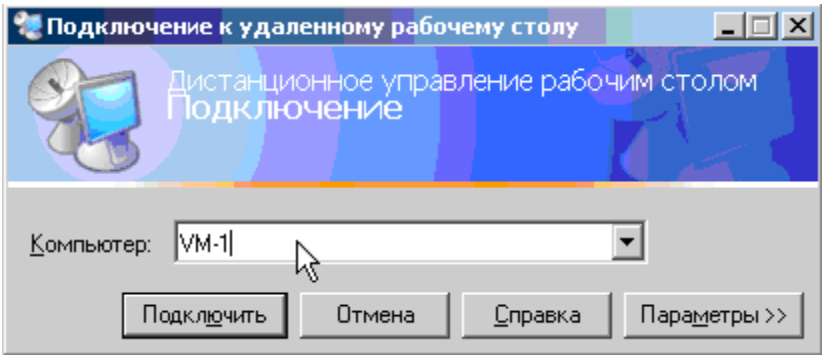


Рис.1. Окно подключения к удаленному рабочему столу

1. Настройте подключение через медленный канал связи:
2. Отобразите параметры Подключения к удаленному рабочему столу кнопкой Параметры;
3. Перейдите на вкладку Дополнительно;
4. Выберите в раскрывающемся списке Модем (28,8 Кбит/с);
5. Выполните подключение кнопкой Подключить.
6. Установите приложение UltraVNC на виртуальный компьютер:

7. Перейдите в каталог с устанавливаемой программой;
8. Запустите процесс установки (UltraVNC-1.0.4-RC6-Setup.exe);
9. Ознакомьтесь с информацией установщика и щелкните Next;
10. Ознакомьтесь с лицензионным соглашением и согласитесь с ним I accept the agreement и щелкните Next;
11. Ознакомьтесь с информацией о версии устанавливаемого программного обеспечения и щелкните Next;
12. Укажите каталог установки - C:\Program Files\UltraVNC и щелкните Next;
13. Укажите тип установки – Full Installation и щелкните Next;
14. введите имя желаемой папки в меню Пуск (например UltraVNC) и подтвердите кнопкой Next;
15. Сбросьте флажок Download Vista addons files now (Скачать дополнительные файлы для Windows Vista) и щелкните Next;
16. Сбросьте флажок Download and Install the mirror driver (Загрузить и установить драйвер mirror) и щелкните Next;
17. Выполните дополнительные задчи 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);

18. Подтвердите изменения кнопкой Next;
19. Инициализируйте установку кнопкой Install;
20. на заднем фоне появится диалоговое окно свойств сервера UltraVNC
21. Ознакомьтесь с послеустановочной информацией и щелкните Next;
22. Завершите установку кнопкой Finish.

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 ОК.

Задание 2. Установите удаленно на виртуальный компьютер браузер Opera.

Подключитесь к виртуальному компьютеру VM-1 с помощью UltraVNC Viewer:

1. Запустите с диска к лабораторным работам UltraVNC Viewer (vncviewer.exe);
2. Введите в поле VNC Server - <имя удаленного компьютера> (VM-1);

3. Установите режим подключения для просмотра (флажок View only);
4. Активируйте подключение кнопкой Connect;
5. Введите пароль для подключения - qwerasdf;
6. Переключитесь из режима просмотра в нормальный (контекстное меню окна UltraVNC Viewer/View only);
7. Установите браузер Opera:
8. Перейдите в каталог с устанавливаемой программой;
9. Запустите процесс установки (Opera_9.24_International_Setup.exe);
10. Укажите желаемый язык установки - Русский (ОК);
11. Активизируйте процесс установки кнопкой Установить;
12. Ознакомьтесь с лицензионным соглашением и согласитесь с ним кнопкой Принимаю;
13. Укажите тип установки – Стандартная и щелкните Далее;
14. Установите приложение кнопкой Установить;
15. Завершите процесс установки кнопкой Готово.
16. Создайте и сохраните в своей домашней папке снимок экрана виртуального компьютера с запущенным браузером Opera.

ПРАКТИЧЕСКАЯ РАБОТА №5.
НАСТРОЙКА БЕСПРОВОДНОЙ СЕТИ WI-FI

Цель работы: Научиться настраивать беспроводную сеть в ОС Windows 7 и Windows XP

Краткие теоретические сведенияи

Wi-Fi был создан в 1991 году NCR Corporation/AT&T (впоследствии — Lucent Technologies и Agere Systems) в Ньивегейн,Нидерланды. Продукты, предназначавшиеся изначально для систем кассового обслуживания, были выведены на рынок под маркой WaveLAN и обеспечивали скорость передачи данных от 1 до 2 Мбит/с. Создатель Wi-Fi — Вик Хейз находился в команде, участвовавшей в разработке таких стандартов, как IEEE 802.11b, IEEE 802.11a и IEEE 802.11g. В 2003 году Вик ушёл из Agere Systems. Agere Systems не смогла конкурировать на равных в тяжёлых рыночных условиях, несмотря на то, что её продукция занимала нишу дешёвых Wi-Fi решений. 802.11abg all-in-one чипсет от Agere (кодовое имя: WARP) плохо продавался, и Agere Systems решила уйти с рынка Wi-Fi в конце 2004 года

Термин «Wi-Fi» изначально был придуман как игра слов для привлечения внимания потребителя "намёком" на Hi-Fi (High Fidelity, высокая точность). Несмотря на то, что поначалу в некоторых пресс-релизах WECA фигурировало словосочетание «Wireless Fidelity» («беспроводная точность»), на данный момент от такой формулировки отказались, и термин «Wi-Fi» никак не расшифровывается

Что такое технология Wi-Fi?

Wi-Fi - сокращение от английского Wireless Fidelity, обозначающее стандарт беспроводной (радио) связи, который объединяет несколько протоколов и имеет официальное наименование IEEE 802.11 (от Institute of Electrical and Electronic Engineers - международной организации, занимающейся разработкой стандартов в области электронных технологий). Самым известным и распространенным на сегодняшний день является протокол IEEE 802.11b (обычно под сокращением Wi-Fi подразумевают именно его), определяющий функционирование беспроводных сетей, в которых для передачи данных используется диапазон частот от 2,4 до 2.4835 Гигагерца и обеспечивается максимальная скорость 11 Мбит/сек. Максимальная дальность передачи сигнала в такой сети составляет 100 метров, однако на открытой местности она может достигать и больших значений (до 300-400 м).

Помимо 802.11b существуют еще беспроводной стандарт 802.11a, использующий частоту 5 ГГц и обеспечивающий максимальную скорость 54 Мбит/с, а также 802.11g, работающий на частоте 2,4 ГГц и тоже обеспечивающий 54 Мбит/с. Однако, из-за меньшей дальности, значительно

большей вычислительной сложности алгоритмов и высокого энергопотребления эти технологии пока не получили большого распространения. Кроме того, в данное время ведется разработка стандарта 802.11n, который в обозримом будущем сможет обеспечить скорости до 320 Мбит/с.

Принцип работы Wi-Fi

Обычно схема Wi-Fi сети содержит не менее одной точки доступа и не менее одного клиента. Также возможно подключение двух клиентов в режиме точка-точка (Ad-hoc), когда точка доступа не используется, а клиенты соединяются посредством сетевых адаптеров «напрямую». Точка доступа передаёт свой идентификатор сети (SSID) с помощью специальных сигнальных пакетов на скорости 0,1 Мбит/с каждые 100 мс. Поэтому 0,1 Мбит/с — наименьшая скорость передачи данных для Wi-Fi. Зная SSID сети, клиент может выяснить, возможно ли подключение к данной точке доступа. При попадании в зону действия двух точек доступа с идентичными SSID приёмник может выбирать между ними на основании данных об уровне сигнала. Стандарт Wi-Fi даёт клиенту полную свободу при выборе критериев для соединения.Подобно традиционным проводным технологиям, Wi-Fi обеспечивает доступ к серверам, хранящим базы данных или программные приложения, позволяет выйти в Интернет, распечатывать файлы и т. д. Но при этом компьютер, с которого считывается информация, не нужно подключать к компьютерной розетке.

Таким образом, Wi-Fi-технология позволяет решить три важных задачи:

1. упростить общение с мобильным компьютером;
2. обеспечить комфортные условия для работы деловым партнерам, пришедшим в офис со своим ноутбуком,
3. создать локальную сеть в помещениях, где прокладка кабеля невозможна или чрезмерно дорога

Преимущества технологии Wi-Fi

К основным преимущества Wi-Fi стоит отметить:

- Позволяет развернуть сеть без прокладки кабеля, что может уменьшить стоимость развёртывания и/или расширения сети. Места, где нельзя проложить кабель, например, вне помещений и в зданиях, имеющих историческую ценность, могут обслуживаться беспроводными сетями.
- Позволяет иметь доступ к сети мобильным устройствам.
- Wi-Fi устройства широко распространены на рынке. Гарантируется совместимость оборудования благодаря обязательной сертификации оборудования с логотипом Wi-Fi.
- Излучение от Wi-Fi устройств в момент передачи данных на два порядка (в 100 раз) меньше, чем у сотового телефона.

Немаловажно и то, что обслуживание Wi-Fi-сети примерно на 75% дешевле обслуживания сети обычной(имеется ввиду Wi-Fi в крупных компаниях) .

Недостатки технологии Wi-Fi

К основным недостаткам Wi-Fi можно отнести:

- В диапазоне 2.4 GHz работает множество устройств, таких как устройства, поддерживающие Bluetooth, и др., и даже микроволновые печи, что ухудшаетэлектромагнитную совместимость.
- Частотный диапазон и эксплуатационные ограничения в различных странах неодинаковы. Во многих европейских странах разрешены два дополнительных канала, которые запрещены в США; В Японии есть ещё один канал в верхней части диапазона, а другие страны, например Испания, запрещают использование низкочастотных каналов. Более того, некоторые страны, например Россия, Беларусь и Италия, требуют регистрации всех сетей Wi-Fi, работающих вне помещений, или требуют регистрации Wi-Fi-оператора.
- Как было упомянуто выше — в России точки беспроводного доступа, а также адаптеры Wi-Fi с ЭИИМ, превышающей 100 мВт (20 дБм), подлежат обязательной регистрации.
- Стандарт шифрования WEP может быть относительно легко взломан[7] даже при правильной конфигурации (из-за слабой стойкости алгоритма). Несмотря на то, что новые устройства поддерживают более совершенный протокол шифрования данных WPA и WPA2, многие старые точки доступа не поддерживают его и требуют замены. Принятие стандарта IEEE 802.11i (WPA2) в июне2004 года сделало доступной более безопасную схему, которая доступна в новом оборудовании. Обе схемы требуют более стойкий пароль, чем те, которые обычно назначаются пользователями. Многие организации используют дополнительное шифрование (например, VPN) для защиты от вторжения. На данный момент основным методом взлома WPA2 является подбор пароля, поэтому рекомендуется использовать сложные цифробуквенные пароли для того, чтобы максимально усложнить задачу подбора пароля.
- В режиме ad-hoc стандарт предписывает лишь реализовать скорость 11 Мбит/сек (802.11b). Шифрование WPA(2) недоступно, только взломанный WEP.

Задания для практического занятия:

Пример 1. Легкая (полуавтоматическая) настройка беспроводного маршрутизатора TL-WR1043ND

Мы подключим к WI-FI маршрутизатор TP-LINK, точнее – модель TL-WR1043ND (рис.1-3). Это современное устройство, у которого максимальная скорость беспроводного соединения: 300 Мбит/сек, а скорость портов 1000 Мбит/сек.

Рис. 1. Wi-Fi-точка доступа (роутер) TL-WR1043ND

Рис. 2. Передняя панель беспроводного маршрутизатора TL-WR1043ND

Светодиодные индикаторы и кнопка-индикатор QSS (быстрая настройка параметров безопасности):

1. **PWR** – питание. Индикатор выкл - питание отключено, вкл - питание включено.
2. **SYS** – система. Вкл. - загрузка исходных параметров или системная ошибка. Мигает - устройство работает в нормальном режиме. Выкл. - системная ошибка.
3. **WLAN** – беспроводная сеть. Выкл. - функция беспроводной передачи данных отключена. Мигает - функция беспроводной передачи данных включена.
4. **WAN** (Интернет), **LAN** (Локальная сеть) 1-4. Выкл. - у порта нет подключенных устройств. Вкл. - к порту подключено устройство, но оно неактивно. Мигает - к порту подключено устройство и оно активно.
5. **QSS** - быстрая настройка параметров безопасности. Медленно мигает - беспроводное устройство производит подключение к сети через функцию QSS. Этот процесс занимает примерно две минуты. Вкл. - беспроводное устройство было успешно подключено к сети посредством функции QSS. Быстро мигает - не удалось подключить беспроводное устройство к сети посредством функции QSS.

Рис. 3. Задняя панель беспроводного маршрутизатора TL-WR1043ND

На задней панели расположены следующие элементы:

1. **POWER** - разъем для подключения питания от адаптера питания, входящего в комплект поставки беспроводного маршрутизатора TL-WR1043ND
2. **RESET** – кнопка сброса конфигурации роутера для его возврата к заводским настройкам. При помощи иголки нажмите и удерживайте кнопку Reset 5 секунд, затем подождите, пока маршрутизатор выполнит перезагрузку.
3. **USB** - разъем для подключения устройства хранения данных или, например, принтера.
4. **WAN** синяя розетка RJ-45 для подключения DSL/кабельного модема или сети Интернет (порт для подключения Сети от провайдера).
5. **Антенна Wi-Fi** черного цвета служит для беспроводного получения и передачи данных.
6. **1,2,3,4 (LAN)** – розетки RJ-45 желтого цвета для подключения маршрутизатора к компьютерам локальной сети.

Итак, наш беспроводный роутер подключен к электросети, от него идет витая пара на стационарный ПК (патчкорд входит в комплект поставки), а Wi-Fi мы будем использовать, чтобы подключить ноутбук. Настройку роутера можно производить как на стационарном ПК (десктопе), так и со стороны ноутбука. Или там, или там нужно выполнить команду **Панель Управления – Центр управления сетями и общим доступом – Настройка нового подключения или сети - Создание и настройка новой сети** (рис. 4).

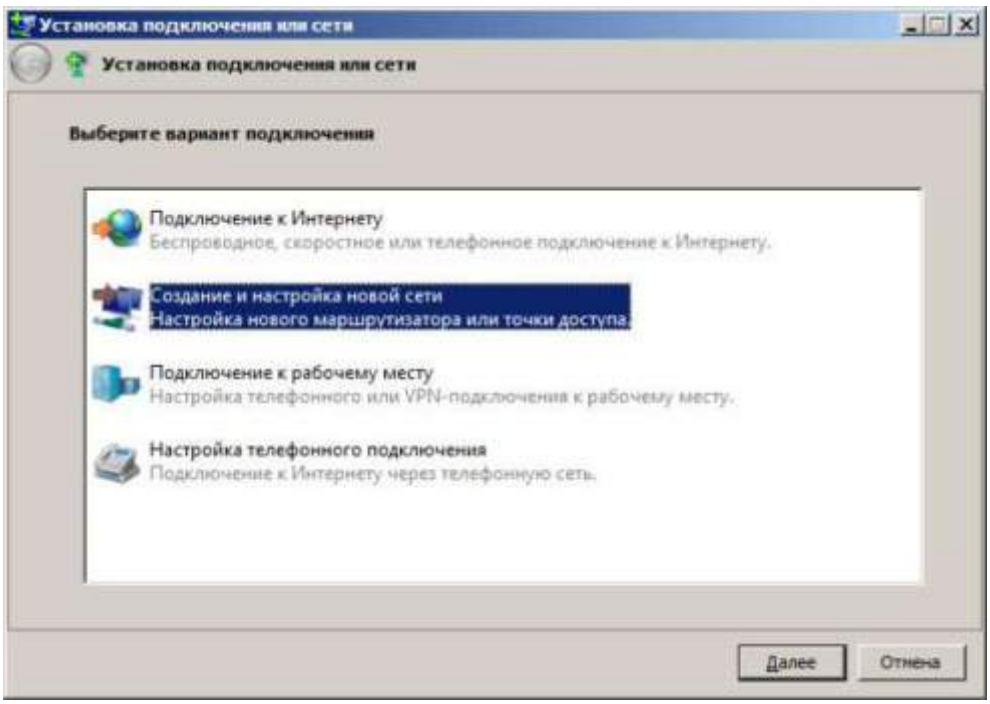


Рис. 4. Окно Установка подключения или сети

Нажимаем на кнопку **Далее**, видим наше беспроводное устройство (рис. 5).

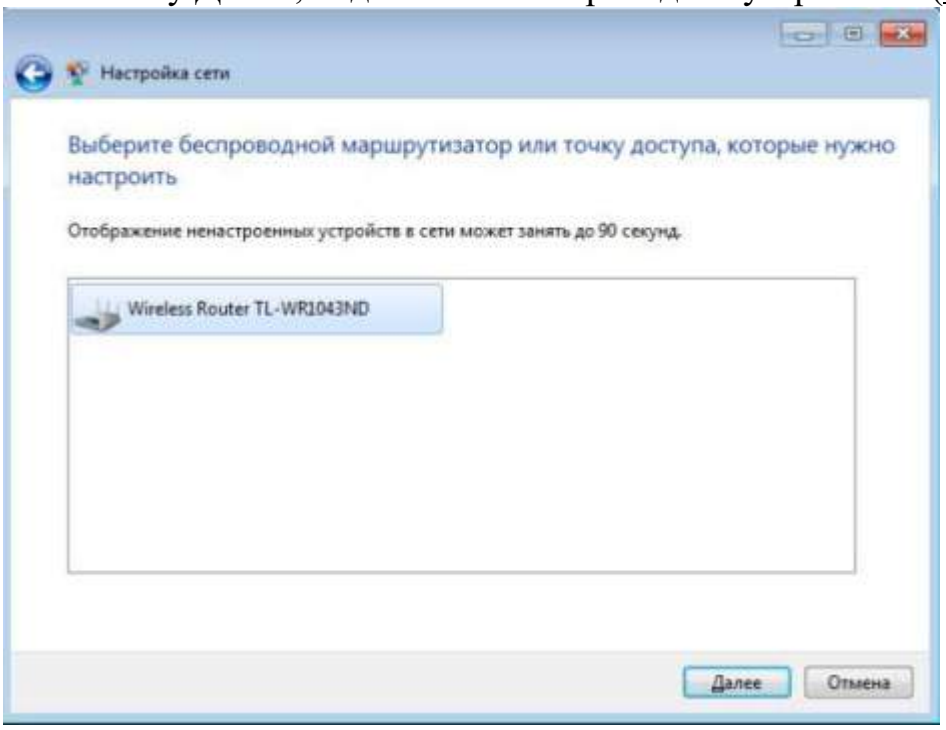


Рис. 5. Обнаружение точки доступа прошло нормально

Следующим этапом необходимо вести PIN-код с этикетки на маршрутизаторе (рис. 6 и рис. 7).

Рис. 6. На этикетке маршрутизатора читаем PIN-код

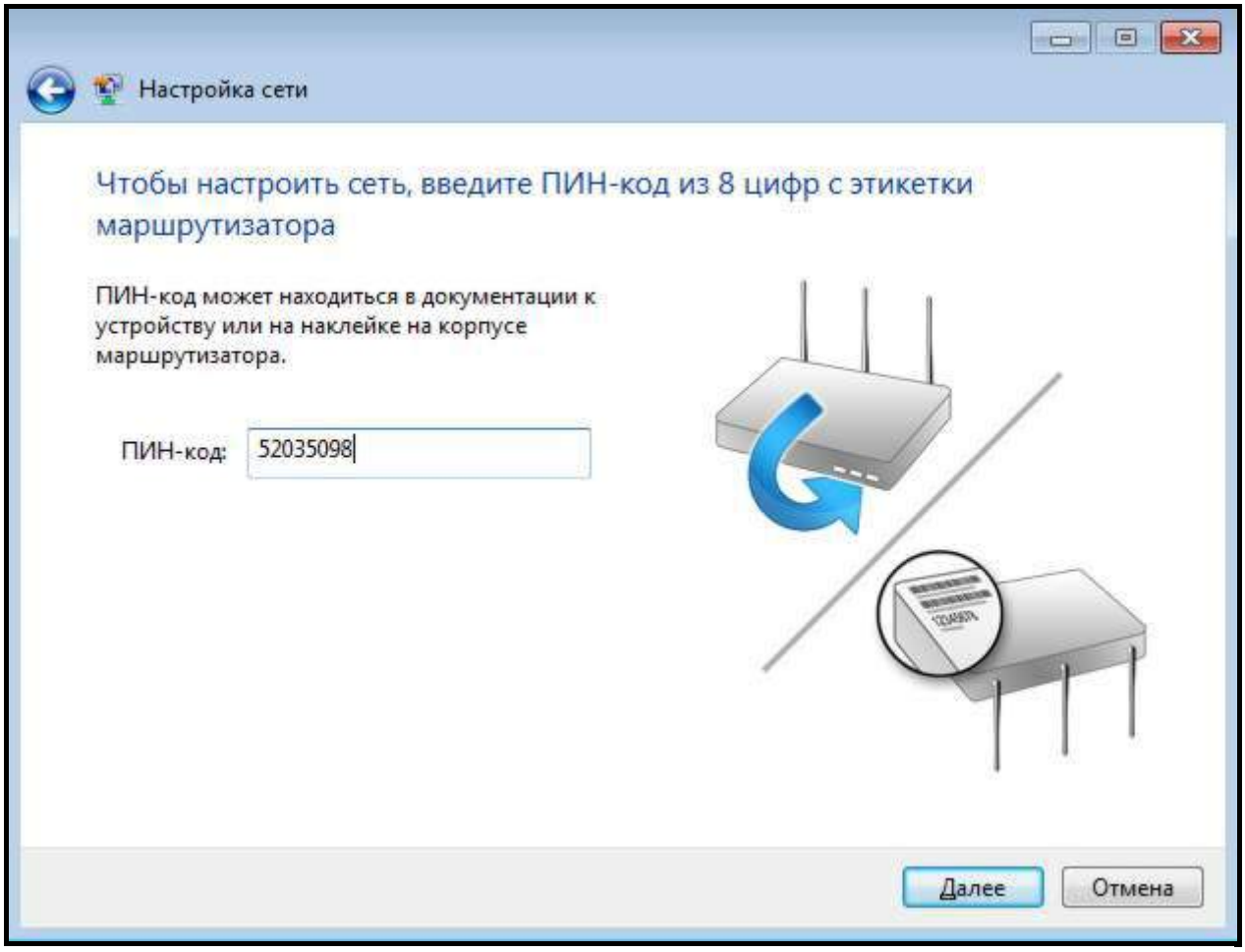


Рис. 7. Вводим PIN-код в окно Настройка сети

После нажатия на кнопку **Далее** следует согласиться с рекомендуемыми настройками точки доступа или задать свои (имя беспроводной сети, пароль для доступа к сети, уровень безопасности и тип шифрования) – рис. 8.

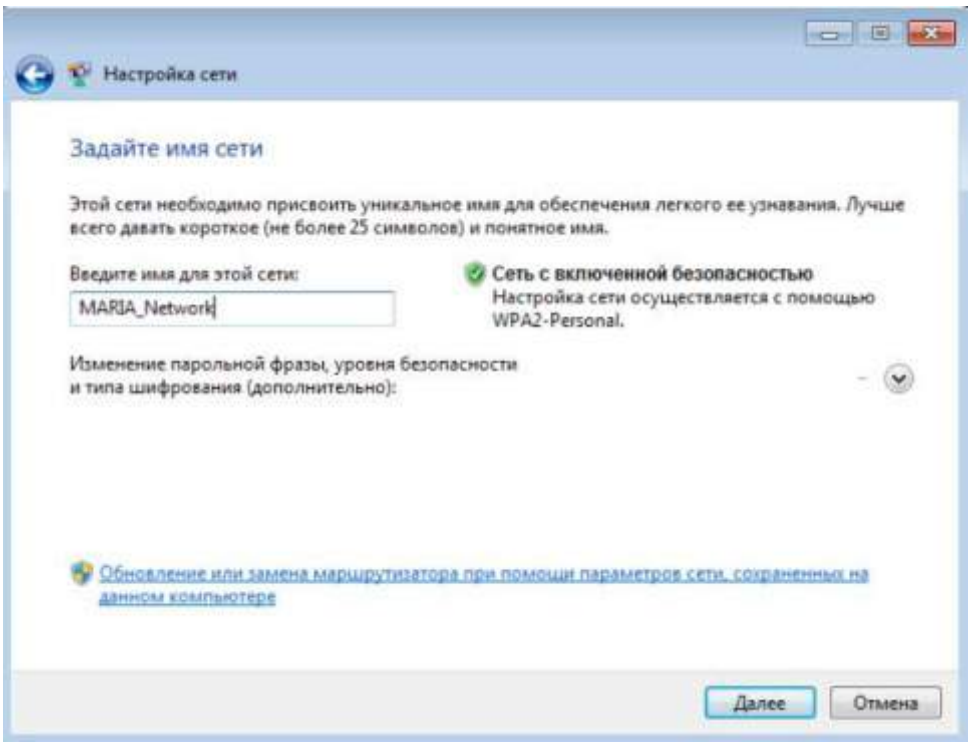


Рис. 8. Вводим имя сети (его придумываем сами)

После нажатия кнопки **Далее** произойдет настройка точки доступа (беспроводного маршрутизатора), генерация ключа безопасности и подключение нашего ноутбука к беспроводной сети (рис. 9 и рис. 10).

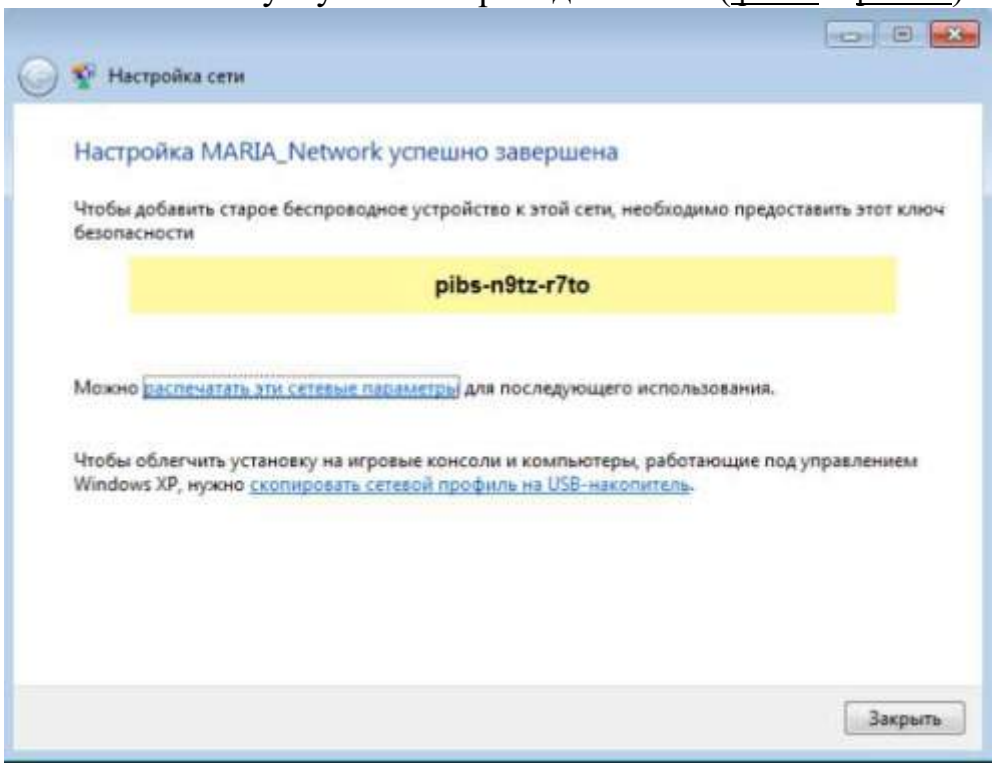


Рис. 9. Создание ключа безопасности

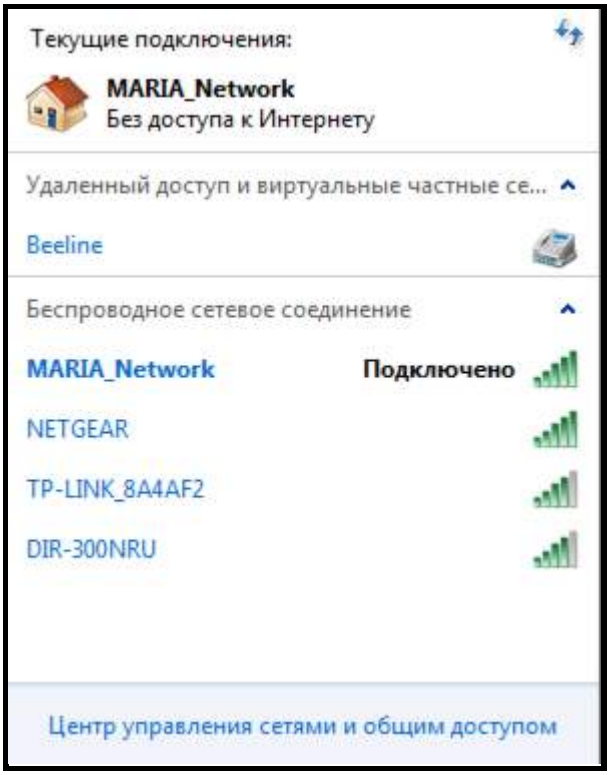


Рис. 10. Беспроводное соединение подключено

Примечание

Модель TL-WR1043ND имеет кнопку быстрой настройки защиты (QSS) для автоматической передачи ключа шифрования клиентскому устройству с такой же функцией. Поэтому, при подключении к нашей беспроводной сети нового компьютера под управлением Windows 7 (их может быть до 20 шт.), можно не вводить ключ безопасности, а просто нажать на эту кнопку на маршрутизаторе. Подключение к беспроводной сети произойдет автоматически (рис. 11).

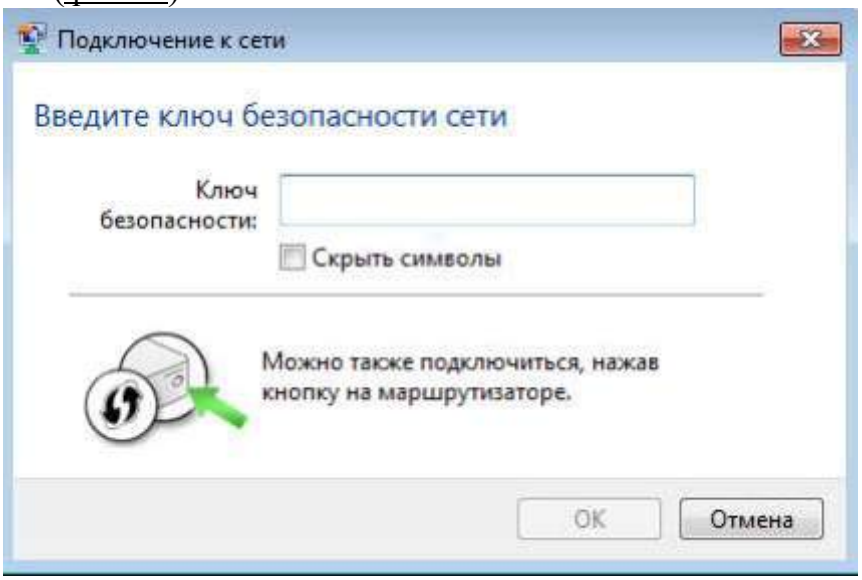


Рис. 11. Окно ввода ключа безопасности

Пример 2. Настройка на работу в Интернет Wi-Fi роутера Net Gear JWNR2000 в ручном режиме

В этой работе мы изучим, как можно с помощью Wi-Fi роутера подключить к Интернет два ПК: стационарный и ноутбук. Порты и индикаторы роутера приведены на рис. 12.

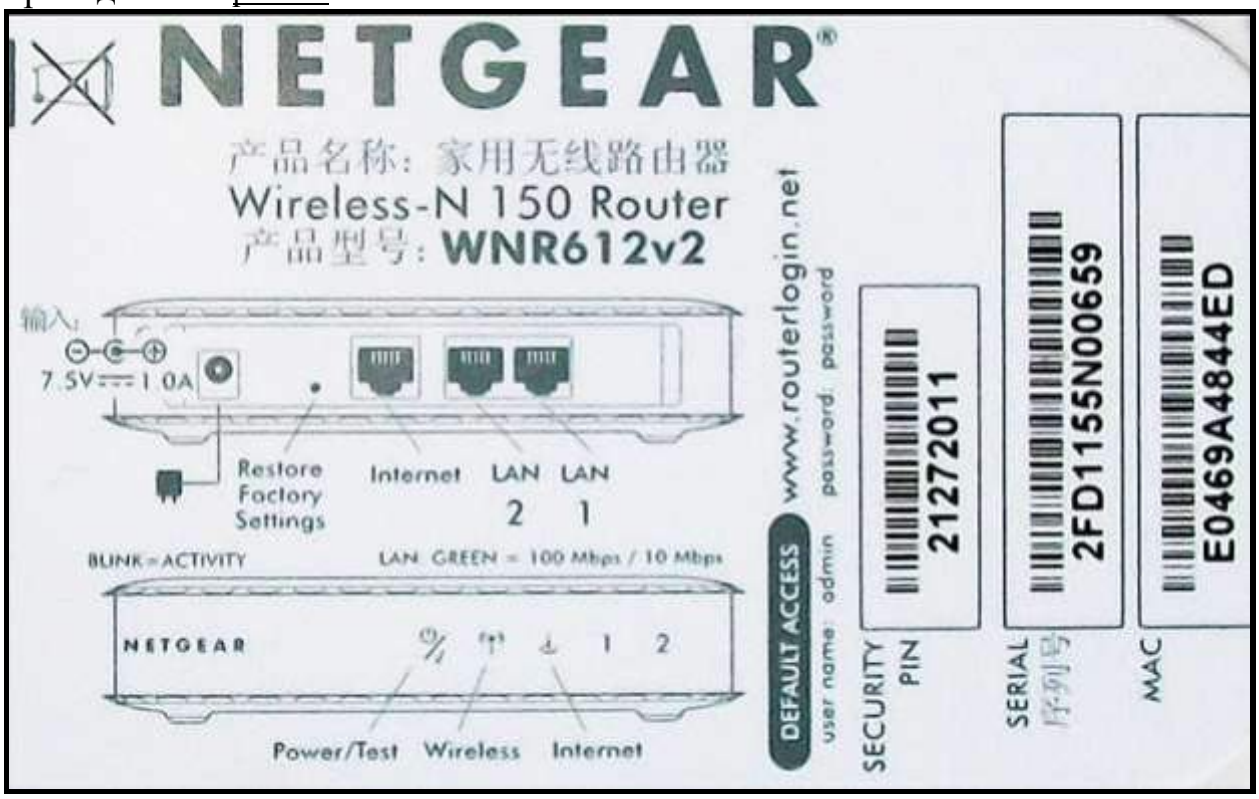


Рис. 12. Обозначение портов и инкикаторов роутера Net Gear JWNR2000

Характеристики этой модели маршрутизатора для выделенной линии таковы:

– Частота - 2,4 Ггц
– Режимы - Infrastructure, WDS-Bridge
– Кнопки - Reset, WPS

Примечание

Кнопка WPS нужна для упрощение процесса настройки беспроводной сети. Нажатие WPS автоматически обозначает имя сети и задает шифрование, для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры.

1. Индикаторы - LAN, Power, WLAN, WPS
2. Порты Fast Ethernet - 4 порта 10/100 Мбит/сек
3. Порты WAN - 1 порт RJ-45
4. Управление - Веб-интерфейс, GUI, SNMP
5. Firewall - фильтрация по MAC-адресу, фильтрация пакетов, защита от DoS-атак

6. Поддержка схем обеспечения безопасности беспроводной передачи WPA2-PSK; WPA-PSK; TKIP; AES; WEP-кодирование с 64- или 128-битным ключом
7. Защищенные VPN-протоколы - PPTP, PPPoE
8. Получение IP-адреса - Static IP, Dynamic IP
9. QoS - Поддерживается
10. Поддержка WMM (Wi-Fi Multimedia) - Есть
11. DMZ - Поддерживается
12. NAT - Поддерживается
13. DHCP-сервер - Есть
14. Максимальная скорость беспроводной передачи данных - 300 Мбит/сек
15. Стандарты беспроводной связи - IEEE 802.11n, IEEE 802.11g, IEEE 802.11b

Шаг 1 – Настройка стационарного ПК для ОС Windows XP

Подключаем роутер согласно схеме на рис.13.">

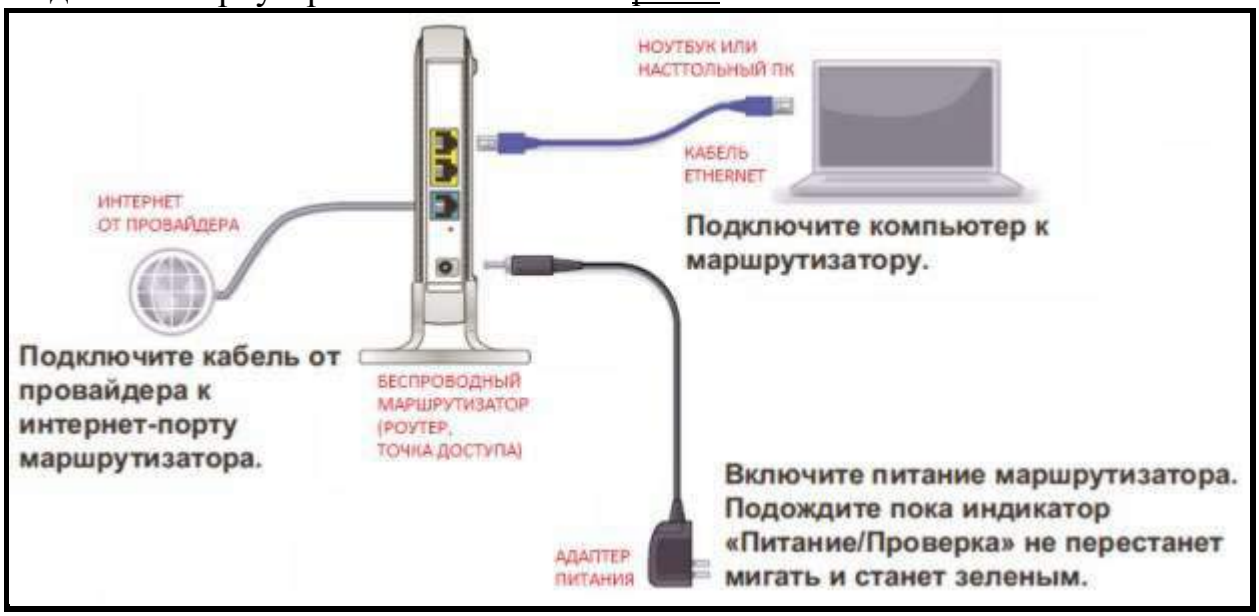


Рис. 13. Схема подключения устройств беспроводной сети к точке доступа

Далее нужно настроить протокол TCP/IP как на рис. 14.

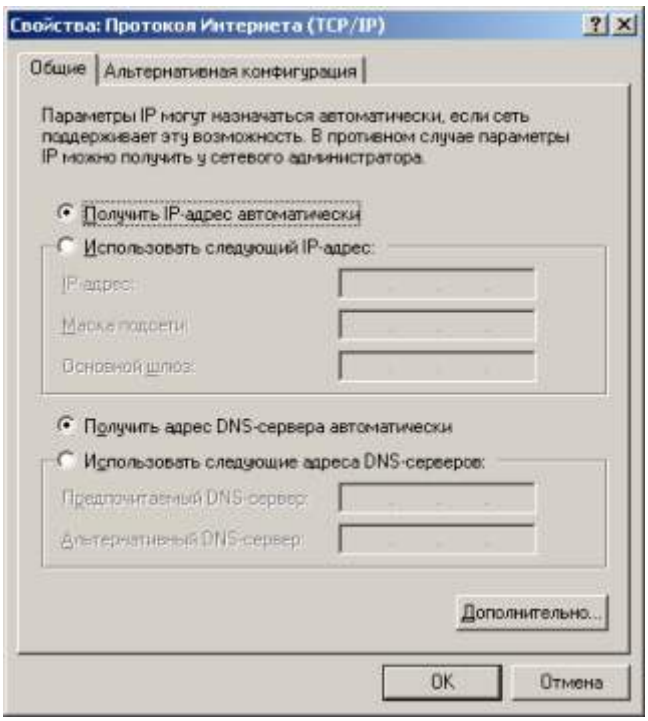


Рис. 14. Настройка протокола Интернет

Затем введите в браузере 192.168.1.1 и получите следующее окно (рис. 15). Вводим сюда Имя пользователя и Пароль (они написаны на этикетке роутера – см. рис. выше"/>).

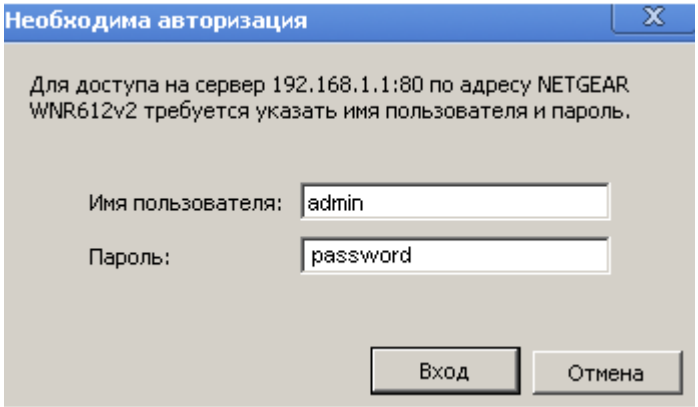


Рис. 15. Окно входа на сервер 192.168.1.1

После нажатия на кнопку **Вход** откроется окно **Основные настройки**. В программе имеется Мастер установки, но он здесь не очень хорош, поэтому лучше воспользоваться ручной настройкой роутера (рис. 16).

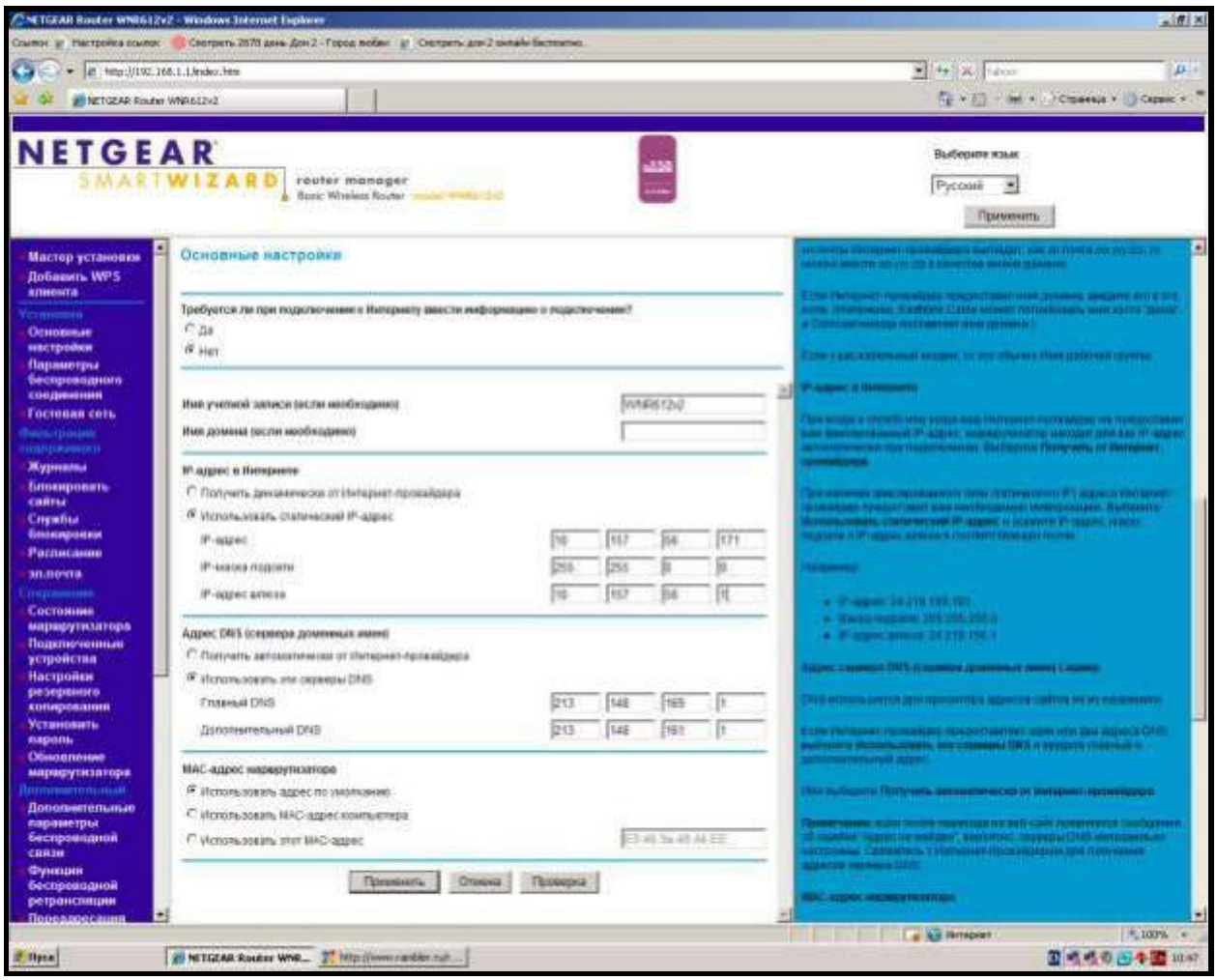


Рис. 16. Эти данные вводите в соответствии с договором провайдера Интернет

В данное окно вводим IP-адрес, IP-маску подсети и IP-адрес шлюза из договора с провайдером. Нажимает на кнопку **Применить** – появляется другое окно **Основные настройки** (рис. 17).

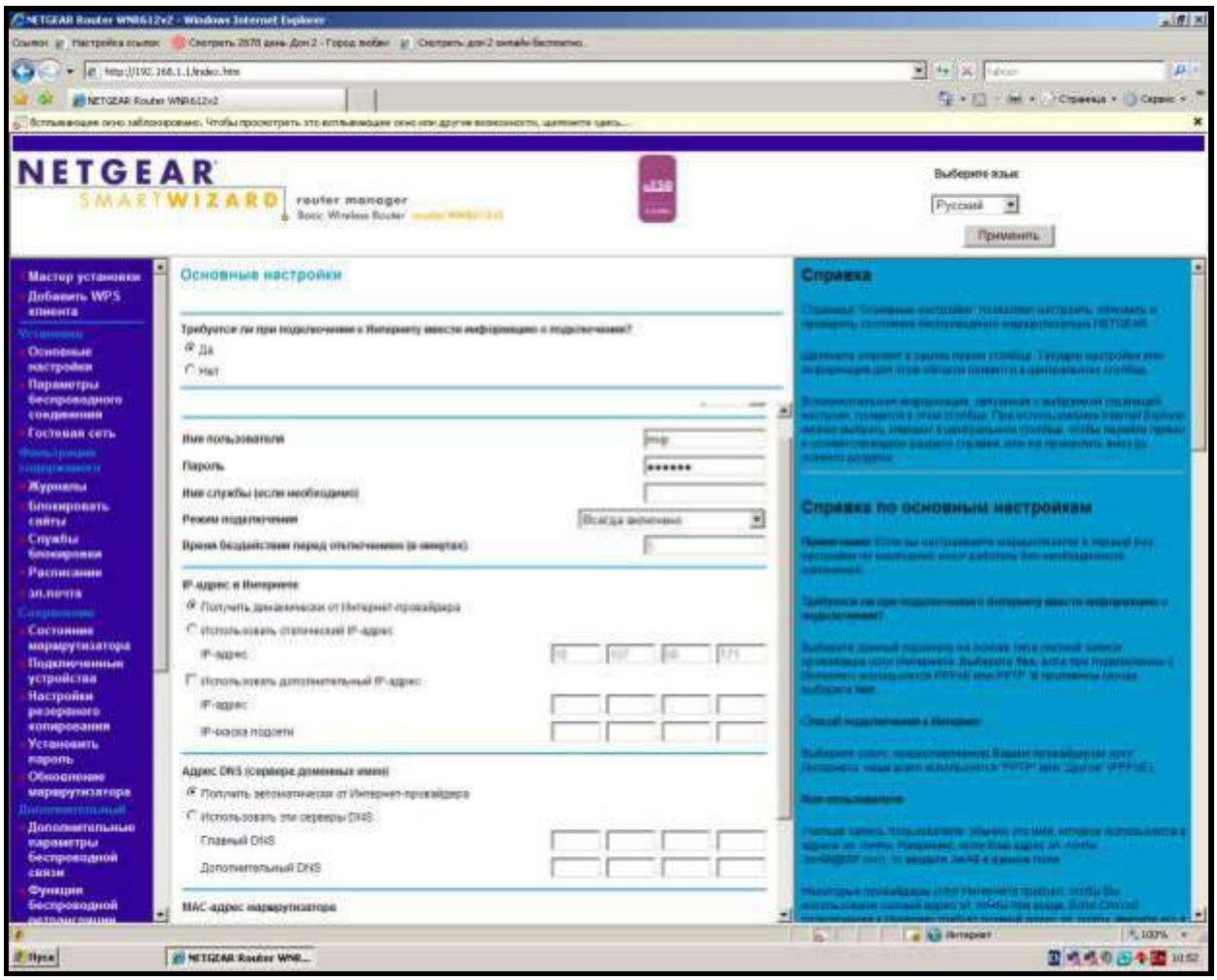


Рис. 17. Окно основные настройки

Здесь в соответствии с договором провайдера Интернет вводим **Имя пользователя** и **Пароль**. В этом окне же окне следует в списке **Поставщик услуг Интернета** выбрать протокол **PPPoE** (рис. 18). Нажимаем **Применить**.

Рис. 18. Из протоколов доступа выбираем протокол PPPoE

После обновления параметров роутера в поле **Сохранение** найдите опцию **Установить пароль** и замените пароль по умолчанию, т.е. **password** на какой-либо свой, например, quthor. Далее настройте окно **Параметры беспроводного соединения** – рис. 19.

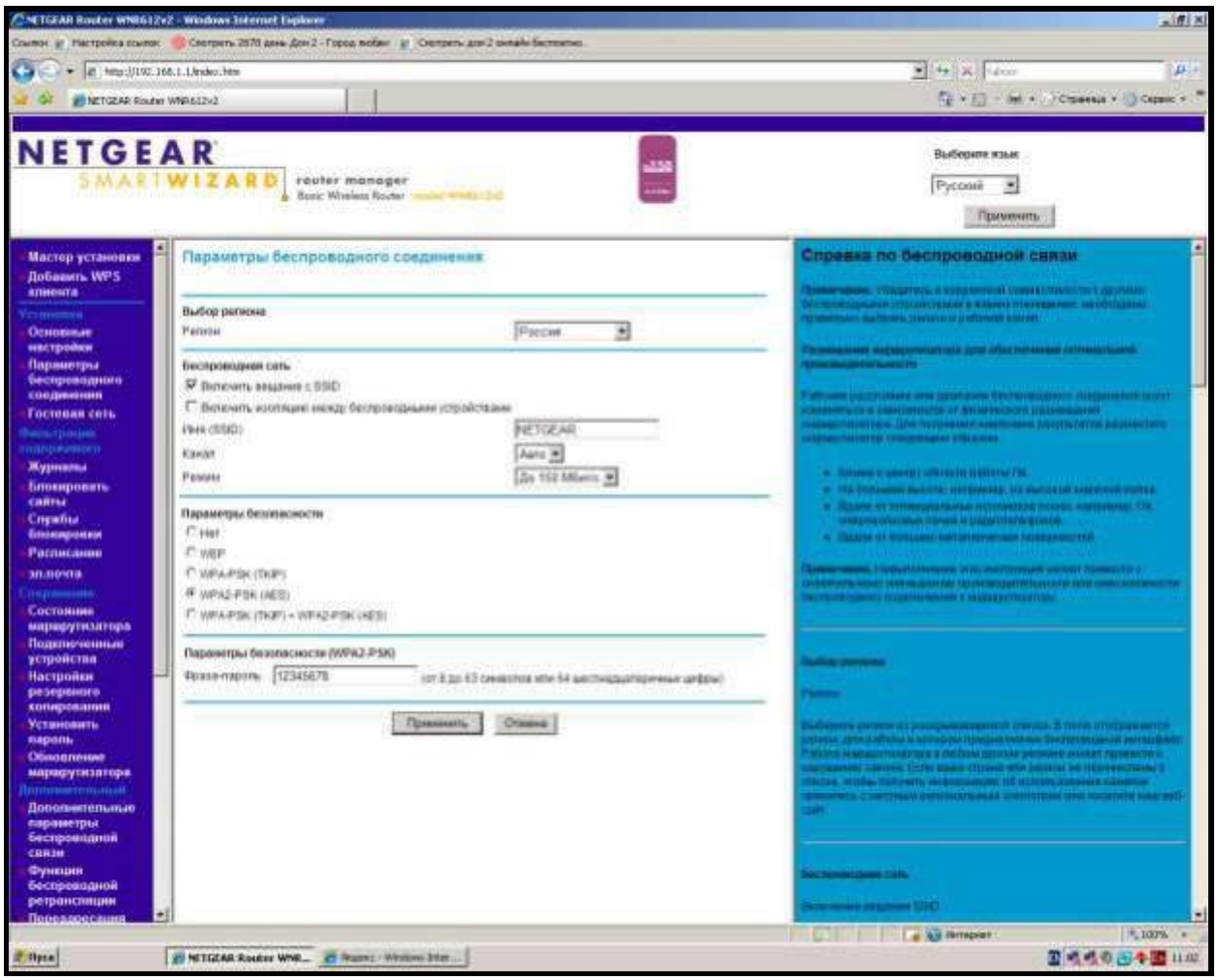


Рис. 19. Окно Параметры беспроводного соединения

Примечание

SSID – название беспроводной сети

Фраза – пароль здесь задана 12345678, но лучше ввести что-либо более сложное.

Для замены пароля наберите 192.168.1.1., введите admin и quthor, выберите команду **Параметры беспроводного соединения**и введите новый пароль, например, masha+vova=love

ШАГ 2 – Настройка Wi-Fi сети на ноутбуке для ОС Windows 7

Настроим работу Wi-Fi адаптера на ноутбуке, чтобы он смог получить Интернет от роутера NetGear. Выполните на ноутбуке команду **Панель управления-Сеть и Интернет-Подключение к сети** (рис. 20).

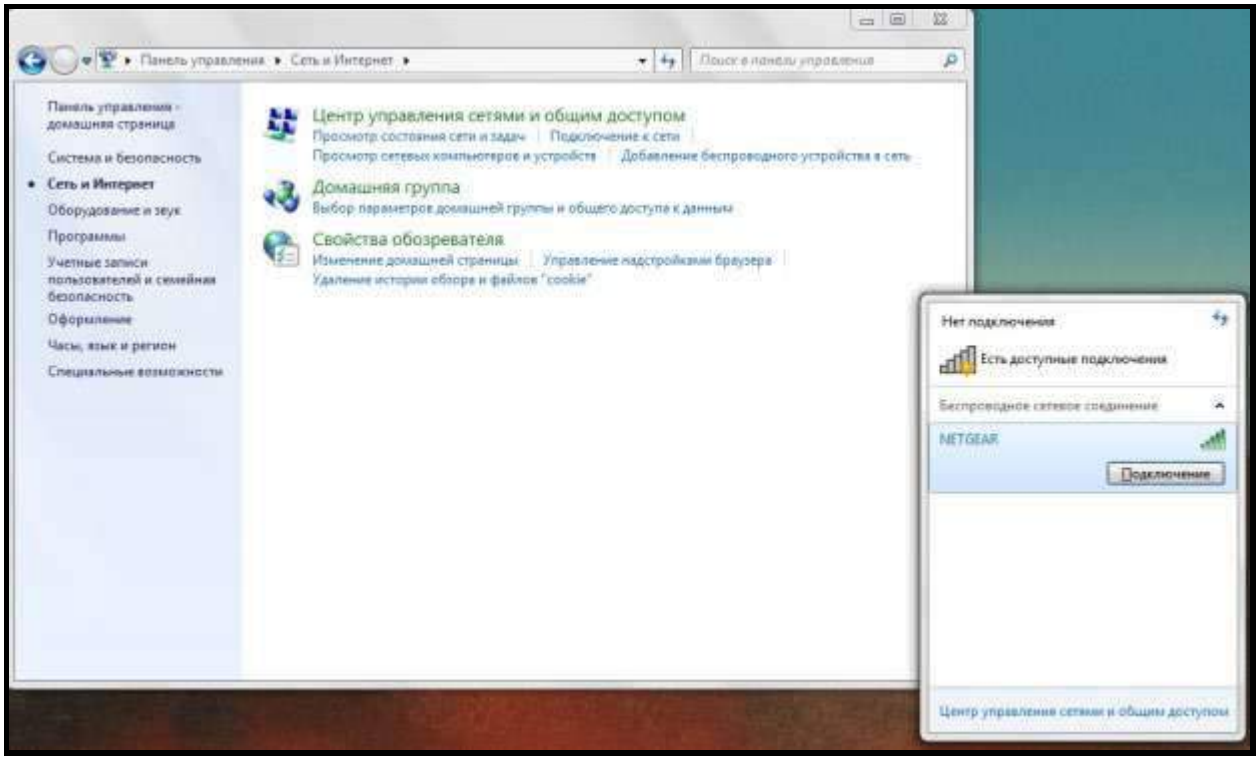


Рис. 20. Беспроводное сетевое соединение (роутер) ноутбук обнаружил

После нажатия на кнопку **Подключение** необходимо ввести фразу-пароль ключа безопасности (в нашем случае 12345678 или, если вы этот пароль изменили, то masha+vova=love) и Интернет на ноутбук будет подключен. Интернет запускается через любой браузер как при включенном стационарном ПК, так и без оного. Лишь бы роутер был включен.

Контрольные вопросы:

1. Какие типы Wi-fi вы знаете?
2. Назовите преимущества Wi-fi сетей.
3. Напишите недостатки Wi-fi сетей.
4. Опишите принцип работы Wi-fi.

ПРАКТИЧЕСКАЯ РАБОТА №6-7.
ИЗУЧЕНИЕ ТИПОВ СЕРВЕРОВ, ИХ НАСТРОЙКА И КОНФИГУРИРОВАНИЕ

Цель работы: Научиться создавать DNS сервер, производить его настройку и конфигурирование

Задания для практического занятия:
Выбор для сервера роли DNS сервера
DNS (Domain Name System — система доменных имён) — компьютерная система для получения IP-адреса по имени хоста и обратно.
Назначим нашему серверу роль DNS сервера (рис. 1).

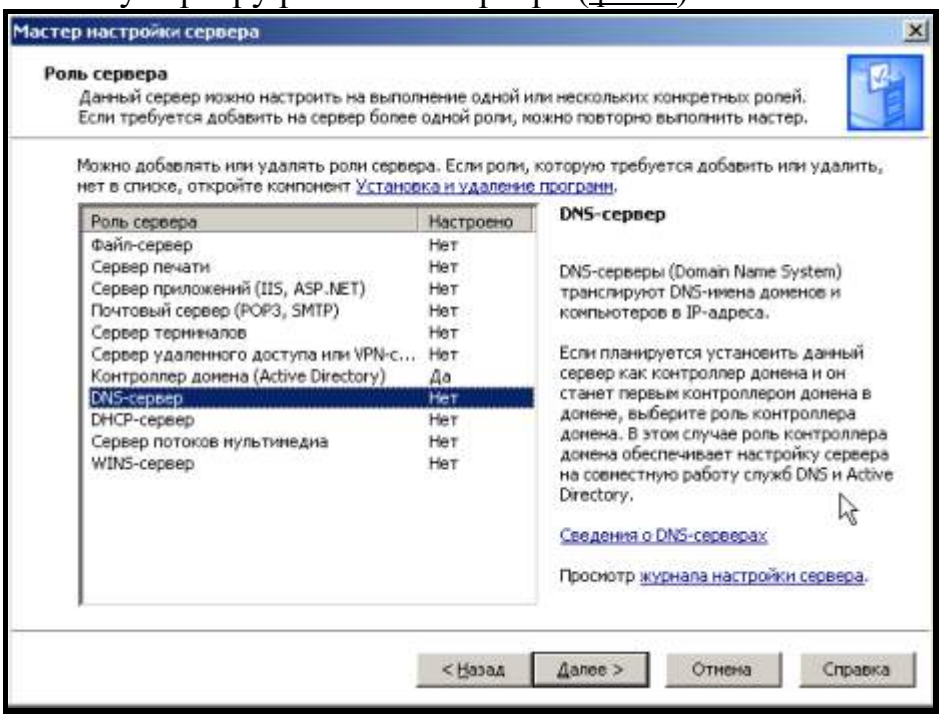


Рис. 1. Мастер настройки сервера-DNS сервер

Далее появиться предложение изменить динамический IP адрес на статический (рис. 2).

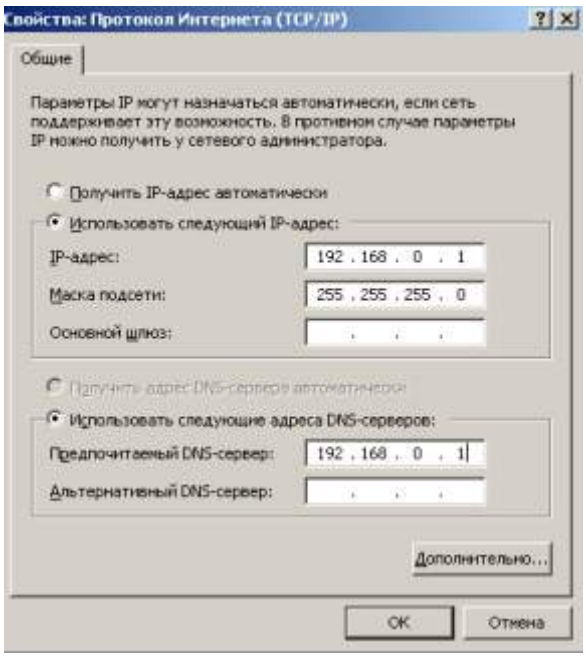


Рис. 2. Задаем серверу статический IP адрес

Далее появится Мастер настройки DNS сервера (рис. 3).

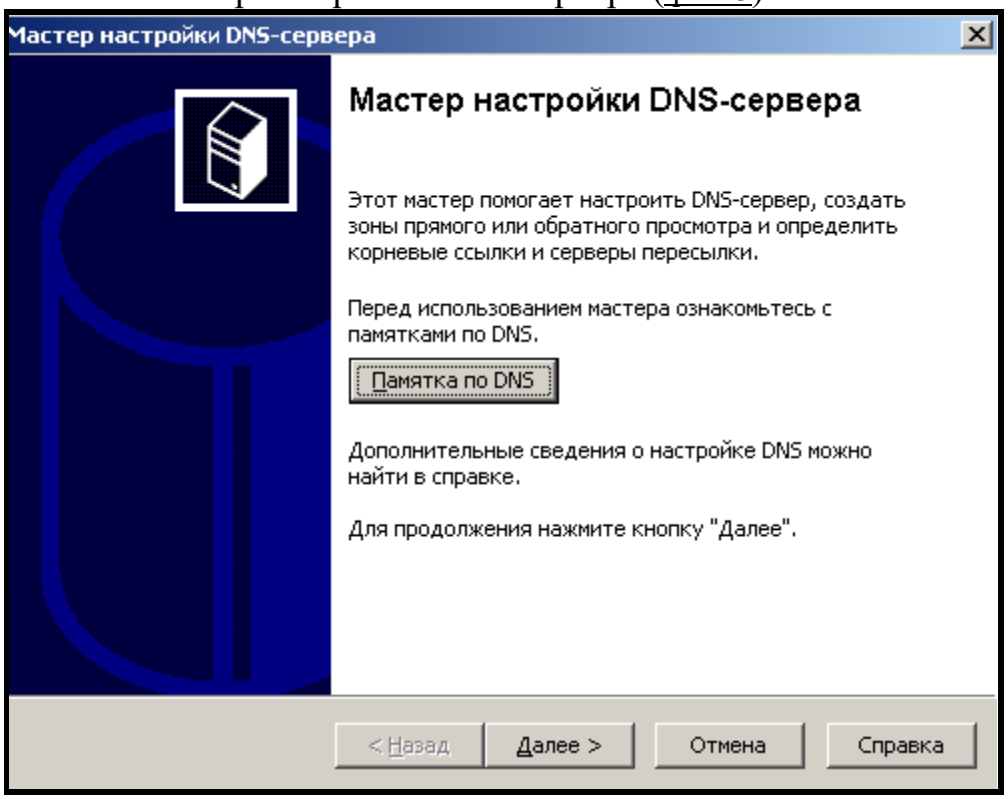


Рис. 3. Окно Мастер настройки DNS сервера

Поскольку сеть у нас небольшая, то установим верхний переключатель (рис. 4).

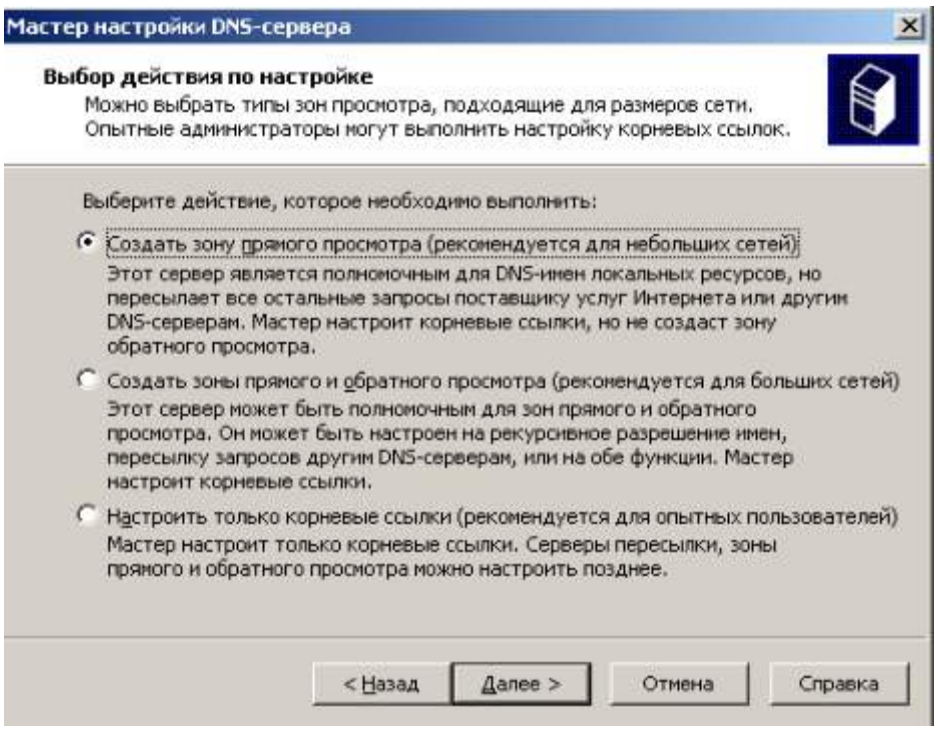


Рис. 4. Создание зоны прямого просмотра

Зону прямого просмотра назовем так же, как и домен – domain.110. Далее исходим из того, что у нас только один DNS сервер, больше пересылать запросы некому (рис. 49.5).

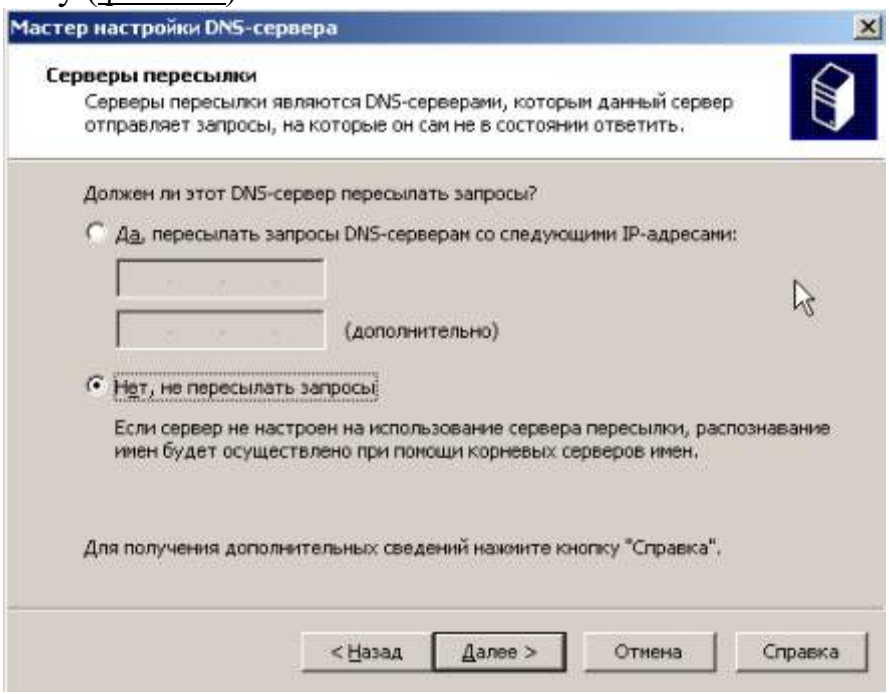


Рис. 5. Активируем нижний переключатель

Настройка сервера завершена (рис. 6).

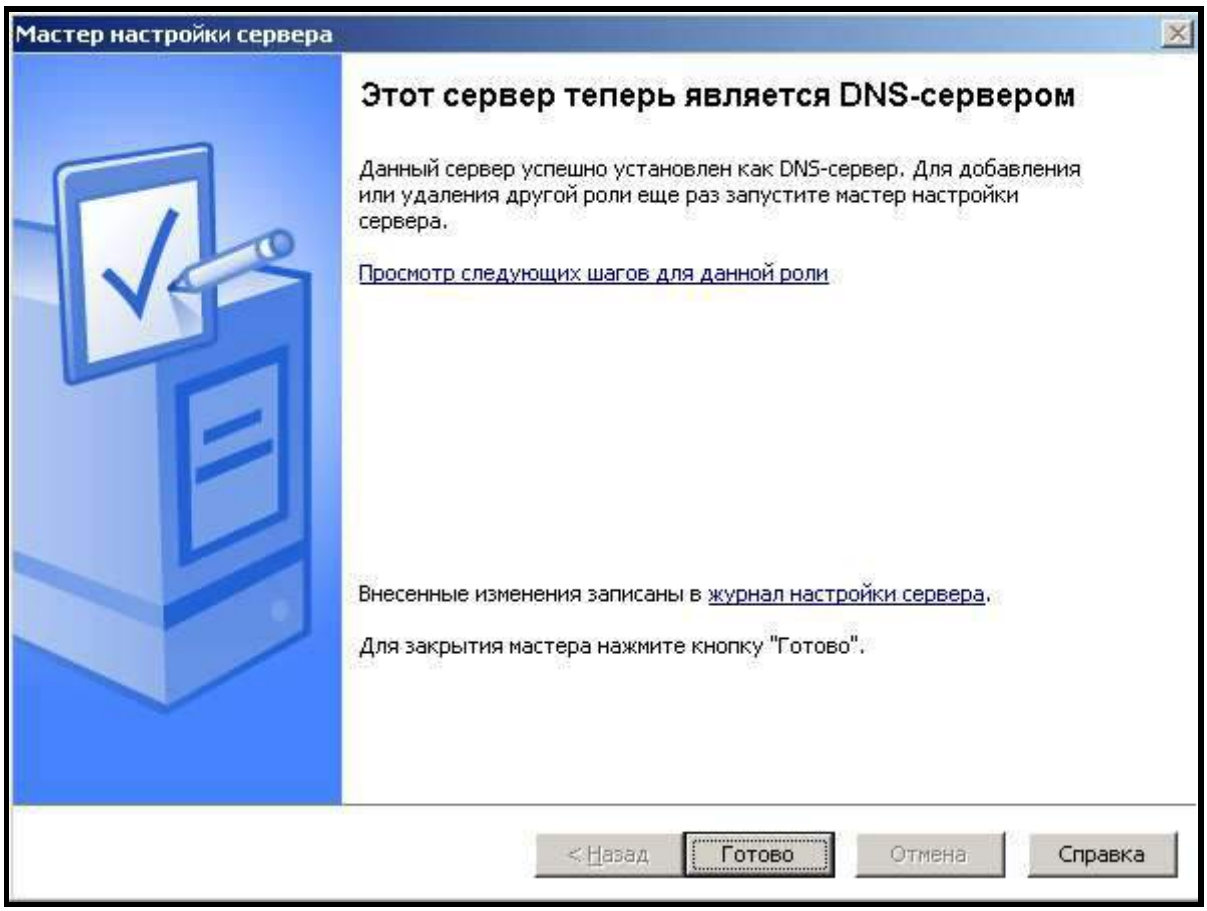


Рис. 6. Сервер получил роль DNS сервера

Выполнив команду, **Пуск-Все программы-Администрирование** мы увидим, что появилась новая оснастка (рис.7).

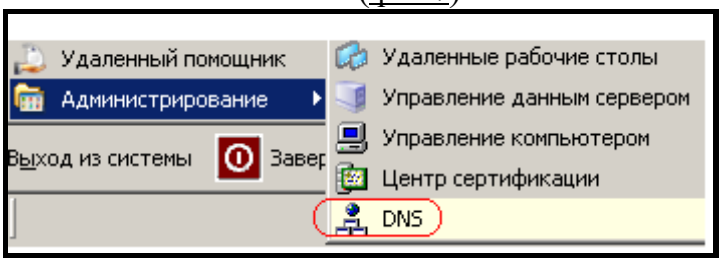


Рис. 7. На рисунке новая оснастка отмечена красным

Откроем ее (рис. 8). Здесь в зоне прямого просмотра вы можете увидеть соответствие имени сервера srv-2003 его IP адресу 192.168.0.1.

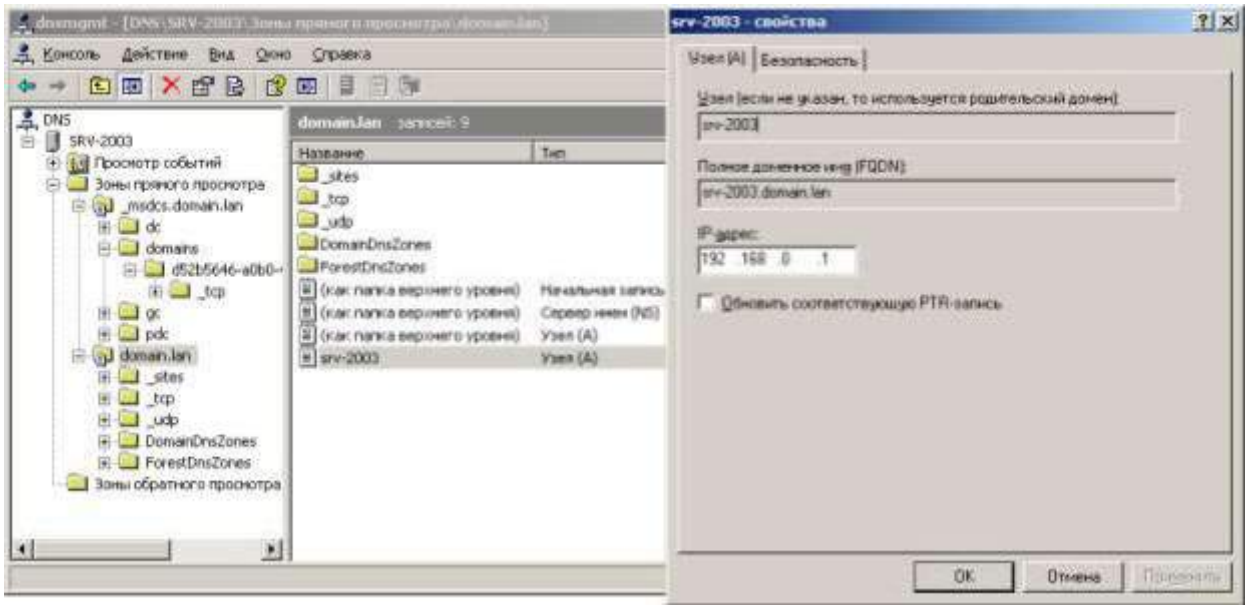


Рис. 8. На рисунке открыта зона прямого просмотра

Создание зоны обратного просмотра

Щелкните на строчку **Зона обратного просмотра** и выберите команду **Создать новую зону** (рис. 9).

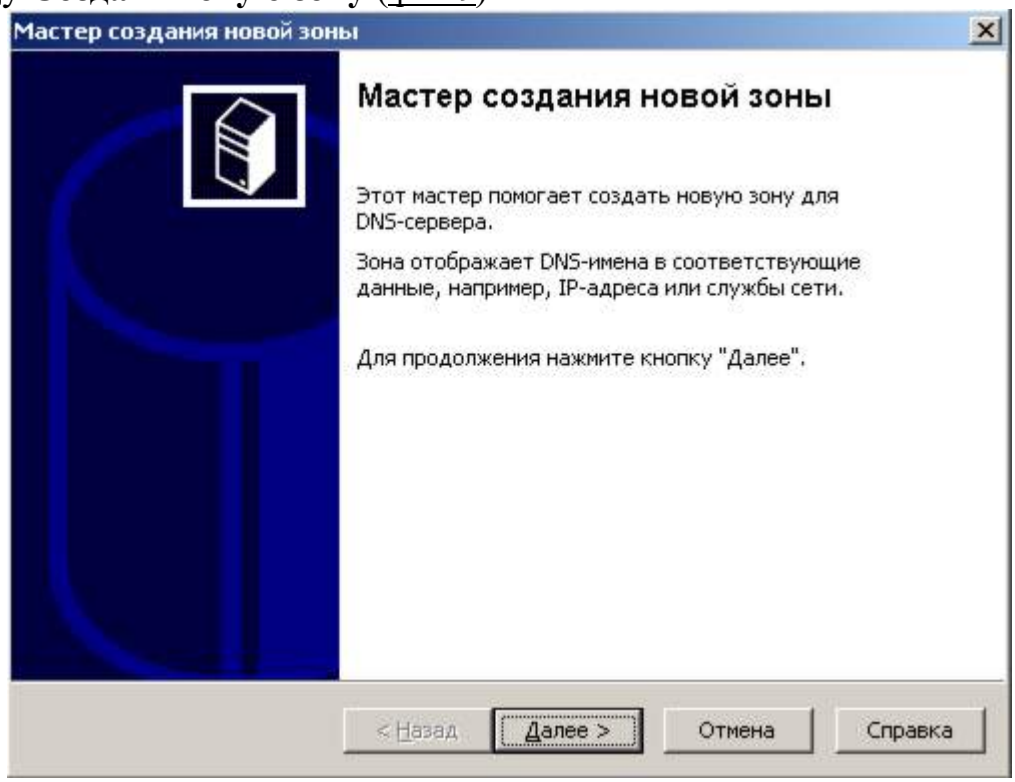


Рис. 9. Окно мастера создания новой зоны

Далее устанавливаем верхний переключатель - рис. 12.

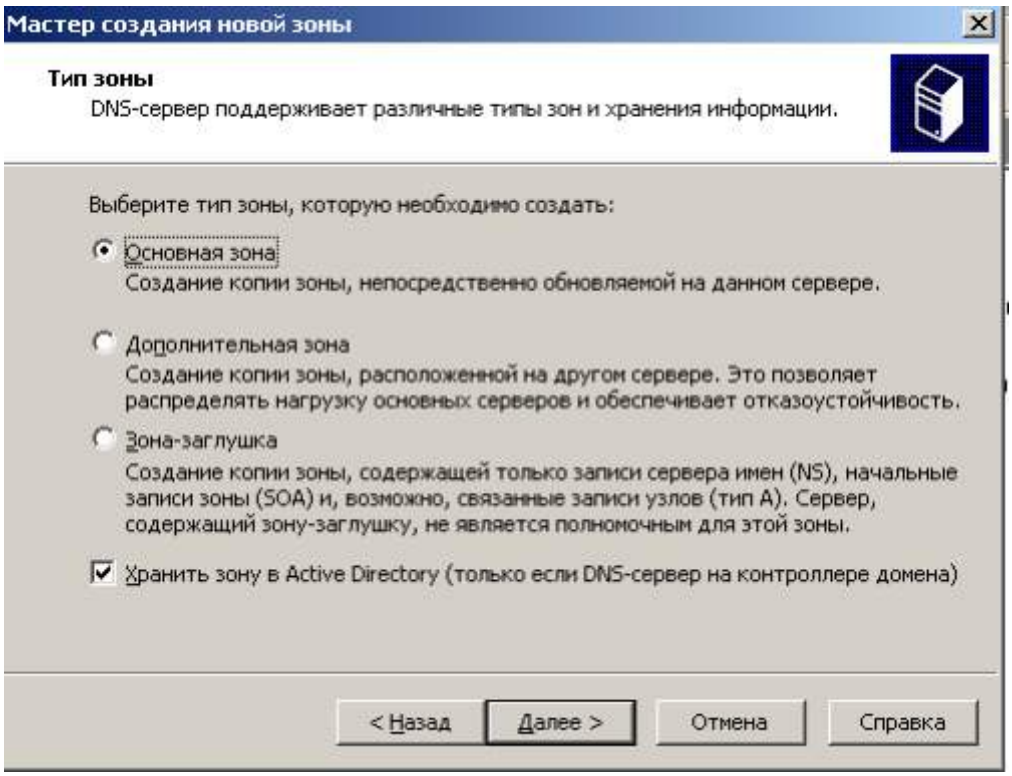


Рис. 10. Устанавливаем переключатель Основная зона

Примечание

Основная зона устанавливается на основной сервер (она - главная).

Дополнительная зона необходима для резервирования и разгрузки основного сервера. Если загрузка первого DNS сервера велика (или он отключился), то часть запросов можно отправить на второй, альтернативный DNS и отказоустойчивость системы повышается (рис. 11). Зона - заглушка содержит IP адрес сервера, который может обслужить запрос.

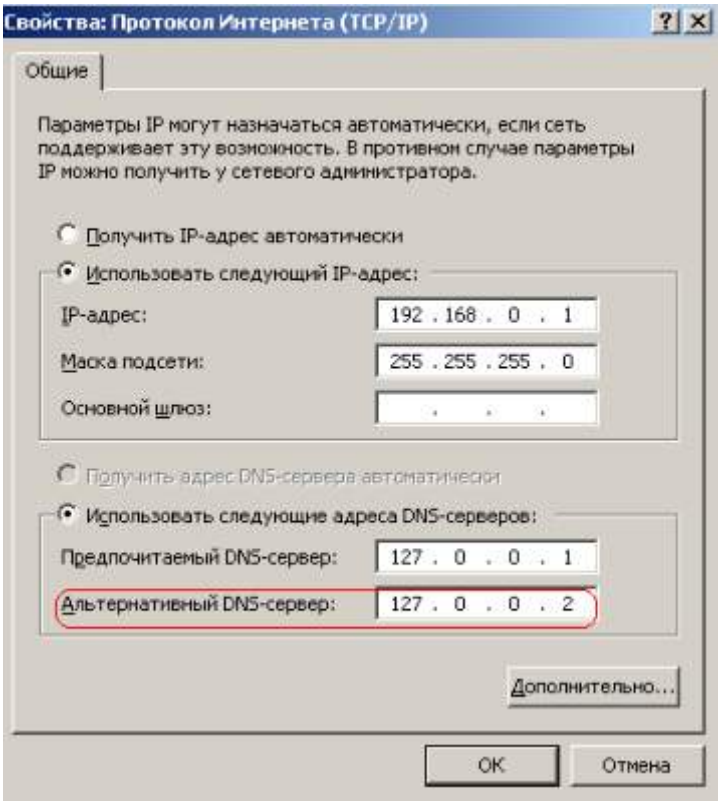


Рис. 11. Пример использования альтернативного DNS сервера

Наша сеть 192.168.0.1 относится к классу сетей С, поэтому значение 192.168.0 мы менять не можем - это и есть код сети (ID) –рис. 12.

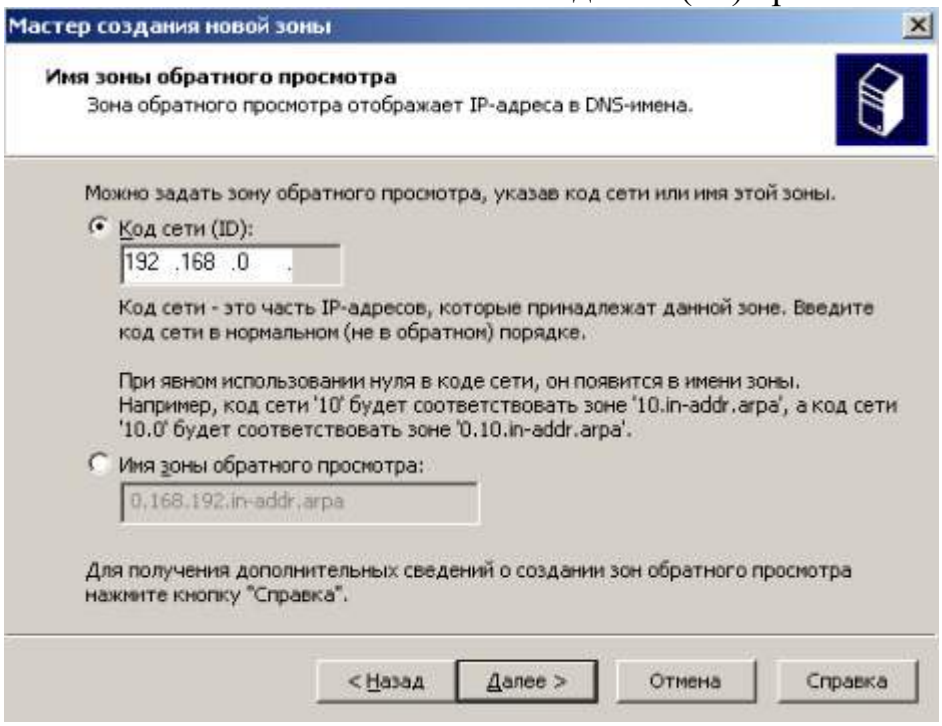


Рис. 12. Задаем код сети

Зона обратного просмотра создана. После подключения первого ПК здесь появится соответствие IP адреса ПК его имени.

Записи ресурсов DNS

Вся DNS состоит из этих RR записей, по которым пользователь может искать ресурсы в сети. Запустим консоль управления DNS и зайдем в зону прямого просмотра (рис. 13).

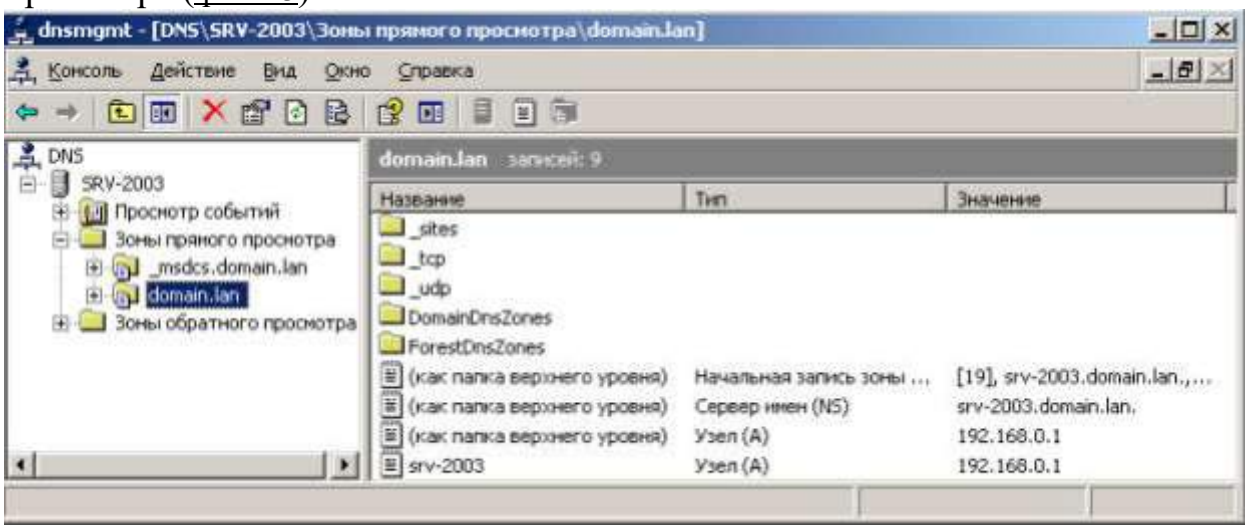


Рис. 13. Зоны прямого просмотра

Выполним двойной щелчок на строчке **Начальная запись зоны** (рис. 14). В данном окне наиболее интересный параметр**Срок жизни (TTL**). Предположим, что компьютер с именем ПК-1 и IP адресом 192.168.0.1 хочет соединиться с именем ПК-2 и IP адресом 192.168.0.2. Он выдает запрос на DNS сервер и тот сообщает, что с компьютер с именем ПК-2 имеет IP адрес 192.168.0.2. Эта запись кэшируется (помещается в память) на **Срок жизни (TTL).** Подобный подход к запросам снижает нагрузку на DNS сервер.

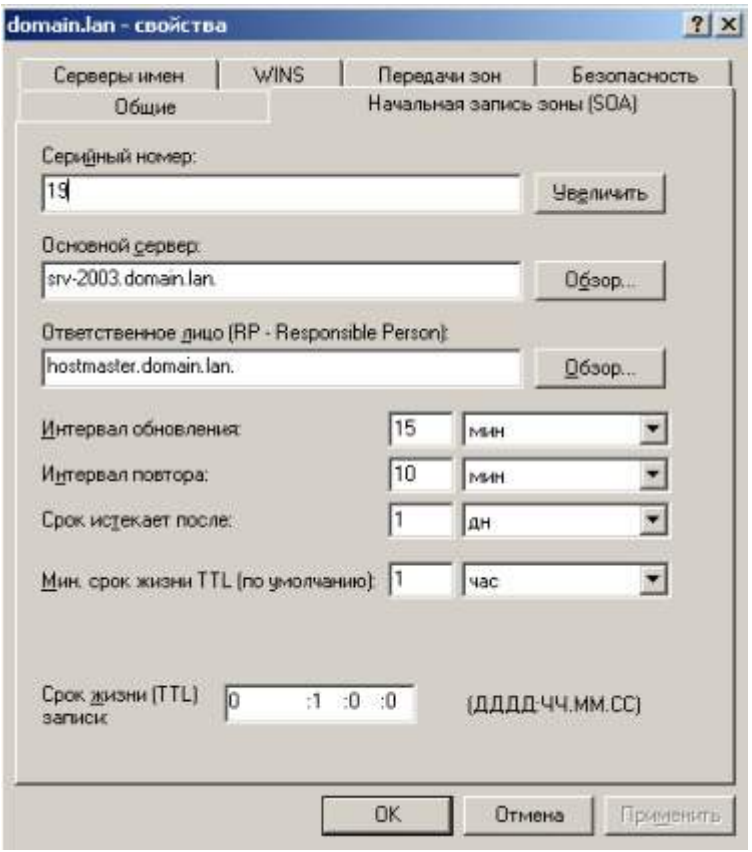


Рис. 14. Вкладка Начальная запись зоны

Теперь выполним двойной щелчок на строчке **Сервер имен** (рис. 15). У нас DNS сервер один, поэтому запись здесь одна. Но, здесь записей может быть столько, сколько имеется DNS серверов.

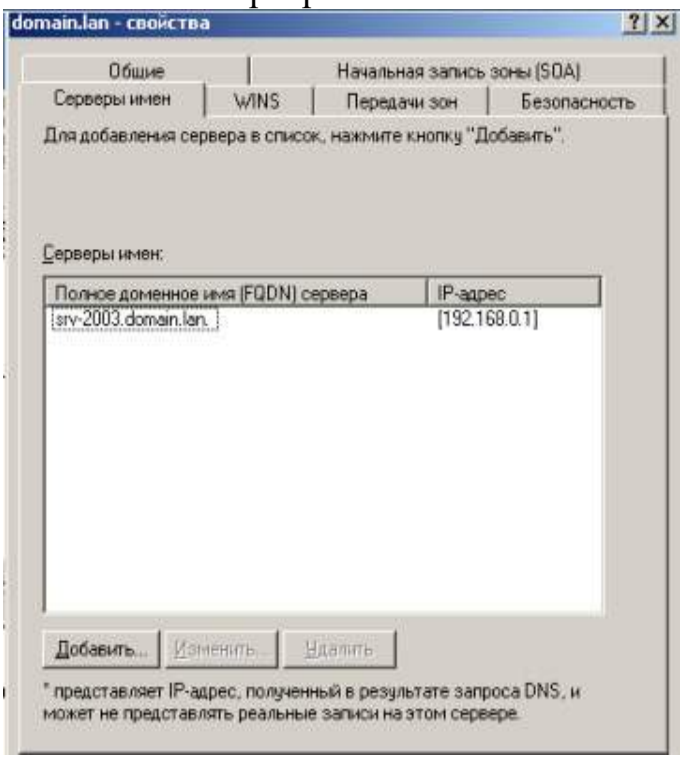


Рис. 15. Вкладка Серверы имен

Выполним двойной щелчок на строчке **Узел А** (рис. 16). Эта запись устанавливает прямое соответствие между именем ПК и его IP адресом.

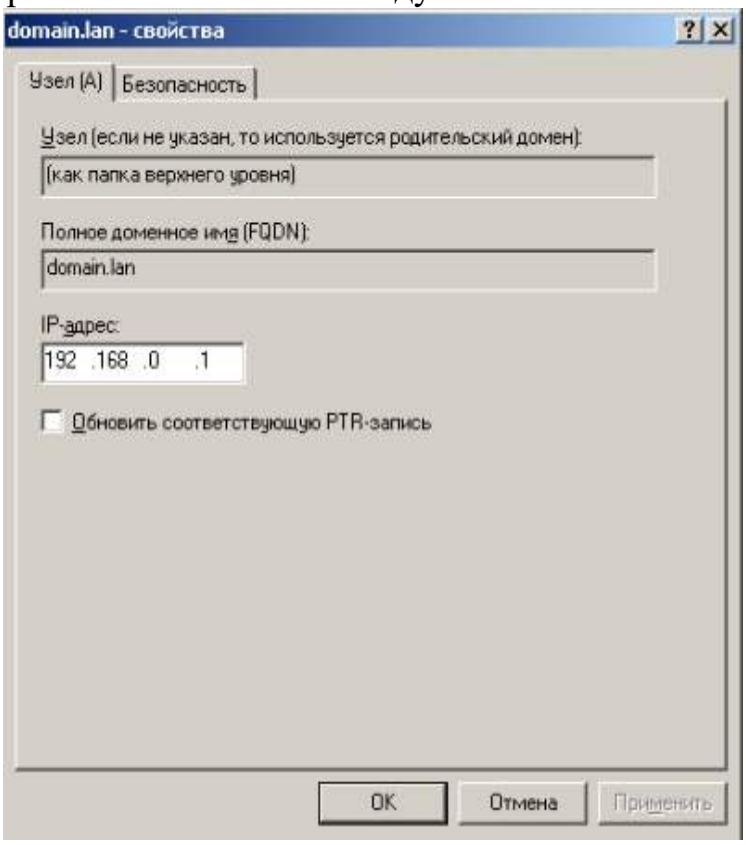


Рис. 16. Вкладка Узел А

Теперь изучим записи зоны обратного просмотра. После перезагрузки ПК здесь будет три записи (рис. 17).

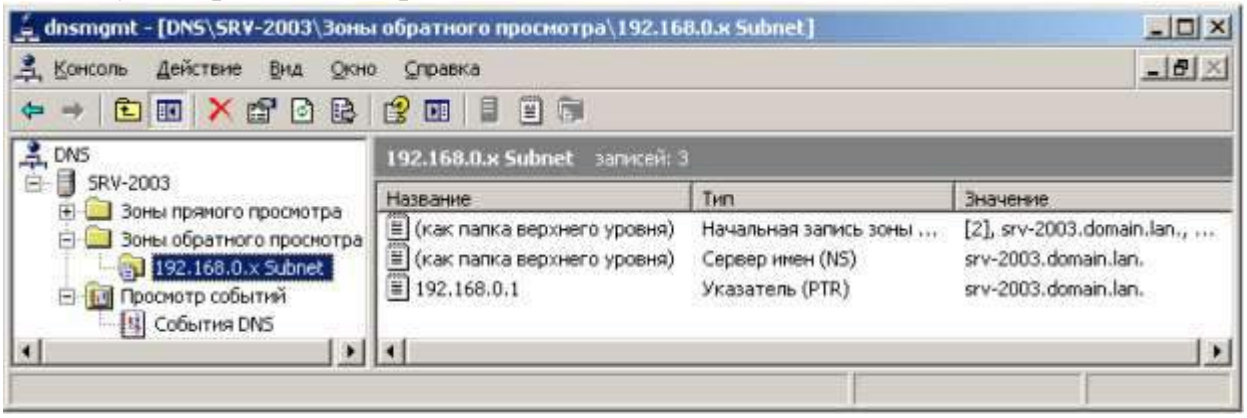


Рис. 17. Записи зоны обратного просмотра

Двойным щелчком мыши зайдем в **Указатель (PTR)** – рис. 18. Как видим, именно здесь задается обратное соответствие IP адреса и имени ПК.

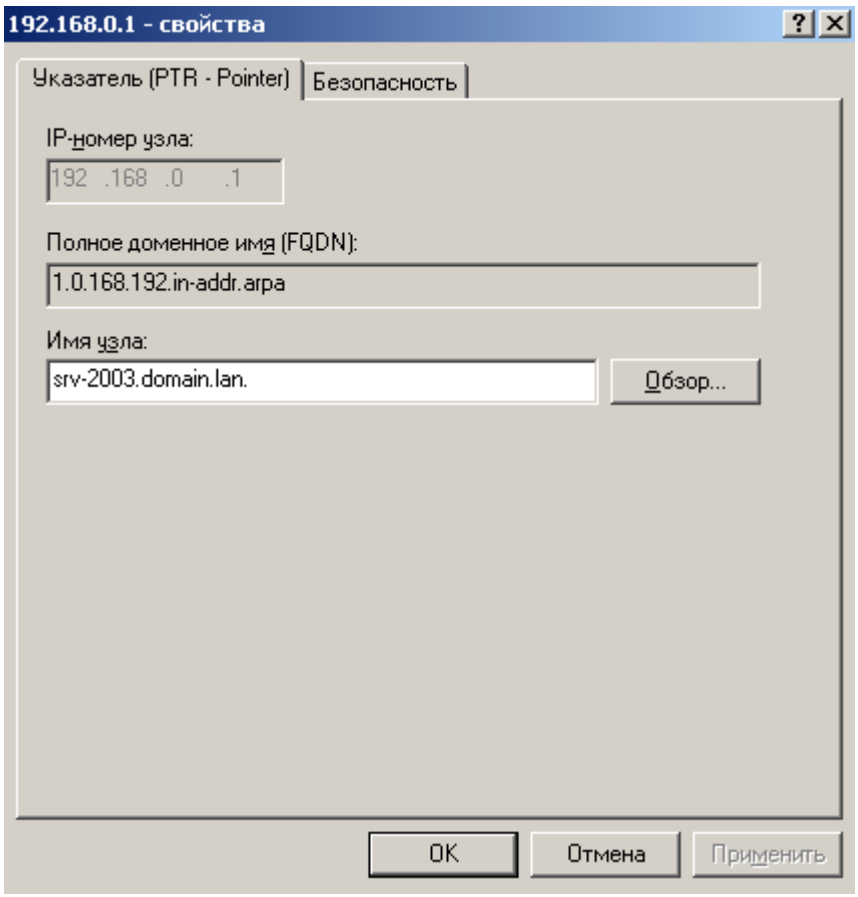


Рис. 18. Вкладка Указатель (PTR)

Проверка работы зон прямого и обратного просмотра

Далее вызовем командную строку и пропингуем наш сервер (рис. 19). Видим, что зона прямого просмотра работает нормально и имени SRV-2003 ставится в соответствие IP адрес 192.168.0.1.

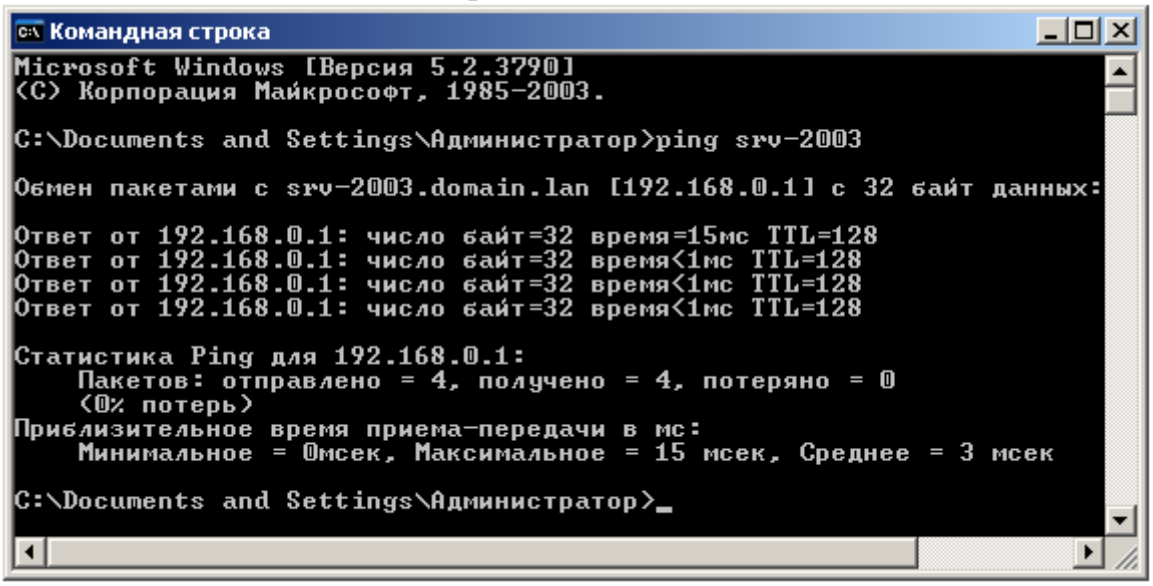


Рис. 19. Окно Командная строка

Если пропинговать не имя, а IP адрес и использовать ключ "-a", то увидим, что зона обратного просмотра также работает хорошо (рис. 20). Обмен данными идет нормально.

```
Командная строка
C:\Documents and Settings\Администратор>ping -a 192.168.0.1

Обмен пакетами с srv-2003.domain.lan [192.168.0.1] с 32 байт данных:

Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128
Ответ от 192.168.0.1: число байт=32 время<1мс TTL=128

Статистика Ping для 192.168.0.1:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

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

Рис. 20. Зона обратного просмотра работает хорошо

ПРАКТИЧЕСКАЯ РАБОТА №8.
РАБОТА С СЕРВЕРАМИ HTTP И FTP

Цель работы: научиться устанавливать и просматривать *Active Directory*, научится подключать компьютеры к домену.

Основные сведения

Сервер - в локальных вычислительных сетях - специализированная ЭВМ, управляющая использованием разделяемых между терминалами сети дорогостоящих ресурсов системы.

Сервер (англ. *server* от англ. *to serve* — служить) — в информационных технологиях — программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента, предоставляя ему доступ к определённым ресурсам.

Сервер сети (*Server*) - это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработка запроса к СУБД, удаленная обработка заданий и т.д. Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему это задание.

Обычно связь между клиентом и сервером поддерживается посредством передачи сообщений, и при этом используется определенный протокол для кодирования запросов клиента и ответов сервера. Виды серверов: FTP; Файловый; Web; Телефонный; Терминальный; Факс; Суперсервер и т.д.

Файл-серверы представляют собой серверы для обеспечения доступа к файлам на диске сервера. Прежде всего это серверы передачи файлов по заказу, по протоколам **FTP и HTTP**. Протокол **HTTP** ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например динамически

созданные веб-страницы, картинки, музыку и т. п. *Другие серверы* позволяют монтировать дисковые разделы сервера в дисковое пространство клиента и п
FTP-сервер - это понятие, за которым скрывается обычный компьютер. Но так как он содержит общедоступные файлы и настроен на поддержку протокола **FTP**, то его называют сервером - поставщиком информации. *FTP-клиент* - это сервисная программа, с помощью которой можно произвести соединение с **FTP** сервером. Обычно эта программа имеет командную строку, но некоторые имеют оконный интерфейс и не требуют запоминания команд. *WEB-сервер* необходим для обслуживания WEB-страниц вашего сайта

Доступ к WEB-серверу имеет пять уровней:

- Общедоступный с возможностью только чтения всех **URL** за исключением тех, что помещены в каталогах ***/private***.
- Доступ сотрудников организации, которой принадлежит сервер. Здесь также допустимо только чтение, но доступны и секции каталога ***/private***.
- Разработчики **WEB-сервера**. Имеют возможность модифицировать содержимое сервера, инсталлировать CGI-скрипты, прерывать работу сервера.
- Администраторы узла (сервера). Имеют те же привилегии, что и разработчики, но могут также реконфигурировать сервер и определять категорию доступа.
- Системные администраторы. Имеют идентичные привилегии с администраторами сервера.

Оснастка Internet Information Service (IIS) обеспечивает средства управления сервером для контроля над доступом и содержимым веб-узлов и узлов **FTP**. Например, разработчикам это средство позволит выполнить доскональную проверку работы узла перед окончательной загрузкой на сервер интрасети организации или Интернета. Оснастка **IIS** имеет следующие особенности:

Дополнительные параметры настройки сервера, в частности, для управления узлом **FTP**, независимого выполнения приложений, настройки типов **MIME** и назначения дополнительных средств обработки сценариев.

Мастер создания виртуальных каталогов.

Возможность управления установками **Internet Information Services** в сети.

На сегодняшний день существует огромное множество программного обеспечения для работы с протоколом **FTP** под все операционные системы. Все это множество программного обеспечения можно разделить на две части: *серверное ПО* и *клиентское ПО*.

Серверное ПО служит для создания и управления ftp-сервером.

Клиентское ПО используется для просмотра ресурсов на ftp-сервере. Этот класс программ призван обеспечить комфортную работу с удаленными ресурсами.

Сюда относятся такие программы как:

- ftp.exe – стандартное приложение Windows;
- FileZilla – мощный ftp-клиент с открытым исходным кодом (т.е. при желание вы можете что-нибудь новое добавить в эту программу самостоятельно);
- RigthFTP, CuteFTP – графические ftp-клиенты;
- Total commander (или любой другой с интерфейсом Norton Commander)– имеет встроенный ftp клиент;
- Explorer.exe – стандартное приложение Windows;
- Любой браузер.

Задания для практического занятия:

Задание 1. Подготовьте файловый сервер.

1. Подключите к виртуальной машине **VM-2** образ установочного диска ***win2003-2.iso***.
2. Запустите виртуальную машину **VM-2**.
3. Добавьте новую **роль** серверу – *Файл-сервер*:
    a. откройте диалоговое окно **Управление данным сервером (*Пуск/дминистрирование/Управление Данным Сервером*)**;
    b. активизируйте добавление ролей кнопкой ***Добавить или удалить роль***;
    c. выберите **Файловый сервер** и щелкните ***Далее***;
    d. установите параметры файлового сервера:
        i. Предоставить доступ UNIX-системам к файлам;
        ii. Предоставить доступ Apple--системам к файлам;
        iii. подтвердите введенные параметры кнопкой ***Далее***;
    e. запустите установку роли сервера кнопкой ***Далее***.
4. Перезагрузите виртуальный компьютер кнопкой Перезегрузить.
5. Откройте диалоговое окно Настройки файлового сервера (Пуск/дминистрирование/Управление Данным Сервером/Управление этим файловым сервером).
6. Установите стандартные квоты использования места на диске:
    f. установите флажок *Установить дисковые квоты по умолчанию для новых пользователей данного сервера*;
    g. укажите **размер квот** - *50Мб*;
    h. установите **предупреждение о квоте** - *40Мб*;
    i. установите флажок *Не выделять место на диске при превышении дискового пространства*;
    j. завершите ввод стандартных квот кнопкой ***Далее***.
7. Откажитесь от включения службы индексирования.
8. Укажите папку на сервере, для хранения файлов, например ***C:\Documents and settings\Администратор\Рабочий стол\PUB***.

Далее мастер установки завершит свою работу. Попробуйте теперь зайти на созданную вами сетевую папку с другого компьютера сети. Обратите

внимание на способ подключения. Попробуйте заполнить папку для превышения квоты.

Задание 2. Настройте Web-сервер.

- Установите **Internet Information Service (IIS)** (***Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS***):
- Подготовьте тестовую страницу:
  - создайте временную страницу, вызываемую по умолчанию: наберите в **Блокноте** и сохраните в файле с именем ***Default.html*** в каталоге ***\Inetpub\wwwroot***.
  -

```
<HTML>
    <HEAD>
        <TITLE>Тестовая страница<TITLE>
    </HEAD>
<BODY>
    <H1 align="center"> Тестовая страница </H1>
    <P align="center">
        <FONT color="green">
            На этом месте будет размещена страница нашей организации. В настоящий момент сайт находиться в стадии разработки
            </FONT>
    </P>
</BODY>
</HTML>
```

  -
- Настройте Web-сервер:
- откройте консоль управления сервером IIS (***Пуск/администрирование/Управление Данным Сервером/Управление этим сервером приложений***);
- перейдите к web-узлу, заданному по умолчанию (Диспетчер служб IIS/Веб-узлы/Веб-узел по умолчанию);

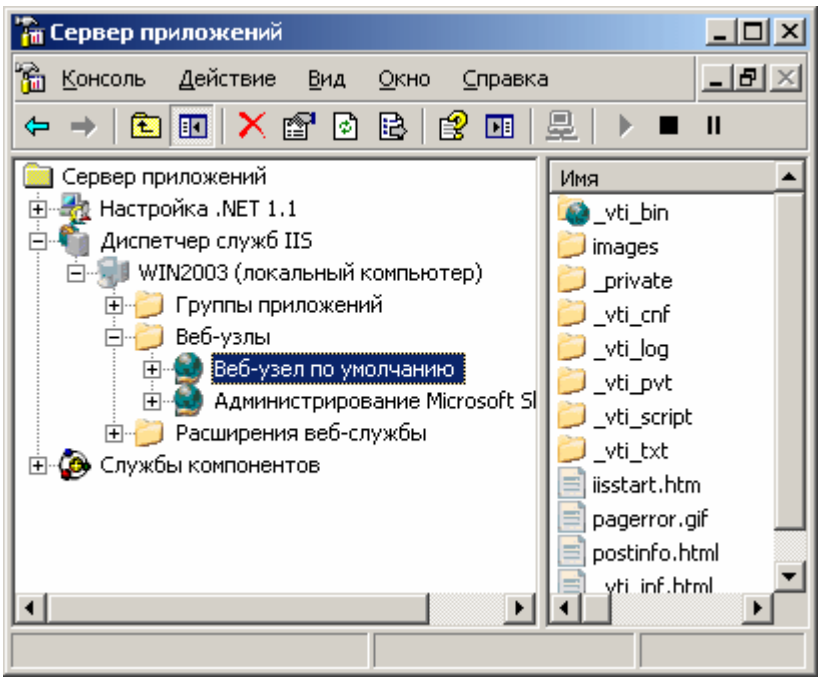


Рисунок 1. Консоль управления сервером приложений (IIS).

- откройте диалоговое окно Свойства узла по умолчанию (контекстное меню/Свойства);
- добавьте страницу по умолчанию:
- перейдите на вкладку Документы;
- установите флажок Задать страницу содержания по умолчанию;
- откройте окно добавления кнопкой Добавить;
- введите в поле Default.html;
- подтвердите добавление кнопкой ОК.
- закройте окно свойств кнопкой ОК.
- Проверьте настройку Web-сервера:
- на вашем компьютере откройте Internet Explorer (Пуск/Программы/Internet Explorer);
- наберите в адресной строке http://127.0.01/;
- сделайте скриншот происходящего на экране и сохраните его в своей папке.

Задание 3. Установите и настройте сервер FTP

- Установите сервер FTP - FileZilla.
- Запустите FileZilla Server Interface.

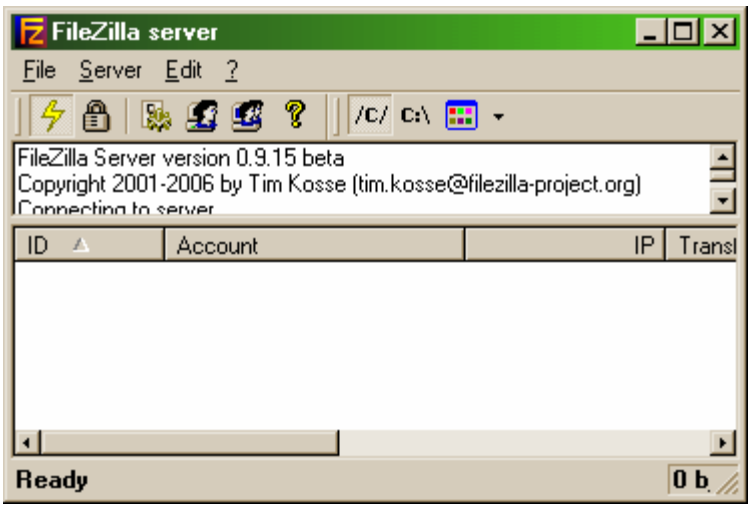


Рисунок 2. Интерфейс управления FTP-сервером ***FileZilla***

- Ограничьте количество одновременных подключений к серверу:
- откройте окно настройки сервера (Edit/Settings);

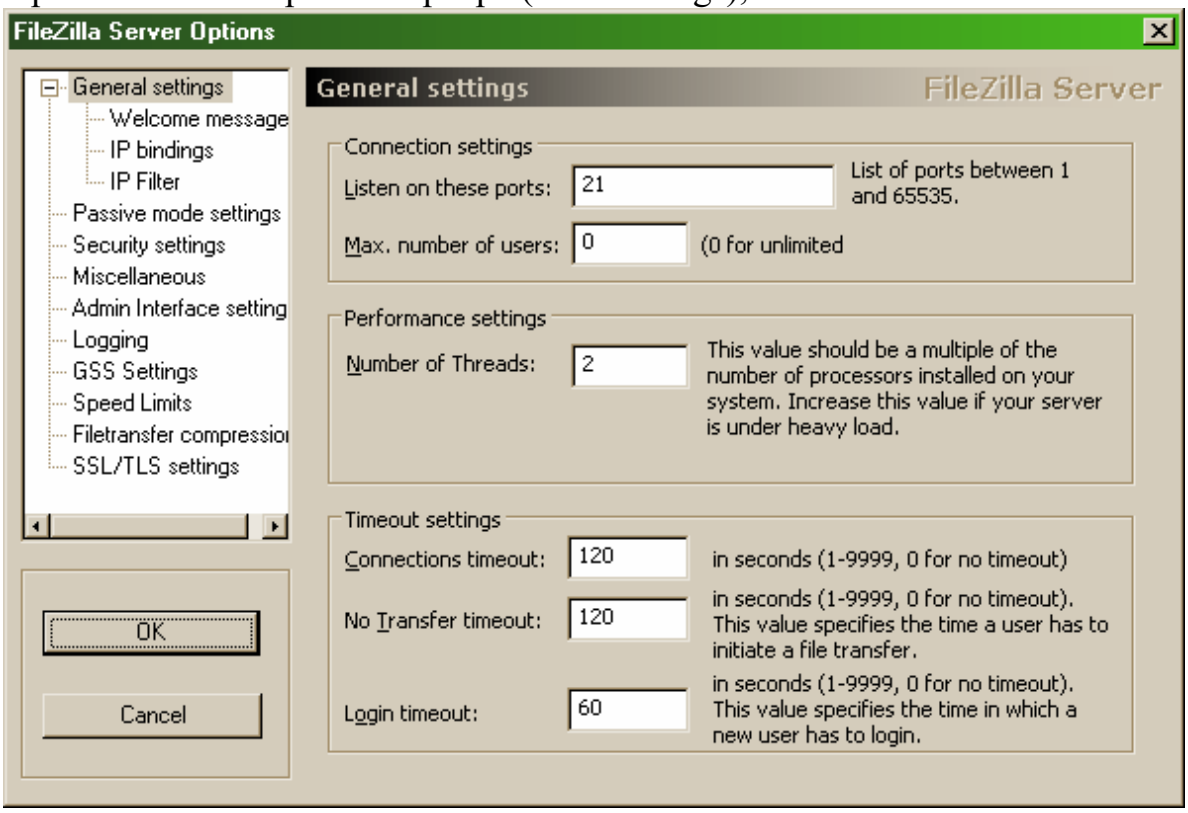


Рисунок 3. Настройки FTP-сервера

- перейдите в раздел General Settings (общие настройки);
- введите в поле Max.number of users – 2;
- Установите текст приветствия:
- перейдите в раздел Welcome message;
- введите в поле Custom welcome message – Добро пожаловать на мой сервер;
- Установите ограничения по скорости:

- перейдите в раздел Speed Limits (ограничения скорости);
- включите использование правил ограничения скорости радиокнопкой Use Speed Limit rules;
- добавьте ограничение по скорости не более 3 Кб/с в понедельник:
- откройте окно задания параметров ограничений кнопкой Add (Добавить);
- сбросьте все флажки кроме Monday (Понедельник);
- введите в поле Speed – 3;
- подтвердите ввод данных кнопкой ОК;
- примените параметры кнопкой ОК.
- Создайте группы пользователей FTP-сервера:
- откройте диалоговое окно добавления групп кнопкой на панели инструментов;
- активируйте добавление групп кнопкой Add (Добавить);
- введите имя группы, например Students (ОК);
- задайте общую папку для созданной группы:
- перейдите в раздел Shared Folders (Общие папки);
- активируйте добавление папок кнопкой Add (Добавить);
- укажите общую папку, например C:\Documents and settings\Администратор\Рабочий стол и подтвердите выбор кнопкой ОК;
- разрешите чтение и удаление содержимого общей папки – установите флажок Write и Delete;
- завершите добавление групп пользователей кнопкой ОК.
- Добавьте нового пользователя:
- откройте диалоговое окно добавления пользователей кнопкой на панели инструментов;
- активируйте добавление пользователей кнопкой Add (Добавить);
- введите имя группы, например justuser;
- выберите в списке User should be member of the following group созданную ранее группу и подтвердите создание пользователя кнопкой ОК;
- установите пароль для созданного пользователя:
- перейдите на вкладку General (Общие);
- введите в поле Password новый пароль, например 123;
- завершите добавление групп пользователей кнопкой ОК.
- Проверьте работу сервер:
- запустите командную строку (Пуск/Программы/Стандартные/Командная строка);
- введите команду для подключения к FTP-серверу на текущем компьютере: FTP 127.0.0.1
- введите имя пользователя - justuser (ENTER);

- введите пароль - 123 (ENTER);
- просмотрите содержимое домашней папки: DIR
- отключитесь от сервера: QUIT
- закройте командную строку.
- Закройте интерфейс управления FTP-сервером.

Задание 4. Выполните самостоятельные задания 5-6**.П**олноценно работать с файлами на них. Это позволяют серверы протоколов **NFS и SMB**. Серверы **NFS и SMB** работают через интерфейс **RPC**.

Недостатки файл-серверной системы:

1. Очень большая нагрузка на сеть, повышенные требования к пропускной способности. На практике это делает практически невозможной одновременную работу большого числа пользователей с большими объемами данных.
2. Обработка данных осуществляется на компьютере пользователей. Это влечет повышенные требования к аппаратному обеспечению каждого пользователя. Чем больше пользователей, тем больше денег придется потратить на оснащение их компьютеров.
3. Блокировка данных при редактировании одним пользователем делает невозможной работу с этими данными других пользователей.
4. Безопасность. Для обеспечения возможности работы с такой системой Вам будет необходимо дать каждому пользователю полный доступ к целому файлу, в котором его может интересовать только одно поле

Файловый сервер выполняет следующие функции:

5. хранение данных,
6. архивирование данных,
7. согласование изменений данных, выполняемых разными пользователями, передача данных.

ПРАКТИЧЕСКАЯ РАБОТА №9.
ИЗУЧЕНИЕ СТЕКА ПРОТОКОЛОВ TCP/IP

Цель работы: Изучить основные сетевые протоколы и принцип их работы.

Основные сведения
Сетевые протоколы
Сетевой протокол — набор правил, позволяющий осуществлять обмен данными между составляющими сеть устройствами, например, между двумя сетевыми картами (рис. 1).

Рис. 1. Иллюстрация к понятию Сетевой протокол

TCP/IP

Стек протоколов TCP/IP — это два протокола, являющиеся основой связи в сети Интернет. Протокол TCP разбивает передаваемую информацию на порции (пакеты) и нумерует их. С помощью протокола IP все пакеты передаются получателю. Далее с помощью протокола TCP проверяется, все ли пакеты получены. При получении всех порций TCP располагает их в нужном порядке и собирает в единое целое. В сети Интернет используются две версии этого протокола:
Маршрутизируемый сетевой протокол IPv4. В протоколе этой версии каждому узлу сети ставится в соответствие IP-адрес длиной 32 бита (т.е. 4 октета по 4 байта).
IPv6 позволяет адресовать значительно большее количество узлов, чем IPv4. Протокол Интернета версии 6 использует 128-разрядные адреса, и может определить значительно больше адресов.
Примечание
IP-адреса стандарта IPv6 имеют длину 128 бит и поэтому в четыре раза длиннее, чем IP-адреса четвертой версии. IP-адреса версии v6 записываются

в следующем виде:X:X:X:X:X:X:X:X, где X является шестнадцатеричным числом, состоящим из 4-х чисел (16 бит), а каждое число имеет размер 4 бит. Каждое число располагаться в диапазоне от 0 до F. Вот пример IP-адреса шестой версии: 1080:0:0:0:7:800:300C:427A. В подобной записи незначащие нули можно опускать, поэтому фрагмент адреса: 0800: записывается, как 800:.

ARP

Для взаимодействия сетевых устройств друг с другом необходимо, чтобы у передающего устройства был IP- и MAC-адреса получателя. Набор протоколов TCP/IP имеет в своем составе специальный протокол, называемый ARP (Address Resolution Protocol — протокол преобразования адресов), который позволяет автоматически получить MAC-адрес по известным IP-адресам

DHCP-протокол

Распределением IP-адресов для подключения к сети Интернет занимаются провайдеры, а в локальных сетях – сисадмины. Назначение IP-адресов узлам сети при большом размере сети представляет для администратора очень утомительную процедуру. Поэтому для автоматизации процесса разработан протокол Dynamic Host Configuration Protocol (DHCP) , который освобождает администратора от этих проблем, автоматизируя процесс назначения IP-адресов всем узлам сети.

HTTP протокол

HTTP протокол служит для передачи гипертекста, т.е. для пересылки Web-страниц с одного компьютера на другой. Основой HTTP является технология "клиент-сервер", то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), которые ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом.

FTP протокол

FTP протокол передачи файлов со специального файлового сервера на компьютер пользователя. Установив связь с удаленным компьютером, пользователь может скопировать файл с удаленного компьютера на свой или скопировать файл со своего компьютера на удаленный.

POP протокол

POP стандартный протокол получения почтового соединения. Серверы POP обрабатывают входящую почту, а протокол POP предназначен для обработки запросов на получение почты от клиентских почтовых программ.

SMTP протокол

SMTP протокол, который задает набор правил для отправки почты. Сервер SMTP возвращает либо подтверждение о приеме, либо сообщение об ошибке, либо запрашивает дополнительную информацию.

IP адрес по протоколу IPv4

Одной из самых важных тем при рассмотрении TCP/IP является адресация IP. Адрес IP — числовой идентификатор, приписанный каждому компьютеру в сети IP и обозначающий местонахождение в сети устройства, которому он приписан. Адрес IP - это адрес программного, а не аппаратного обеспечения. IP-адрес узла идентифицирует точку доступа модуля IP к сетевому интерфейсу, а не всю машину.

IP-адрес — сетевой (программный) адрес узла в компьютерной сети, построенной по протоколу IP.

Каждый из 4х октет десятичной записи IP адреса может принимать значение в диапазоне от 0 до 255 и в теории такой адрес в десятичной форме записи может быть в диапазоне от 0.0.0.0 до 255.255.255.255. IP адрес - двоичное число, но для человека вместо записи в 32 бит 11000000.10101000.00000000.00000001 удобнее запись в 4 байта вида 192.168.0.1.

Задание 1. Определить IP адрес вашего ПК

Узнать свой собственный IP адрес вы можете, если запустите в ОС Windows XP на выполнение команду **Пуск – Программы – Стандартные – Командная Строка** и наберете в ней **ipconfig** (рис. 6.2).

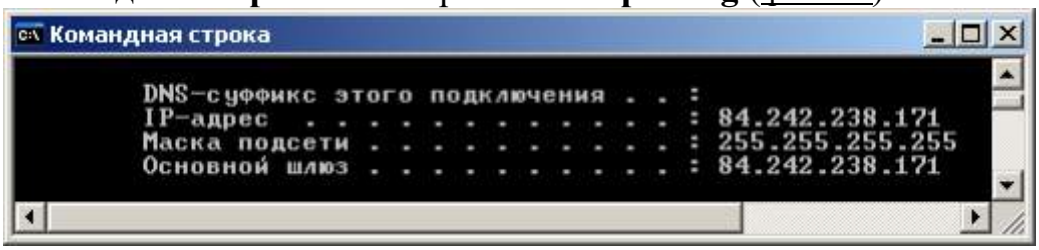


Рис. 2. IP адрес вашего ПК в десятичной системе счисления

Ту же команду можно выполнить в командной строке Windows 7 (рис.3).

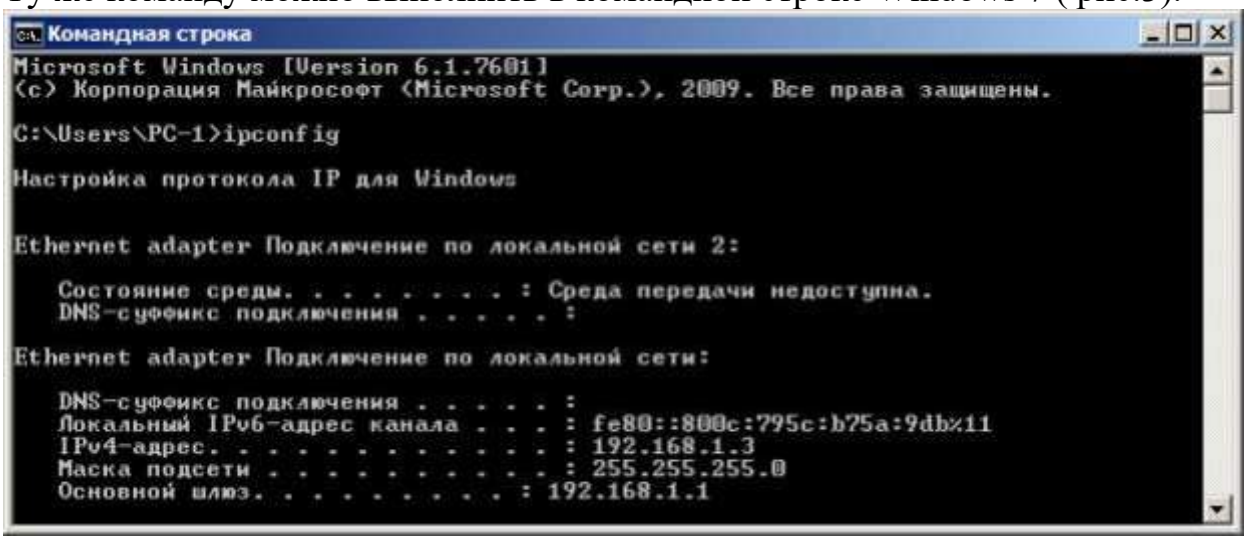


Рис. 6.3. Здесь мы видим IP в двух версиях: IPv4 и IPv6

Задание 2. Перевод чисел из двоичной системы в десятичную и наоборот

При работе с IP-адресами может возникнуть необходимость перевода двоичных чисел в десятичные и наоборот. Это можно сделать, например, так, как учат в школе:

$10110110_2 = (1\cdot2^7)+(0\cdot2^6)+(1\cdot2^5)+(1\cdot2^4)+(0\cdot2^3)+(1\cdot2^2)+(1\cdot2^1)+(0\cdot2^0) = 128+32+16+4+2 = 182_{10}$ Но, удобнее это делать на Windows-калькуляторе. Выполните в Windows-7 команду **Пуск-Программы-Стандартные-Калькулятор**, потом **Вид-Программист** (рис. 4 и 5).

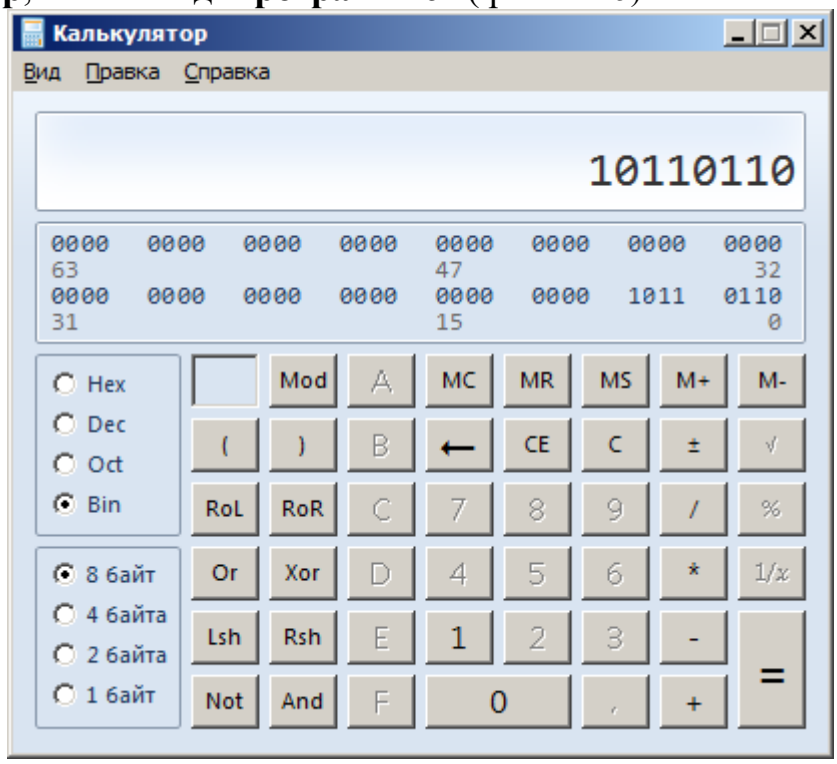


Рис. 4. Двоичный режим (Bin)

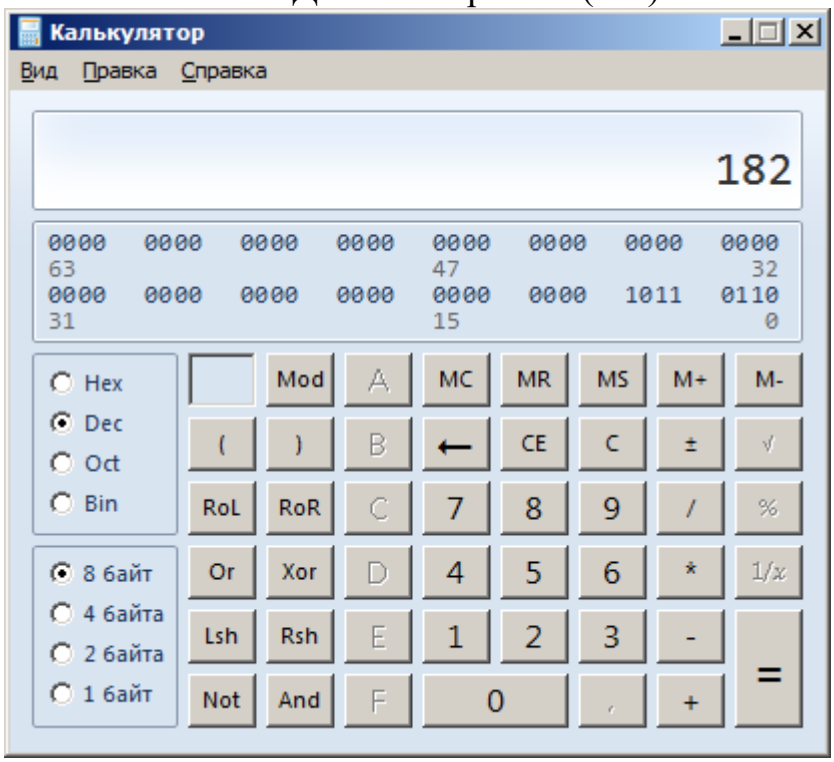


Рис. 5. Десятичный режим (Dec)

Пример: $1010101_2 = 85_{10}$.

ПРАКТИЧЕСКАЯ РАБОТА №10-11.
НАСТРОЙКА СТЕКА ПРОТОКОЛОВ TCP/IP

Цель работы: Научиться настраивать и тестировать стек протоколов TCP/IP

Задание №1. Определение маски сети

Маской подсети (маской сети) называется битовая маска, определяющая, какая часть IP-адреса узла сети относится к адресу сети, а какая — к адресу узла. Например, узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети 12.34.56.0/24 с длиной префикса 24 бита с числом узлов 254 (рис. 1).

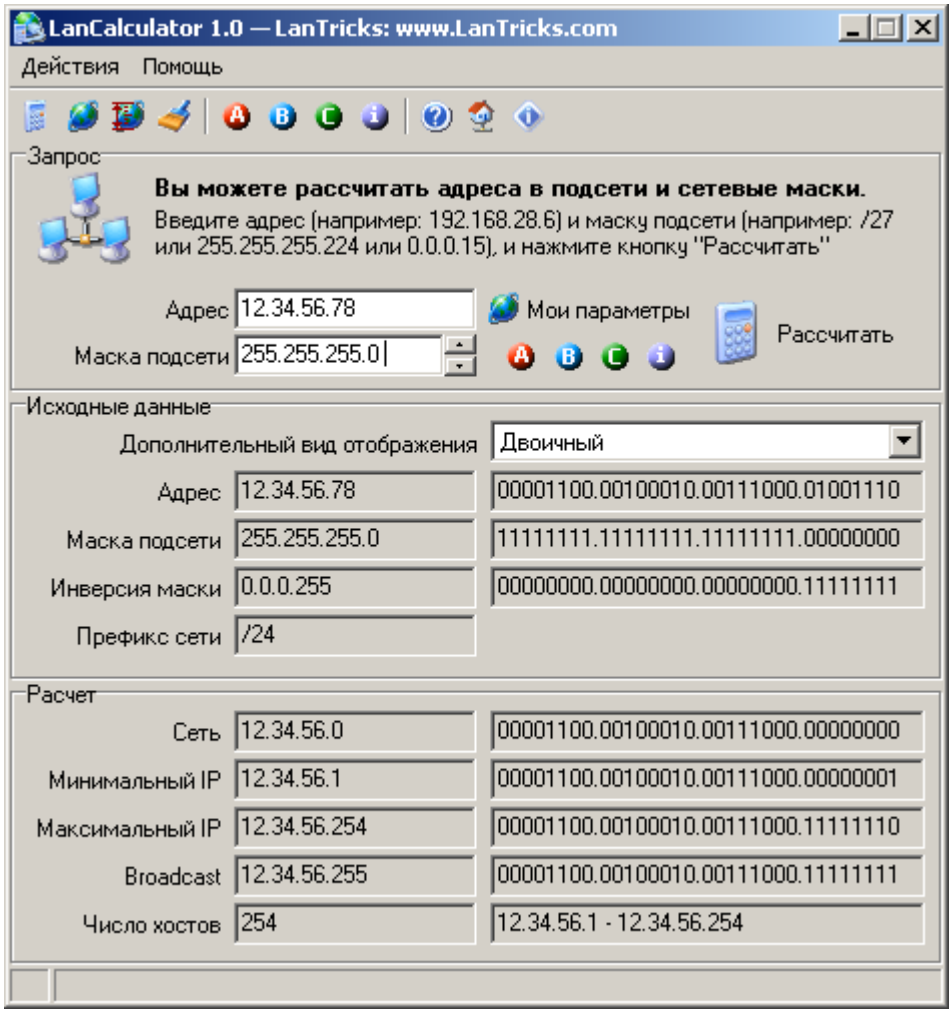


Рис. 1. Пояснение к термину Маски подсети (расчеты выполнены в программе LAN Calculator)

Примечание

IP калькуляторов довольно много. Для ОС Windows 7 можно пользоваться, например, программой **IP Subnet Calculator** 3.2.1. К сожалению, этот вариант только англоязычный (рис. 6.7). Здесь также видно, что узел с IP-адресом 12.34.56.78 и маской подсети 255.255.255.0 находится в сети

12.34.56.0/24 с длиной префикса 24 бита с числом узлов 254. Другой вариант IP-калькулятора для Windows 7 – программа **Advanced IP Address calculator** (рис. 2).

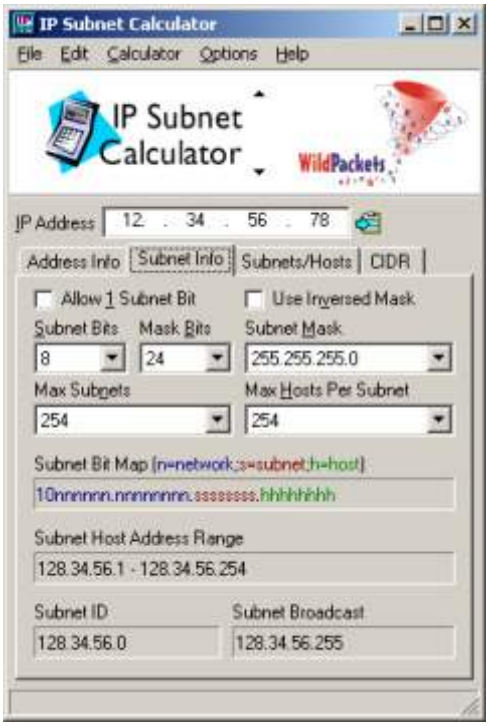


Рис. 2. IP Subnet Calculator

Рис. 3. Advanced IP Address calculator

С точки зрения математики маска подсети накладывается на IP адрес и применяется логическая операция конъюнкции – "И". Если бит в маске подсети равен "1", то соответствующий бит IP-адреса является частью номера сети. Если бит в маске подсети равен "0", то соответствующий бит IP-адреса является частью идентификатора хоста. Пример логического И (1+1=1, а 1+0=0) приведен в таблице 1.

IP-адрес десятичный	192	168	1	2
IP-адрес двоичный	11000000	10101000	00000001	00000010
Маска подсети двоичная	11111111	11111111	11111111	00000000
Где единицы в маске, там сеть. Где нули в маске, там узел	Номер сети			Номер узла
Номер сети двоичный (складываем IP и маску).	11000000	10101000	00000001	
Идентификатор хоста двоичный.				00000010

Пример выделения маской номера сети и хоста в IP-адресе

Классы сетей

Для того, чтобы как-то структурировать сети, их поделили на классы.

Класс А. Большие сети

В сети класса А для описания адреса сети используется первый октет, а остальная часть адреса - это адрес узла. Возможное кол-во узлов 16777214. Маска сети класса А - 11111111. 00000000. 00000000. 00000000 (255.0.0.0).

Класс В. Средние сети

В сети класса В для описания адреса сети используется первые два октета, а остальная часть - это адреса узлов. Возможное кол-во узлов 65534. Маска сети
класса В - 11111111. 11111111. 00000000. 00000000 (255.255.0.0).

Класс С. Малые сети

Адреса сетей класса С используют три первых октета для описания адреса сети, а последний октет обозначает адрес узла. Возможное кол-во узлов 254. Маска сети
класса С - 11111111.11111111.11111111.00000000 (255.255.255.0).

Итак, для стандартного деления IP-адресов на номер сети и номер узла, определенного классами А, В и С маски подсети имеют следующий вид:

Класс	**Двоичная форма**	**Десятичная форма**
А	11111111 00000000 00000000 00000000	255.0.0.0
В	11111111 11111111 00000000 00000000	255.255.0.0
С	11111111 11111111 11111111 00000000	255.255.255.0

В настоящее время классовая модель считается устаревшей и маршрутизация осуществляются по модели CIDR.

Маски при бесклассовой маршрутизации (CIDR)

Бесклассовая адресация CIDR (Classless InterDomain Routing) - метод IP-адресации, позволяющий гибко управлять пространством IP-адресов, не используя жёсткие рамки классовой адресации. Использование этого метода позволяет экономно использовать конечный ресурс IP-адресов. Пример записи IP-адреса с применением бесклассовой адресации: 10.1.2.33/27. По-другому такая запись называется запись IP-адреса не в классическом виде и стиле Cisco. При этом подходе маску подсети записывают вместе с IP-адресом в формате IP-адрес/количество единичных бит в маске. Число после слэша означает количество единичных разрядов в маске подсети. Рассмотрим пример записи диапазона IP-адресов в виде 10.96.0.0/11. В этом случае маска подсети будет иметь двоичный вид 11111111 11100000 00000000 00000000, или то же самое в десятичном виде: 255.224.0.0. 11 разрядов IP-адреса отводятся под номер сети, а остальные 32 - 11 = 21 разряд полного адреса - под локальный адрес в этой сети. Итого, 10.96.0.0/11 означает диапазон адресов от 10.96.0.1 до 10.127.255.255.

Задание 4. Задание диапазона IP-адресов. IP калькуляторы

С помощью IP калькуляторов, расположенных в Интернет, можно легко и быстро рассчитать маску сети или подсети, посмотреть, сколько IP-адресов входит в заданный диапазон, узнать число хостов и получить ряд других полезных записей (рис. 4-6).

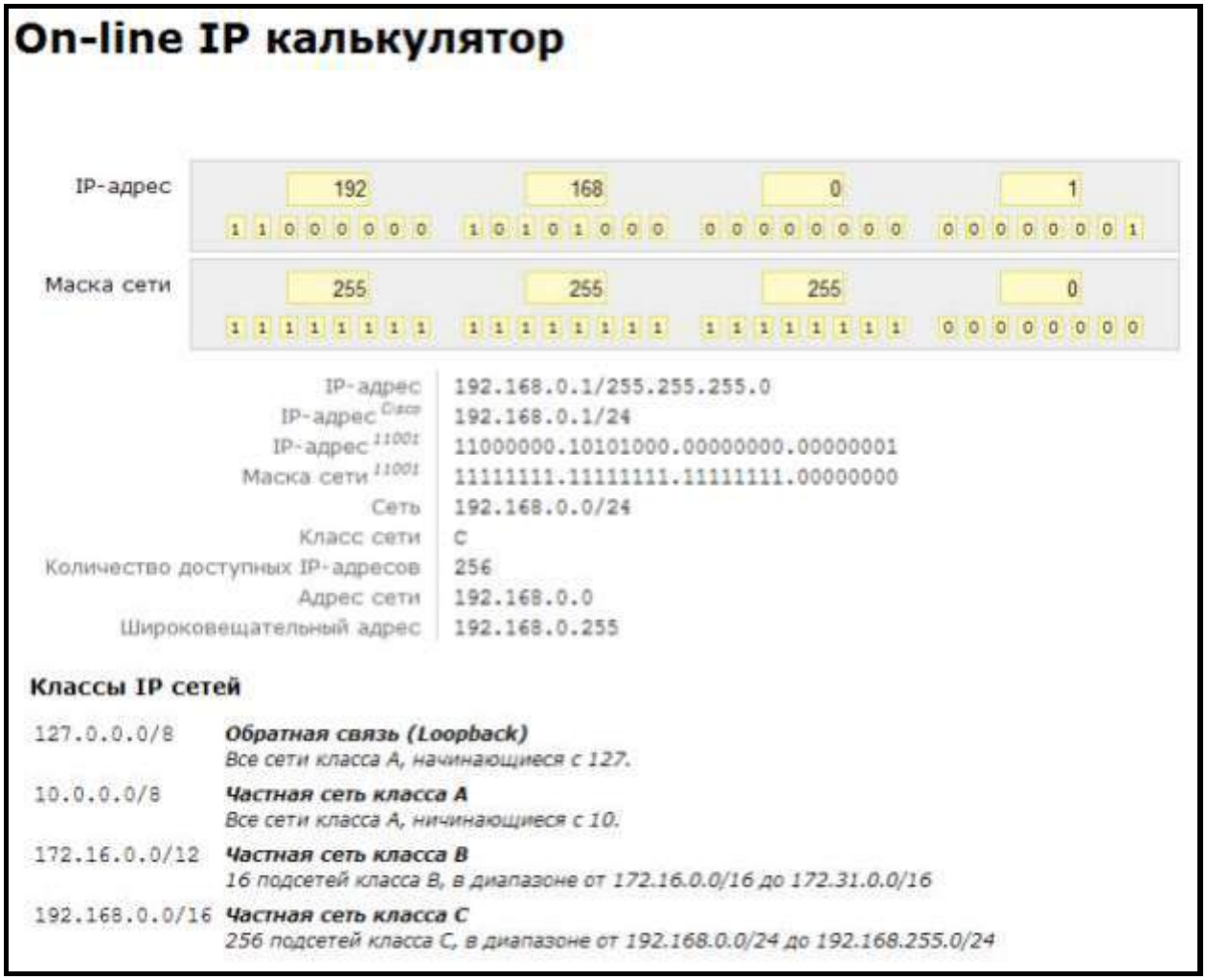


Рис. 4. IP калькулятор на http://ip.waldimord.ru/

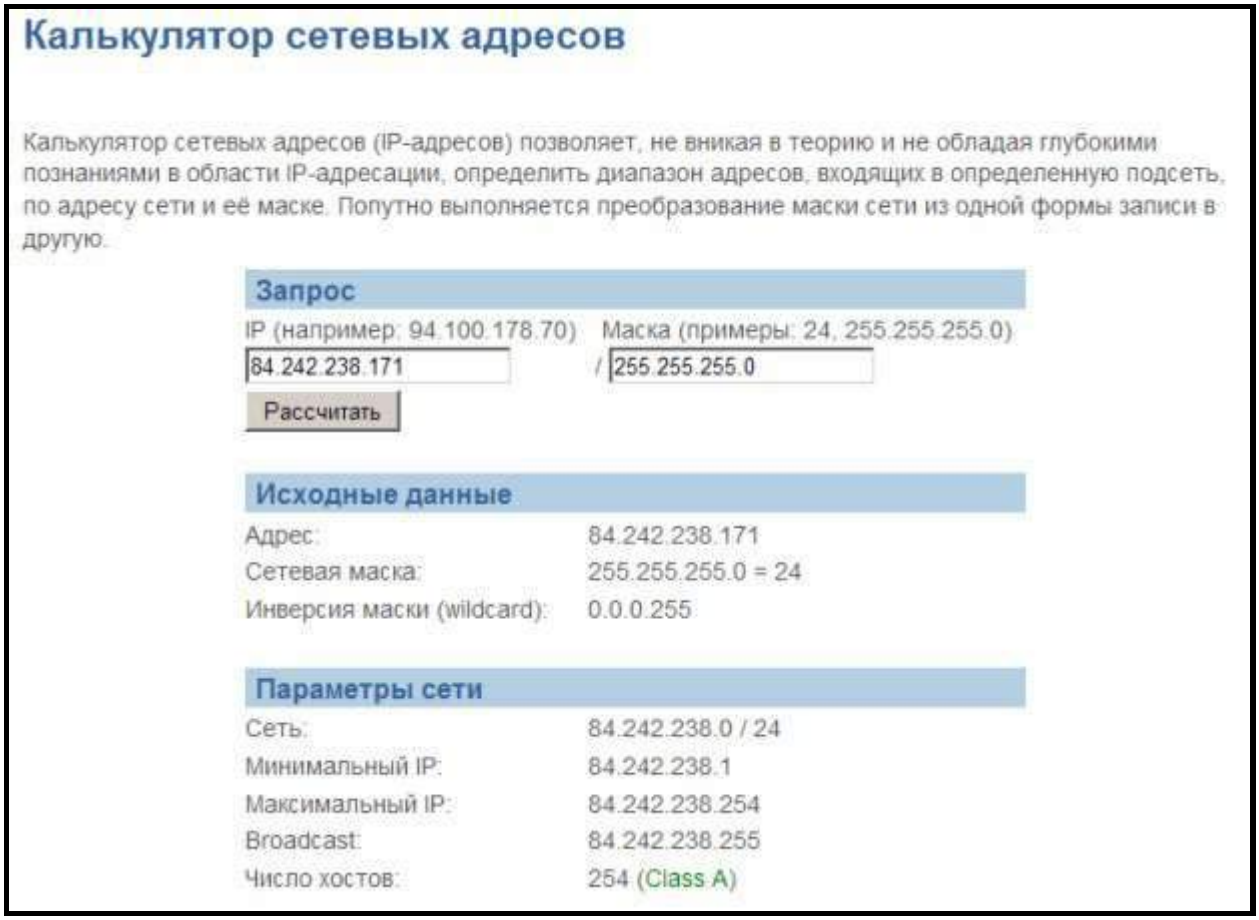


Рис. 5. IP калькулятор на http://azbukaweb.ru/ip-calc

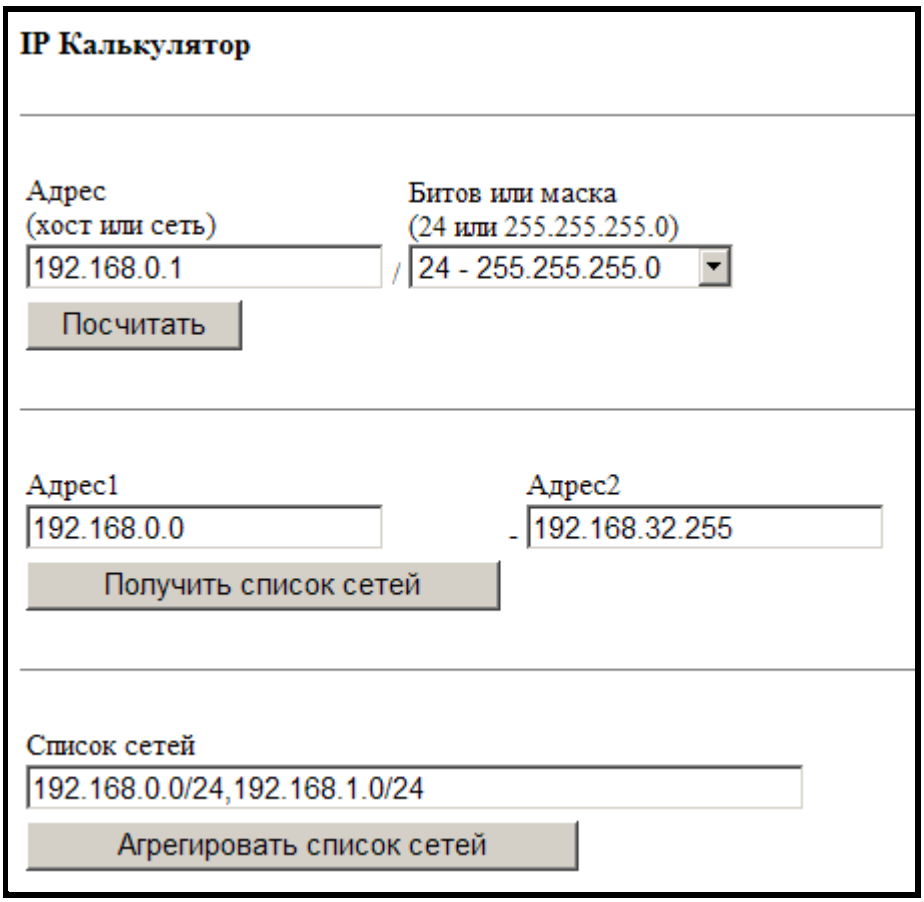


Рис. 6. IP калькулятор на http://ip-calculator.ru/

Путем ввода в калькулятор вашего IP и маски вы можете рассчитать диапазоны IP-адресов от начального (минимального) до конечного (максимального). Диапазон IP адресов записывают в виде префикса. Иначе говоря, если вам встречается запись IP-адресов вида 10.96.0.0/11, то здесь 11 это префикс. Он означает количество единичных разрядов в маске подсети. Для приведённого примера маска подсети будет иметь 11 единиц, потом нули, т.е. двоичный вид 11111111 11100000 00000000 00000000 или то же самое в десятичном виде: 255.224.0.0. 11 разрядов IP-адреса отводятся под номер сети, а остальные из 32 бит, т.е. 32 - 11 = 21 разряд полного адреса — под локальный адрес в этой сети. Итого, 10.96.0.0/11 означает диапазон адресов от 10.96.0.1 до 10.127.255.254. Для автоматизации подобных расчетов воспользуйтесь программой **LanCalculator для Windows XP**. Просто введите IP и Маску и нажмите на кнопку **Рассчитать.** Тот же результат вы получите проще и быстрее (рис. 7).

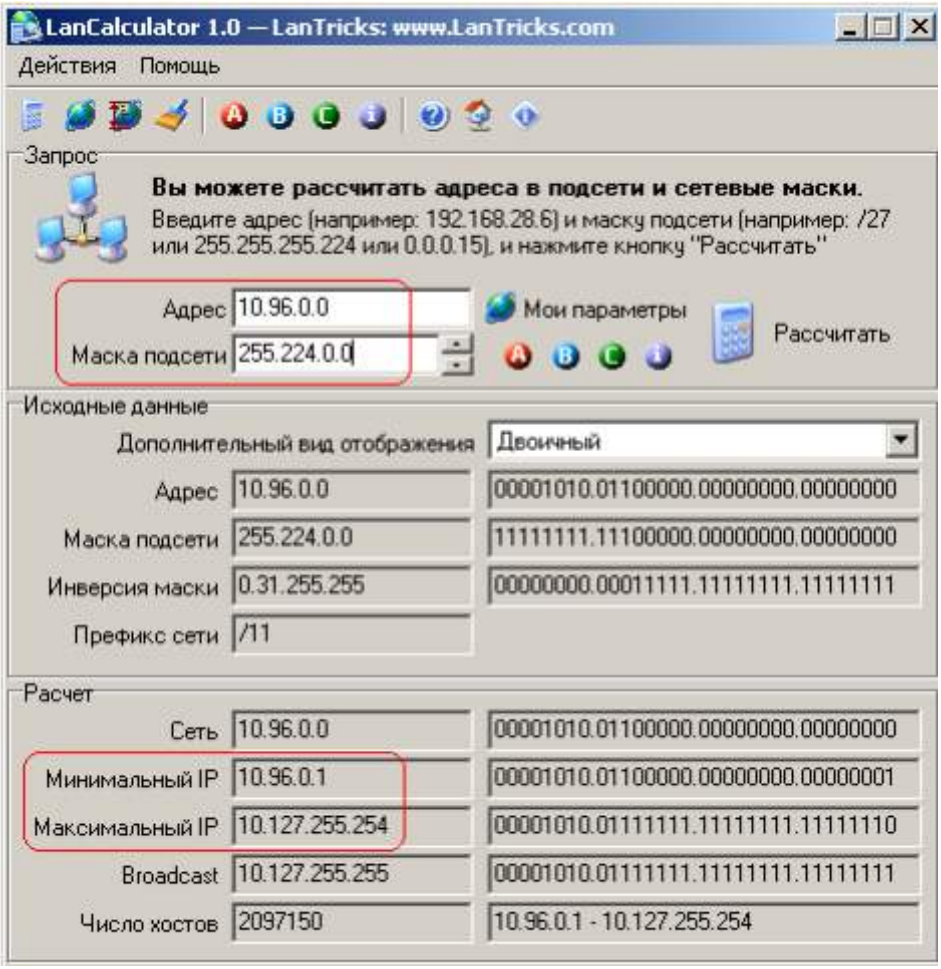


Рис. 7. Расчет диапазона IP адресов по IP адресу и Маске подсети

Задание 5. Определить MAC-адрес ПК

Помимо IP адреса, есть еще и такое понятие, как MAC адрес.

MAC-адрес (или аппаратный адрес) - это цифровой код длиной 6 байт, устанавливаемый производителем сетевого адаптера и однозначно идентифицирующий данный адаптер. Согласно стандартам на сеть Ethernet, не может быть двух сетевых адаптеров с одинаковым MAC-адресом. Пример записи MAC-адреса: 00:E0:18:C3:11:89.

Для того, чтобы узнать MAC-адрес сетевой карты в ОС Windows XP нужно выполнить следующие действия: **Пуск-Выполнить-cmd**и нажимаем OK;

В командной строке набираем **ipconfig /all** и нажимаем **Enter** (рис. 8).

```
Ethernet адаптер:

DNS-суффикс этого подключения . . :
Описание  . . . . . . . . . . . . : Marvell Yukon 88E
Ethernet Controller
Физический адрес. . . . . . . . . : 00-17-31-A7-CD-21
Dhcp включен. . . . . . . . . . . : да
Автонастройка включена  . . . . . : да
IP-адрес  . . . . . . . . . . . . : 192.168.13.81
Маска подсети . . . . . . . . . . : 255.255.255.0
Основной шлюз . . . . . . . . . . : 192.168.13.150
DHCP-сервер . . . . . . . . . . . : 192.168.13.101
DNS-серверы . . . . . . . . . . . : 192.168.13.101
```

Рис. 8. Показан аппаратный адрес ПК

Находим пункт "физический адрес" — это и есть MAC-адрес. Если на компьютере установлено несколько сетевых карт, то пунктов "физический адрес" может быть несколько. В Widows XP можно MAC адрес определять специальными утилитами (рис. 9).

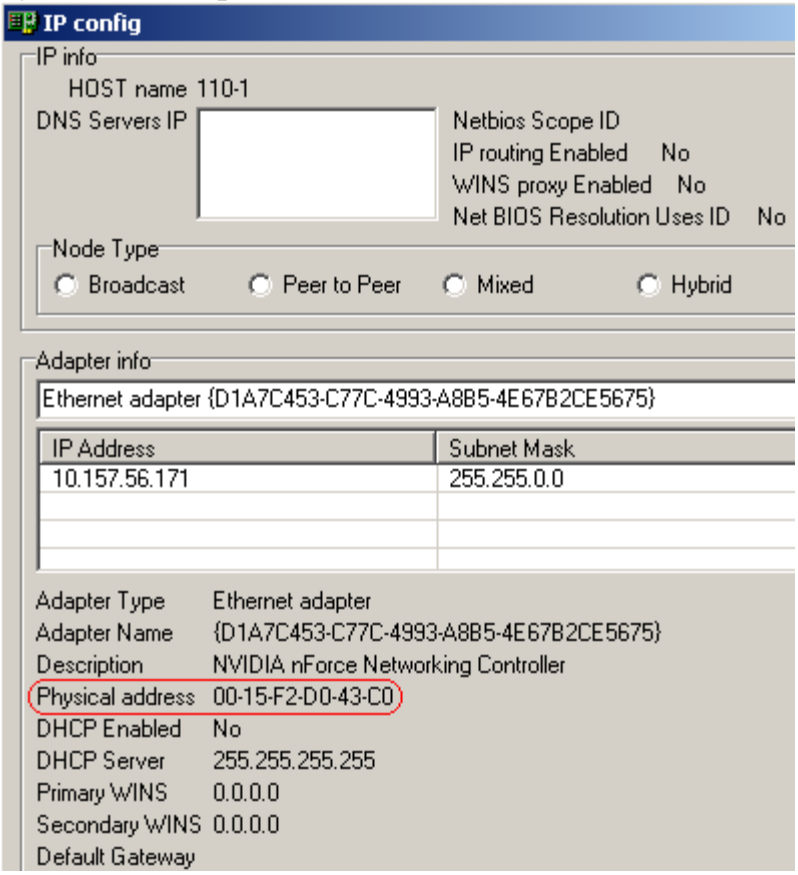


Рис. 9. Окно утилиты IP config

ПРАКТИЧЕСКАЯ РАБОТА №12-13.
ИЗУЧЕНИЕ ВИРТУАЛЬНЫХ ЛОКАЛЬНЫХ СЕТЕЙ VLAN

Цель работы: Изучить виртуальные локальные сети VLAN

Основные сведения

Локальные сети в настоящее время принято строить на основании технологи коммутируемого Ethernet. Стремятся минимизировать число используемых концентраторов (хабов-hab) и использовать преимущественно коммутаторы (свичи - switch). В коммутаторе между приёмником и передатчиком на время соединения образуется виртуальный канал (virtual circuit) точка-точка. Такая сеть может быть рассмотрена как совокупность независимых пар приёмник-передатчик, каждая из которых использует всю полосу пропускания. Коммутатор позволяет осуществлять параллельную
передачу информации. Коммутация уменьшает вероятность переполнения в сетях Ethernet.

Если коммутатору необходимо передать пакет на какой-то выходной порт, и этот порт занят, то пакет помещается в буферную память. Это позволяет согласовать скорости передатчиков и приёмников пакетов.

Для отправки фрейма через коммутатор используются два метода:

Отправка с промежуточным хранением (store-and-forward). Пакет должен быть принят полностью до того как будет начата его отправка.

Сквозной метод (cut-through). Коммутатор принимает начало пакета, считывает в нём адрес пункта назначения и начинает отправлять пакет ещё до его полного получения.

Ethernet-коммутатор узнаёт MAC адреса устройств в сети путём чтения адресов источников в принимаемых пакетах. Коммутатор запоминает в своих внутренних таблицах информацию на какие порты и с каких MAC адресов приходят пакеты. При подключении к одному порту нескольких устройств через концентратор (hub) в таблице одному порту будет соответствовать несколько MAC- адресов. Таблицы хранятся в памяти, адресуемой по смыслу (content-addressable memory, CAM): если адрес отправителя отсутствует в таблице, то он туда заносится. Наряду с парами адрес-порт, в таблице хранится и метка времени. Метка времени в строке таблицы изменяется либо при приходе на коммутатор пакета с таким же адресом, либо при обращении коммутатора по этому адресу. Если строка таблицы не использовалась определённый период времени, то она удаляется.

Это позволяет коммутатору поддерживать правильный список адресов устройств для передачи пакетов.

Используя CAM таблицу адресов и содержащийся в пришедшем пакете адрес получателя, коммутатор организует виртуальное соединение порта отправителя с портом получателя и передает пакет через это соединение.

Виртуальное соединение между портами коммутатора сохраняется в течение передачи одного пакета, т.е. для каждого пакета виртуальное соединение организуется заново на основе содержащегося в этом пакете адреса получателя.

Поскольку пакет передается только в тот порт, к которому подключен адресат, остальные устройства подключенные к коммутатору, не получат этот пакет.

В коммутаторах Ethernet передача данных между любыми парами портов происходит независимо и, следовательно, для каждого виртуального соединения выделяется вся полоса канала.

При передаче широковещательного пакета, в коммутаторе образуется «веер» каналов по принципу один ко многим. Примерами источников широковещательного трафика являются ARP и маршрутизирующие протоколы.

Коммутаторы можно соединять друг с другом. При этом группа попарно прямо либо косвенно связанных коммутаторов образует один логический коммутатор с теоретически произвольным числом портов. То есть коммутаторы позволяют создавать теоретически сколь угодно большую локальную сеть. Правильное соединение коммутаторов, то есть выбор топологии сети составляет одну из важнейших задач проектирования локальных сетей.

Рекомендуется осуществлять соединение коммутаторов по слоям (рисунок 1): серверный слой, слой распределения (distribution) и слой доступа (access). Рядовые компьютеры подключаются к слою доступа, а сервера к серверному слою.

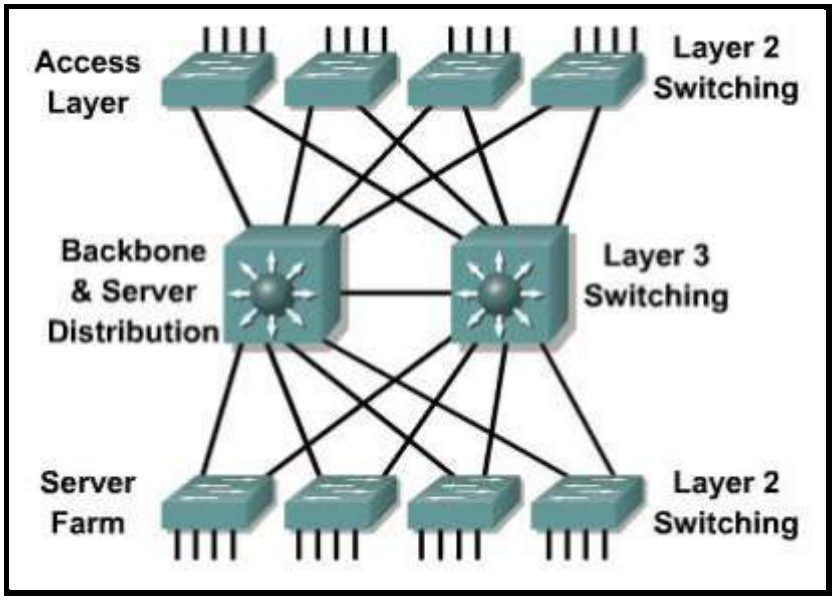


Рисунок 1.

Главным препятствием для создания больших локальных сетей с помощью одних только коммутаторов является нелинейный рост объёма широковещательного трафика с ростом числа устройств в сети. При числе

устройств в сети более, чем 2000 (по другим оценкам 500, по третьим 4000 – всё зависит от топологии сети и класса решаемых задач) объём широковещательного трафика резко возрастает. Добавление новых устройств резко снижает производительность сети. Например. Если в сети из нескольких тысяч устройств один из компьютеров А впервые осуществляет IP соединение с другим компьютером
В в этой сети, то он должен предварительно послать ко всем устройствам сети широковещательный ARP запрос для определения MAC адреса компьютера В.
Локальная сеть, созданная с помощью одних только коммутаторов представляет один домен широковещания. Уменьшить домен широковещания можно, физически разделив локальную сеть на независимые подсети (независимые группы попарно связанных коммутаторов) и соединить их в единое целое с использованием маршрутизаторов. Такую задачу можно решить только на этапе построения сети, но не в момент её эксплуатации. Здесь на помощь приходят виртуальные локальные сети
VLAN (virtual local area network).
Виртуальная локальная сеть VLAN представляет собой совокупность портов одного или более коммутаторов (Рисунок 2).

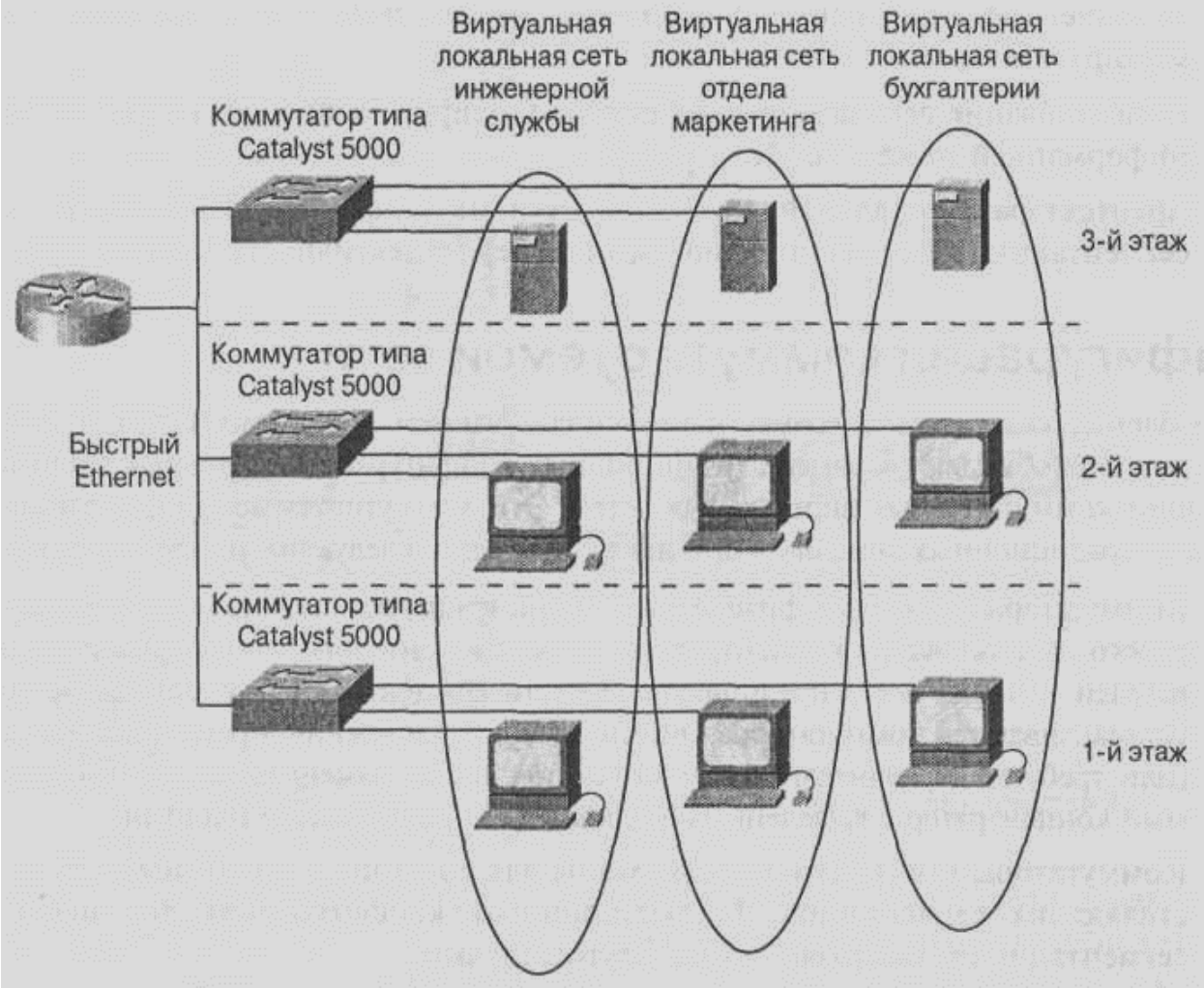


Рисунок 2.

VLAN позволяют логически разбить исходную локальную сеть на несколько независимых локальных сетей без физического обрыва сетевых соединений. Для этого администратор сети должен на каждом коммутаторе назначить, какие его порты относятся к каким VLAN. По умолчанию все порты коммутатора относятся к одной VLAN с номером 1. Максимальное число VLAN в коммутаторе равно общему числу его портов. Правильная разбивка локальной сети на VLAN составляет одну из важнейших задач проектирования.

VLAN ведут себя так же, как и физически разделённые локальные сети. То есть после разбивки сети на VLAN мы получим несколько локальных сетей, которые далее необходимо объединить в единое целое с помощьюмаршрутизации на третьем сетевом уровне.

Концепция VLAN, помимо решения проблемы с широковещательным трафиком даёт также ряд дополнительных преимуществ: формирование локальных сетей не по месту расположения ближайшего коммутатора, а по принадлежности компьютеров к решению той или иной производственной задачи; создание сети по типу потребляемого вычислительного ресурса и требуемой серверной услуги (файл-сервер, сервер баз данных). VLAN позволяют вести различную политику безопасности для разных виртуальных сетей; переводить компьютер из одной сети в другую без осуществления физического перемещения или переподключения.

Для обмена информацией о VLAN коммутаторы используют магистральный (транковый) протокол. Для осуществления обмена информацией о VLAN между коммутаторами вы должны создать магистральные порты. Магистральный порт это порт, используемый для передачи информации о VLAN в другие сетевые устройства, присоединенные к этому порту. Обычные порты не рекламируют информацию о VLAN, но любой порт может быть настроен для приема/передачи информации о VLAN. Вы должны активизировать магистральный протокол на нужных портах, так как он выключен по умолчанию.

Порт коммутатора работает либо в режиме доступа либо в магистральном режиме. Соответственно связь, подсоединённая к порту является либо связью доступа либо магистральной связью. В режиме доступа порт принадлежит только одной VLAN. Порт доступа присоединяется к оконечному устройству: ПК, рабочей станции, серверу, хабу. Фреймы, проходящие через порт доступа, являются обычными Ethernet фреймами.

Магистральные связи способны поддерживать несколько VLAN. VLAN на различных коммутаторах связываются через магистральный протокол. Магистральные порты не принадлежат определённой VLAN и используются для подсоединения к другим коммутаторам, маршрутизаторам или серверам,

имеющим сетевые адаптеры с возможностью для подключения ко многим VLAN.

Магистрали могут расширить VLAN по всей сети. Для магистральных целей назначают высокоскоростные порты коммутаторов: Gigabit Ethernet и 10Gigabit .

Для мультиплексирования трафика VLAN существуют специальные протоколы, позволяющие приёмным портам определить, какому VLAN принадлежит пакет. Для связи между устройствами Cisco используется протокол Inter-Switch Link (ISL). При наличии в сети оборудования нескольких производителей применяется протокол IEEE 802.1Q

Без магистральных связей для поддержки VLAN должно быть организовано по одной связи доступа для каждой VLAN. Такой подход дорог и неэффективен, поэтому магистральные связи абсолютно необходимы при проектировании локальных сетей.

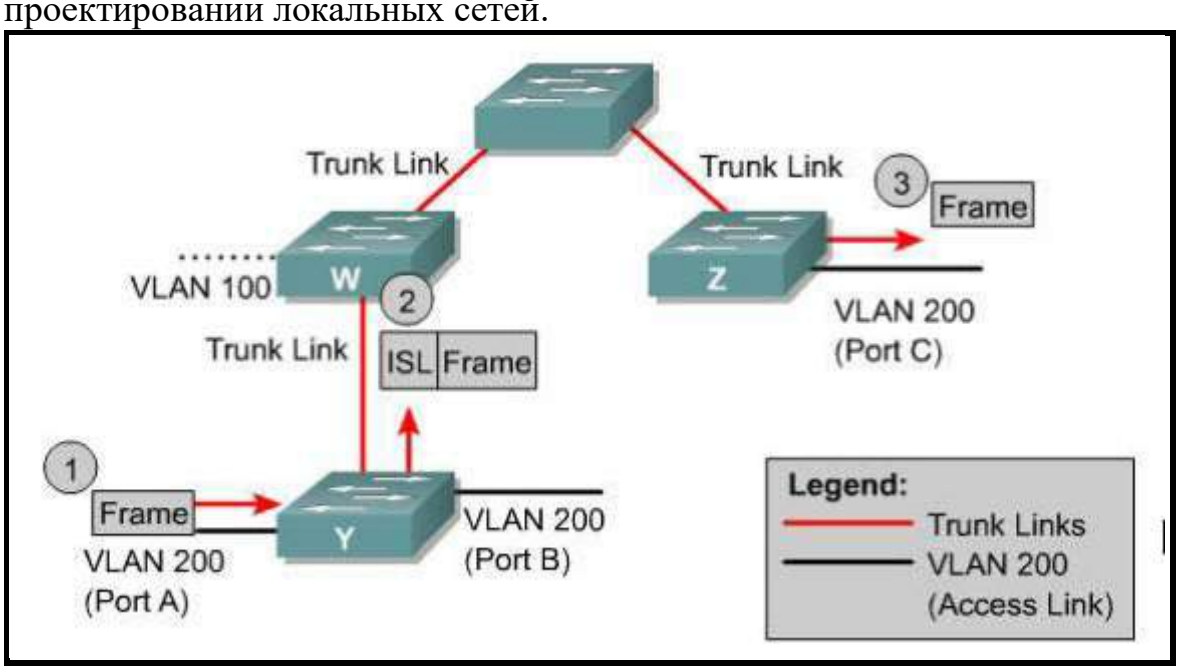


Рисунок 3.

На рисунке 3 порты A и B на коммутаторе Y определены как связи доступа на одной и той же VLAN 200. По определению они могут принадлежать только одной VLAN и не могут получать ethernet фреймы, содержащие идентификатор VLAN. Например, когда Y получает трафик от порта A к порту B, то он не добавляет ISL заголовокок в ethernet фреймы.

Порт C на коммутаторе Z также является портом доступа и также принадлежит к VLAN 200. Если порт A пересылает фрейм в порт C, то происходит следующее:

1. Коммутатор Y получает фрейм и, сопоставляя номер порта назначения с номером VLAN, определяет его как трафик, направленный к VLAN 200 на другом коммутаторе,

2. Коммутатор Y добавляет к фрейму ISL заголовок с номером VLAN и пересылает фрейм через промежуточный коммутатор на магистральную связь.
3. Этот процесс повторяется на каждом коммутаторе по пути фрейма к конечному порту C.
4. Коммутатор Z получает фрейм, удаляет ISL заголовок и направляет фрейм на порт C.

Если порт находится в магистральном режиме, то он может быть настроен или для транспорта всех VLAN или ограниченного множества VLAN. Магистральные связи используются для связи коммутаторов с другими коммутаторами, маршрутизаторами или с серверами, имеющими поддержку VLAN.

Согласно базовой терминологии магистраль это связь точка-точка, поддерживающая несколько VLAN. Целью магистрали является сохранение номеров портов при создании связи между двумя устройствами, образующими VLAN.

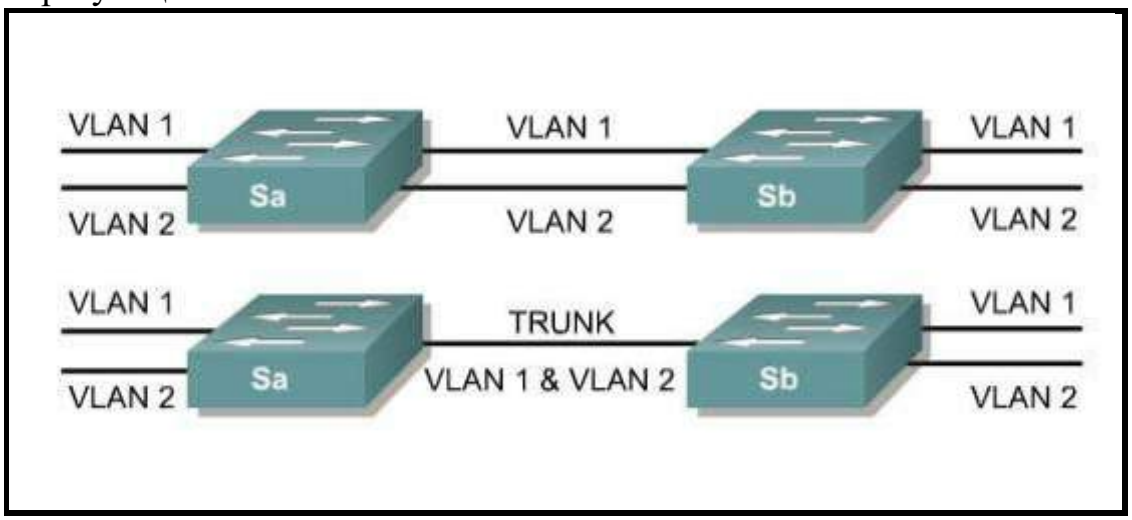


Рисунок 4.

Верхняя фигура на рисунке 4 показывает способ создания VLAN путём использования двух физических связей между коммутаторами (по одной на каждую VLAN). Это решение плохо масштабируется: при добавлении третьего VLAN надо пожертвовать ещё двумя портами. Это решение неэффективно и в смысле разделения нагрузки: малый трафик на некоторых связях может не стоить того, что эта связь является пучком виртуальных связей через одну физическую связь. На нижней фигуре одна физическая связь способна нести трафик для любой VLAN. Для достижения этого коммутатор Sa так оформляет фреймы, что Sb знает, на какую VLAN они направляется. Для такого оформления пакетов используются либо стандарт IEEE 802.1Q либо Cisco протокол ISL (Inter-Switch Link).

Для больших сетей ручная конфигурация VLAN становится весьма трудоёмкой задачей. Cisco VLAN Trunk Protocol (VTP) служит для автоматического обмена информацией о VLAN через магистральные порты.

Преимуществом использования VTP является то, что вы можете контролировать добавление, удаление или изменение сетей VLAN из коммутаторов на котором созданы VTP сервера. После настройки ваших коммутаторов как VTP серверов, остальные коммутаторы вашей сети могут быть настроены как клиенты, которые только получают VLAN информацию.
Недостатком является ненужный трафик, создаваемый на магистральный портах для устройств, которым возможно не нужна эта информация. Если ваша сеть будет содержать много коммутаторов, содержащих много виртуальных сетей, расположенных в разных коммутаторах, возможно, имеет смысл использовать VTP. Если ваша сеть останется
достаточно статической, и VLAN не будут добавляться или изменяться по отношению к начальной конфигурации, то лучше использовать статическое определение виртуальных сетей.
В топологии локальных сетей возможны циклы (петли). Например, уже
три коммутатора соединённых друг с другом по кругу образуют цикл в топологии. Петли приводят к неоднозначности при определении пути от источника пакетов к приёмнику. Для решения этой серьёзной проблемы был разработан протокол связующего дерева STP (spanning tree protocol). Для графа топологии каждой VLAN, которая определена в сети, строится минимальное покрывающее дерево (граф без циклов) с вершиной в
некотором коммутаторе. Для физической реализации таких деревьев STP переводит избыточные порты в состояние блокировки. Расчёт деревьев производится параллельно на всех коммутаторах. Далее пакеты во VLAN идут только по путям, определённым в построенных покрывающих деревьях.
При изменении топологии, активации/остановке портов происходит пересчёт покрывающих деревьев.
Для создания топологии связующего дерева существуют специальные фреймы, называемые модулями данных мостового протокола (bridge protocol data units, BPDU). Эти фреймы отправляются и принимаются всеми коммутаторами в сети через равные промежутки времени.

Задание №1 Выполнить Конфигурирование статических VLAN
1. Статические VLAN это совокупность портов на коммутаторе, которые вручную назначаются командой IOS при конфигурировании интерфейса.
Для создания пустой VLAN с номером №VLAN на коммутаторах Cisco серии 2950 используются команды
Switch#**vlan database**
Switch(vlan)#**vlan №VLAN**
Switch(vlan)# **exit**
Например, команды
Switch#**vlan database**
Switch(vlan)#**vlan 33**
Switch(vlan)# **exit**

создадут пустую VLAN с номером 33 и система даст VLAN имя VLAN0033.
Заметим, что команды выполняются не в режиме конфигурации.
Команда **switchport mode** используется для установки интерфейса в динамический режим, режимы доступа или режим магистрали (trunk).
Switch(config-if)**#switchport mode [access | dynamic | trunk]**
Хотя режим доступа является режимом по умолчанию, но в ряде случаев устройство, присоединённое к порту коммутатора, может перевести его в магистральный режим. Поэтому рекомендуется все немагистральные порты переводить в режим доступа командой **switchport mode access.**
Для статического помещения текущего интерфейса во VLAN используются команды
Switch(config-if)#**switchport mode access**
Switch(config-if)#**switchport access vlan №number**
где **№number –** число – номер VLAN.
Команда **interface range** определяет диапазон интерфейсов для последующих конфигураций. Например, порты с первого по шестой могут быть помещены во VLAN 10 командами
Switch(config)#**interface range fa0/1 – 6**
Switch(config-if-range)#**switchport access vlan 10**
После настройки VLAN проверьте настройку командами **show runningconfig**,
show vlan и **show vlan brief**.
При настройке VLAN помните, что по умолчанию все порты находятся
во VLAN 1.
Для создания или конфигурирования магистрали VLAN вы должны настроить порт как магистральный
Switch(config-if)#**switchport mode trunk**
По умолчанию последняя команда определяет порт как магистральный для всех VLAN в сети. Однако существуют ситуации, когда магистраль не должна поддерживать все VLAN. Типичной является ситуация с подавлением широковещания. Широковещание посылается на каждый порт во VLAN. Магистральная связь выступает как член VLAN и должна
пропускать всё широковещание. Если на другом конце магистрали нет портов нужной VLAN, то полоса пропускания и процессорное время устройств тратится попусту.
Если VLAN не используется на другом конце магистрали, нет нужды разрешать эту VLAN на этой магистрали. По умолчанию магистральные порты принимают и передают трафик со всех VLAN в сети. Для сокращения магистрального трафика используйте команду
Switch(config-if)#**switchport trunk allowed vlan vlan-list**
Например, команда
Switch(config-if)#**switchport trunk allowed vlan 3**
Switch(config-if)#**switchport trunk allowed vlan 6-10**

разрешает на магистрали VLAN 3 и затем VLAN с 6 по 10. О том, какие VLAN разрешены на магистрали можно посмотреть командой **show runningconfig.**

Для удаления большого числа VLANs из магистрали проще вначале удалить все VLAN, а затем выборочно разрешать. Простейший способ перевести связь в режим доступа это задать на интерфейсах с её двух сторон по команде

SwitchA(config-if)#**switchport mode access**

Простейший способ перевести связь в режим доступа это задать на интерфейсах с её двух сторон по команде

SwitchA(config-if)#**switchport mode trunk**

Практическая часть

1. Соберите топологию изображенную на рисунке 5. Коммутаторы соедините двумя GigabitEthernet (gi1/1 и gi1/2) соединениями. Компьютеры подсоедините к интерфейсам согласно таблице 1. Назначьте компьютерам адреса, согласно таблице 1. Все компьютеры входят в одну подсеть 172.16.0.0 255.255.0.0. Маршруты по умолчанию на компьютерах не устанавливайте.

Пропингуйте сеть.

Организуем в нашей сети два VLAN. Компьютеры 20_1 и 20_2 поместим во VLAN с номером 20, а компьютеры 30_1 и 30_2 поместим во VLAN с номером 30.

Switch1(conf)#**interface fa0/2**

Switch1(conf-if)#**switchport access vlan 20**

Switch1 (conf-if)#**interface fa0/3**

Switch1(conf-if)#**switchport access vlan 30**

Switch2 (conf)#**interface fa0/2**

Switch2(conf-if)#**switchport access vlan 20**

Switch2 (conf-if)#**interface fa0/3**

Switch2(conf-if)#**switchport access vlan 30**

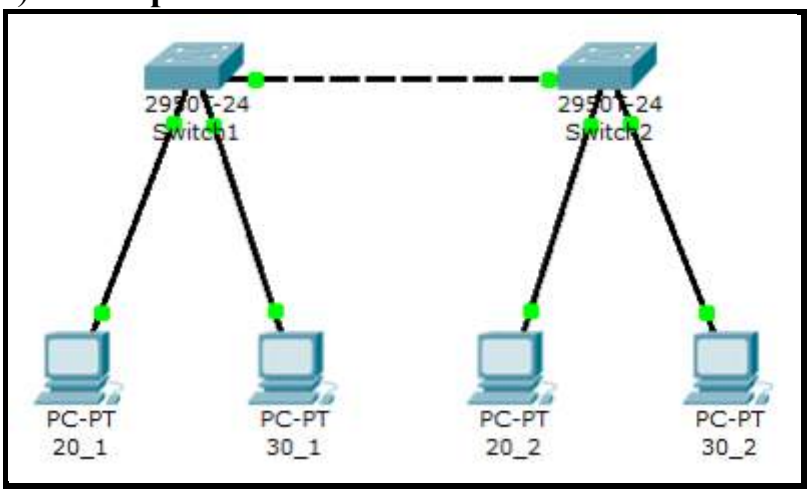


Рисунок 5.

Таблица 1.

Компьютер	Switch1	Switch2	Адрес
20_1	Fa0/2		172.16.20.1/16
30_1	Fa0/3		172.16.20.2/16
20_2		Fa0/2	172.16.30.1/16
30_2		Fa0/3	172.16.30.2/16
	Gi1/1	Gi1/1	

На обеих коммутаторах проверьте результаты создания VLAN, например Switch1# sh vl name 20

```
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
20   20                               active    Fa0/2

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0
```

И

```
Switch1#sh  vl br

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/4, Fa0/5, Fa0/6
                                                Fa0/7, Fa0/8, Fa0/9, Fa0/10
                                                Fa0/11, Fa0/12, Fa0/13, Fa0/14
                                                Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                Fa0/23, Fa0/24
20   20                               active    Fa0/2
30   30                               active    Fa0/3
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
```

Так как нет обмена информации о VLAN между коммутаторами, то компьютеры будут пинговать только самих себя.

Организуем магистрали на коммутаторах. Для этого используем GigabitEthernet порт

Switch1(conf)#**interface gi1/1**
Switch1 (conf-if)#**switchport trunk allowed vlan add 20**
Switch1 (conf-if)#**switchport trunk allowed vlan add 30**
Switch1 (conf-if)#**no shutdown**
Switch2 (conf)#**interface gi1/1**
Switch2 (conf-if)#**switchport trunk allowed vlan add 20**
Switch2 (conf-if)#**switchport trunk allowed vlan add 30**
Switch2 (conf-if)#**no shut**

Теперь компьютеры в переделах одной VLAN должны пинговаться, а компьютеры, находящиеся в различных VLAN не должны пинговаться (см.

таблицу 2).

Таблица 2.

Ping из/в	20_1	30_1	20_2	30_2
20_1	**Да**	**Нет**	**Да**	**Нет**
30_1	**Нет**	**Да**	**Нет**	**Да**
20_2	**Да**	**Нет**	**Да**	**Нет**
30_2	**Нет**	**Да**	**Нет**	**Да**

Сохраните конфигурации коммутаторов.

2. Сохраним топологию предыдущего задания в новом файле. В этой топологии маршрутизатор соединён двумя связями с интерфейсами fa0/1 коммутаторов (рисунок 6). Снова проверьте, что компьютеры в переделах одной VLAN пингуются, а компьютеры, находящиеся в различных VLAN не пингуются.

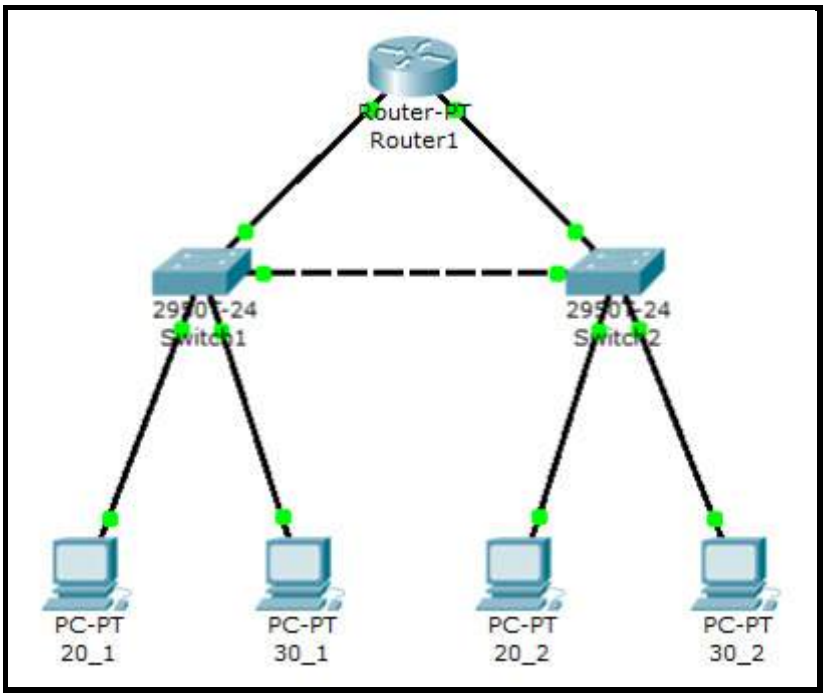


Рисунок 6.

Поставим задачу объединения виртуальных сетей с помощью маршрутизатора. Для этого следует разбить нашу сеть 172.16.0.0/16 на две подсети 172.16.20.0/24 и 172.16.30.1/24. Для этого просто поменяем маски у компьютеров на 255.255.255.0.

Теперь компьютеры пингуются в переделах одной VLAN и в пределах одной IP подсети, а это значит только сами на себя.

Введём на коммутаторах интерфейсы, подсоединённые к маршрутизатору в виртуальные сети

Switch1(conf)#**interface fa0/1**

Switch1(conf-if)#**switchport access vlan 20**

Switch2(conf)#**interface fa0/1**

Switch2(conf-if)#**switchport access vlan 30**

Настроим IP адреса на маршрутизаторе
Router(conf)#**interface fa0/0**
Router(conf-if)#**ip address 172.16.20.254 255.255.255.0**
Router(conf-if)#**no shutdown**
Router(conf-if)#**interface fa1/0**
Router(conf-if)#**ip address 172.16.30.254 255.255.255.0**
Router(conf-if)**#no shutdown**
Теперь маршрутизатор маршрутизитует наши две сети 172.16.20.0/24 и 172.16.30.1/24. Добавим на наших компьютерах маршрутизацию по умолчанию на интерфейсы маршрутизатора.

Host	Gataway
20_1	172.16.20.254
20_2	172.16.20.254
30_1	172.16.30.254
30_2	172.16.30.254

Теперь изо всех устройств нашей сети мы можем пинговать все наши IP адреса.
3. Покажем, как с использованием транзитных линий, мы можем сэкономить порты.
Изменим топологию, перебросив магистраль gi1/2 от коммутаторов к интерфейсу fa0/0 маршрутизатора (рисунок 7). Загрузим топологию в симулятор. Загрузим по очерёдно в каждое устройство, кроме маршрутизатора, сохранённые конфигурации. Заметим, что в конфигурации коммутатора Switch2 установка магистрали на gi1/2 не нужна, хотя она и не мешает.

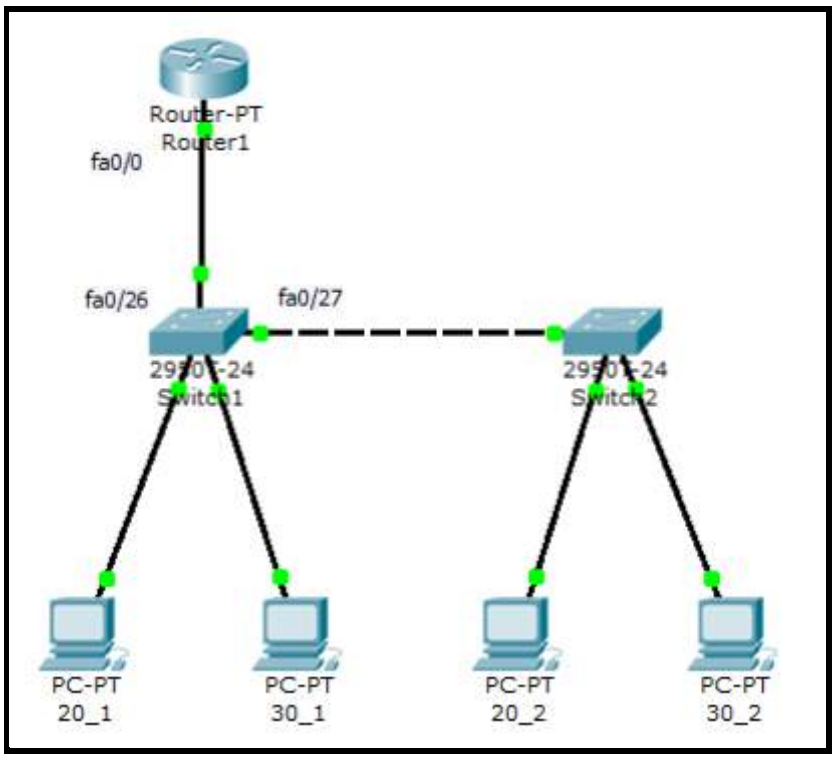


Рисунок 7.

На маршрутизаторе разобъём интерфейс fa0/0 на два подинтерфейса fa0/0.20 и fa0/0.30. Определим на них инсапсуляцию dot1q и поместим их в виртуальные сети 20 и 30, соответственно.

Router(conf)#**interface FastEthernet0/0.20**
Router(conf-subif)#**encapsulation dot1q 20**
Router(conf-subif)#**ip address 172.16.20.254 255.255.255.0**
Router(conf-subif)#**interface FastEthernet0/0.30**
Router(conf-subif)#**encapsulation dot1q 30**
Router(conf-subif)#**ip address 172.16.30.254 255.255.255.0**

Посмотрим таблицу маршрутов

Router#**show ip route**

Проверьте, что из каждого устройства вы можете пинговать все адреса в сети.

Выполните на Router команду расширенного пинга от адреса 172.16.20.1 компьютера 20_1 из VLAN 20, подключённого к коммутатору Switch1 к адресу 172.16.30.2 компьютера 30_2 из VLAN 30, подключённого к коммутатору Switch2

```
Router#ping
Protocol [ip]:
Target IP address: 172.16.30.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:y
Source address or interface:172.16.20.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.30.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

Задание для получения повышенного бала

Повторить все пункты практической части для IP сети предприятия, согласно вариантам. Практическая часть проделана для сети 172.16.0.0/16.

Вар.	Сеть	Вар.	Сеть	Вар.	Сеть
1	2.1.0.0/16	5	6.1.0.0/16	9	10.1.0.0/16
2	3.1.0.0/16	6	7.1.0.0/16	10	11.1.0.0/16
3	4.1.0.0/16	7	8.1.0.0/16	11	12.1.0.0/16
4	5.1.0.0/16	8	9.1.0.0/16	12	13.1.0.0/16

Создать те же скриншоты, что и при выполнении практической части.

ПРАКТИЧЕСКАЯ РАБОТА №14.
ИСПОЛЬЗОВАНИЕ СЕТЕВЫХ ПРОГРАММНЫХ УТИЛИТ WINDOWS

Цель работы: Изучить и научиться работать в утилитах для работы с локальными сетями Windows

Задания для практического занятия:
Radmin - программа удаленного управление ПК по сети
Суть в следующем: на каждый ПК с локальной сети ставим серверную и клиентскую часть программы Radmin. После этого по сети вы каждым удаленным ПК сможете управлять как своим. Итак, установим сервер и клиент на машина 110-1 и 110-2. При этом права пользователей на сервере пока настраивать не будем (сделаем это позднее) – рис. 1.

Рис. 1. Сервер и клиент установлены на ПК 110-1
Запустим на ПК 110-1 программу **Настройки Radmin Server** и в правах доступа установим переключатель в положение **Radmin** (рис. 2 и рис. 3).

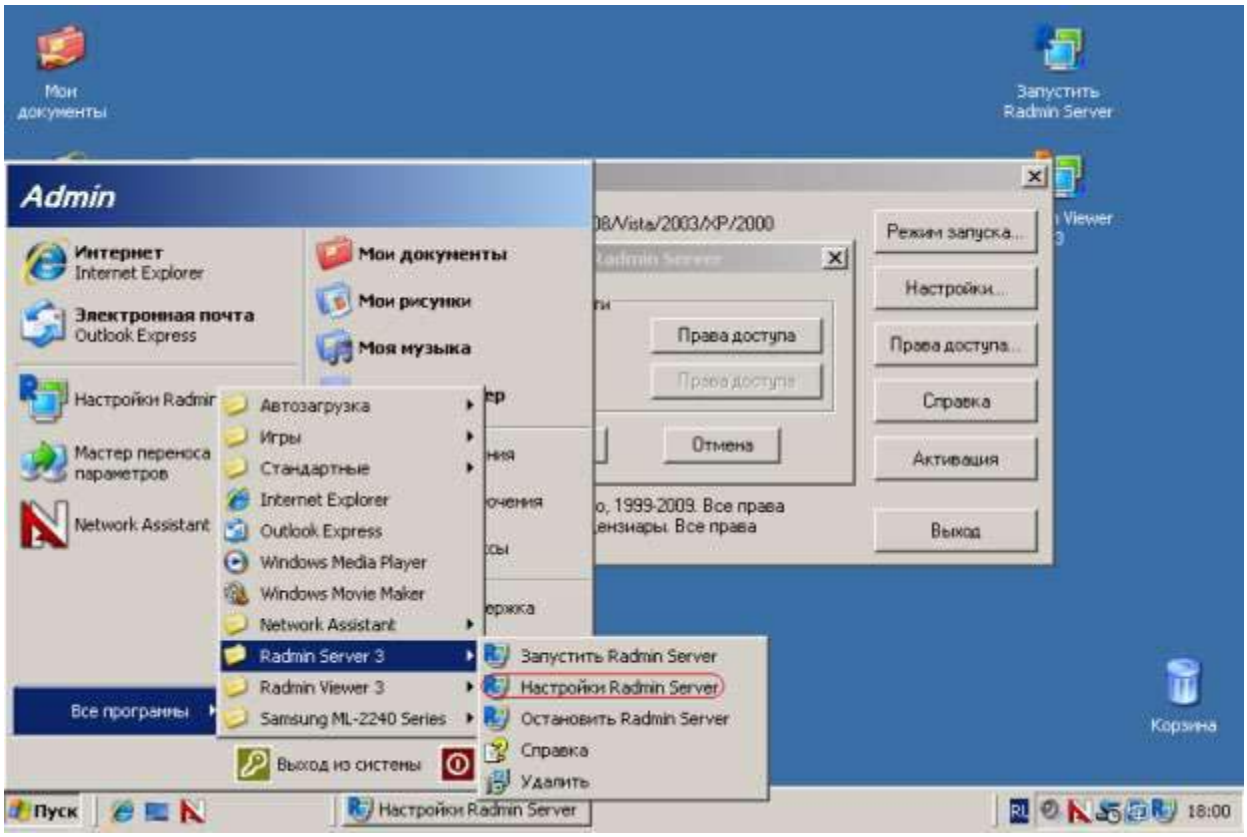


Рис. 2. Запускаем команду Настройки Radmin Server

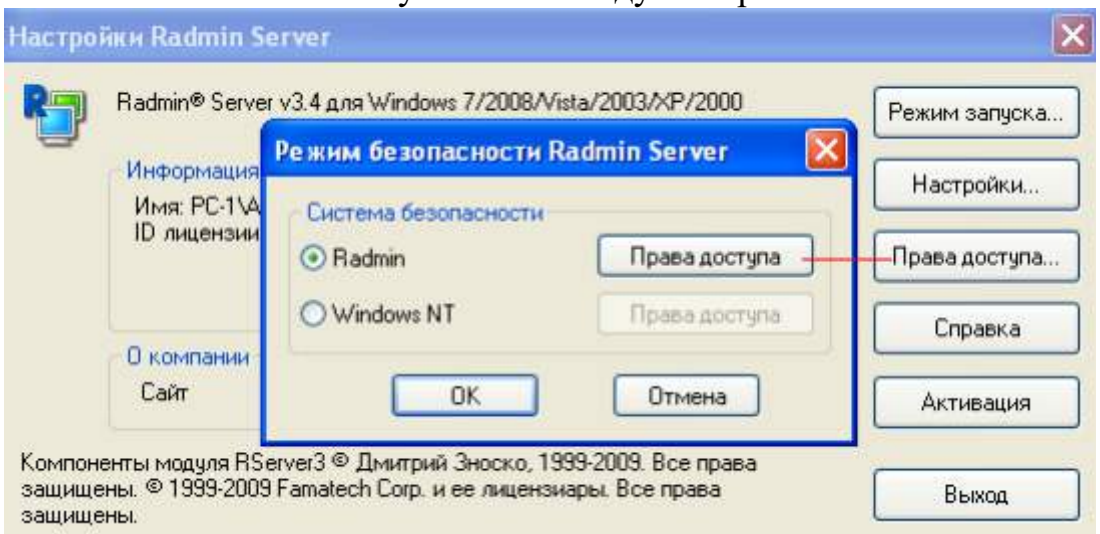


Рис. 3. Выставляем режим безопасности Radmin Server

Нажмем на кнопку **Права доступа** и создадим пользователя серверной частью программы Radmin на ПК 110-1, т.е. организуем пользователя User-1 с паролем 123456 (рис. 4).

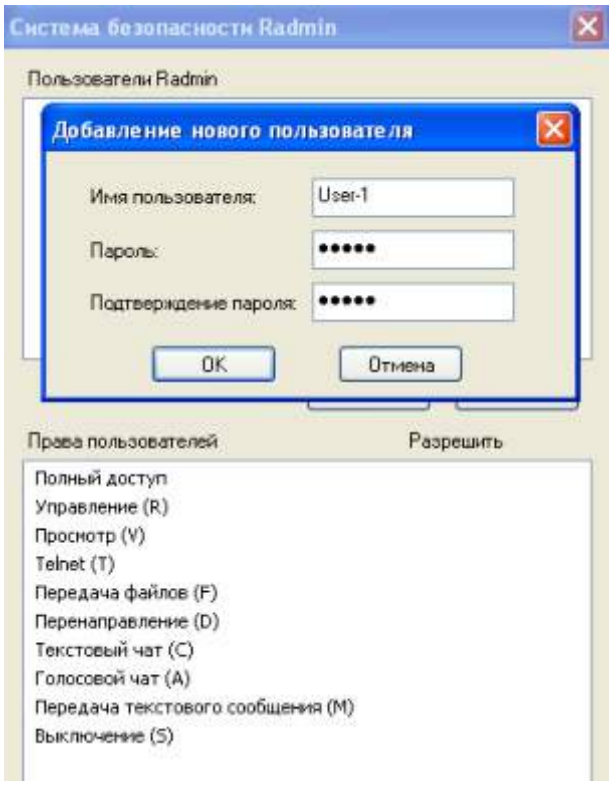


Рис. 4. Добавление нового пользователя

Этому пользователю дадим все права (рис. 5).

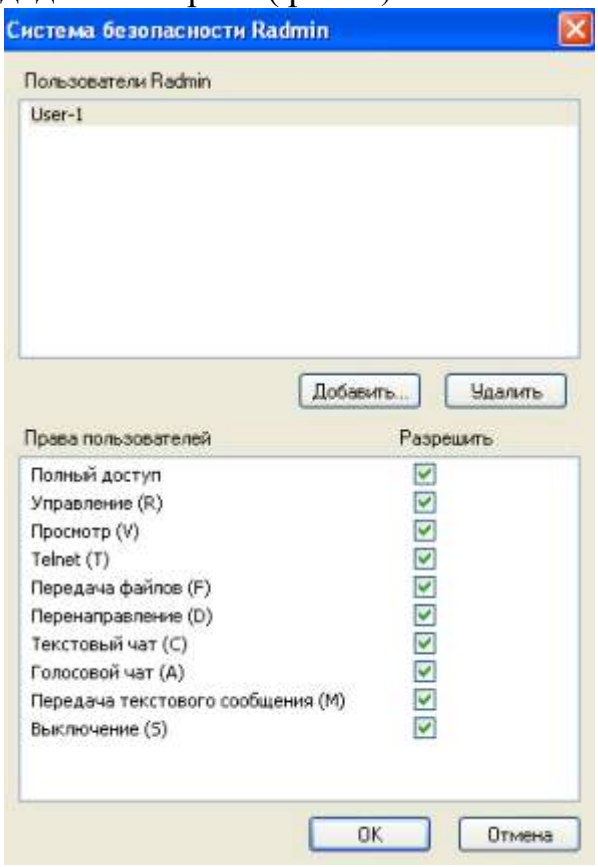


Рис. 5. Права пользователя User-1 на ПК 110-1

Теперь на ПК 110-2 запускаем Radmin Viewer, выполняем команду **Соединение-Соединиться с-110-1** (рис. 6).

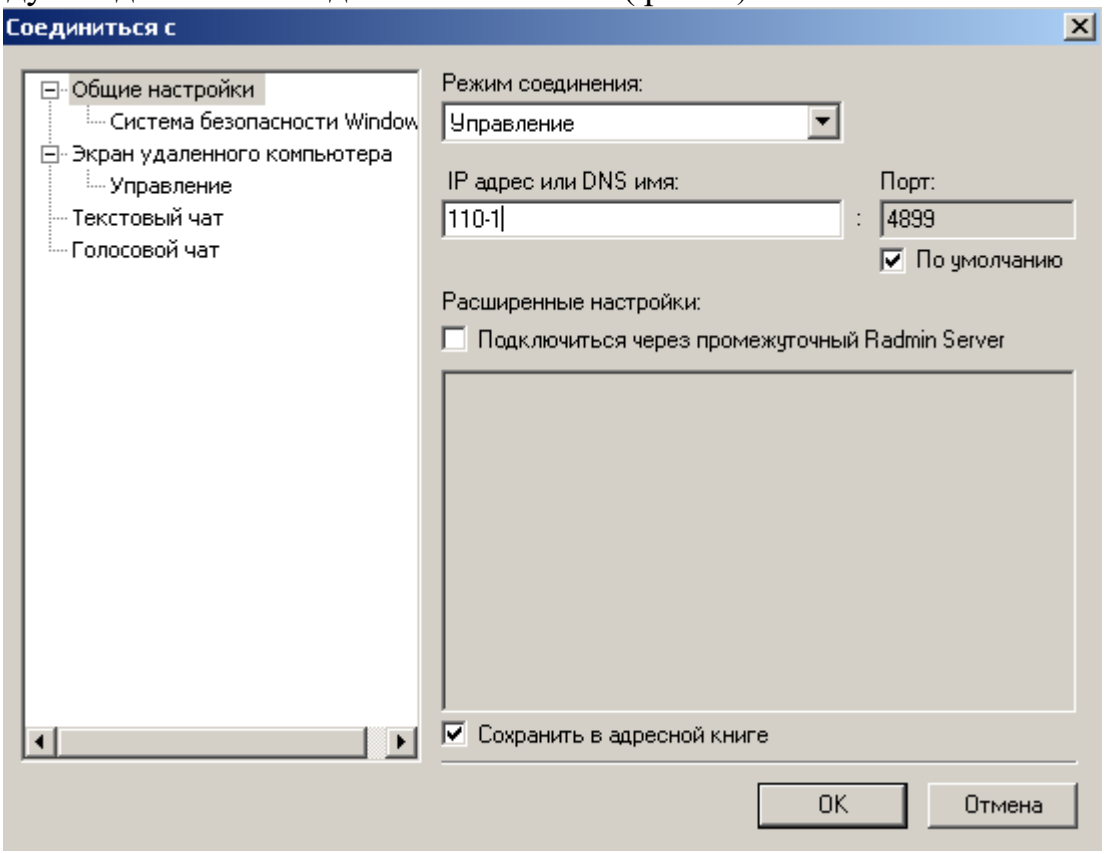


Рис. 6. Окно соединения клиента 110-2 с сервером 110-1

Теперь следует ввести имя User-1 с паролем 123456 и нажать OK (рис. 7).

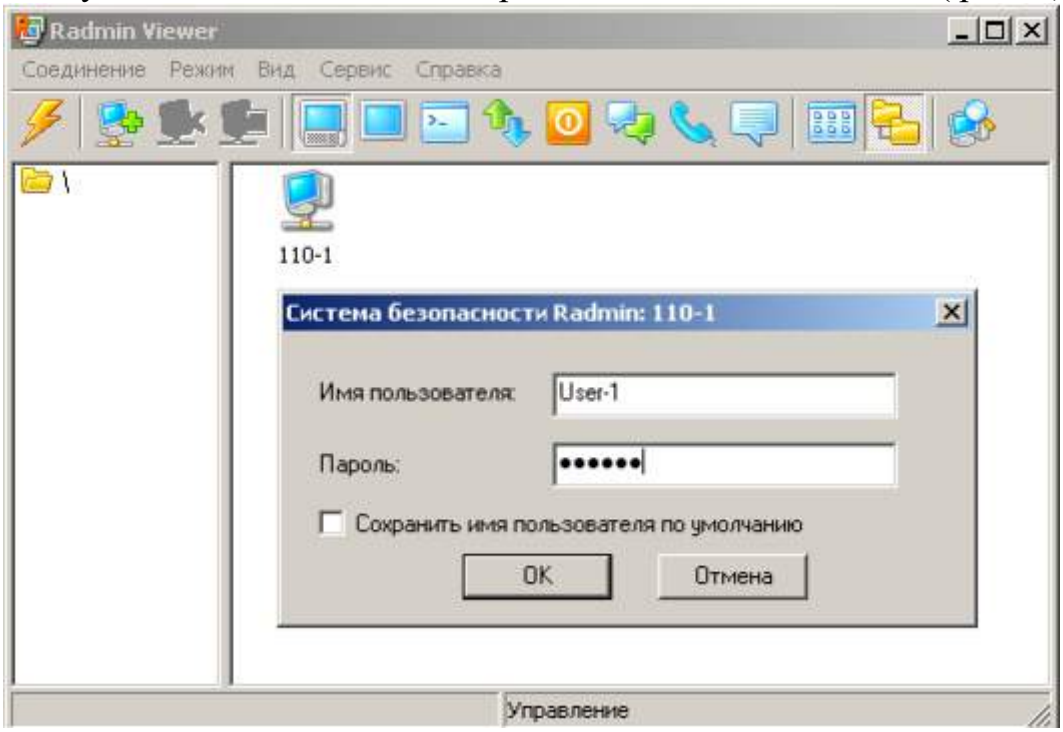


Рис. 7. После нажатия OK вы увидите рабочий стол ПК 110-1

Теперь мы полностью можем управлять с ПК 110-2 компьютером 110-1, как будто вы физически сидите не на ПК 110-2, а на ПК 110-1. Иначе говоря, с помощью Radmin, вы можете администрировать удаленный ПК удаленно.

Примечание

Полезной особенностью Radmin является возможность подключения к удаленному компьютеру в **режиме Telnet**. Это позволит осуществлять перенос текстовых команд на удаленный компьютер с помощью командной строки. Это практически терминальный доступ, только ограниченный режимом командной строки. Положительной стороной этого метода является экономия и уменьшение расхода трафика в тысячи раз по сравнению с графическим режимом.

Nassi - система общения пользователей в локальной сети

Для обмена сообщениями и файлами в локальной сети удобно использовать чат под названием **Net Work Assistant** (Nassi). Установим эту программу на ПК 110-1 и ПК 110-2 и запустим ее (рис. 8).

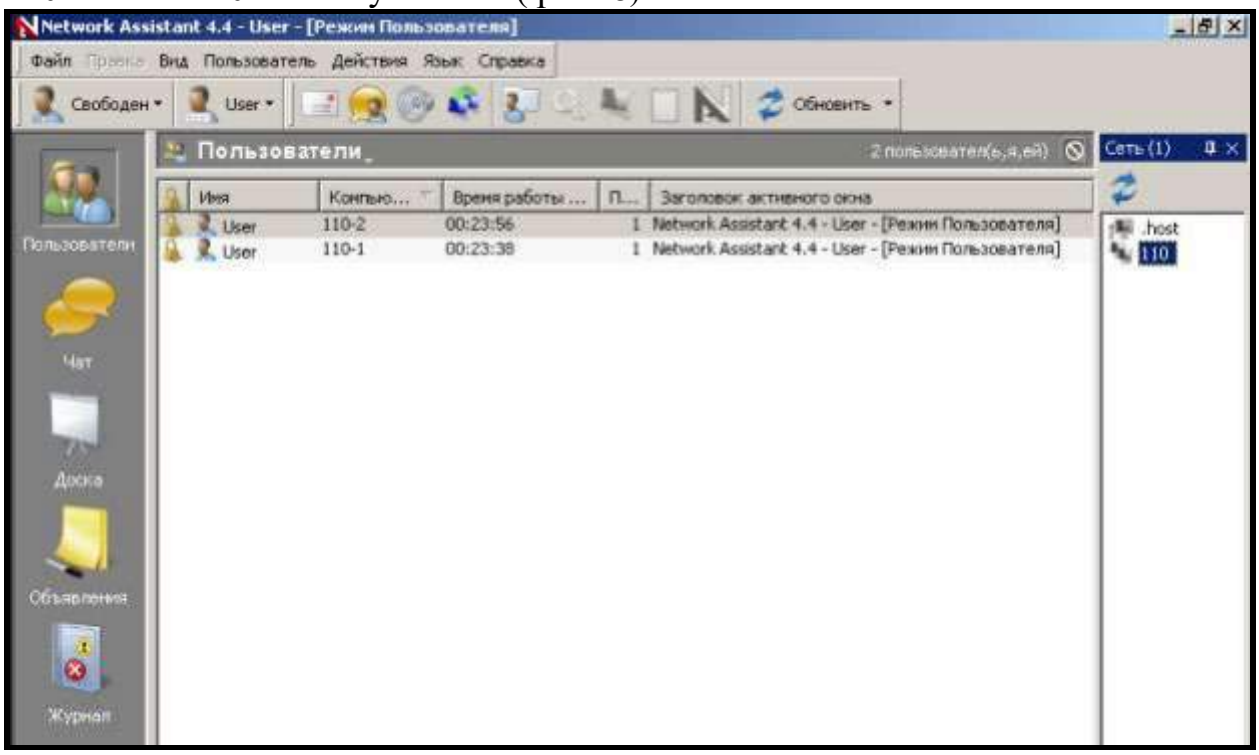


Рис. 8. Network Assistant (интерфейс)

Теперь вы можете отправлять с одного ПК на другой сообщения, файлы, разобраться в этой простой программе совсем не сложно. Например, вы можете на удаленный ПК послать звуковой сигнал (типа телефонного звонка), который сигнализирует ему "Подойди к ПК, поговорим".

Основные возможности Nassi:

1. Многоканальный чат
2. Общая доска для рисования
3. Мгновенные сообщения
4. Передача файлов
5. Управление процессами на удаленном компьютере

6. Сигнализаторы удаленных событий
7. И другое...

Задание 1. Групповая работа в чате и на доске для рисования

Войдите в **Чат** и попробуйте пообщаться с другими ПК. Для этого в низу есть поле ввода, в которое набрать нужное сообщение и нажать /Enter/. Для отправки личного сообщения, щелкните по нику пользователя в списке справа и в появившееся окно вводите ваше сообщение. Если же хотите, чтобы личное сообщение было отправлено всем, то вызовите контекстное меню (правым щелчком мыши) на списке пользователей главного окна, и выберите "сообщение всем". Перейдите на пиктограмму **Доска**. Здесь все пользователи могут вместе (одновременно) рисовать общий рисунок. Изучите другие возможности программы самостоятельно.

Примечание

Если брандмауэр не выключен, то программа **Nassi** должна быть включена в его исключения.

Команда отправки текстовых сообщений Net send

Текстовые сообщения по локальной сети можно отправлять не только в специальных программах (Radmin, Nassi), но и из командной строки Windows XP. Команда **Net send** служит для отправки текстовых сообщений другому компьютеру, доступному в сети. Однако, для того, чтобы команда работала, первоначально необходимо включить службу доставки сообщений. Для этого зайдите в **Панель управления**. Откройте папку **Администрирование, Службы**. Найдите в списке службу сообщений (рис. 9).

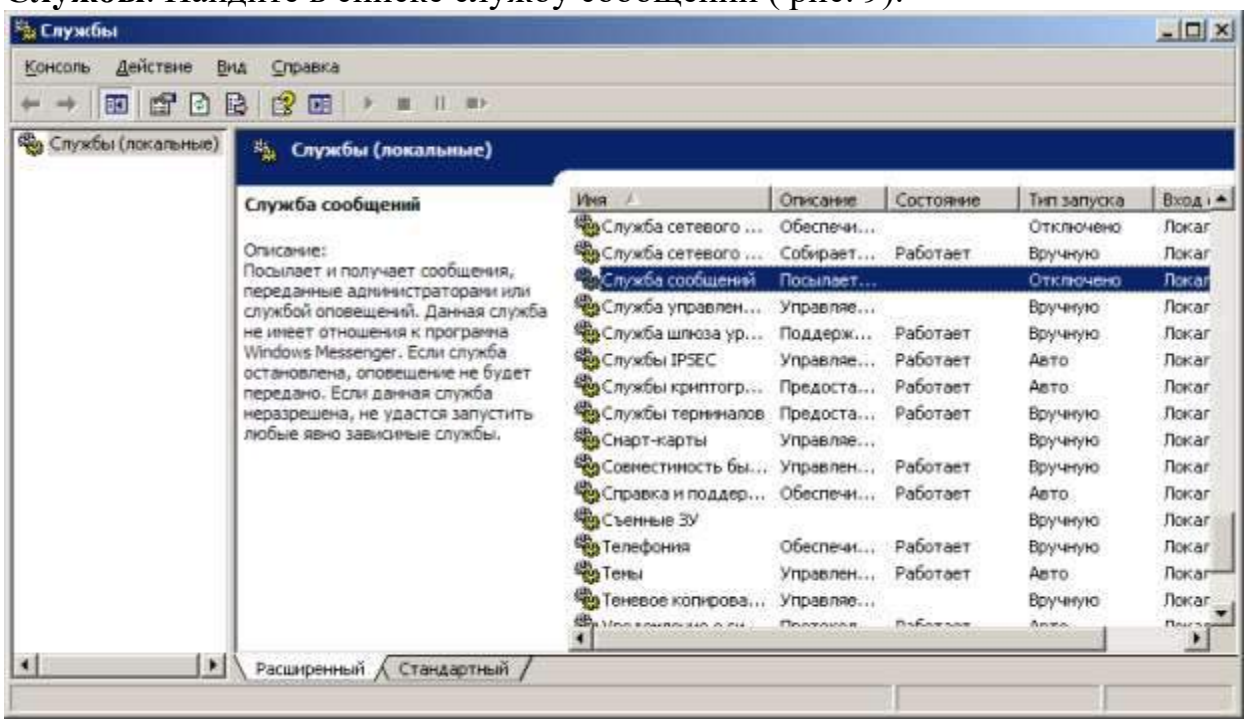


Рис. 9. Служба сообщений отключена

Откройте ее свойства. Выберите значение **Авто** из списка **Тип запуска,** если вы хотите, чтобы служба автоматически запускалась при загрузке Windows. Затем нажмите на кнопку **Пуск** и **ОК** (рис. 10 и рис. 11).

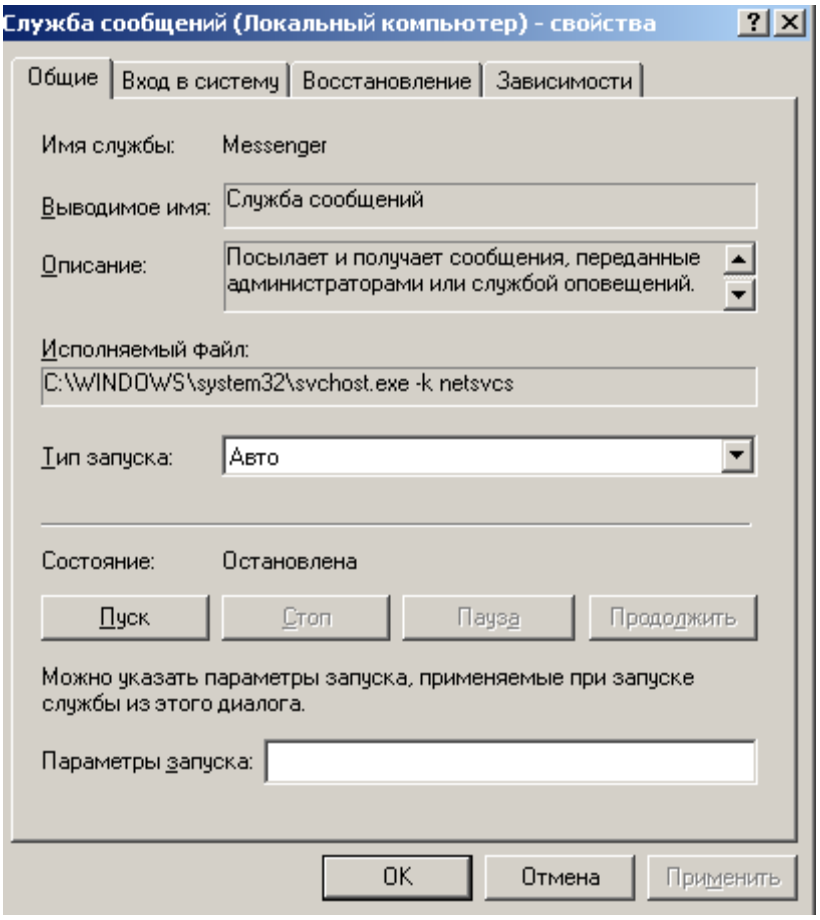


Рис. 10. Окно Служба сообщений

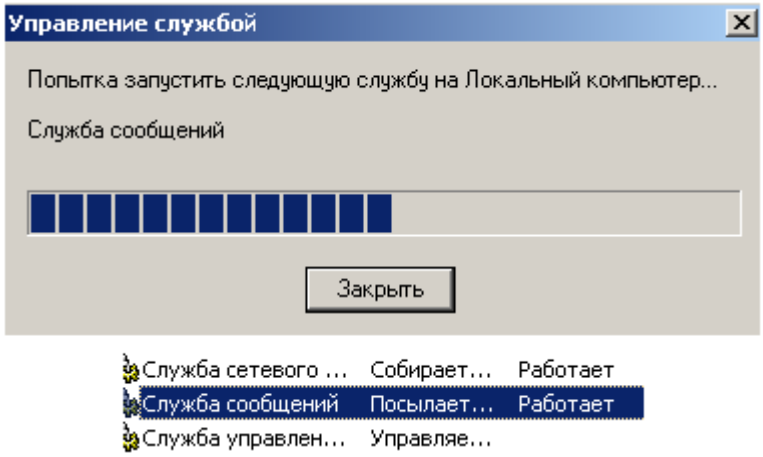
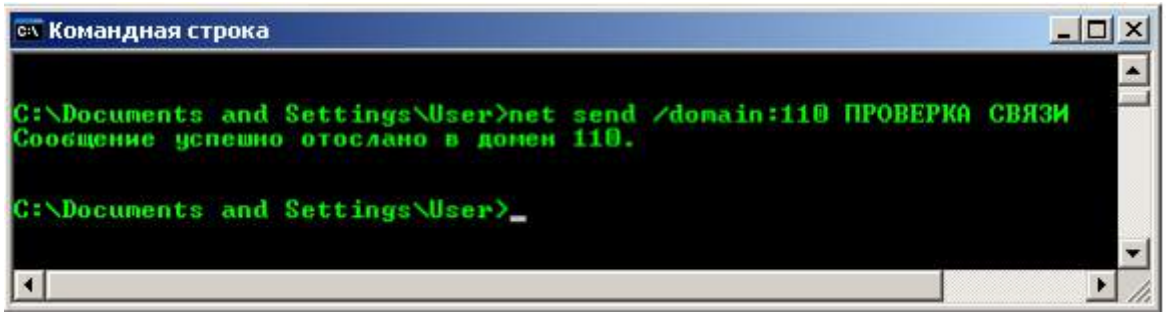


Рис. 11. Служба сообщений работает

Давайте рассмотрим примеры использования команды **net send** при отправке сообщений в рабочей группе (домене) 110. Чтобы отправить сообщение всем пользователям в рабочей группе 110 введите: **net send /domain:110 ПРОВЕРКА СВЯЗИ.** Другой вариант подобной команды: чтобы отправить сообщение всем пользователям в вашем домене введите: **net send * проверка связи** (рис. 12 и 13)



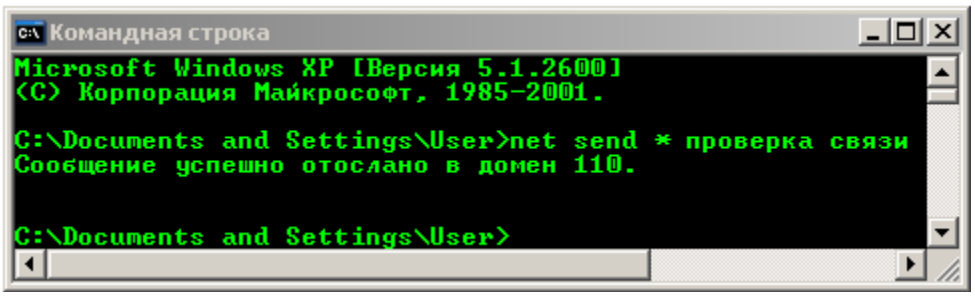


Рис. 12. Пример успешной отправки сообщения всем пользователям домена 110

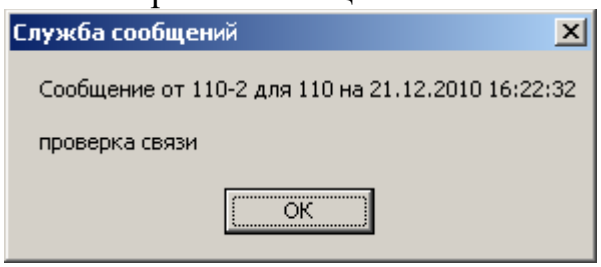


Рис. 13. Пример успешного получения сообщения от ПК 110-2 в рабочую группу 110

Чтобы отправить сообщение конкретному пользователю, например, 110-1, введите: **net send 110-1 ПРИВЕТ!** (рис. 14).

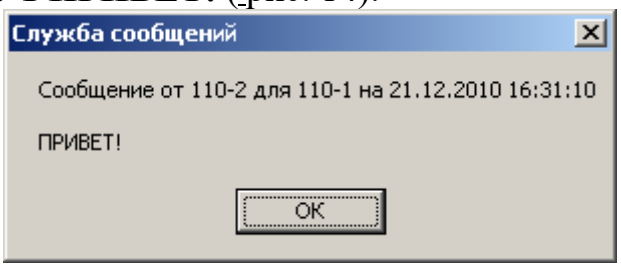


Рис. 14. Сообщение пользователю 110-1 доставлено

В Windows XP есть еще одна возможность отправки сообщений по сети. Выполните команды **Панель управления-Администрирование-Управление компьютером**. Дальше: **Действие-Все задачи-Отправка сообщения консоли**. Далее выбираете ПК и отправляете ему текст (рис. 15).

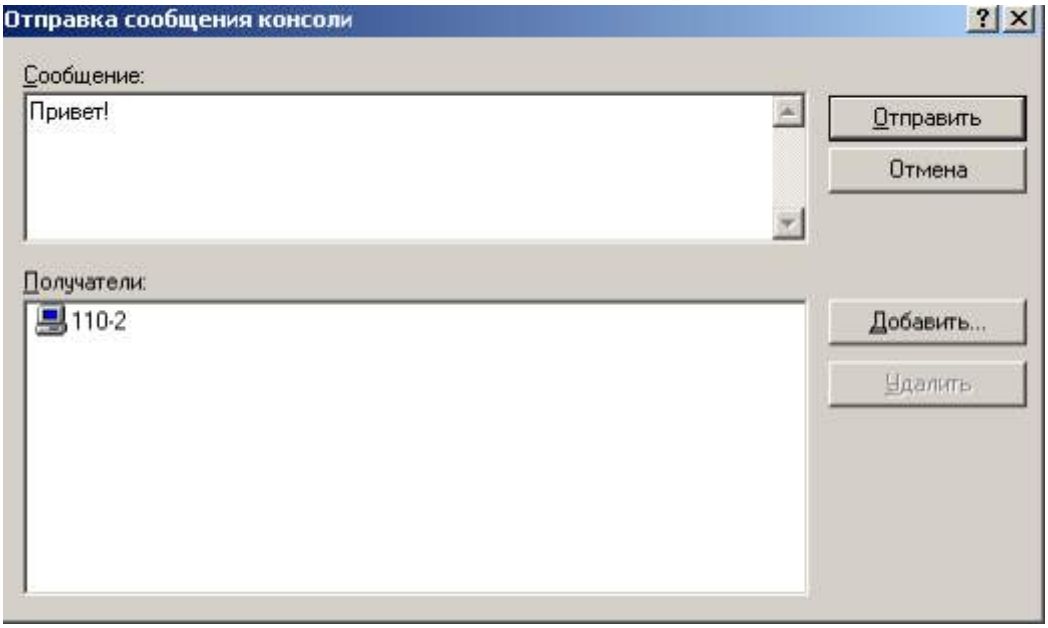


Рис. 15. Вариант отправки сообщения по сети без команды >net send

Примечание

Команда **net send** может блокироваться брандмауэром, поэтому его необходимо настроить или отключить (не желательно).

ПРАКТИЧЕСКАЯ РАБОТА №15.
МОНИТОРИНГ СОСТОЯНИЯ ЭЛЕМЕНТОВ СЕТИ

Цель работы: Научиться использовать команды Ping для проверки наличия связи компьютеров в сети и для анализа качества связи ПК, пользоваться командами PathPing, Ipconfig, Net view и Tracert

Задания для практического занятия:

Применение команды Ping для проверки наличия связи компьютеров в сети

Наиболее быстрым способом проверки работоспособности локальной можно назвать системную команду PING, которая посылает сетевой запрос на заданный IP-адрес компьютера, получает ответ и выводит отчет на экран. Если посланный запрос получен обратно - связь физически существует, то ваша сеть настроена и работает корректно. Если же на экране вы увидите надпись "Превышен интервал ожидания запрос" - вы допустили ошибку либо в настройках, либо в подключении компьютеров. Перед запуском команды Ping необходимо посмотреть доступные компьютеры в сети. Заходим в **Компьютер** 

и видим, что в нашей рабочей группе 110 имеется четыре ПК (рис. 1).

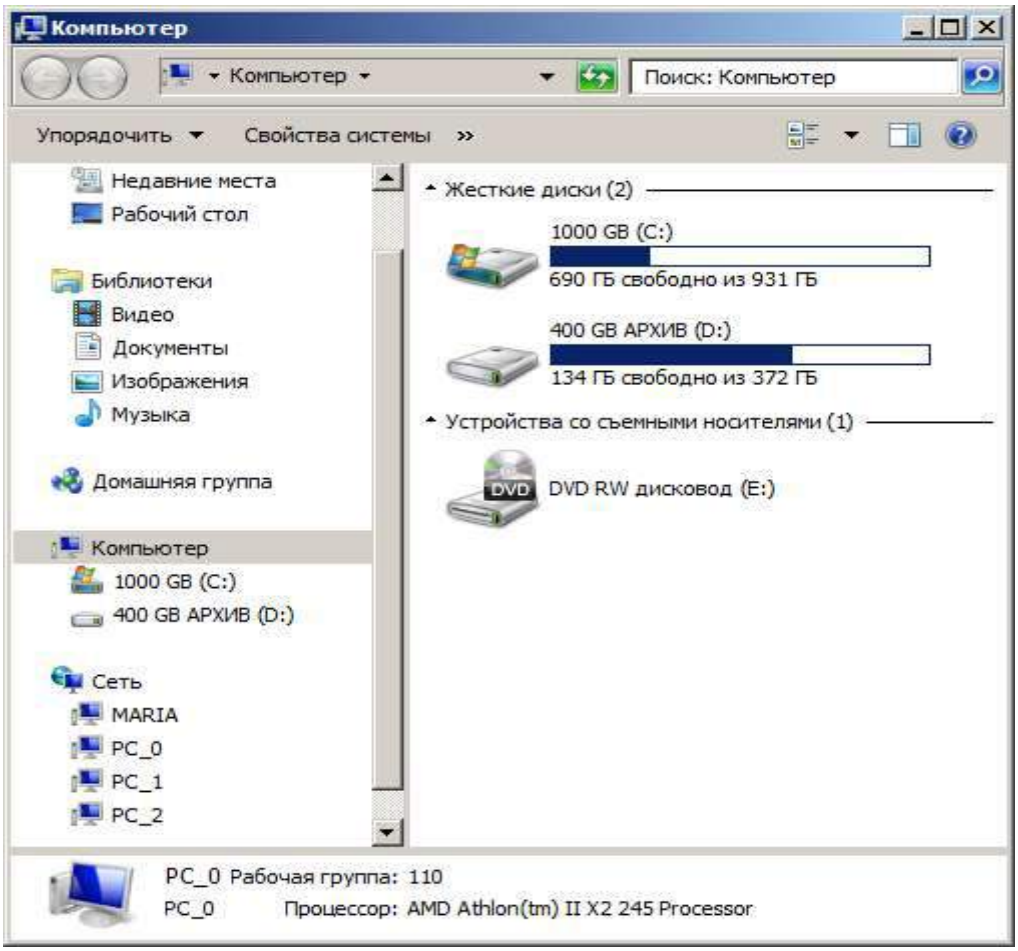


Рис. 1. В рабочей группе 110 мы видим 4 ПК

Для того чтобы воспользоваться командой ping, откройте окно командной строки командой **Пуск-Все программы-Стандартные-Командная строка** и введите там команду ping, укажите имя или IP-адрес удаленного компьютера (или его ИМЯ"/>) (рис. 2). По умолчанию утилита ping отправляет 4 пакета и ожидает каждый ответ в течение четырех секунд. По умолчанию команда посылает пакет 32 байта. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 миллисекунды"/>).

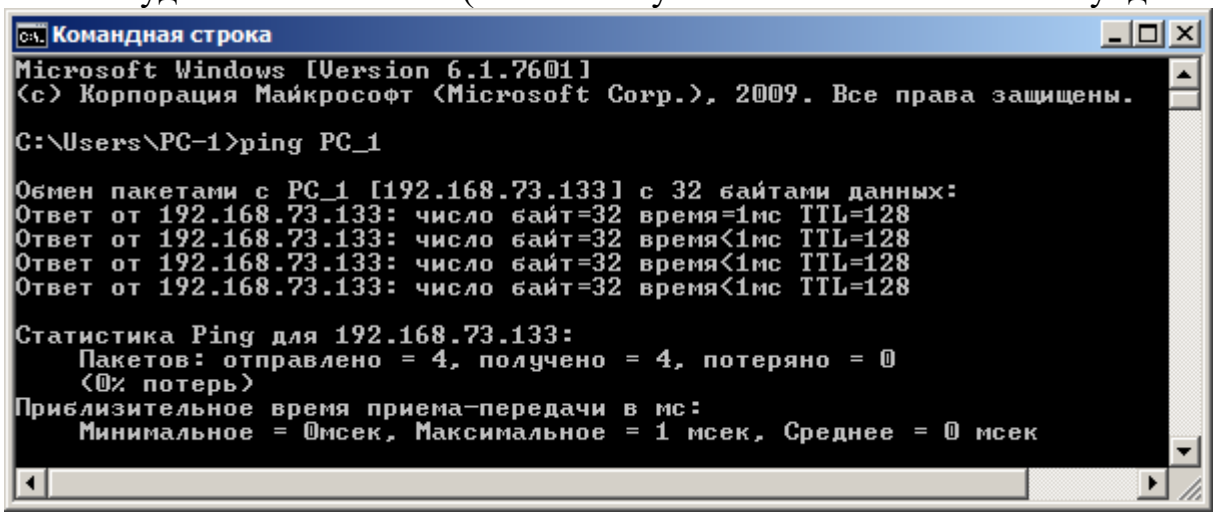


Рис. 2. Пингование машины PC_1 с IP-адресом 192.168.73.133

При необходимости для этой команды вы можете использовать следующие параметры:
-t. Данный параметр указывает на то, что производится проверка связи с указанным узлом до прекращения вручную;
-n. Текущий параметр определяет количество отправляемых Echo-запросов;
-f. Этот параметр устанавливает бит "не фрагментировать" на ping-пакете. По умолчанию фрагментация разрешается;
-w. Данный параметр позволяет настроить тайм-аут для каждого пакета в миллисекундах (по умолчанию установлено значение 4000"/>);
-a. Текущий параметр определяет имена узлов по адресам;
-l. При помощи этого параметра вы можете указать размер буфера отправки;
-i. Использование данного параметра позволяет вам задать срок жизни пакета;
-v. Этот параметр задает тип службы для IPv4 и не влияет на поле TOS в IP-заголовке;
-r. Текущий параметр записывает маршрут для указанного числа прыжков;
-s. Данный параметр позволяет отмечать время для указанного числа прыжков;
-j. Используя этот параметр, вы можете указать свободный выбор маршрута по списку узлов;
-k. При помощи данного параметра вы можете определить жесткий выбор маршрута по списку узлов;
-R. Текущий параметр позволяет использовать заголовок для проверки также и обратного маршрута только для IPv6;
-S. Данный параметр указывает используемый адрес источника;
-4. Параметр определяет принудительное использование протокола IP версии 4;
-6. Параметр определяет принудительное использование протокола IP версии 5.
Итак, выше было показано, что утилита **Ping** используется в том случае, когда необходимо проверить, может ли компьютер подключиться к сети TCP/IP или сетевым ресурсам. Иначе говоря, мы пингуем для того, чтобы проверить, что отправляемые пакеты доходят до получателя. ПК-отправитель отправляет Echo-запрос, а ПК-получатель, в ответ должен отправить ICMP-сообщение с ответом. Если удаленный компьютер реагирует на запрос ping, то подключение к удаленному компьютеру работает. Также, утилита ping ведет статистику, из которой понятно, сколько пакетов получено, а сколько потеряно. Но, это еще не все.

Применение команды Ping для анализа качества связи ПК в сети

Для тестирования качества связи запустите Ping со следующими параметрами: **ping.exe -l 16384 -w 5000 -n 100** 192.168.73.133. Это обеспечит отправку 100 запросов (n) пакетами по 16 килобайт (l) на заданный IP адрес с интервалом ожидания ответа в 0,5 секунды (w). То есть:
L – размер буфера отправки.
N – число отправляемых запросов,
W – время ожидания ответа на запрос в миллисекундах,
Подождите, пока пройдут все 100 пакетов. Ответ должен будет быть приблизительно такой (рис. 3).

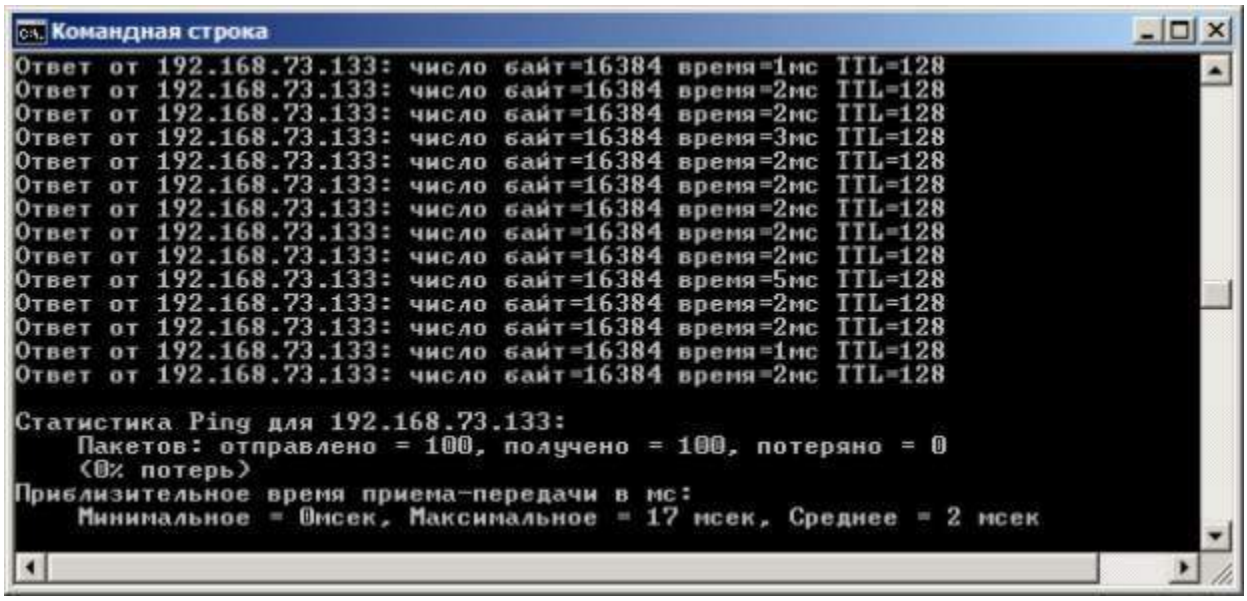


Рис. 3. Ответ на команду ping.exe с ключами

Проанализируем результат выполнения команды:

6. 0% потерь – сеть работает отлично.
7. Если потери информации составили не более 3%, то сеть работает хорошо.
8. При потерях 3-10% дошли не все пакеты, но сеть, благодаря алгоритмам коррекции ошибок, работает удовлетворительно. Необходимости повторной доставки потерянной информации снижается эффективная скорости работы сети – сеть тормозит.
9. Если число потерянных пакетов превышает 10-15%, то необходимо принять меры по устранению неисправности. Качество связи ПК неудовлетворительное.

Далее: как видим, время отклика удаленной системы среднее 2 мсек, а максимальное 17 мсек. Анализируя отклик по миллисекундам, надо иметь ввиду следующее. По стандарту, нормальное время отклика 16-килобайтного пакета для 100-мегабитной сети - 3-8 мс. Для 10-мегабитной - 30-80 мс. Получается, что у нас сеть работает на скорости порядка 100 мбит/сек.

Использование утилиты PathPing

Pathping это утилита, которая позволяет обнаружить потери пакетов на маршруте между вашим компьютером и заданным адресом IP. Потери пакетов могут сильно повлиять на работу сети, например, когда вы играете в видеоигру. Иначе говоря, утилита PathPing отправляет многочисленные сообщения с Echo-запросом каждому маршрутизатору, который находится между исходным пунктом и пунктом назначения, после чего, на основании пакетов, полученных от каждого из них, вычисляет процентное соотношение пакетов, возвращаемых в каждом прыжке. Поскольку утилита PathPing показывает степень потери пакетов на каждом маршрутизаторе или узле, то с ее помощью вы можете точно определить маршрутизаторы и узлы, на которых возникают сетевые проблемы. Пример использования данной команды приведен на рис. 4.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\PC-1>pathping MARIA

Трассировка маршрута к MARIA [192.168.1.2]
с максимальным числом прыжков 30:
  0  PC_0 [192.168.1.3]
  1  MARIA [192.168.1.2]

Подсчет статистики за: 25 сек. ...
            Исходный узел      Маршрутный узел
Прыжок   RTT    Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                              PC_0 [192.168.1.3]
                                 0/ 100 =  0%    |
  1    2мс      0/ 100 =  0%     0/ 100 =  0%  MARIA [192.168.1.2]

Трассировка завершена.
```

Рис. 4. Поиск потерь пакетов на маршруте от ПК PC_0 до ПК MAIRIA

Итак, в строке поиска наберем **CMD**, чтобы вызвать командную строку (рис. 5).

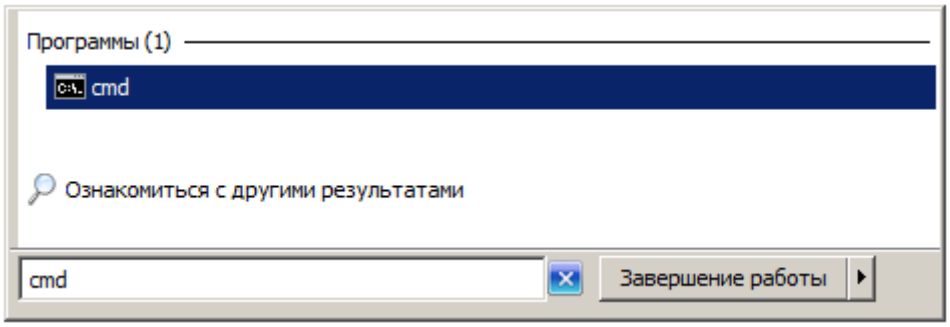


Рис. 5. Один из способов вызова командной строки в ОС Windows 7

Далее произведет трассировку маршрута от нашего ПК до поискового сервера Яндекс (_рис. 6).

```
C:\Windows\system32\cmd.exe

C:\Users\PC-1>pathping yandex.ru

Трассировка маршрута к yandex.ru [213.180.204.11]
с максимальным числом прыжков 30:
  0  PC_0 [192.168.1.3]
  1  192.168.1.1
  2  lo0-at66-2.natm.ru [213.148.173.214]
  3  at66-ats66-L3-giga-core.natm.ru [213.148.163.81]
  4  ATS3-TGE1-8-TTS-TGE1-4.natm.ru [78.81.0.37]
  5  GWay-TGE0-2.natm.ru [78.81.0.254]
  6  ge-0-1-0-vl988-10g.M320-1-NOVG.nwtelecom.ru [212.48.214.53]
  7  ae1-30g.MX960-1-MMT.nwtelecom.ru [212.48.198.246]
  8  as13238-yandex.gateway.nwtelecom.ru [212.48.214.102]
  9     *        *        *
Подсчет статистики за: 200 сек. ...
           Исходный узел      Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                            PC_0 [192.168.1.3]
                                 0/ 100 =  0%    |
  1    1мс     0/ 100 =  0%      0/ 100 =  0%  192.168.1.1
                                 0/ 100 =  0%    |
  2    1мс     0/ 100 =  0%      0/ 100 =  0%  lo0-at66-2.natm.ru [213.148.1
4]
                                 0/ 100 =  0%    |
  3    2мс     0/ 100 =  0%      0/ 100 =  0%  at66-ats66-L3-giga-core.natm.
13.148.163.81]
                                 0/ 100 =  0%    |
  4    1мс     0/ 100 =  0%      0/ 100 =  0%  ATS3-TGE1-8-TTS-TGE1-4.natm.r
.81.0.37]
                                 0/ 100 =  0%    |
  5    3мс     0/ 100 =  0%      0/ 100 =  0%  GWay-TGE0-2.natm.ru [78.81.0.

                                 0/ 100 =  0%    |
  6    2мс     0/ 100 =  0%      0/ 100 =  0%  ge-0-1-0-vl988-10g.M320-1-NOV
elecom.ru [212.48.214.53]
                                 0/ 100 =  0%    |
  7   11мс     0/ 100 =  0%      0/ 100 =  0%  ae1-30g.MX960-1-MMT.nwtelecom
212.48.198.246]
                               100/ 100 =100%    |
  8  ---     100/ 100 =100%      0/ 100 =  0%  as13238-yandex.gateway.nwtele
u [212.48.214.102]

Трассировка завершена.
```

Рис. 6. Пример использования утилиты Pathping

Проанализируем результат:

7. Первый блок информации представляет собой трассировку. Вы может пропустить его и перейти ко второму блоку информации, в котором будет указано процентное отношение потерь пакетов.
8. Если пакеты не терялись на данном маршруте подключения, то вы увидите 0% потерь пакетов. Если вы увидите значения, отличающиеся от 0%, это означает, что на пути к нашим серверам были потери пакетов. Потери выше 1% начиная с первого шага, могут указывать на некорректную работу узлов сети или маршрутизаторов. Если эти устройства вам доступны, то нужно попробовать обновить их программное обеспечение или полностью заменить их. Иначе, о потерях, возникших после первого шага и до последнего шага, следует сообщить вашему Интернет провайдеру.

Примечание

Если последние строки указывают на 100% потерь, то это не является показателем проблемы, а происходит потому, что сервера защищены от нежелательного трафика и атак.

С данной командой вы можете использовать следующие параметры:

-g. Данный параметр определяет использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных мест назначения для сообщений с Echo-запросом, который указывается в списке компьютеров.

-h. Данный параметр задает максимальное количество переходов на пути при поиске конечного объекта;

-i. Этот параметр указывает IP-адрес источника;

-n. Текущий параметр предотвращает попытки сопоставления IP-адресов промежуточных маршрутизаторов с их именами, что существенно ускоряет вывод результатов;

-p. Используя данный параметр, вы можете задать время ожидания между последовательными проверками связи, где значением по умолчанию указано 250 миллисекунд;

-q. При помощи текущего параметра вы можете указать количество сообщений с Echo-запросом, отправленных каждому маршрутизатору пути (по умолчанию - 100);

-w. Данный параметр определяет время ожидания для получения Echo-ответов протокола ICMP или ICMP-сообщений об истечении времени в миллисекундах, которые соответствуют данному сообщению Echo-запроса. Значение по умолчанию 4 секунды;

-4. Параметр определяет принудительное использование протокола IP версии 4;

-6. Параметр определяет принудительное использование протокола IP версии 5.

Другие команды командной строки. Отображение параметров TCP/IP-протокола командой Ipconfig

Команда **IPCONFIG** используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола DHCP. Предположим, что у нас имеется сеть, изображенная на- рис. 7.

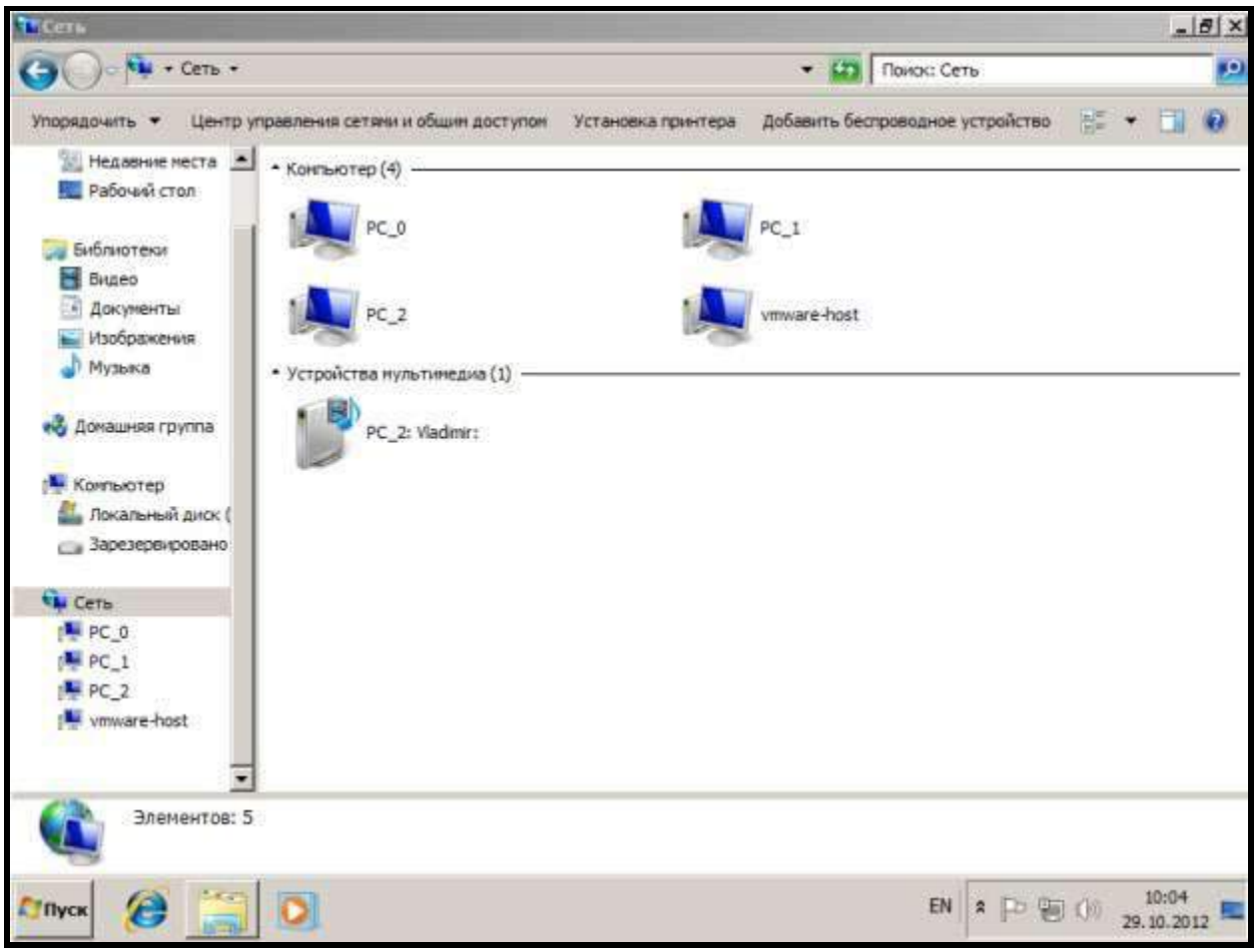
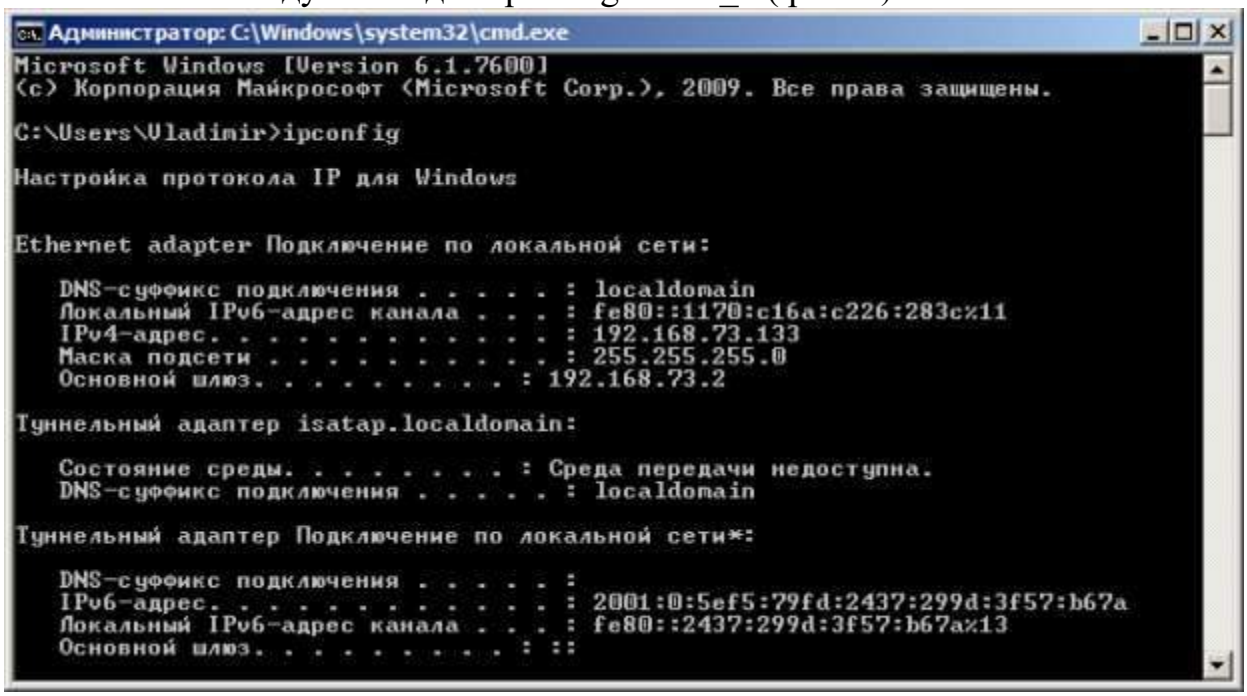


Рис. 7. Небольшая локальная сеть

Выполним команду командой Ipconfig на PC_2 (рис. 8).



```
Администратор: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Vladimir>ipconfig

Настройка протокола IP для Windows


Ethernet adapter Подключение по локальной сети:

   DNS-суффикс подключения . . . . . : localdomain
   Локальный IPv6-адрес канала . . . : fe80::1170:c16a:c226:283c%11
   IPv4-адрес. . . . . . . . . . . . : 192.168.73.133
   Маска подсети . . . . . . . . . . : 255.255.255.0
   Основной шлюз. . . . . . . . . . : 192.168.73.2

Туннельный адаптер isatap.localdomain:

   Состояние среды. . . . . . . . . : Среда передачи недоступна.
   DNS-суффикс подключения . . . . . : localdomain

Туннельный адаптер Подключение по локальной сети*:

   DNS-суффикс подключения . . . . . :
   IPv6-адрес. . . . . . . . . . . . : 2001:0:5ef5:79fd:2437:299d:3f57:b67a
   Локальный IPv6-адрес канала . . . : fe80::2437:299d:3f57:b67a%13
   Основной шлюз. . . . . . . . . . : ::
```

Рис. 8. Отображение параметров TCP/IP-протокола командой Ipconfig

Из отчета мы видим такую информацию:

– DNS-суффикс подключения - local domain (из настроек сетевого подключения)
– Локальный IPv6-адрес канала - локальный IPv6 адрес, если используется адресация IPv6
– IPv4-адрес - используемый для данного адаптера IPv4 – адрес
– Маска подсети - 255.255.225.0
– Основной шлюз - IP - адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Примечание

Туннельный адаптер isatap.localdomain это эмуляция IPV6 в сетях IPV4. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) — Протокол автоматической внутрисайтовой адресации туннелей, позволяющий передавать между сетями IPv6 пакеты через сети IPv4

Ключи команды:

/all Отображение полной информации по всем адаптерам.

/release [адаптер] Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан) или для заданного адаптера. Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

/renew [адаптер] Обновление IP-адреса для определённого адаптера или если адаптер не задан, то для всех. Доступно только при настроенном автоматическом получении IP-адресов.

/flushdns Очищение DNS кэша.

/registerdns Обновление всех зарезервированных адресов DHCP и перерегистрация имен DNS.

/displaydns Отображение содержимого кэша DNS.

/showclassid адаптер Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическим получением IP-адресов.

/setclassid адаптер [код_класса] Изменение кода класса DHCP. Доступно только при настроенном автоматическим получением IP-адресов.

/? Справка. TCP/IP: значения IP адреса, маски и шлюза.

Команда вывода списка компьютеров рабочей группы Net view

В командной строке введите команду **net view,** и вы увидите список компьютеров своей рабочей группы (рис. 9).

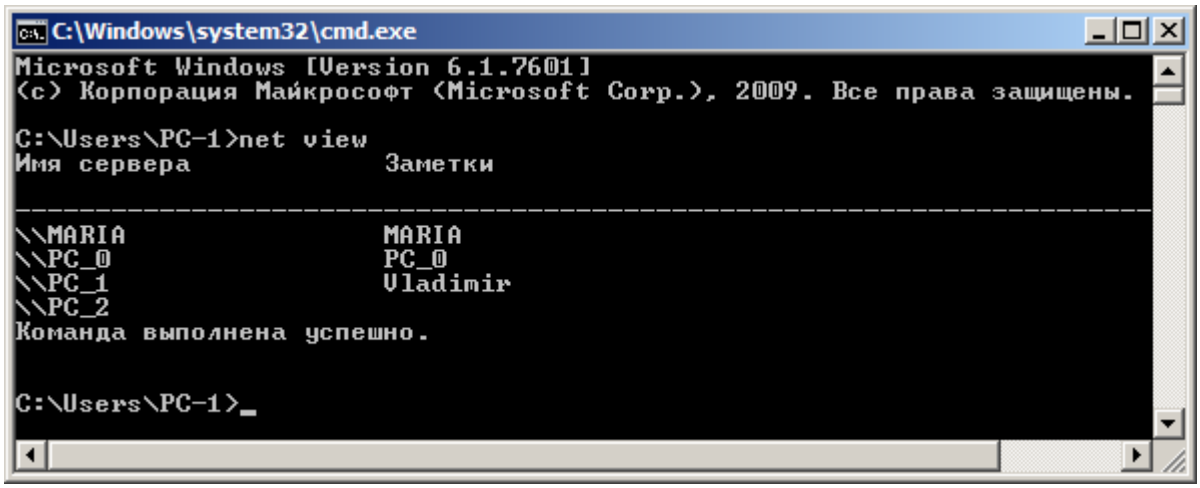


Рис. 9. В рабочей группе имеется 4 ПК

Трассировка

Tracert — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Программа tracert выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

Запуск программы производится из командной строки. Для этого вы должны войти в неё. Для операционной системы Windows 7 существует несколько способов запуска командной строки:

Сочетание клавиш Win (кнопка с логотипом Windows) + R (должны быть нажаты одновременно) — В графе "Открыть" написать "cmd" и нажать Ок.

Пуск — Все программы— Стандартные — Командная строка.

В открывшемся окне мы напишем **tracert ya.ru**. Принцип действия этой программы схож с принципом действия программы ping. Команда отправляет на сервер данные и при этом фиксирует все промежуточные маршрутизаторы, через которые проходят эти данные на пути к серверу (целевому узлу). Если при доставке данных до одного из узлов происходит проблема, программа определяет участок сети, на котором возникли неполадки. Время отклика показывает загруженность канала. А вот если вместо времени отклика вы видите надпись **"Превышен интервал ожидания для запроса"**, это значит, что на данном узле связи происходит потеря данных, а значит, проблема именно в нем – рис. 10.

```
C:\Windows\system32\cmd.exe
C:\Users\PC-1>tracert ya.ru

Трассировка маршрута к ya.ru [87.250.250.3]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  192.168.1.1
  2     4 ms     1 ms     1 ms  lo0-at66.natm.ru [213.148.173.223]
  3     4 ms     2 ms     2 ms  at66-ats66-L3-giga-core.natm.ru [213.148.163.81]

  4     4 ms    14 ms     6 ms  ATS3-TGE1-8-TTS-TGE1-4.natm.ru [78.81.0.37]
  5     3 ms     3 ms     4 ms  GWay-TGE0-2.natm.ru [78.81.0.254]
  6     4 ms     1 ms     1 ms  ge-0-1-0-vl988-10g.M320-1-NOVG.nwtelecom.ru [212
.48.214.53]
  7    10 ms     9 ms     9 ms  ae1-30g.MX960-1-MMT.nwtelecom.ru [212.48.198.246
]
  8    10 ms     9 ms     9 ms  as13238-yandex.gateway.nwtelecom.ru [212.48.214.
102]
  9     *        *        *     Превышен интервал ожидания для запроса.
 10    16 ms    16 ms    16 ms  s600-61.yandex.net [87.250.239.36]
 11    17 ms    18 ms    18 ms  13-s3600-s600.yandex.net [213.180.213.53]
 12    18 ms    17 ms    17 ms  www.yandex.ru [87.250.250.3]

Трассировка завершена.

C:\Users\PC-1>
```

Рис. 10. Пример трассировки домена ya.ru

Параметры команды tracert:

-d не определять доменные имена маршрутизаторов

-h <значение-> установить максимальное количество переходов

-w <значение> установить максимальное время ожидания ответа (в миллисекундах)

Итак, трассировка маршрута помогает определить проблемный узел. Если данные проходят нормально и "стопорятся" на самом пункте назначения, то проблема действительно с сайтом. Если трассировка маршрута прекращается на середине пути, то проблема в одном из промежуточных маршрутизаторов. Если прохождение пакетов прекращается в пределах сети вашего провайдера — то и проблему нужно решать "на местном уровне". Попутно хочется отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети.

ПРАКТИЧЕСКАЯ РАБОТА №16.
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛОКАЛЬНОЙ СЕТИ

Цель работы:
Научиться обеспечивать безопасность локальной сети

Шаг 1. Меняем учетную запись администратора (Пользователь Администратор с пустым паролем - это уязвимость)

Часто при установке Windows пароль администратора пустой и этим может воспользоваться злоумышленник. Иначе говоря, при установке Windows XP в автоматическом режиме с настройками по умолчанию мы имеем пользователя **Администратор** с пустым паролем и любой **User** может войти в такой ПК с правами администратора. Чтобы решить проблему выполним команду **Мой компьютер-Панель управления-Администрирование-Управление компьютером-Локальные пользователи-Пользователи**

(рис. 1).

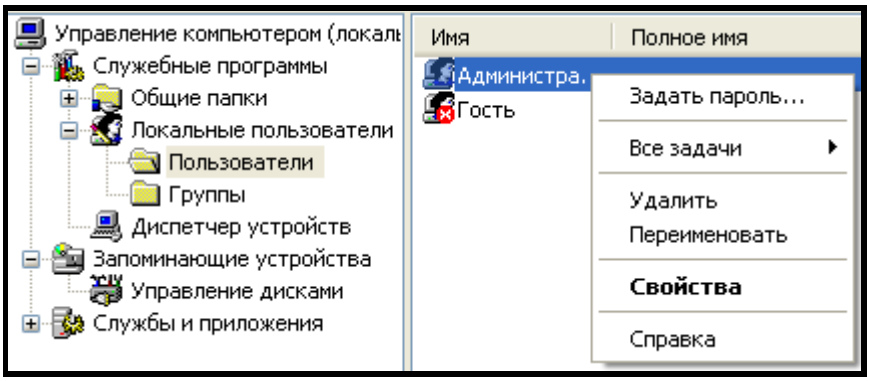


Рис. 1. Окно Управление компьютером

Здесь по щелчку правой кнопкой мыши на **Администраторы** зададим администратору пароль, например, 12345. Это плохой пароль, но лучше, чем ничего. Теперь в окне **Администрирование** зайдем в **Локальную политику безопасности**. Далее идем по веткам дерева: **Локальные политики-Параметры безопасности-Учетные записи: Переименование учетной записи Администратор** (рис. 2).

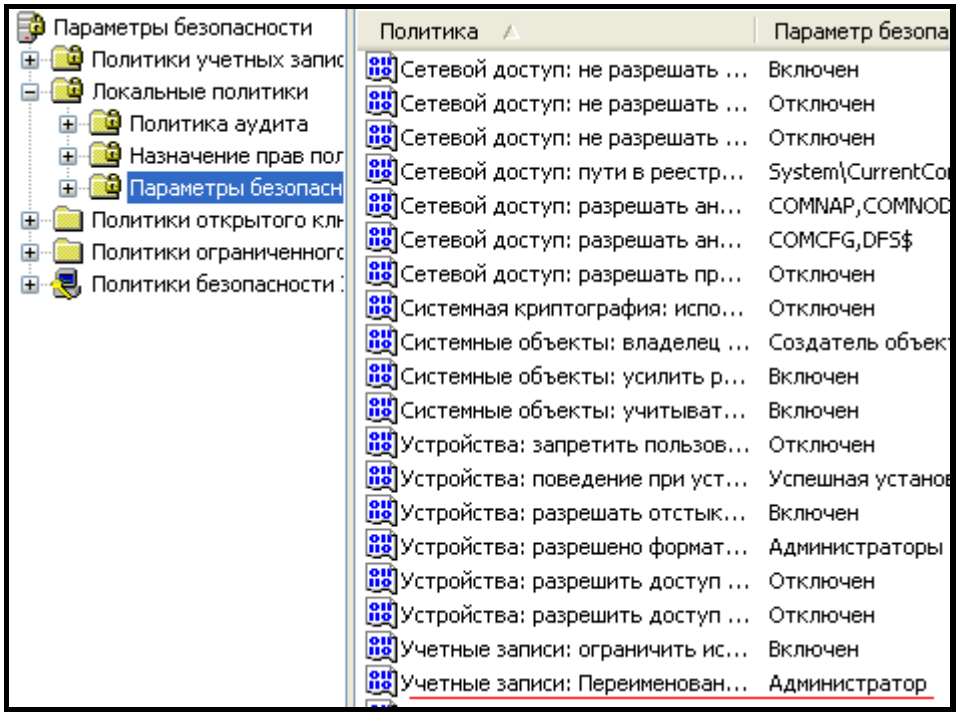


Рис. 2. Находим в системном реестре запись Переименование учетной записи Администратор

Здесь пользователя **Администратор** заменим на **Admin** (рис. 3).

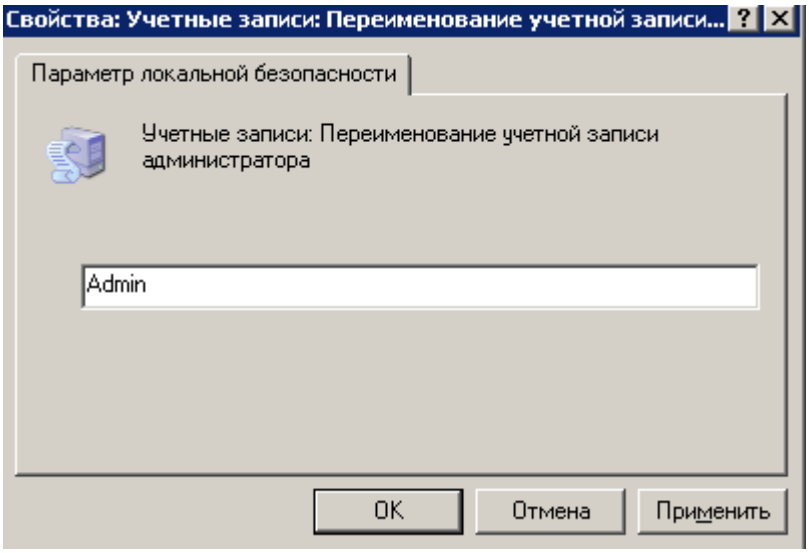


Рис. .3. Пользователю Администратор присваиваем новое имя

Перезагружаем ОС. После наших действий у нас получилась учетная запись Admin с паролем 12345 и правами администратора (рис. 4).

Рис. 4. Окно входа в ОС Windows XP

Все, теперь мы имеем пользователя **Администратор** с паролем, одна из уязвимостей системы устранена.

Примечание

Операцию по изменению имени пользователя и заданию пароля мы также могли бы выполнить без использования системного реестра, использовав окно **Учетные записи пользователей**, что гораздо проще (рис. 5).

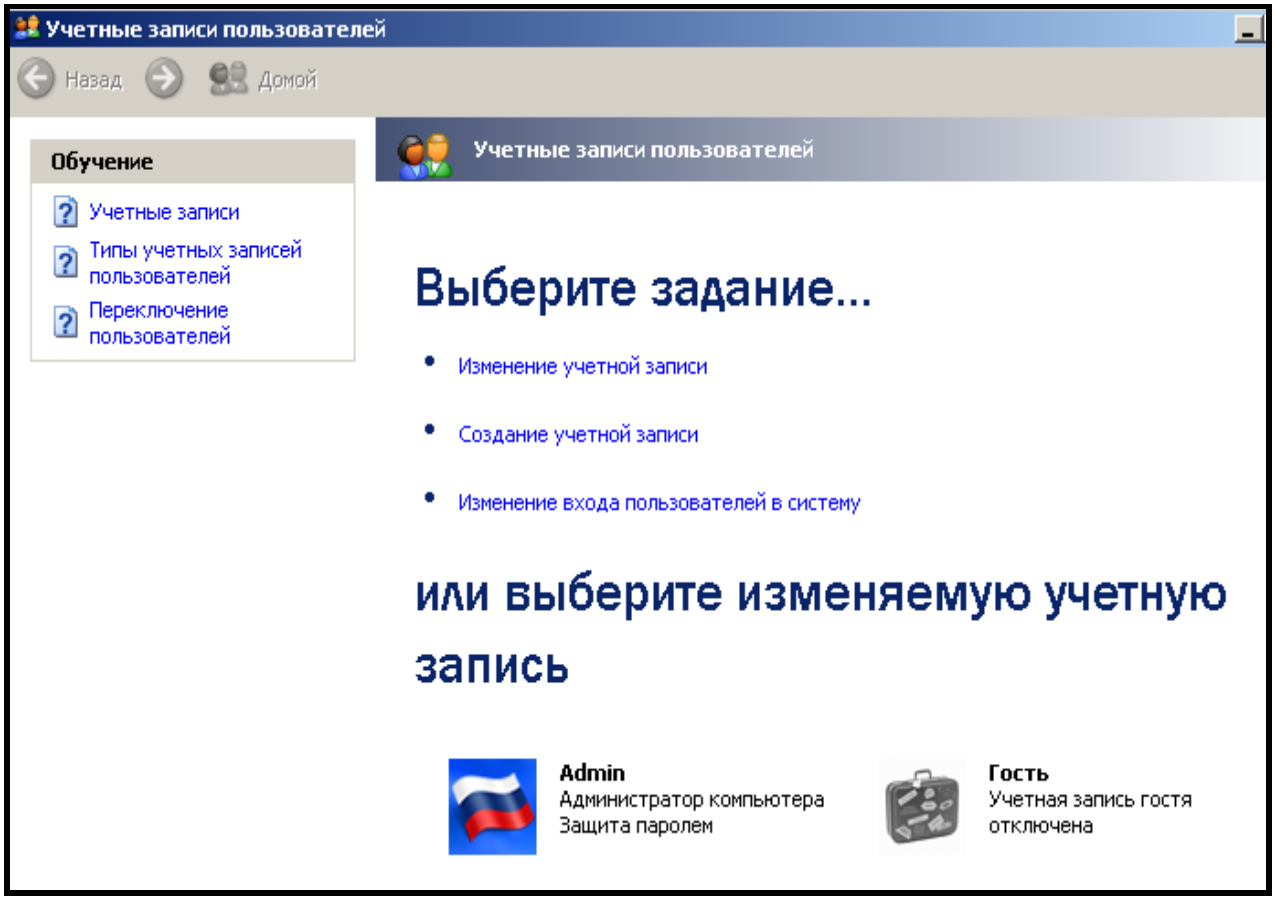


Рис. 5. Окно Учетные записи пользователей

Примечание

Учетная запись Гость позволяет входить в ПК и работать на нем (например, в Интернет) без использования специально созданной учетной записи. Запись Гость не требует ввода пароля и по умолчанию блокирована. Гость не может устанавливать или удалять программы. Эту учетную запись можно отключить, но нельзя удалить.

Шаг 2. **Делаем окно приветствия пустым (убираем уязвимость 2)**

У нас окно входа в систему содержит подсказку Admin, давайте ее уберем, сделав окно пустым. Для начала в окне **Учетные записи пользователей** жмем на кнопку **Изменение входа пользователей в систему** и уберем флажок **Использовать страницу приветствия** (рис. 6 и рис. 7).

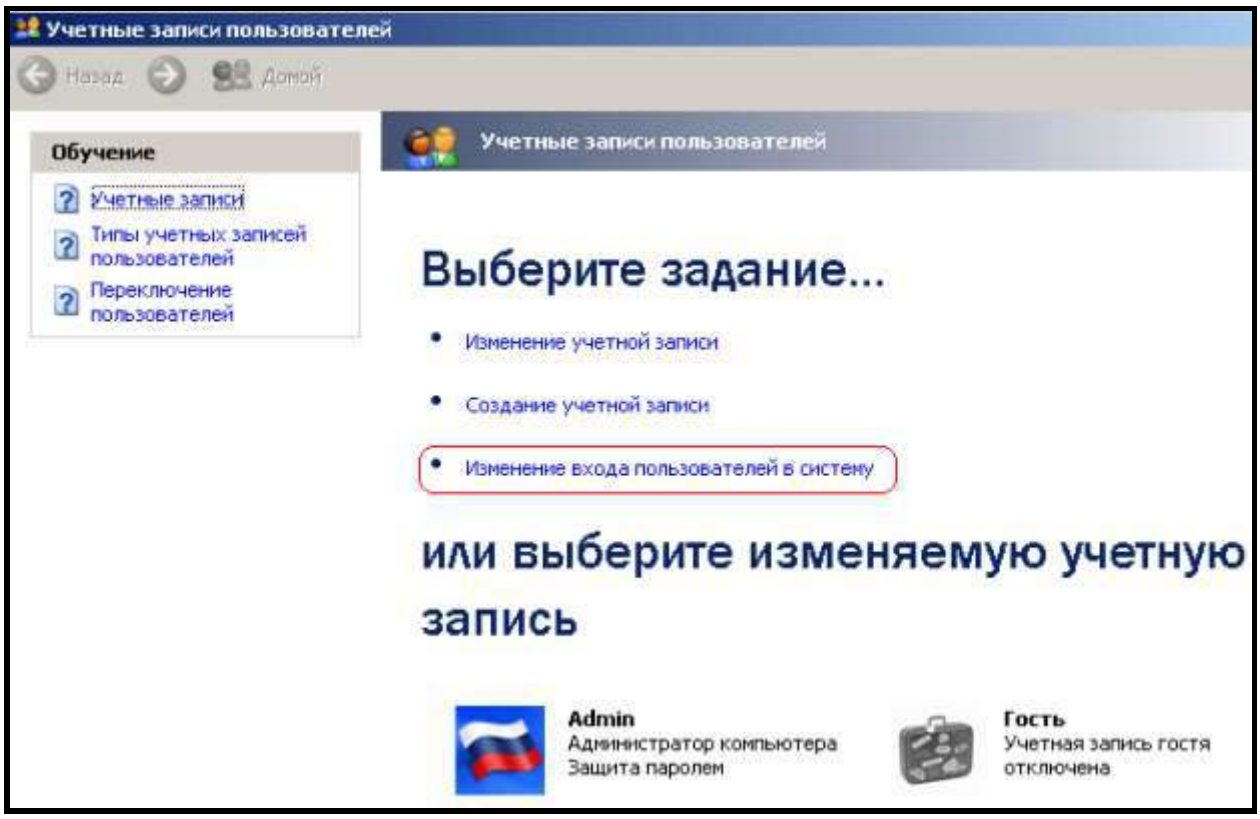


Рис. 6. Окно Учетные записи пользователей

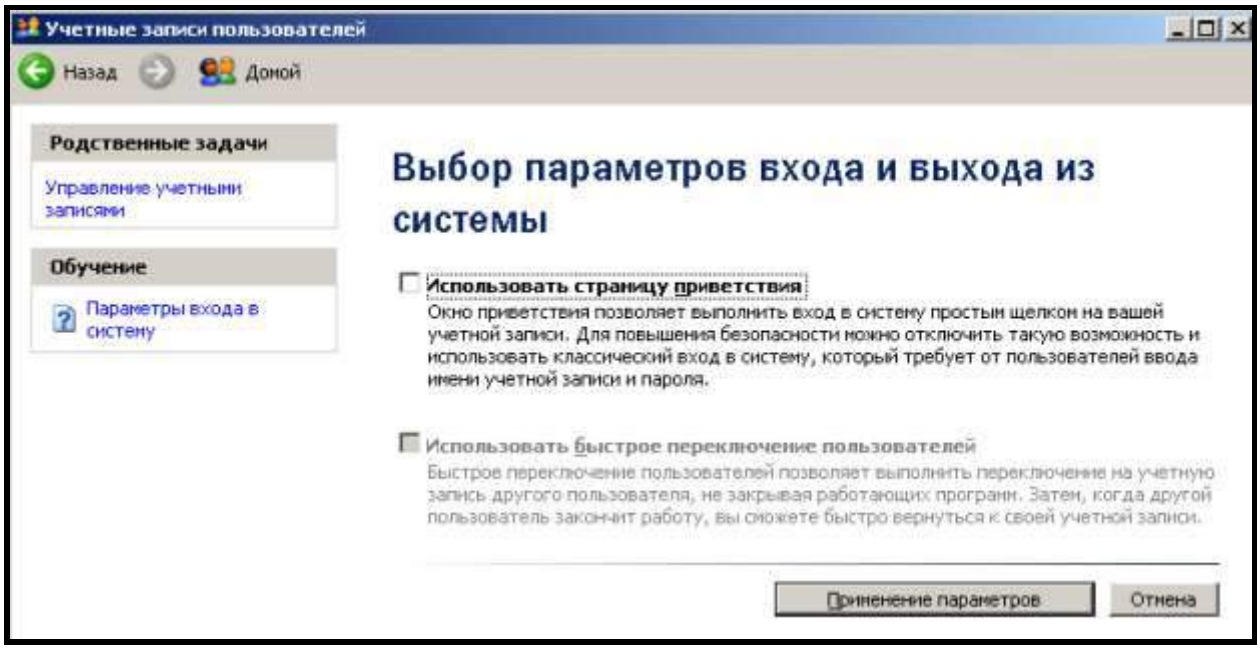


Рис. 7. Убираем флажок Использовать страницу приветствия

Но, это только половина дела. Теперь повысим безопасность сети еще на одну условную ступень, сделав оба поля окна приветствия пустыми (рис. 8).

Рис. 8. Обе строки данного окна сделаем пустыми

Выполним команду **Панель управления-Администрирование – Локальные политики безопасности- Локальные политики-Параметры безопасности-Интерактивный вход: не отображать последнего имени пользователя**. Эту запись необходимо включить (рис. 9).

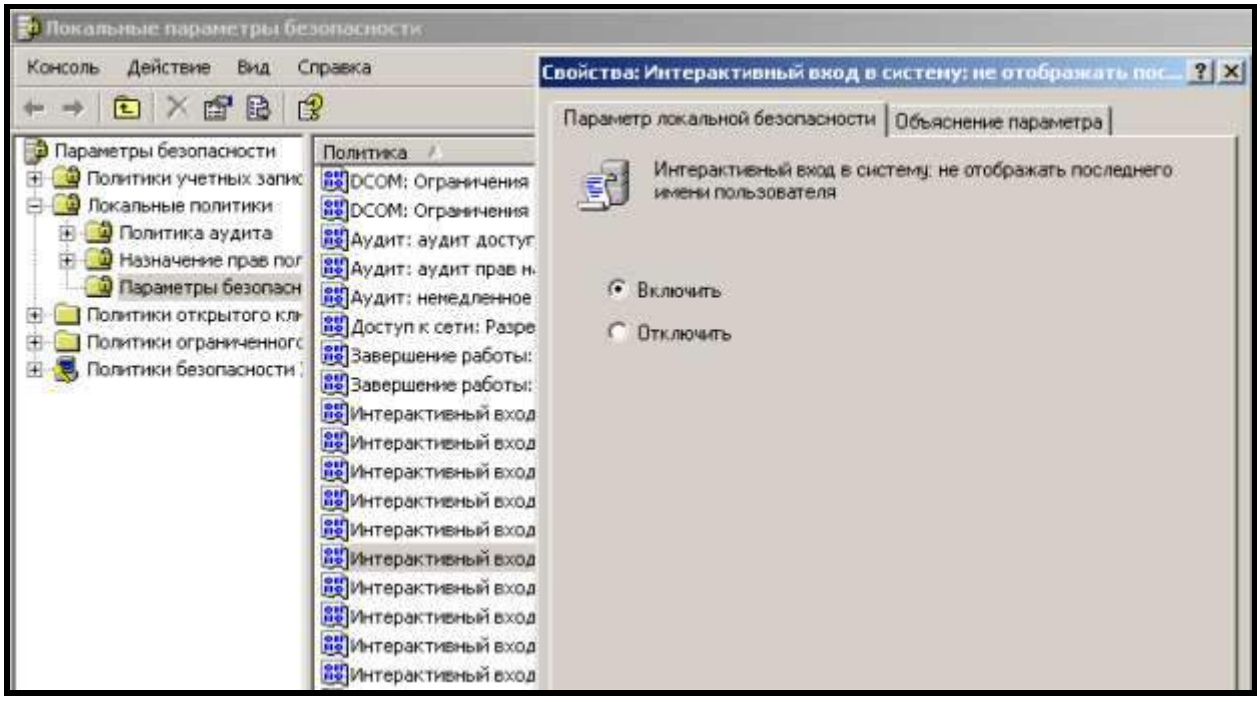


Рис. 9. Активируем переключатель Включить

Теперь после завершения сеанса пользователь должен угадать не только пароль, но и имя пользователя (рис. 10).

Рис. 10. Обе строки окна приветствия пусты

Выявление сетевых уязвимостей сканированием портов ПК

Злоумышленники используют сканирование портов ПК для того, чтобы воспользоваться ресурсами чужого ПК в Сети. При этом необходимо указать **IP** адрес ПК и открытый **port,** к примеру, **195.34.34.30:23**. После этого происходит соединение с удаленным ПК с некоторой вероятностью входа в этот ПК.

- TCP/IP port — это адрес определенного сервиса (программы), запущенного на данном компьютере в Internet. Каждый открытый порт — потенциальная лазейка для взломщиков сетей и ПК. Например, SMTP (отправка почты) — 25 порт, WWW — 80 порт, FTP —21 порт.
- Хакеры сканируют порты для того, чтобы найти дырку (баг) в операционной системе. Пример ошибки, если администратор или пользователь ПК открыл полный доступ к сетевым ресурсам для всех или оставил пустой пароль на вход к компьютер.

Одна из функций администратора сети (сисадмина) - выявить недостатки в функционировании сети и устранить их. Для этого нужно просканировать сеть и закрыть (блокировать) все необязательные (открытые без необходимости) сетевые порты. Ниже, для примера, представлены службы TCP/IP, которые можно отключить:

- finger - получение информации о пользователях
- talk- возможность обмена данными по сети между пользователями
- bootp - предоставление клиентам информации о сети
- systat - получение информации о системе
- netstat - получение информации о сети, такой как текущие соединения
- rusersd - получение информации о пользователях, зарегистрированных в данный момент

Просмотр активных подключений утилитой Netstat

Команда **netstat** обладает набором ключей для отображения портов, находящихся в активном и/или пассивном состоянии. С ее помощью можно получить список серверных приложений, работающих на данном компьютере. Большинство серверов находится в режиме **LISTEN** - ожидание запроса на соединение. Состояние **CLOSE_WAIT** означает, что соединение разорвано. **TIME_WAIT** - соединение ожидает разрыва. Если соединение находится в состоянии **SYN_SENT**, то это означает наличие процесса, который пытается, установить соединение с сервером. **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются).

Итак, команда netstat показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций. Для сокетов (программных интерфейсов) TCP допустимы следующие значения состояния

- CLOSED - Закрыт. Сокет не используется.
- LISTEN - Ожидает входящих соединений.
- SYN_SENT - Активно пытается установить соединение.
- SYN_RECEIVED - Идет начальная синхронизация соединения.
- ESTABLISHED - Соединение установлено.
- CLOSE_WAIT - Удаленная сторона отключилась; ожидание закрытия сокета.
- FIN_WAIT_1 - Сокет закрыт; отключение соединения.
- CLOSING - Сокет закрыт, затем удаленная сторона отключилась; ожидание подтверждения.
- LAST_ACK - Удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения.
- FIN_WAIT_2 - Сокет закрыт; ожидание отключения удаленной стороны.
- TIME_WAIT - Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки

Примечание

Что такое "сокет" поясняет рис. 11. Пример сокета – 194.86.6..54:21

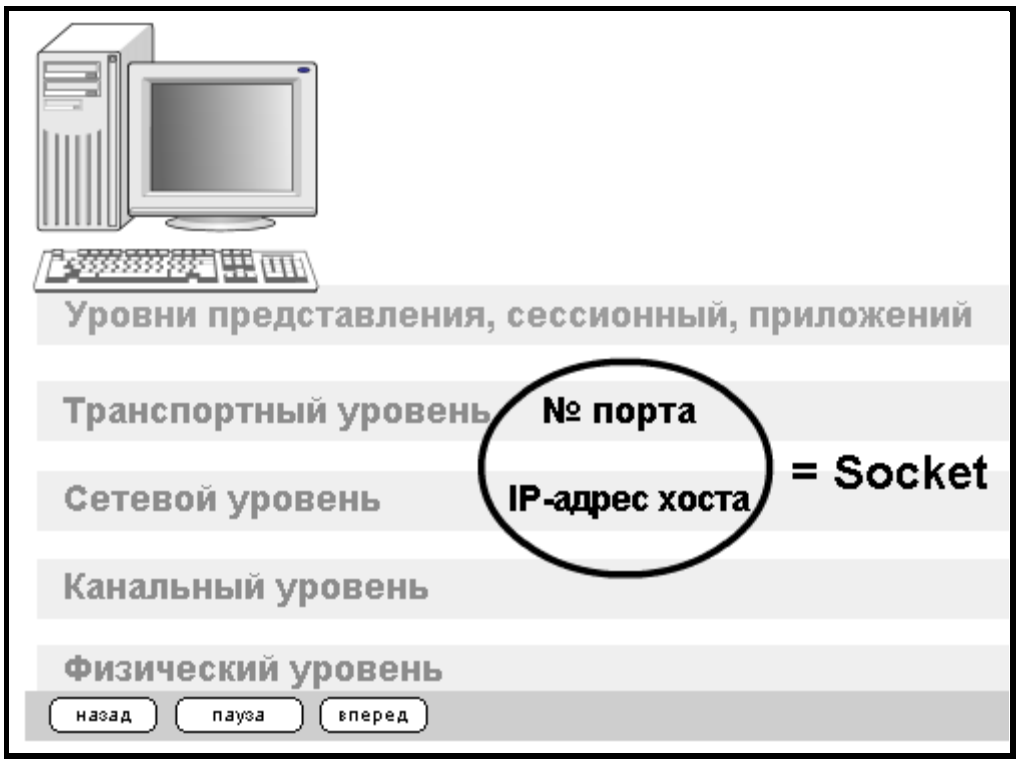


Рис. 11. Сокет это № порта + IP адрес хоста

Практический пример. Обнаружение открытых на ПК портов утилитой Netstat

Для выполнения практического задания на компьютере необходимо выполнить команду **Пуск-Выполнить**. Откроется окно **Запуск программы**, в нем введите команду **cmd** (рис. 12).

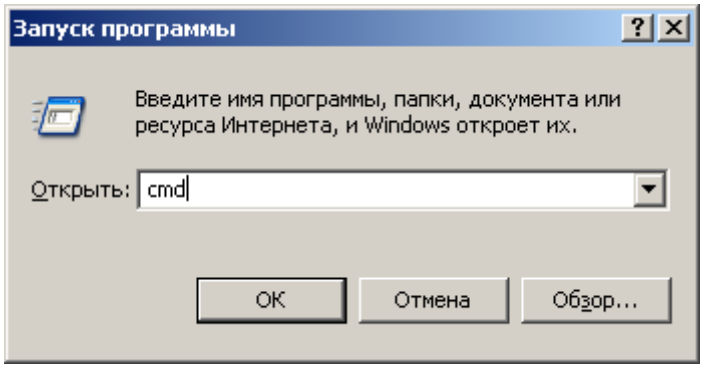


Рис. 12. Окно Запуск программы

Чтобы вывести все активные подключения TCP и прослушиваемые компьютером порты TCP/ UDP введите команду **netstat** (рис. 13). Мы видим Локального адреса (это ваш ПК) прослушиваются 6 портов. Они нужны для поддержки сети. На двух портах мы видим режим **ESTABLISHED** — соединения установлены, т.е. сетевые службы работают (используются). Четыре порта используются в режиме **TIME_WAIT** - соединение ожидает разрыва.

```
Активные подключения

  Имя     Локальный адрес         Внешний адрес           Состояние
  TCP     D:3086                  localhost:3087          ESTABLISHED
  TCP     D:3087                  localhost:3086          ESTABLISHED
  TCP     D:3414                  localhost:1110          TIME_WAIT
  TCP     D:3416                  localhost:1110          TIME_WAIT
  TCP     D:3415                  OCSP.AMS1.VERISIGN.COM:http  TIME_WAIT
  TCP     D:3417                  OCSP.AMS1.VERISIGN.COM:http  TIME_WAIT

D:\Documents and Settings\110>
```

Рис. 13. Список активных подключений на тестируемом ПК

Запустите на вашем ПК Интернет и зайдите, например на **www.yandex.ru**. Снова выполните команду **netstat** (рис. 14). Как видим, добавилось несколько новых активных портов с их различными состояниями.

```
D:\Documents and Settings\110>netstat

Активные подключения

  Имя     Локальный адрес         Внешний адрес           Состояние
  TCP     D:1110                  localhost:3433          TIME_WAIT
  TCP     D:1110                  localhost:3436          TIME_WAIT
  TCP     D:1110                  localhost:3441          TIME_WAIT
  TCP     D:1110                  localhost:3442          TIME_WAIT
  TCP     D:1110                  localhost:3443          TIME_WAIT
  TCP     D:1110                  localhost:3448          ESTABLISHED
  TCP     D:1110                  localhost:3452          TIME_WAIT
  TCP     D:1110                  localhost:3454          ESTABLISHED
  TCP     D:1110                  localhost:3456          TIME_WAIT
  TCP     D:3430                  localhost:3431          ESTABLISHED
  TCP     D:3431                  localhost:3430          ESTABLISHED
  TCP     D:3432                  localhost:1110          TIME_WAIT
  TCP     D:3438                  localhost:1110          TIME_WAIT
  TCP     D:3440                  localhost:1110          TIME_WAIT
  TCP     D:3448                  localhost:1110          ESTABLISHED
  TCP     D:3450                  localhost:1110          TIME_WAIT
  TCP     D:3454                  localhost:1110          ESTABLISHED
  TCP     D:3458                  localhost:1110          TIME_WAIT
  TCP     D:3460                  localhost:1110          TIME_WAIT
  TCP     D:3461                  localhost:1110          TIME_WAIT
  TCP     D:3462                  localhost:1110          TIME_WAIT
  TCP     D:3434                  addons-star.zlb.phx.mozilla.net:https  TIME_WAIT

  TCP     D:3445                  static.yandex.net:http  TIME_WAIT
  TCP     D:3449                  mc.yandex.ru:http       ESTABLISHED
  TCP     D:3455                  suggest.yandex.net:http  ESTABLISHED
  TCP     D:3463                  suggest.yandex.net:http  TIME_WAIT
  TCP     D:3464                  www.yandex.ru:http      TIME_WAIT
  TCP     D:3465                  yabs.yandex.ru:http     TIME_WAIT
```

Рис. 14. Активные подключения при работе ПК в Интернет

Команда **netstat** имеет следующие опции – табл. 1.

Таблица 1. Ключи для команды netstat	
Опция (ключ)	**Назначение**

-a	Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются.
-A	Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки.
-i	Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются.
-n	Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа.
-r	Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации.
-s	Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации.
-f семейство_адресов	Ограничить показ статистики или адресов управляющих блоков только указанным семейством_адресов, в качестве которого можно указывать: **inet** Для семейства адресов **AF_INET**, или **unix** Для семейства адресов **AF_UNIX**.
-I интерфейс	Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле

	конфигурации системы, например, emd1 или lo0.
-p	Отобразить идентификатор/название процесса создавшего сокет (-p, --programs display PID/Program name for sockets)

Программа NetStat Agent

Представьте ситуацию: ваше Интернет-соединение стало работать медленно, компьютер постоянно что-то качает из Сети. Вам поможет программа NetStat Agent. С ее помощью вы сможете найти причину проблемы и заблокировать ее. Иначе говоря, **NetStat Agent** - полезный набор инструментов для мониторинга Интернет соединений и диагностики сети. Программа позволяет отслеживать TCP и UDP соединения на ПК, закрывать нежелательные соединения, завершать процессы, обновлять и освобождать DHCP настройки адаптера, просматривать сетевую статистику для адаптеров и TCP/IP протоколов, а также строить графики для команд **Ping** и **TraceRoute** (рис. 15).

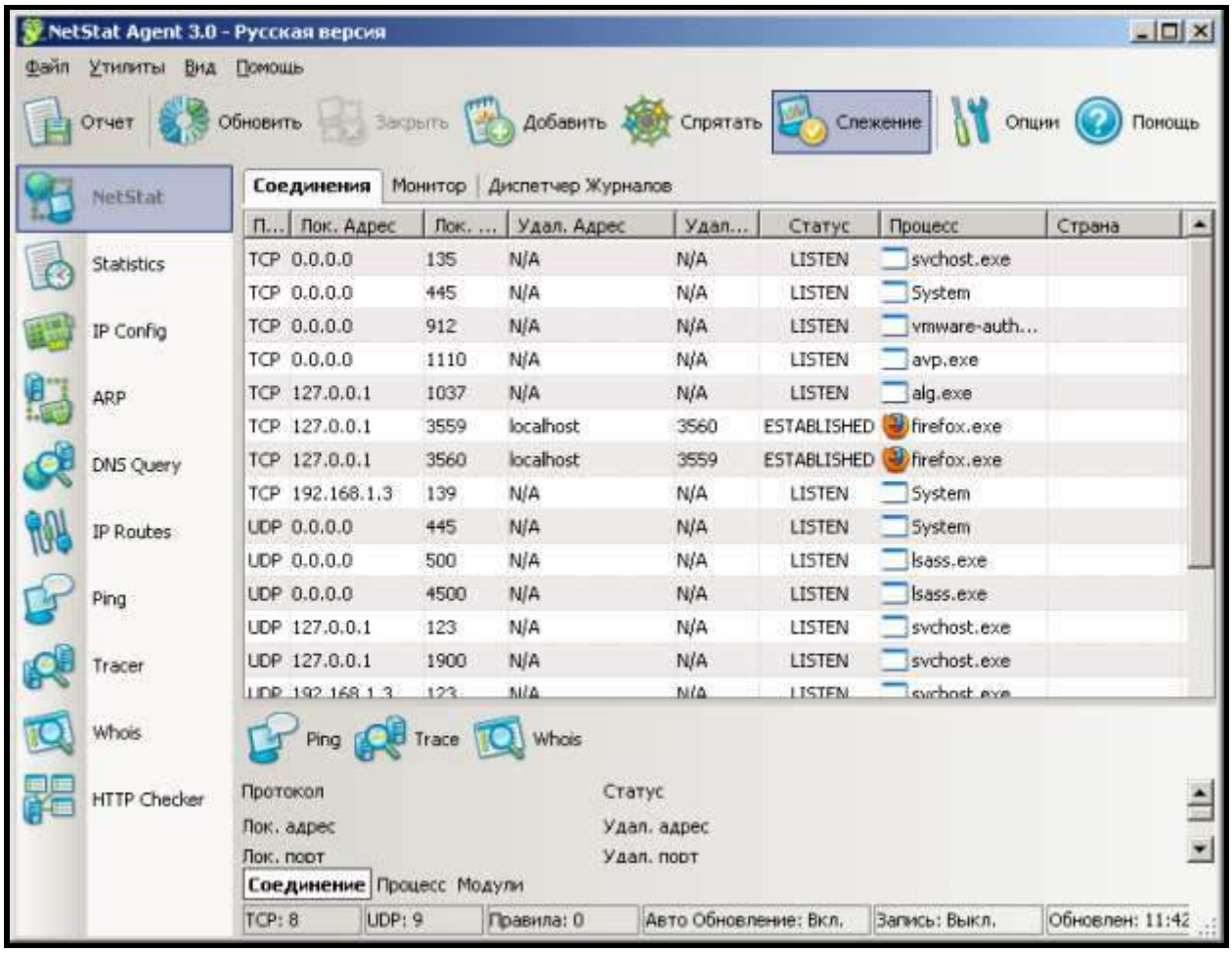


Рис. 15. Главное окно программы NetStat Agent

В состав программы NetStat Agent вошли следующие утилиты:

- **NetStat** - отслеживает TCP и UDP соединения ПК (при этом отображается географическое местоположение удаленного сервера и имя хоста).

- **IPConfig** - отображает свойства сетевых адаптеров и конфигурацию сети.
- **Ping** - позволяет проверить доступность хоста в сети.
- **TraceRoute** - определяет маршрут между вашим компьютером и конечным хостом, сообщая все IP-адреса маршрутизаторов.
- **DNS Query** - подключается к DNS серверу и находит всю информацию о домене (IP адрес сервера, MX-записи (Mail Exchange) и др.).
- **Route** - отображает и позволяет изменять IP маршруты на ПК.
- **ARP** - отслеживает ARP изменения в локальной таблице.
- **Whois** - позволяет получить всю доступную информацию об IP-адресе или домене.
- **HTTP Checker** - помогает проверить, доступны ли Ваши веб-сайты.
- **Statistics** - показывает статистику сетевых интерфейсов и TCP/IP протоколов.

Сканер портов Nmap (Zenmap)

Nmap - популярный сканер портов, который обследует сеть и проводит аудит защиты. Использовался в фильме "Матрица: Перезагрузка" при взломе компьютера. Наша задача не взломать, а защитить ПК, поскольку одно и то же оружие можно использовать как для защиты, так и для нападения. Иначе говоря, сканером портов **nmap** можно определить открытые порты компьютера, а для безопасности сети пользователям рекомендуется закрыть доступ к этим портам с помощью брандмауэра (рис. 16).

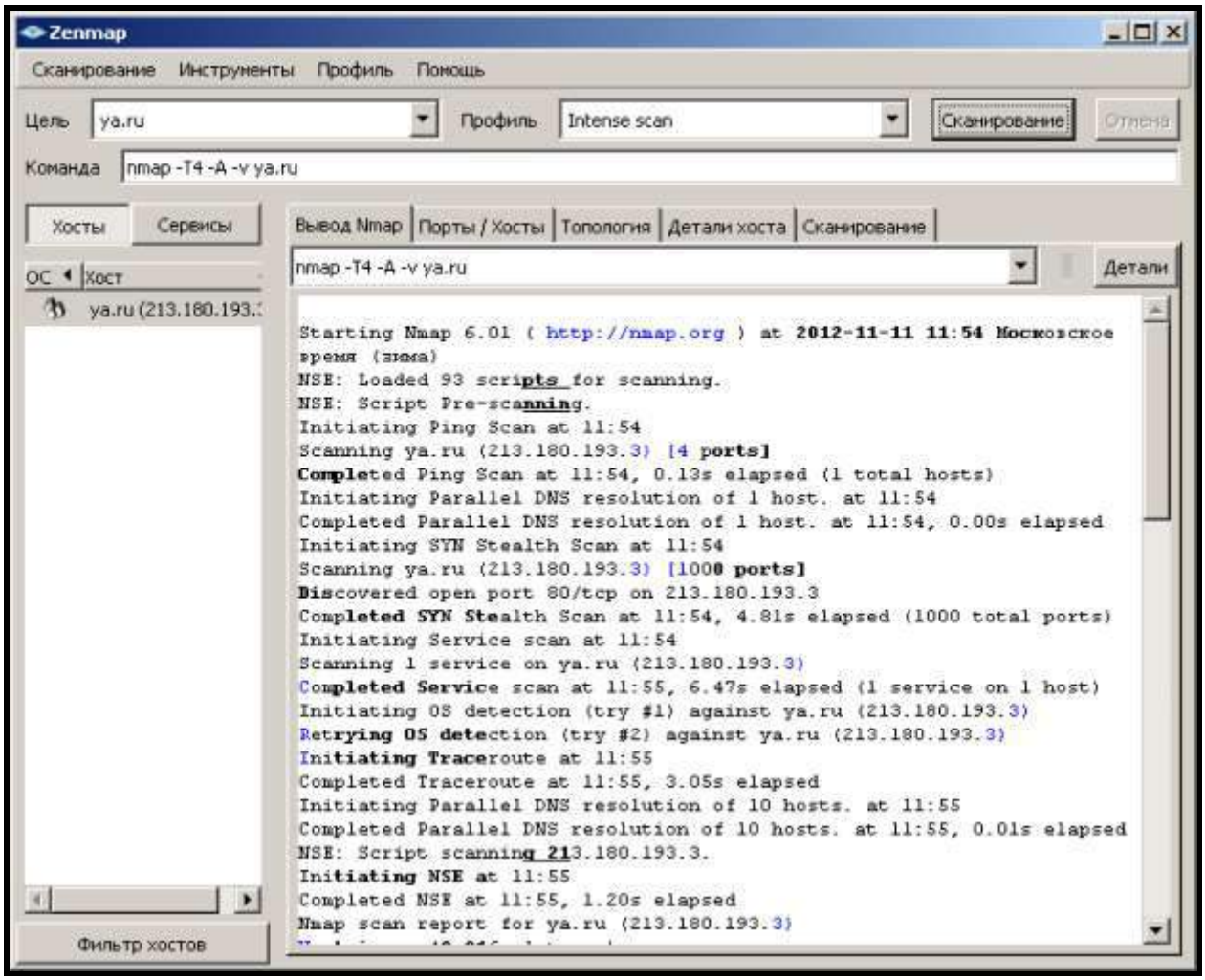


Рис. 16. Интерфейс программы Nmap

Обычно для того, чтобы просканировать все порты какого-либо компьютера в сети вводится команда **nmap –p1-65535 IP-адрес**_компьютера или **nmap –sV IP-адрес компьютера,** а для сканирования сайта - команда **nmap –sS –sV –O -P0 адрес сайта.**

Монитор портов TCPView

TCPView - показывает все процессы, использующие Интернет-соединения. Запустив **TCPView**, можно узнать, какой порт открыт и какое приложение его использует, а при необходимости и немедленно разорвать соединение – рис. 17.

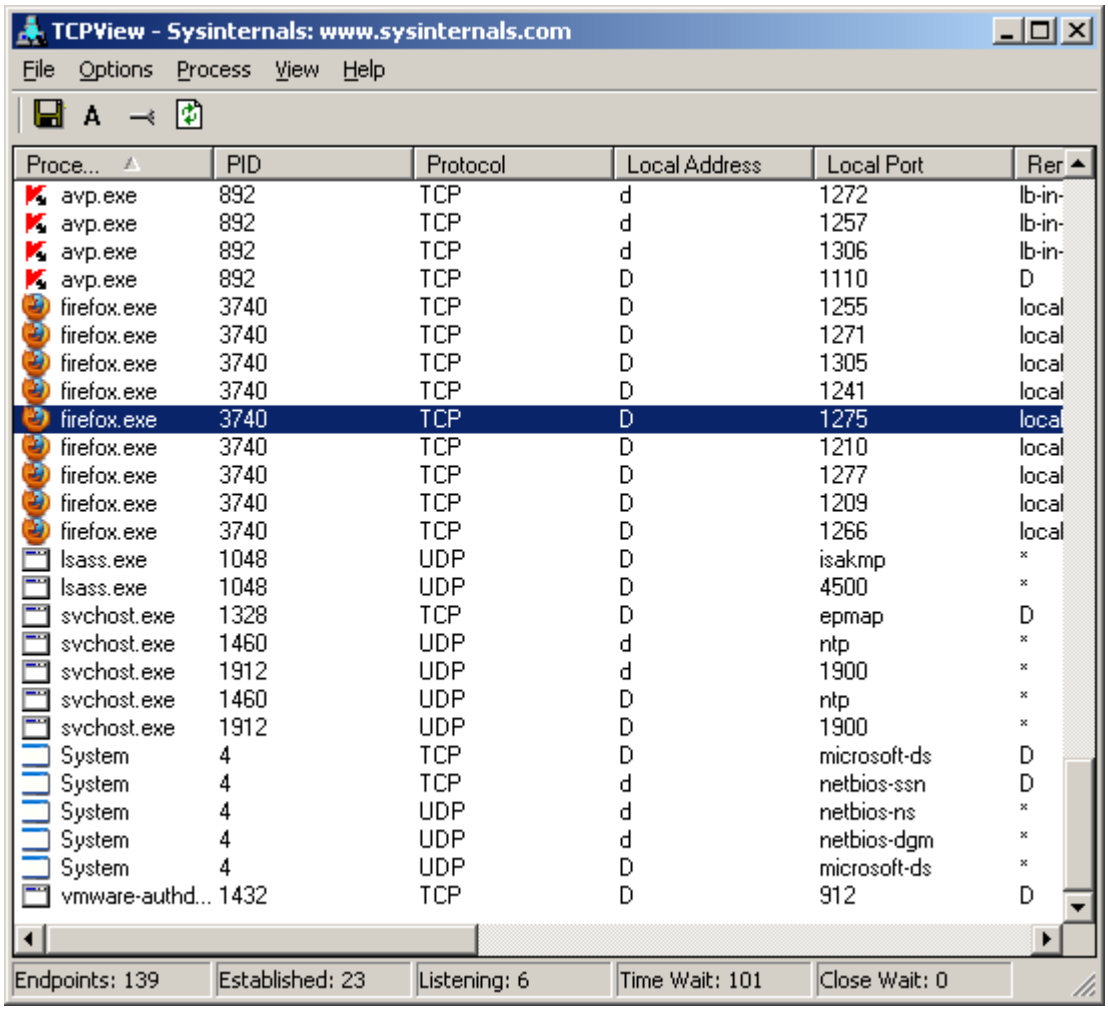


Рис. 17. Главное окно программы TCPView

Просмотрите активные сетевые подключения локального ПК с помощью монитора портов tpiview. Определите потенциально возможные угрозы (какие порты открыты, и какие приложения их используют). При необходимости можно закрыть установленное приложением TCP-соединение или процесс правой кнопкой мыши

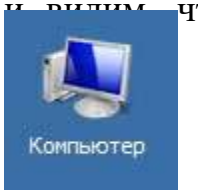
ПРАКТИЧЕСКАЯ РАБОТА №17.
ДИАГНОСТИКА IP ПРОТОКОЛА

Цель работы:
Научиться выполнять диагностику IP протокола локальной сети, а также - утилиты командной строки для проверки качества сетевых соединений (работоспособности локальной сети).

Рассмотрим диагностику IP-протокола локальной сети, а также - утилиты командной строки для проверки качества сетевых соединений (работоспособности локальной сети).

Применение команды **Ping** для проверки наличия связи компьютеров в сети

Наиболее быстрым способом проверки работоспособности локальной можно назвать системную команду PING, которая посылает сетевой запрос на заданный IP-адрес компьютера, получает ответ и выводит отчет на экран. Если посланный запрос получен обратно - связь физически существует, то ваша сеть настроена и работает корректно. Если же на экране вы увидите надпись "Превышен интервал ожидания запрос" - вы допустили ошибку либо в настройках, либо в подключении компьютеров. Перед запуском команды Ping необходимо посмотреть доступные компьютеры в сети. Заходим в **Компьютер** и видим, что в нашей рабочей группе 110 имеется четыре ПК (рис. 1).



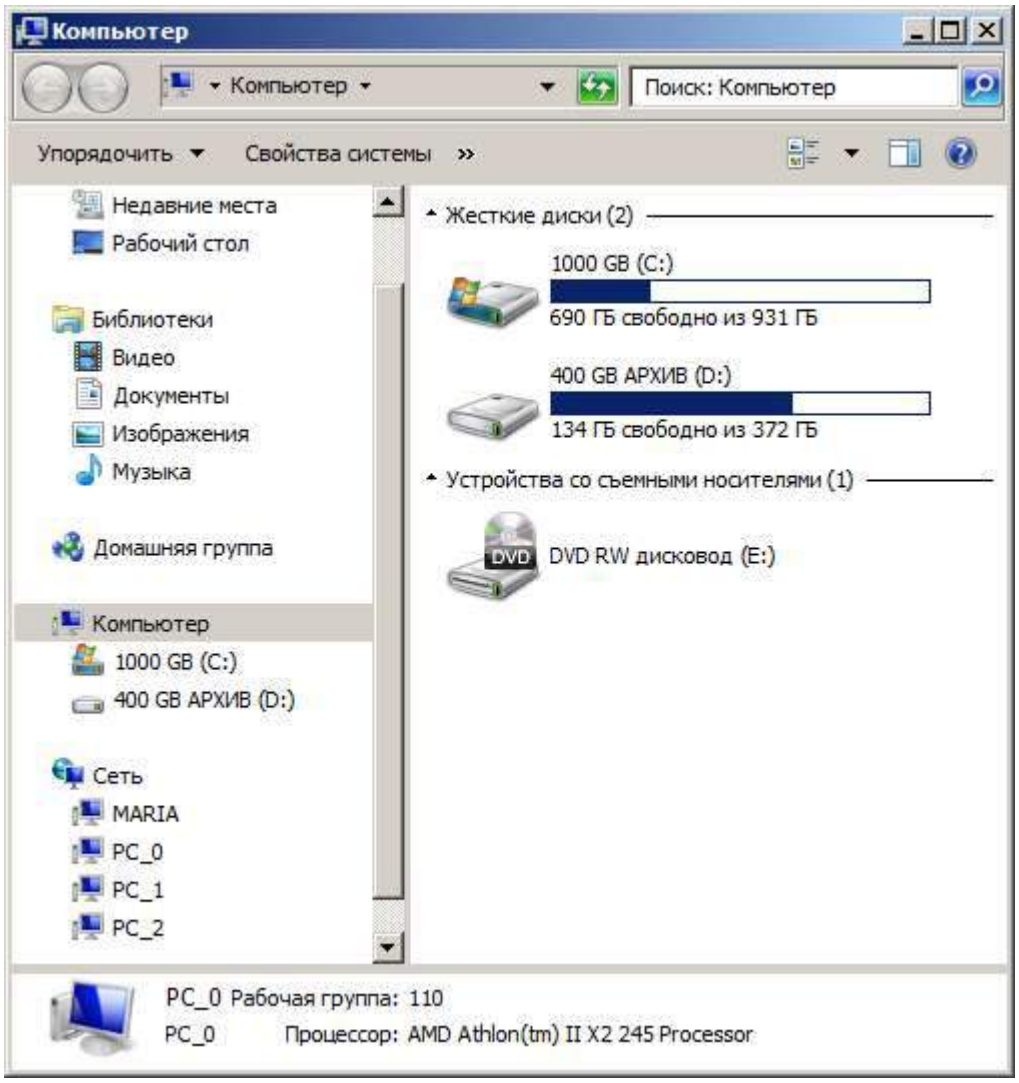


Рис. 1. В рабочей группе 110 мы видим 4 ПК

Для того чтобы воспользоваться командой ping, откройте окно командной строки командой **Пуск-Все программы-Стандартные-Командная строка** и введите там команду ping, укажите имя или IP-адрес удаленного компьютера

(или его ИМЯ"/>) (рис. 2). По умолчанию утилита ping отправляет 4 пакета и ожидает каждый ответ в течение четырех секунд. По умолчанию команда посылает пакет 32 байта. За размером тестового пакета отображается время отклика удаленной системы (в нашем случае — меньше 1 миллисекунды"/>).

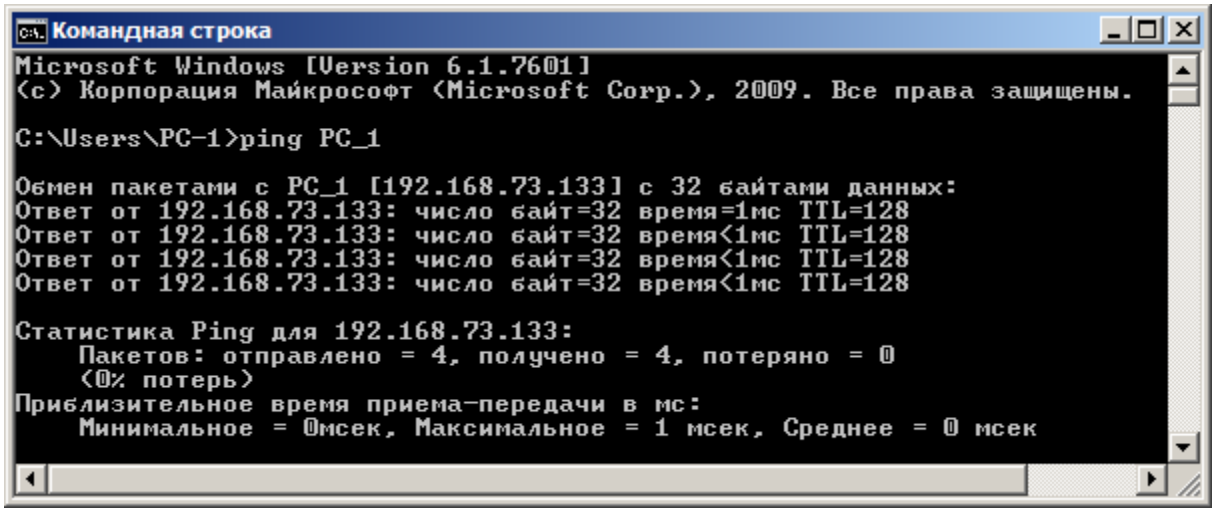


Рис. 2. Пингование машины PC_1 с IP-адресом 192.168.73.133

При необходимости для этой команды вы можете использовать следующие параметры:

-t. Данный параметр указывает на то, что производится проверка связи с указанным узлом до прекращения вручную;

-n. Текущий параметр определяет количество отправляемых Echo-запросов;

-f. Этот параметр устанавливает бит "не фрагментировать" на ping-пакете. По умолчанию фрагментация разрешается;

-w. Данный параметр позволяет настроить тайм-аут для каждого пакета в миллисекундах (по умолчанию установлено значение 4000"/>);

-a. Текущий параметр определяет имена узлов по адресам;

-l. При помощи этого параметра вы можете указать размер буфера отправки;

-i. Использование данного параметра позволяет вам задать срок жизни пакета;

-v. Этот параметр задает тип службы для IPv4 и не влияет на поле TOS в IP-заголовке;

-r. Текущий параметр записывает маршрут для указанного числа прыжков;

-s. Данный параметр позволяет отмечать время для указанного числа прыжков;

-j. Используя этот параметр, вы можете указать свободный выбор маршрута по списку узлов;

-k. При помощи данного параметра вы можете определить жесткий выбор маршрута по списку узлов;

-R. Текущий параметр позволяет использовать заголовок для проверки также и обратного маршрута только для IPv6;

-S. Данный параметр указывает используемый адрес источника;

-4. Параметр определяет принудительное использование протокола IP версии 4;

-6. Параметр определяет принудительное использование протокола IP версии 6.

Утилита **Ping** используется в том случае, когда необходимо проверить, может ли компьютер подключиться к сети TCP/IP или сетевым ресурсам. Иначе говоря, мы пингуем для того, чтобы проверить, что отправляемые пакеты доходят до получателя. ПК-отправитель отправляет Echo-запрос, а ПК-получатель, в ответ должен отправить ICMP-сообщение с ответом. Если удаленный компьютер реагирует на запрос ping, то подключение к удаленному компьютеру работает. Также, утилита ping ведет статистику, из которой понятно, сколько пакетов получено, а сколько потеряно. Но, это еще не все.

Применение команды Ping для анализа качества связи ПК в сети

Для тестирования качества связи запустите Ping со следующими параметрами: **ping.exe -l 16384 -w 500 -n 100** 192.168.73.133. Это обеспечит отправку 100 запросов (n) пакетами по 16 килобайт (l) на заданный IP адрес с интервалом ожидания ответа в 0,5 секунды (w). То есть:

L – размер буфера отправки.

N – число отправляемых запросов,

W – время ожидания ответа на запрос в миллисекундах,

Подождите, пока пройдут все 100 пакетов. Ответ должен будет быть приблизительно такой (рис. 3).

```
Командная строка
Ответ от 192.168.73.133: число байт=16384 время=1мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=3мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=5мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=1мс TTL=128
Ответ от 192.168.73.133: число байт=16384 время=2мс TTL=128

Статистика Ping для 192.168.73.133:
    Пакетов: отправлено = 100, получено = 100, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 17 мсек, Среднее = 2 мсек
```

Рис. 3. Ответ на команду ping.exe с ключами

Проанализируем результат выполнения команды:

- 0% потерь – сеть работает отлично.
- Если потери информации составили не более 3%, то сеть работает хорошо.
- При потерях 3-10% дошли не все пакеты, но сеть, благодаря алгоритмам коррекции ошибок, работает удовлетворительно. Из-за необходимости повторной доставки потерянной информации снижается эффективная скорости работы сети – сеть тормозит.
- Если число потерянных пакетов превышает 10-15%, то необходимо принять меры по устранению неисправности. Качество связи ПК неудовлетворительное.

Далее: как видим, время отклика удаленной системы среднее 2 мсек, а максимальное 17 мсек. Анализируя отклик по миллисекундам, надо иметь ввиду следующее. По стандарту, нормальное время отклика 16-килобайтного пакета для 100-мегабитной сети - 3-8 мс. Для 10-мегабитной - 30-80 мс. Получается, что у нас сеть работает на скорости порядка 100 мбит/сек.

Использование утилиты PathPing

Pathping это утилита, которая позволяет обнаружить потери пакетов на маршруте между вашим компьютером и заданным адресом IP. Потери пакетов могут сильно повлиять на работу сети, например, когда вы играете в видеоигру. Иначе говоря, утилита PathPing отправляет многочисленные сообщения с Echo-запросом каждому маршрутизатору, который находится между исходным пунктом и пунктом назначения, после чего, на основании пакетов, полученных от каждого из них, вычисляет процентное соотношение пакетов, возвращаемых в каждом прыжке. Поскольку утилита PathPing показывает степень потери пакетов на каждом маршрутизаторе или узле, то с ее помощью вы можете

точно определить маршрутизаторы и узлы, на которых возникают сетевые проблемы. Пример использования данной команды приведен на рис. 4.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\PC-1>pathping MARIA

Трассировка маршрута к MARIA [192.168.1.2]
с максимальным числом прыжков 30:
  0  PC_0 [192.168.1.3]
  1  MARIA [192.168.1.2]

Подсчет статистики за: 25 сек. ...
           Исходный узел      Маршрутный узел
Прыжок   RTT    Утер./Отпр.   %   Утер./Отпр.   %   Адрес
  0                                              PC_0 [192.168.1.3]
                                 0/ 100 =  0%    |
  1    2мс      0/ 100 =  0%     0/ 100 =  0%  MARIA [192.168.1.2]

Трассировка завершена.
```

Рис. 4. Поиск потерь пакетов на маршруте от ПК PC_0 до ПК MAIRIA

Итак, в строке поиска наберем **CMD**, чтобы вызвать командную строку

(рис. 5).

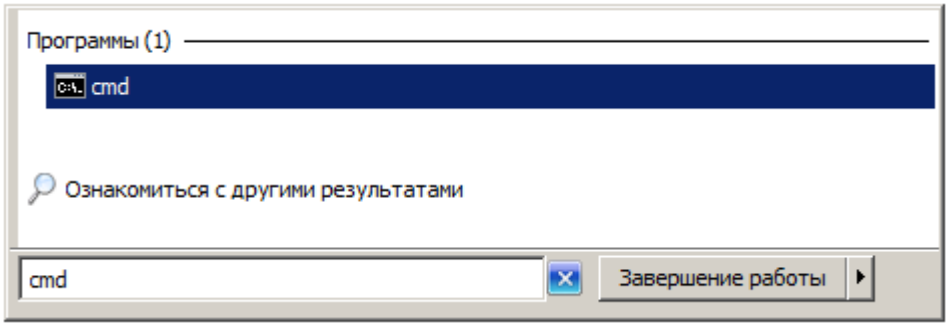


Рис. 5. Один из способов вызова командной строки в ОС Windows 7

Далее произведет трассировку маршрута от нашего ПК до поискового сервера Яндекс (рис. 6).

```
C:\Windows\system32\cmd.exe

C:\Users\PC-1>pathping yandex.ru

Трассировка маршрута к yandex.ru [213.180.204.11]
с максимальным числом прыжков 30:
  0  PC_0 [192.168.1.3]
  1  192.168.1.1
  2  lo0-at66-2.natm.ru [213.148.173.214]
  3  at66-ats66-L3-giga-core.natm.ru [213.148.163.81]
  4  ATS3-TGE1-8-TTS-TGE1-4.natm.ru [78.81.0.37]
  5  GWay-TGE0-2.natm.ru [78.81.0.254]
  6  ge-0-1-0-vl988-10g.M320-1-NOVG.nwtelecom.ru [212.48.214.53]
  7  ae1-30g.MX960-1-MMT.nwtelecom.ru [212.48.198.246]
  8  as13238-yandex.gateway.nwtelecom.ru [212.48.214.102]
  9     *        *        *
Подсчет статистики за: 200 сек. ...
           Исходный узел      Маршрутный узел
Прыжок  RTT   Утер./Отпр.   %   Утер./Отпр.  %   Адрес
  0                                            PC_0 [192.168.1.3]
                                 0/ 100 =  0%    |
  1    1мс     0/ 100 =  0%      0/ 100 =  0%  192.168.1.1
                                 0/ 100 =  0%    |
  2    1мс     0/ 100 =  0%      0/ 100 =  0%  lo0-at66-2.natm.ru [213.148.1
4]
                                 0/ 100 =  0%    |
  3    2мс     0/ 100 =  0%      0/ 100 =  0%  at66-ats66-L3-giga-core.natm.
13.148.163.81]
                                 0/ 100 =  0%    |
  4    1мс     0/ 100 =  0%      0/ 100 =  0%  ATS3-TGE1-8-TTS-TGE1-4.natm.r
.81.0.37]
                                 0/ 100 =  0%    |
  5    3мс     0/ 100 =  0%      0/ 100 =  0%  GWay-TGE0-2.natm.ru [78.81.0.

                                 0/ 100 =  0%    |
  6    2мс     0/ 100 =  0%      0/ 100 =  0%  ge-0-1-0-vl988-10g.M320-1-NOV
elecom.ru [212.48.214.53]
                                 0/ 100 =  0%    |
  7   11мс     0/ 100 =  0%      0/ 100 =  0%  ae1-30g.MX960-1-MMT.nwtelecom
212.48.198.246]
                               100/ 100 =100%    |
  8  ---     100/ 100 =100%      0/ 100 =  0%  as13238-yandex.gateway.nwtele
u [212.48.214.102]

Трассировка завершена.
```

Рис. 6. Пример использования утилиты Pathping

Проанализируем результат:

- Первый блок информации представляет собой трассировку. Вы можете пропустить его и перейти ко второму блоку информации, в котором будет указано процентное отношение потерь пакетов.
- Если пакеты не терялись на данном маршруте подключения, то вы увидите 0% потерь пакетов. Если вы увидите значения, отличающиеся от 0%, это означает, что на пути к нашим серверам были потери пакетов. Потери выше 1% начиная с первого шага, могут указывать на некорректную работу узлов сети или маршрутизаторов. Если эти устройства вам доступны, то нужно попробовать обновить их программное обеспечение или полностью заменить их. Иначе, о потерях, возникших после первого шага и до последнего шага, следует сообщить вашему Интернет провайдеру.

Примечание

Если последние строки указывают на 100% потерь, то это не является показателем проблемы, а происходит потому, что сервера защищены от нежелательного трафика и атак.

С данной командой вы можете использовать следующие параметры:

-g. Данный параметр определяет использование параметра свободной маршрутизации в IP-заголовке с набором промежуточных мест назначения для сообщений с Echo-запросом, который указывается в списке компьютеров.

-h. Данный параметр задает максимальное количество переходов на пути при поиске конечного объекта;

-i. Этот параметр указывает IP-адрес источника;

-n. Текущий параметр предотвращает попытки сопоставления IP-адресов промежуточных маршрутизаторов с их именами, что существенно ускоряет вывод результатов;

-p. Используя данный параметр, вы можете задать время ожидания между последовательными проверками связи, где значением по умолчанию указано 250 миллисекунд;

-q. При помощи текущего параметра вы можете указать количество сообщений с Echo-запросом, отправленных каждому маршрутизатору пути (по умолчанию - 100);

-w. Данный параметр определяет время ожидания для получения Echo-ответов протокола ICMP или ICMP-сообщений об истечении времени в миллисекундах, которые соответствуют данному сообщению Echo-запроса. Значение по умолчанию 4 секунды;

-4. Параметр определяет принудительное использование протокола IP версии 4;

-6. Параметр определяет принудительное использование протокола IP версии 6.

Другие команды командной строки. Отображение параметров TCP/IP-протокола командой Ipconfig

Команда **IPCONFIG** используется для отображения текущих настроек протокола TCP/IP и для обновления некоторых параметров, задаваемых при автоматическом конфигурировании сетевых интерфейсов при использовании протокола DHCP. Предположим, что у нас имеется сеть, изображенная на- рис. 7.

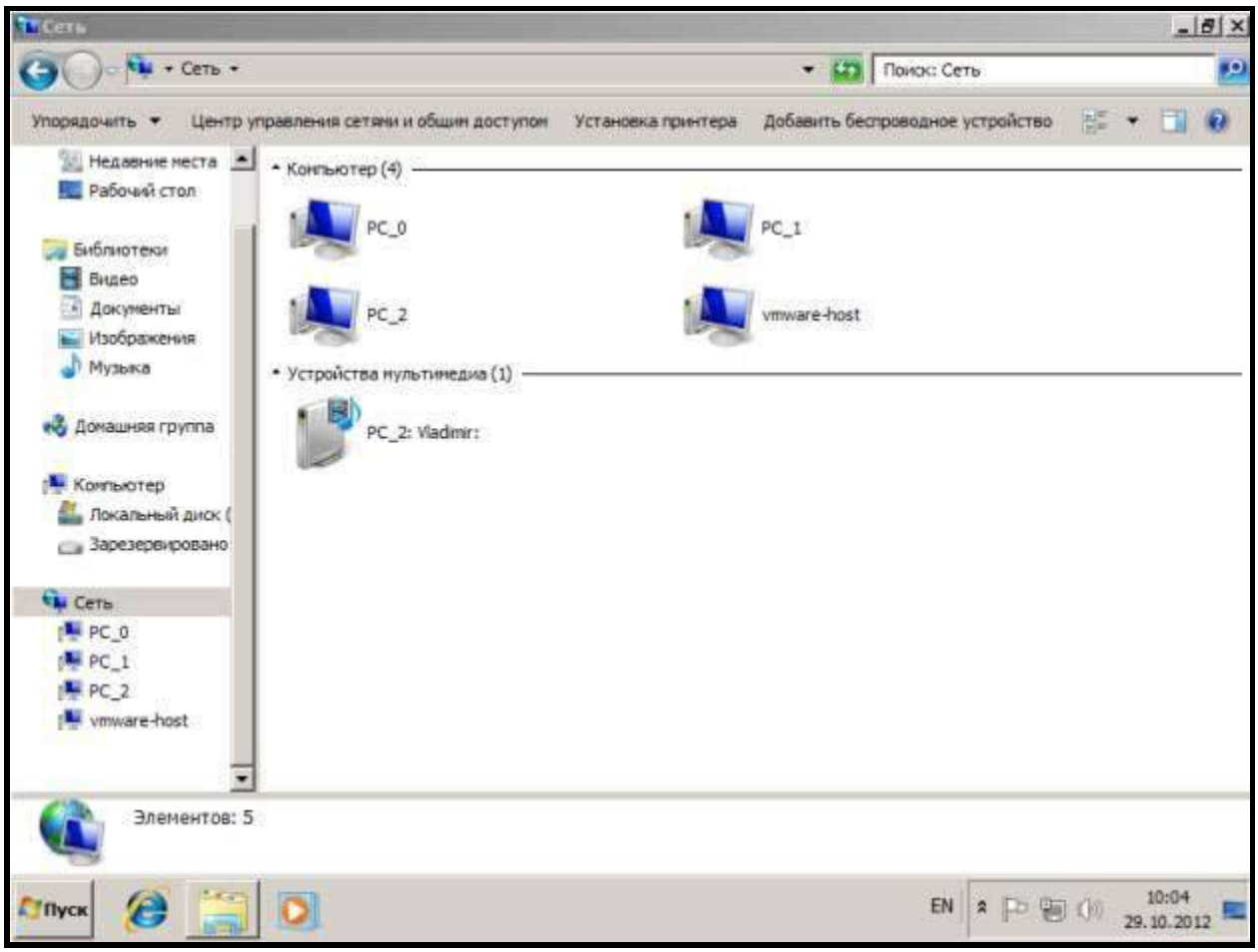


Рис. 7. Небольшая локальная сеть

Выполним команду командой Ipconfig на PC_2 (рис. 8>).

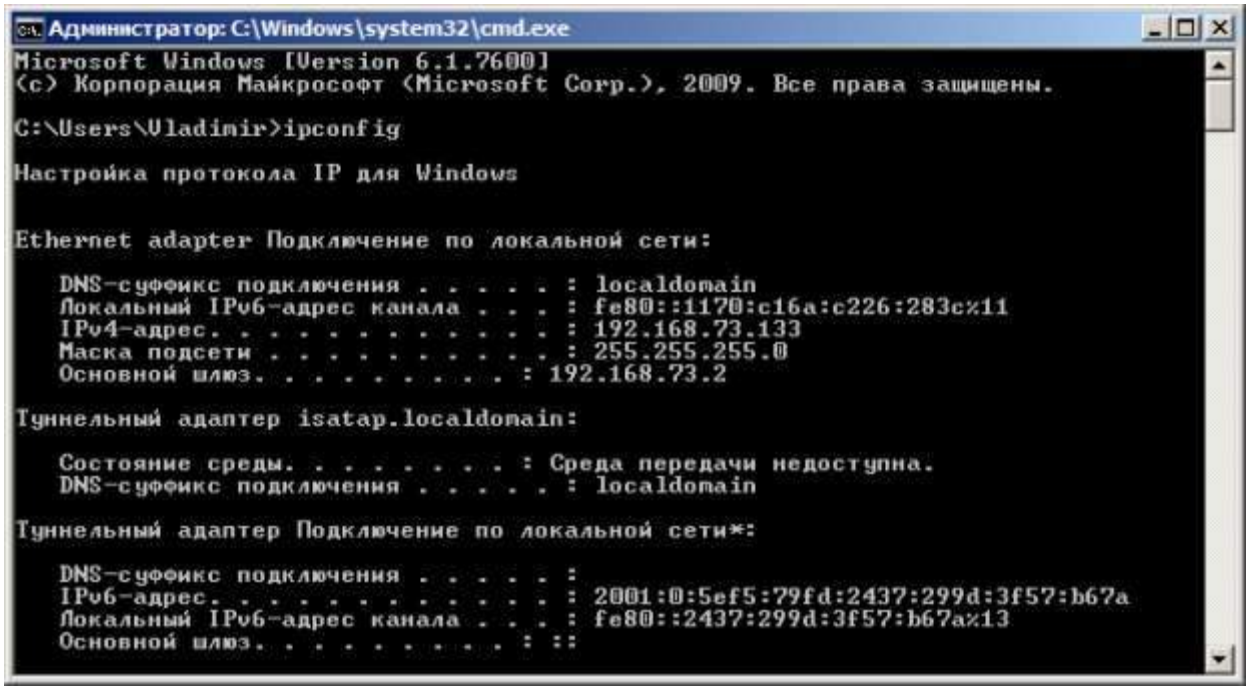


Рис. 8. Отображение параметров TCP/IP-протокола командой Ipconfig

Из отчета мы видим такую информацию:

- DNS-суффикс подключения - localdomain (из настроек сетевого подключения)
- Локальный IPv6-адрес канала - локальный IPv6 адрес, если используется адресация IPv6
- IPv4-адрес - используемый для данного адаптера IPv4 – адрес
- Маска подсети - 255.255.225.0
- Основной шлюз - IP-адрес маршрутизатора, используемого в качестве шлюза по умолчанию.

Примечание

Туннельный адаптер isatap.localdomain это эмуляция IPV6 в сетях IPV4. ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) — Протокол автоматической внутрисайтовой адресации туннелей, позволяющий передавать между сетями IPv6 пакеты через сети IPv4

Ключи команды:

/all Отображение полной информации по всем адаптерам.

/release [адаптер] Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан) или для заданного адаптера. Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.

/renew [адаптер] Обновление IP-адреса для определённого адаптера или если адаптер не задан, то для всех. Доступно только при настроенном автоматическом получении IP-адресов.

/flushdns Очищение DNS кэша.

/registerdns Обновление всех зарезервированных адресов DHCP и перерегистрация имен DNS.

/displaydns Отображение содержимого кэша DNS.

/showclassid адаптер Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическим получением IP-адресов.

/setclassid адаптер [код_класса] Изменение кода класса DHCP. Доступно только при настроенном автоматическим получением IP-адресов.

/? Справка. TCP/IP: значения IP адреса, маски и шлюза.

Команда вывода списка компьютеров рабочей группы Net view

В командной строке введите команду **net view,** и вы увидите список компьютеров своей рабочей группы (рис. 9).

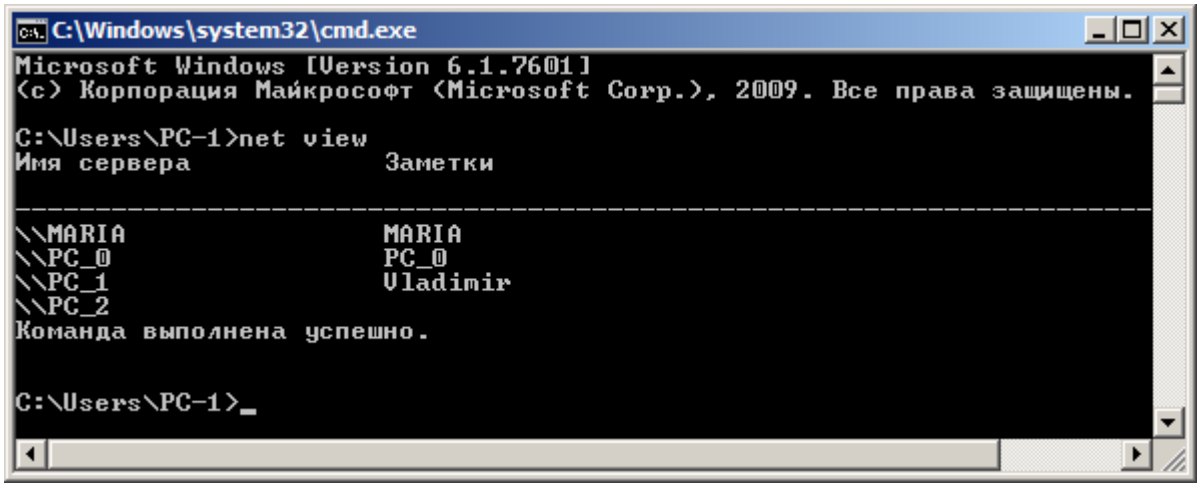


Рис. 9. В рабочей группе имеется 4 ПК

Трассировка

Tracert — это служебная компьютерная программа, предназначенная для определения маршрутов следования данных в сетях TCP/IP. Программа tracert выполняет отправку данных указанному узлу сети, при этом отображая сведения о всех промежуточных маршрутизаторах, через которые прошли данные на пути к целевому узлу. В случае проблем при доставке данных до какого-либо узла программа позволяет определить, на каком именно участке сети возникли неполадки.

Запуск программы производится из командной строки. Для этого вы должны войти в неё. Для операционной системы Windows 7 существует несколько способов запуска командной строки:

1. Сочетание клавиш Win (кнопка с логотипом Windows) + R (должны быть нажаты одновременно) — В графе "Открыть" написать "cmd" и нажать Ок.
2. Пуск — Все программы— Стандартные — Командная строка.

В открывшемся окне мы напишем **tracert ya.ru**. Принцип действия этой программы схож с принципом действия программы ping. Команда отправляет на сервер данные и при этом фиксирует все промежуточные маршрутизаторы, через которые проходят эти данные на пути к серверу (целевому узлу). Если при доставке данных до одного из узлов происходит проблема, программа определяет участок сети, на котором возникли неполадки. Время отклика показывает загруженность канала. А вот если вместо времени отклика вы видите надпись **"Превышен интервал ожидания для запроса"**, это значит, что на данном узле связи происходит потеря данных, а значит, проблема именно в нем – рис. 10.

```
C:\Windows\system32\cmd.exe
C:\Users\PC-1>tracert ya.ru

Трассировка маршрута к ya.ru [87.250.250.3]
с максимальным числом прыжков 30:

  1    <1 мс    <1 мс    <1 мс  192.168.1.1
  2     4 ms     1 ms     1 ms  lo0-at66.natm.ru [213.148.173.223]
  3     4 ms     2 ms     2 ms  at66-ats66-L3-giga-core.natm.ru [213.148.163.81]

  4     4 ms    14 ms     6 ms  ATS3-TGE1-8-TTS-TGE1-4.natm.ru [78.81.0.37]
  5     3 ms     3 ms     4 ms  GWay-TGE0-2.natm.ru [78.81.0.254]
  6     4 ms     1 ms     1 ms  ge-0-1-0-v1988-10g.M320-1-NOVG.nwtelecom.ru [212
.48.214.53]
  7    10 ms     9 ms     9 ms  ae1-30g.MX960-1-MMT.nwtelecom.ru [212.48.198.246
]
  8    10 ms     9 ms     9 ms  as13238-yandex.gateway.nwtelecom.ru [212.48.214.
102]
  9     *        *        *     Превышен интервал ожидания для запроса.
 10    16 ms    16 ms    16 ms  s600-61.yandex.net [87.250.239.36]
 11    17 ms    18 ms    18 ms  13-s3600-s600.yandex.net [213.180.213.53]
 12    18 ms    17 ms    17 ms  www.yandex.ru [87.250.250.3]

Трассировка завершена.

C:\Users\PC-1>
```

Рис. 10. Пример трассировки домена ya.ru

Параметры команды tracert:

-d не определять доменные имена маршрутизаторов

-h <значение-> установить максимальное количество переходов

-w <значение> установить максимальное время ожидания ответа (в миллисекундах)

Итак, трассировка маршрута помогает определить проблемный узел. Если данные проходят нормально и "стопорятся" на самом пункте назначения, то проблема действительно с сайтом. Если трассировка маршрута прекращается на середине пути, то проблема в одном из промежуточных маршрутизаторов. Если прохождение пакетов прекращается в пределах сети вашего провайдера — то и проблему нужно решать "на местном уровне". Попутно хочется отметить, что программа работает только в направлении от источника пакетов и является весьма грубым инструментом для выявления неполадок в сети.

ПРАКТИЧЕСКАЯ РАБОТА №18.
ПРОГРАММЫ ДЛЯ РАБОТЫ В СЕТЯХ LAN И WAN

Цель работы:
Изучить сетевые программы (утилиты) – Winsent, Radmin и Team Viewer.

Рассмотрим три полезные сетевые программы (утилиты) – **Winsent, Radmin и Team Viewer.**

Пример 1. Winsent – бесплатная программа для общения в локальной сети

Чат – является программой для общения с другими пользователями сети (обмен текстовыми сообщениями).

Winsent Messenger это программа, предназначенная для быстрого обмена сообщениями и общения в локальной сети (рис. 1). Сайт программы http://www.winsent.ru/. Программа может использоваться как в домашней локальной сети, так и в локальной сети предприятия, офиса, корпоративной локальной сети. Winsent Messenger не требует использования выделенного сервера, и полностью совместим со службой сообщений (**net send**). Работает в любой версии Windows (7/Vista/XP/2000).

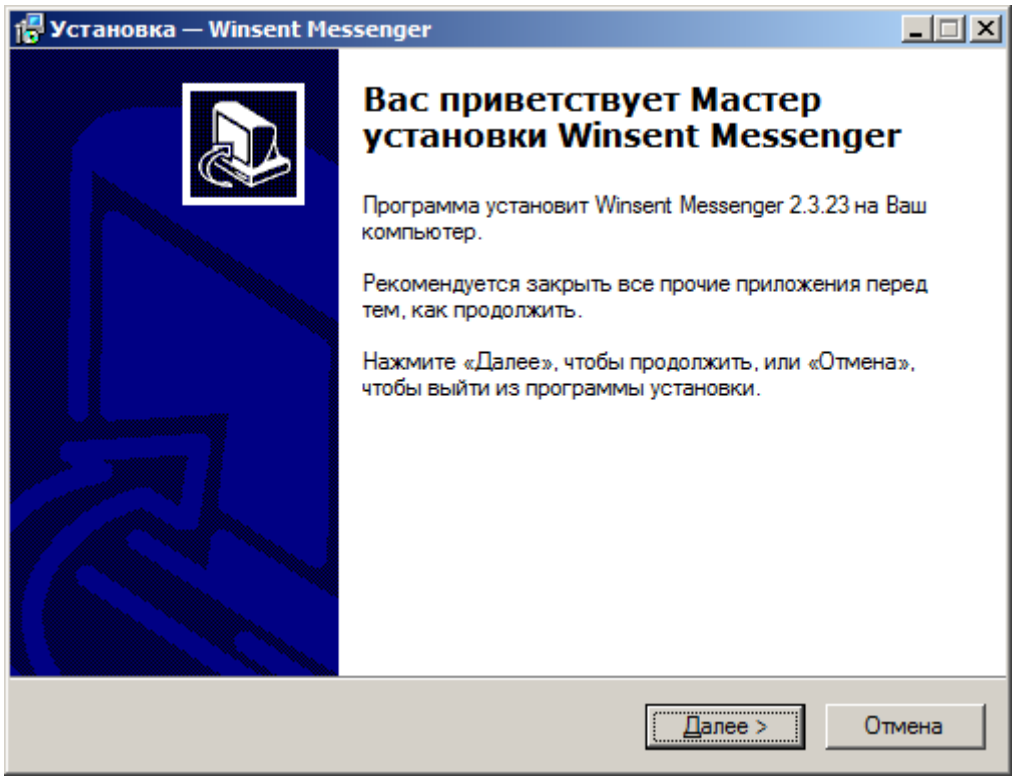


Рис. 1. Окно начальной установки программы Winsent Messenger

Если на вашем ПК программа запущена, то вы можете отправить сообщение любому ПК в сети, даже если на нем эта программа не стоит. Запустите программу – в трее появиться ее значок (рис. 2).

Рис. 2. Значок программы WinSent

Напишите имя рабочей группы или пользователя, затем пишите текст сообщения и отправляйте его (рис. 3)

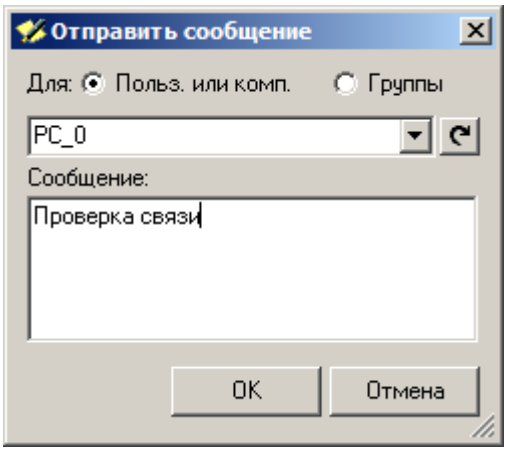


Рис. 3. Указываем получателя, пишем текст сообщения

Пример 2. Radmin - программа удаленного управление ПК по сети

Radmin - популярная программа для работы на удаленном компьютере в режиме реального времени. Она работает и в LAN, и WAN. Radmin включает в себя средство обмена файлами, текстовый и голосовой чат, и другие полезные функции. Во время работы с удаленным компьютером, вы можете не беспокоиться за безопасность своих данных: Radmin работает в режиме защиты данных, при котором все передаваемые данные защищены по стандарту **AES** – рис. 4.

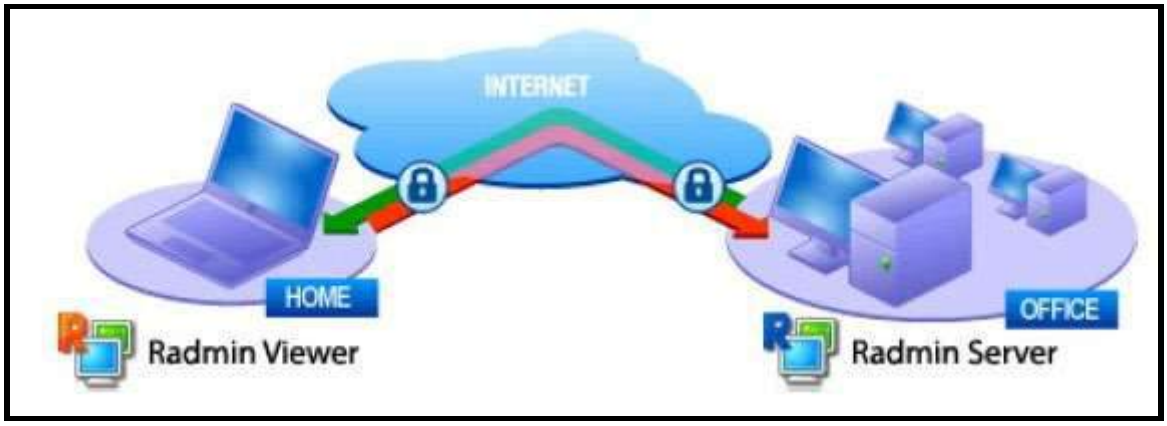


Рис. 4. Схематическое изображение работы с удаленным ПК в программе Radmin

Итак, перед началом работы оба компьютера должны иметь выход в Интернет или быть подсоединенными к общей локальной сети (LAN). Предположим, что вы хотите установить связь вашего домашнего (у вас дома) и вашего офисного (у вас на работе) ПК. Установите на обоих ПК программы Radmin Server и Radmin Viewer.

Настройте Radmin Server на удаленном (ведущем, администраторском) компьютере

Запустите Radmin Server, например, на на PC_1. Щелкните правой кнопкой мыши на иконке Radmin Server в трее и выберите команду **Настройки Radmin**

Server-Права доступа и установите пароль и права доступа к Radmin Server – рис. 5. Например, даем команду разрешить **Полный доступ** (ОК).

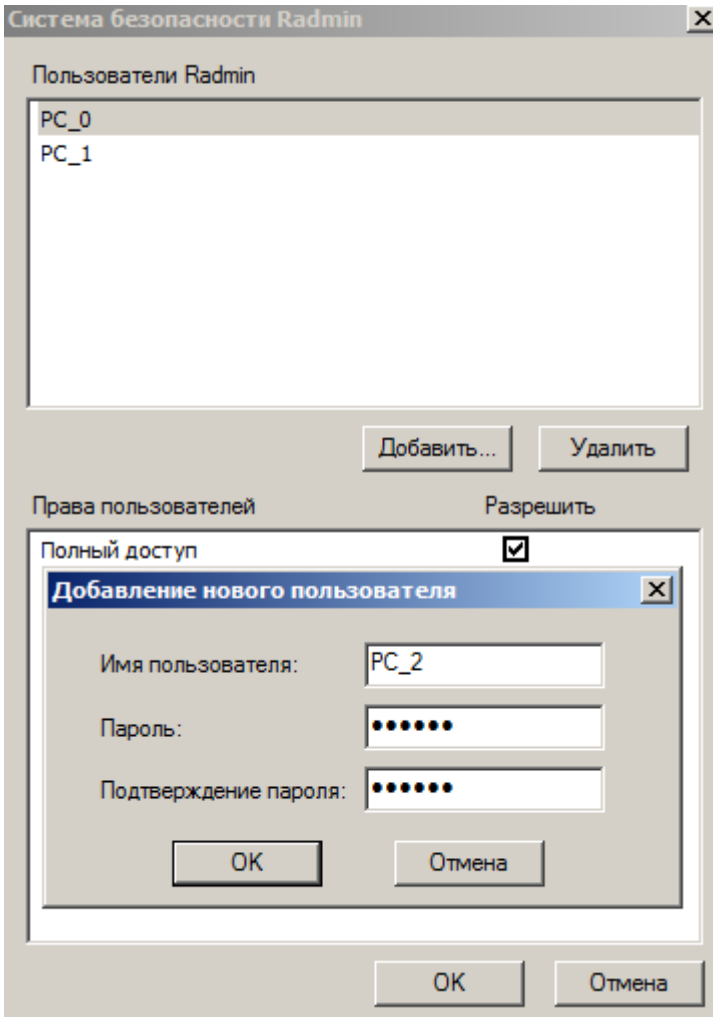


Рис. 5. Добавляем пользователей на Radmin Server

Запишите IP адрес Вашего компьютера, для этого наведите мышкой курсор на иконку Radmin Server (рис. 6).

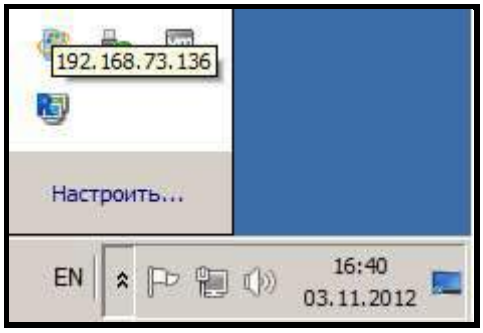


Рис. 6. Узнаем IP для нашего ПК (192.168.73.136)

Настройте Radmin Viewer на локальном (ведомом) компьютере (хосте)

Запустите Radmin Viewer на локальном компьютере, например, PC_2, и создайте новое подключение командой **Соединение-Соединиться с** (рис. 7).

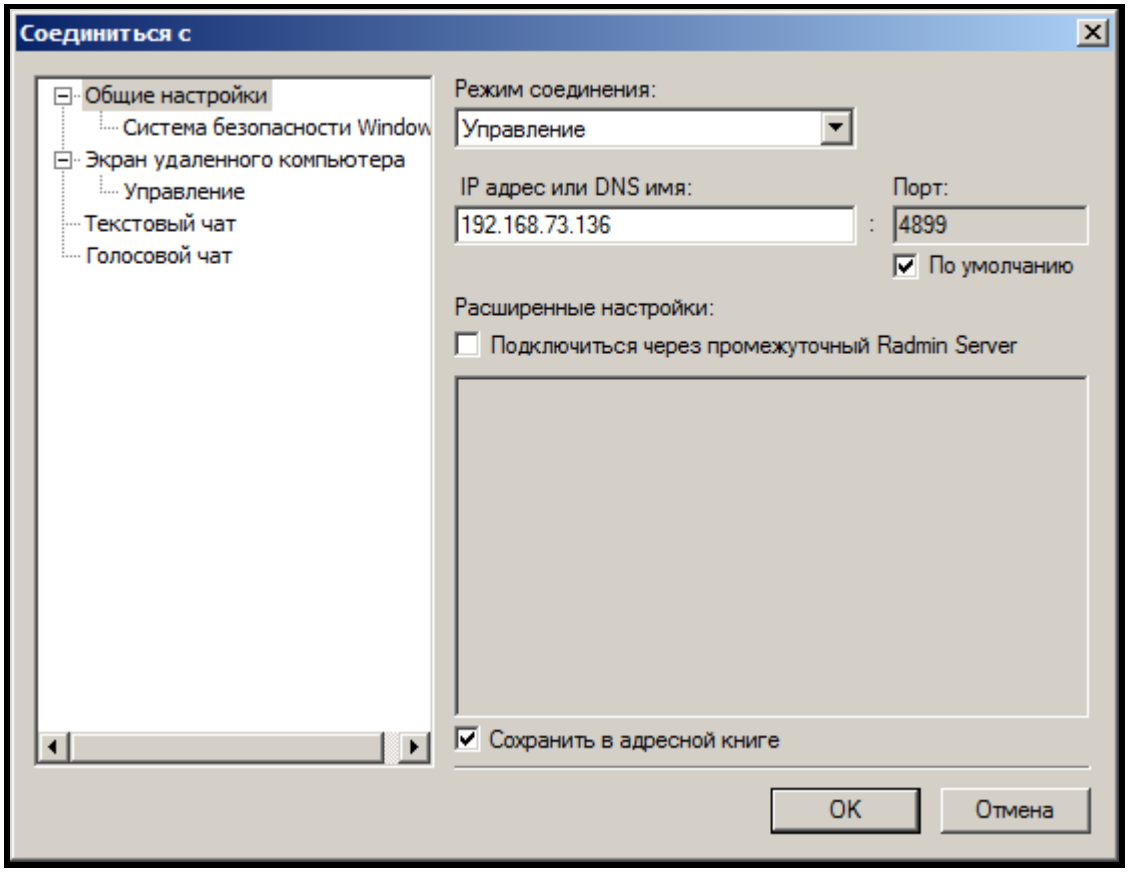


Рис. 7. Одно для соединения с ведущим ПК

Укажите IP адрес компьютера, на котором установлен и настроен Radmin Server. Затем выберите режим подключения и введите имя пользователя и пароль, заданные ранее в настройках Radmin Server на удаленном компьютере (рис. 8).

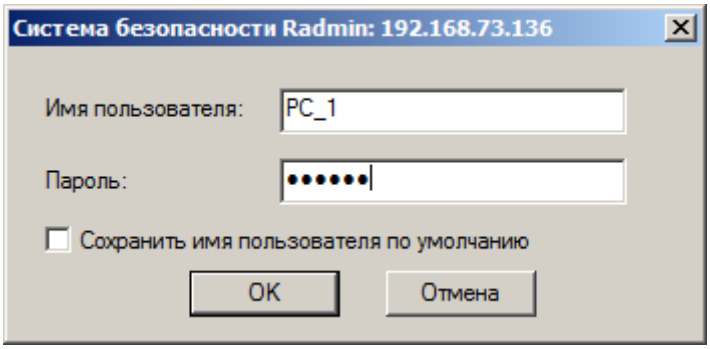


Рис. 8. Вводим заданные ранее на сервере имя и пароль пользователя

После нажатия на кнопку OK видим рабочий стол удаленного ПК (рис. 9).

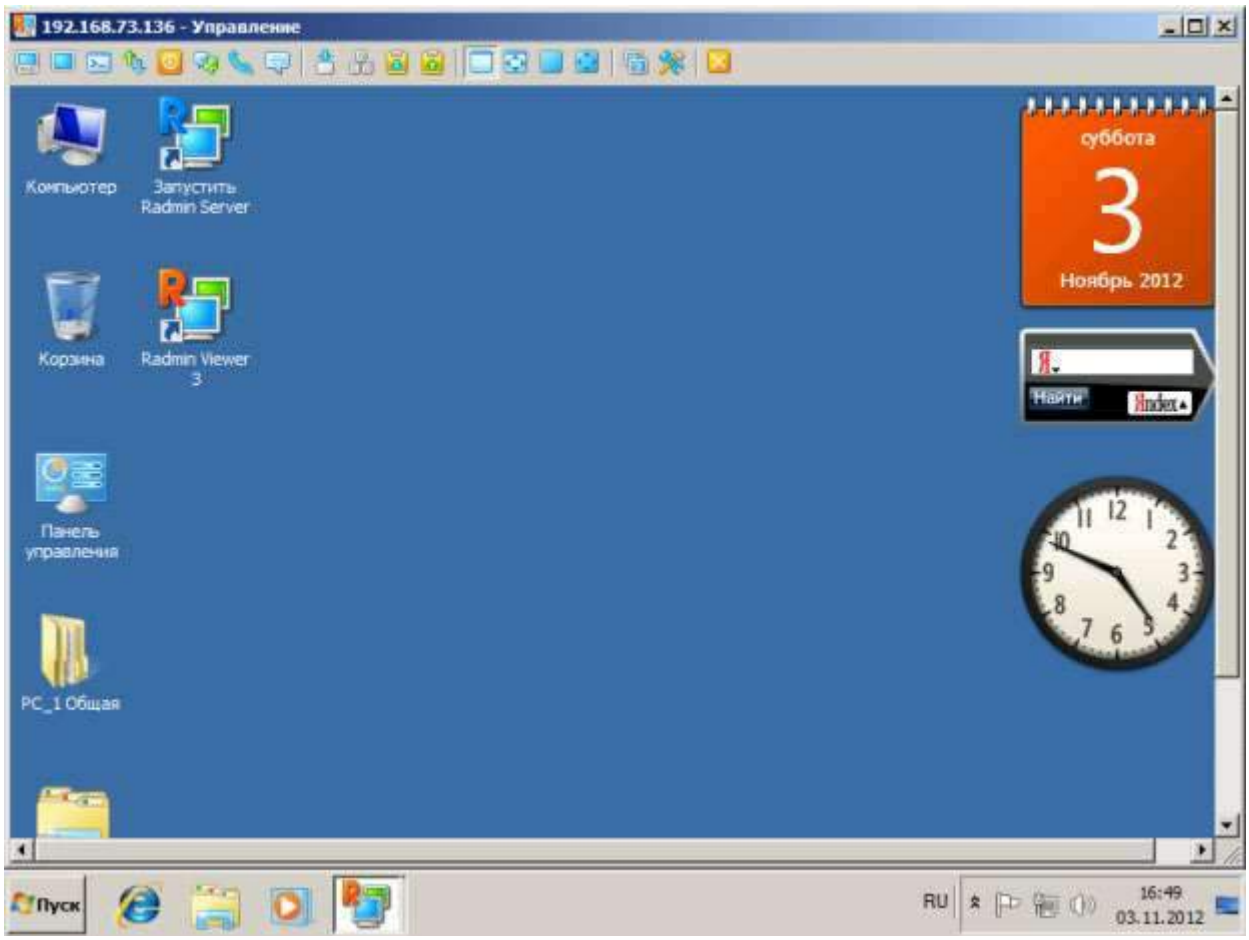


Рис. 9. Окно для управления удаленным (ведущим) ПК с ведомого ПК

Окно программы Radmin Viewer приведено на рис. 10.

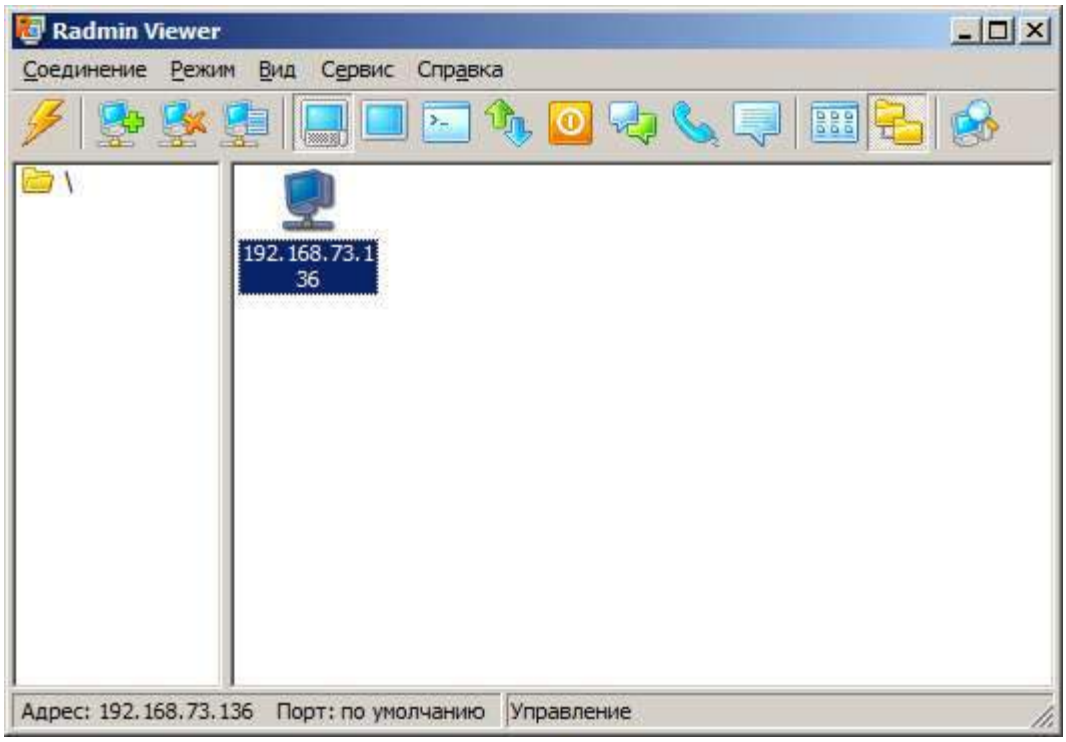


Рис. 10. Окно программы Radmin Viewer

Таким образом, программа Radmin состоит из двух частей: клиентской (Radmin Viewer) и серверной (Radmin Server). Вы устанавливаете Radmin Server на удаленном компьютере и получаете возможность видеть экран удаленного компьютера на экране своего компьютера. Ваши манипуляции передаются на удаленный компьютер. Удаленный компьютер может располагаться в Интернет или в локальной сети. Иначе говоря, с помощью Radmin вы можете работать у себя в офисе, не вставая из-за домашнего компьютера

Примечание

В принципе, на каждом ПК можно установить и запускать одновременно и Radmin Server, и Radmin Viewer. Они друг другу не мешают, зато можно управлять удаленным ПК в обе стороны.

Пример 3. Управление компьютером в программе Team Viewer

TeamViewer (**http://www.teamviewer.com/ru/download/windows.aspx**) - программа для осуществления удаленного доступа к компьютеру по сети. Программ устанавливается на удаленном компьютере (хост) и на компьютере для администрирования (администратор). Единственная настройка администратора – пройти авторизацию. После этого у вас на рабочем столе появится аналогичное окно удаленного компьютера, и вы сможете управлять им как обычным ПК. Помимо управления удаленным компьютером, с помощью данной программы можно передавать файлы и общаться в чате. Итак, устанавливается TeamViewer на оба сетевых ПК, затем запускается программа. После старта автоматически получаются ID и Пароль (рис. 11).

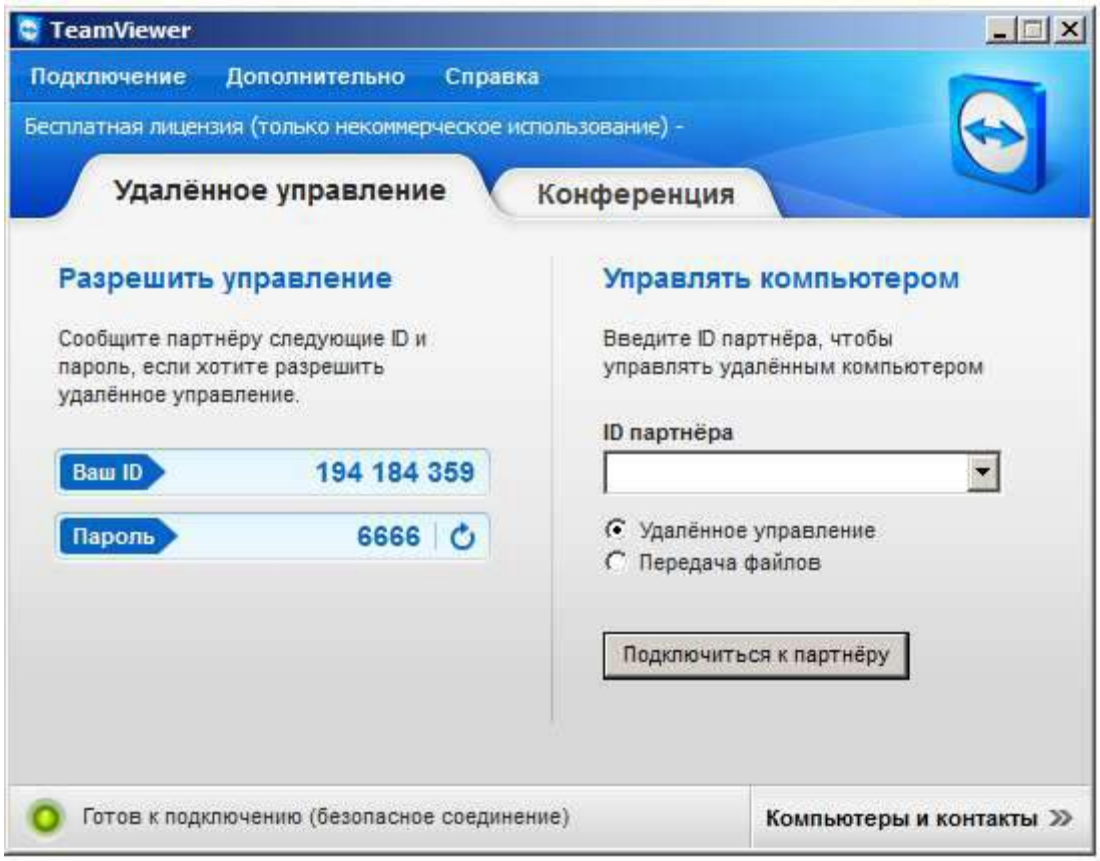


Рис. 11. Получаем уникальный идентификатор нашего ПК и пароль на вход в него

Предположим, что на втором ПК мы получили ID 194 187 481и Пароль 8642. Вводим эти данные. После нажатия на кнопку **Подключиться к партнеру** вы сможете работать на удаленном ПК, как на своем или в режиме **Удаленное управление** (рис. 12), или в режиме **Передача файлов** (рис. 13).

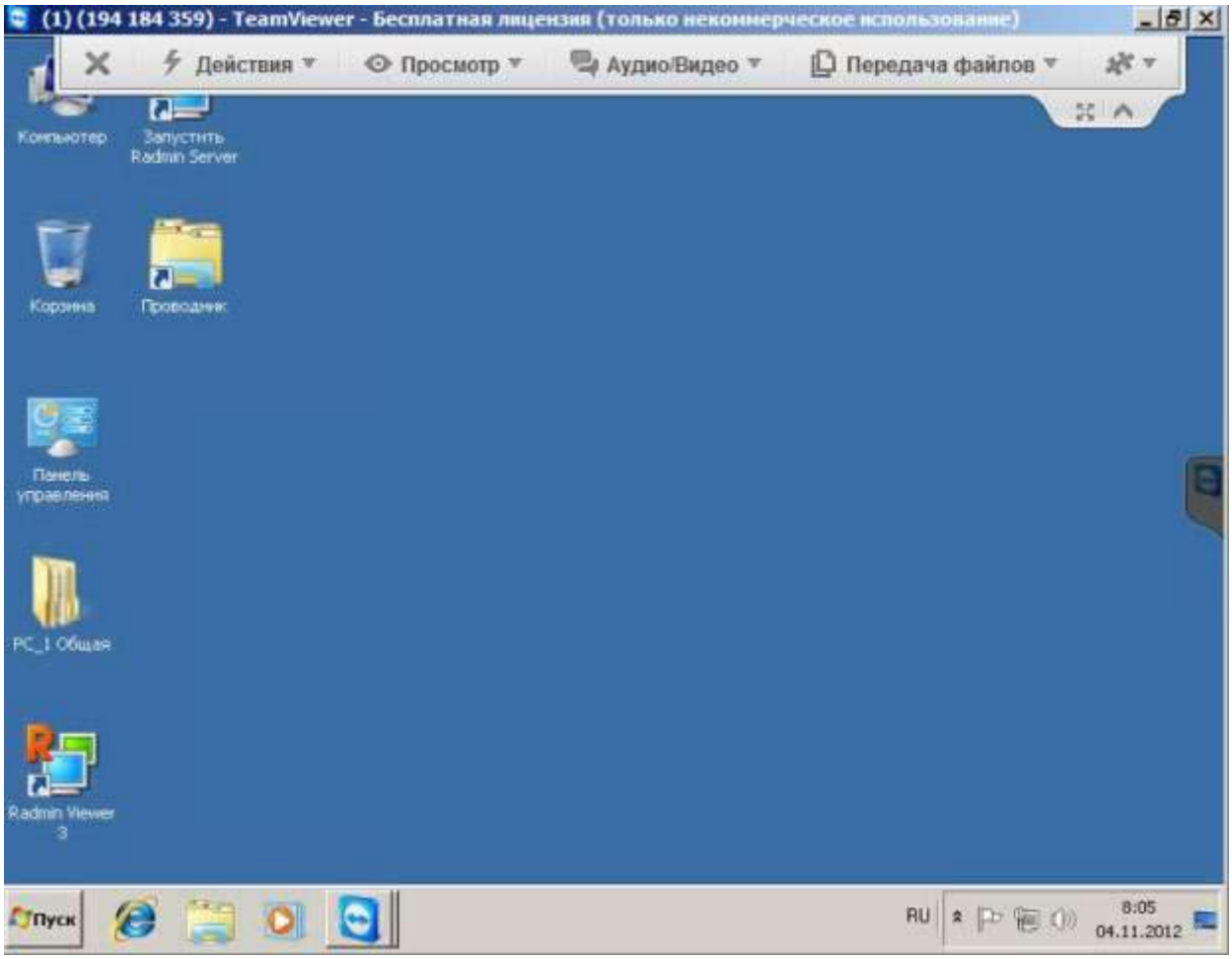


Рис. 12. Главное окно удаленного ПК (режим Удаленное управление)

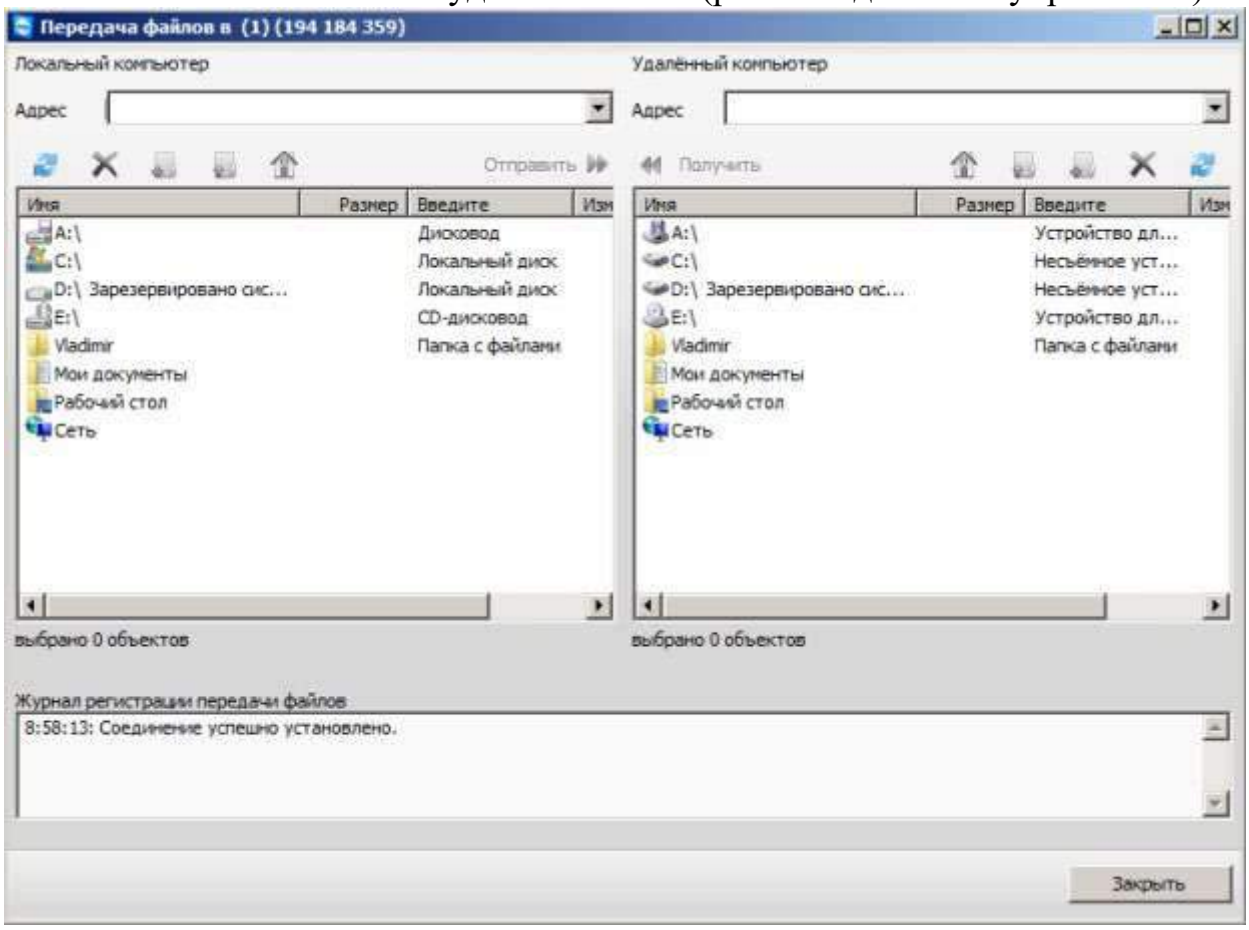


Рис. 13. Главное окно удаленного ПК (режим Передача файлов).
Слева Локальный, а справа – Удаленный ПК

В заключение заметим, что программа полностью работоспособна и бесплатна, но постоянно предлагает приобрести коммерческую лицензию, что может раздражать ее пользователей.

Задания

- Создайте на удаленном ПК сетевой ресурс - папку 123456 и сделайте к ней общий доступ. Какие ограничение в ОС Windows XP устанавливаемое для сетевого ресурса (размер создаваемых файлов; максимальное число пользователей, которые могут подключится к ресурсу; время работы каждого пользователя; дисковое пространство, выделяемое каждому пользователю).
- Установите связь между ведомым и ведущим ПК не через локальную сеть, а через Интернет.
- Осуществите пересылку файлов с локального на удаленный компьютер командой **Режим-Передача файлов** (рис. 14).

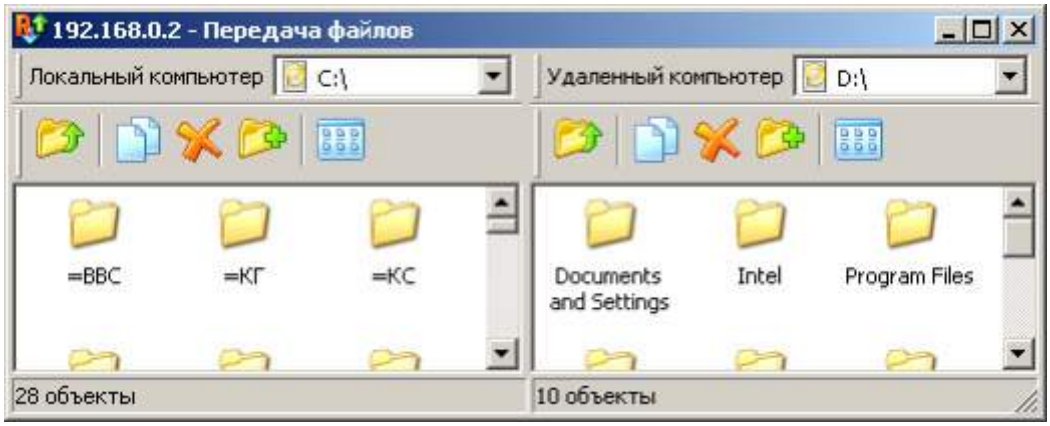


Рис. 14. Окно отправки файлов между компьютерами

Командой **Режим-Текстовый чат** организуйте обмен текстовыми сообщениями между ПК (рис. 15).

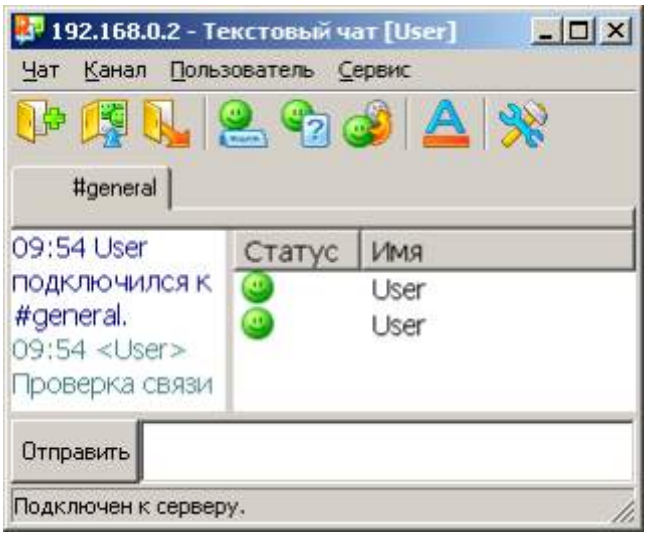


Рис. 15. Режим обмена текстовыми сообщениями между ПК

Произведите выключение удаленного ПК (рис. 16).

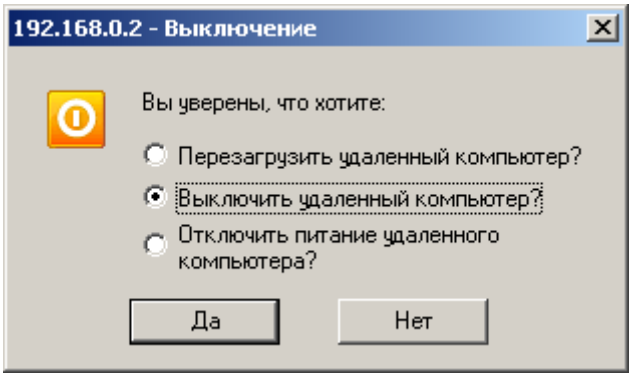


Рис. 16. Выключение удаленного ПК

- Установите программу и научитесь удаленно управлять ПК
- Отправьте файл удаленному ПК
- Отправьте на удаленный ПК текстовое сообщение

Краткие итоги

В лабораторной работе мы научились работать в трех полезных сетевых программах:

- Winsent (программа для общения в локальной сети)
- Radmin (программа удаленного управление ПК по сети)
- Team Viewer (программа управления компьютером с использованием Интернет)

Для лучшего понимания этих тем к работе прилагается скринкаст.

ПРАКТИЧЕСКАЯ РАБОТА №19.
НАЗНАЧЕНИЕ СЕРВЕРУ РОЛИ "КОНТРОЛЛЕР ДОМЕНА"

Цель работы:
Изучить назначение серверу роли "Контроллер домена"

Создаем новый домен в новом лесу

Ниже мы опишем последовательность действий для того, чтобы сервер сделать **Контроллером Домена,** т.е. чтобы "поднять" на нем службу **Active Directory**.

Сервер, на котором расположена служба Active Directory, называется контроллером домена. Active Directory имеет иерархическую структуру базы, состоящей из объектов. Объекты разделяются на три основные категории: **ресурсы** (например, принтеры), **службы** (например, электронная почта) и **учётные записи** (пользователей и компьютеров). Active Directory предоставляет информацию об объектах, позволяет управлять объектами и доступом к ним.

Нажимаем **Пуск - Управление данным сервером** – рис. 1.

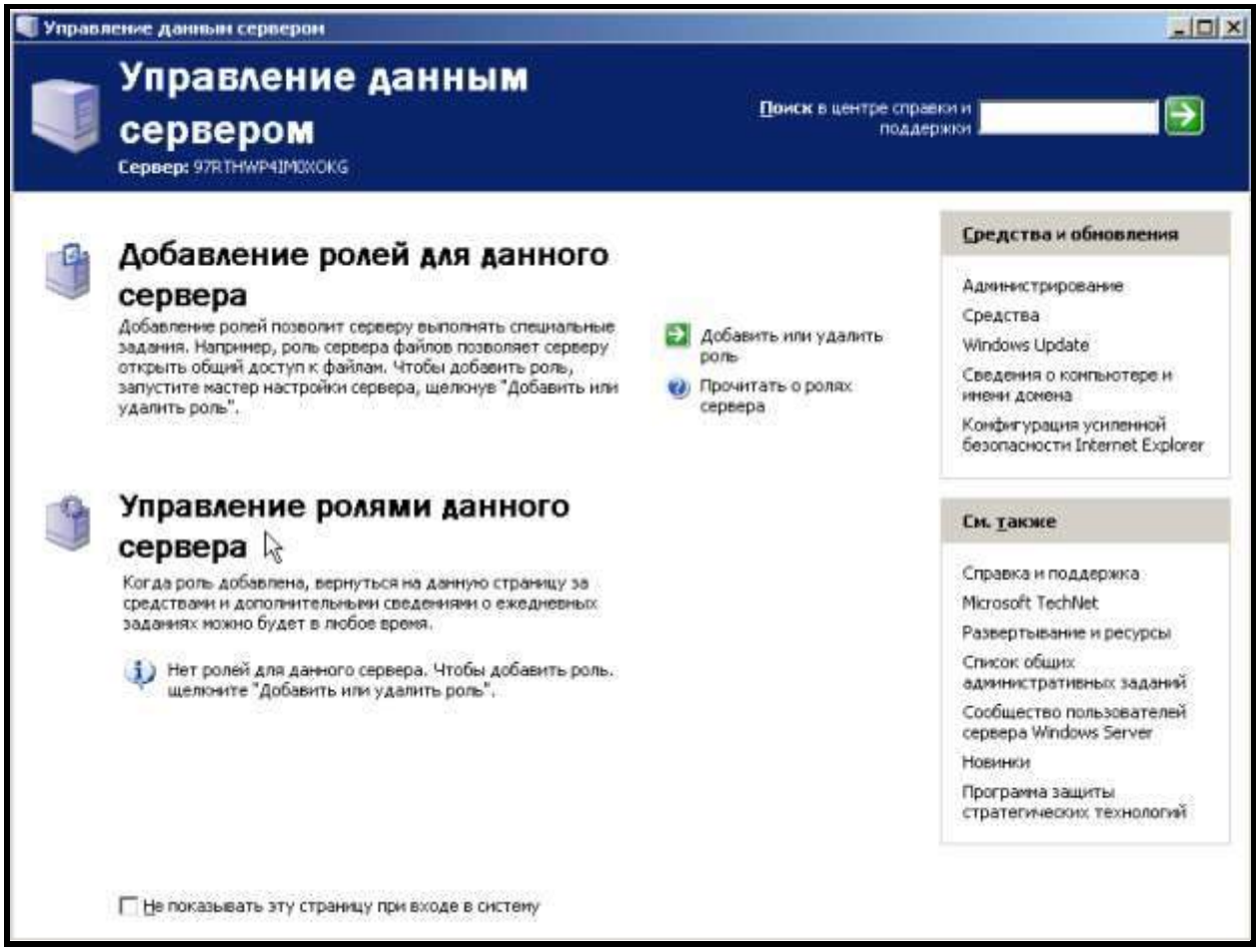


Рис. 1. Окно Управление данным сервером

Нажимаем **Добавить или удалить роль**, устанавливаем переключатель в положение **Особая конфигурация** – рис. 2

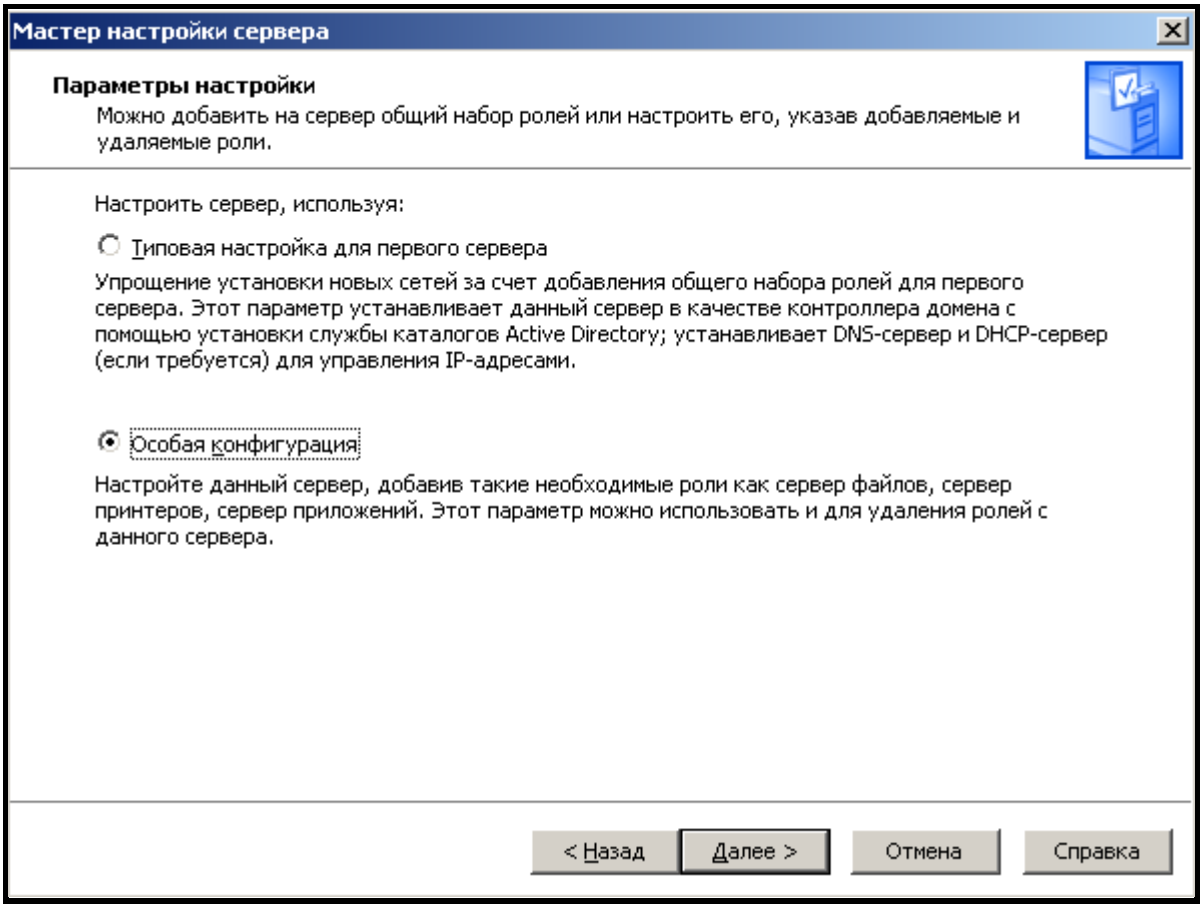


Рис. 2. Переключатель в положении Особая конфигурация

Из списка доступных ролей выбираем **"Контроллер домена" (Active Directory)** – рис. 3.

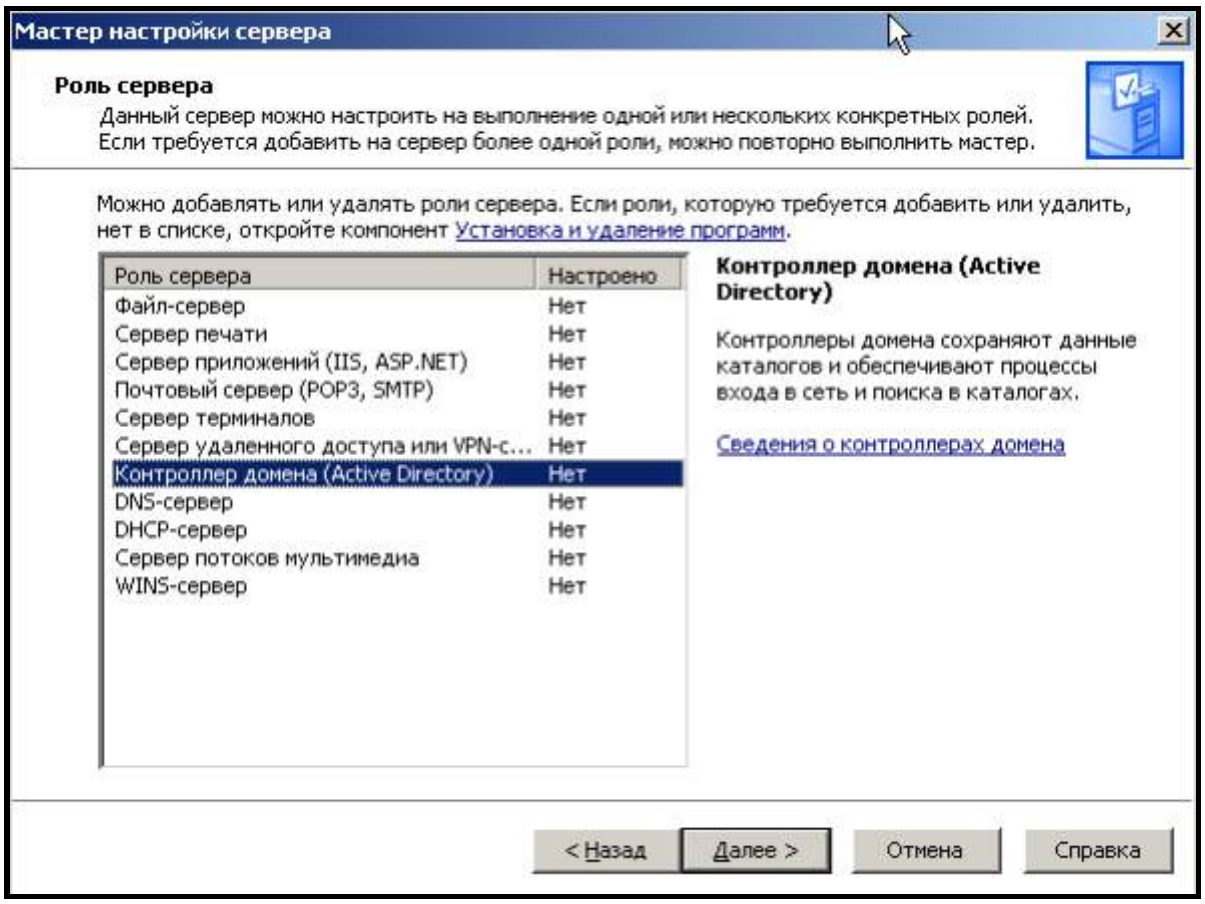


Рис. 3. Выбираем роль для сервера из списка

Добавить контроллер домена в существующем домене мы не можем, так как у нас нет доменов. Поэтому, для создания домена, выбираем переключатель **Контроллер домена в новом домене** – рис. 4.

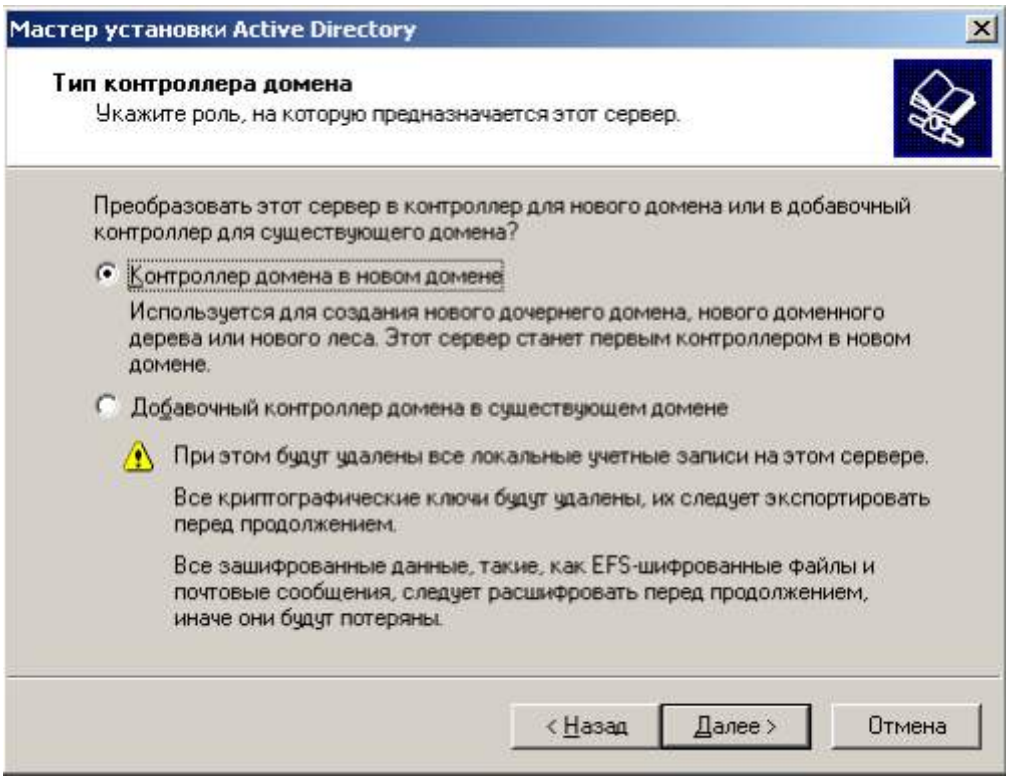


Рис. 4. Устанавливаем переключатель Контроллер домена в новом домене

Далее задействуем переключатель **Новый домен в новом лесу**- рис. 5.

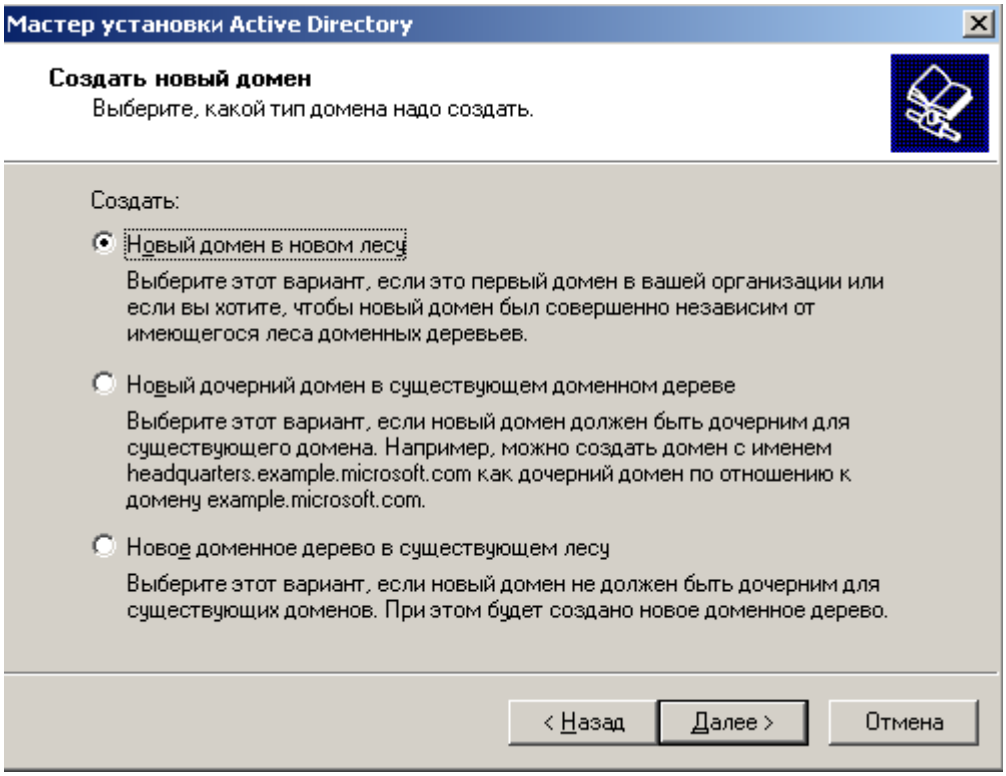


Рис. 5. Включаем опцию Новый домен в новом лесу

На следующем шаге пишем **полное DNS-имя нового домена.** Домены вида **domaine.com** или **domain.ru** имеют внешнее пространство имен,

опубликованных в Интернет. На такой сервер можно зайти из Интернет. Мы же выберем внутреннее пространство имен, чтобы из Интернет доступа не было, и назовем имя домена, например, DOMAIN.LAN - рис. 6. Так мы повышаем безопасность нашей системы. В этом случае через точку можно писать что угодно.

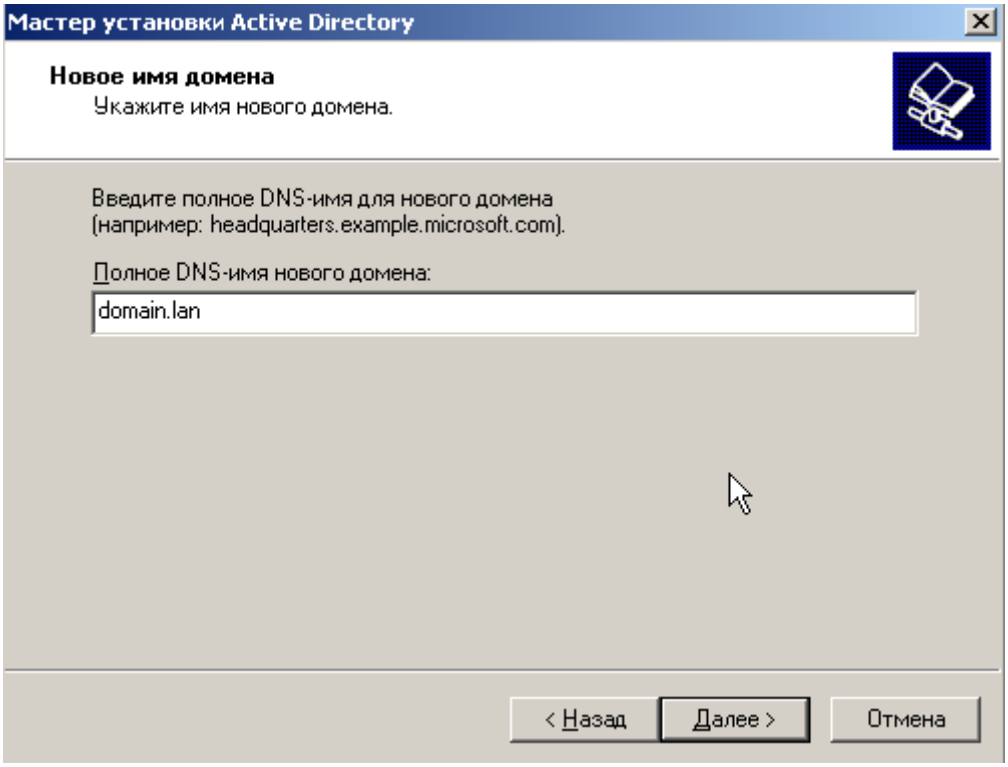


Рис. 6. Вводим полное DNS-имя для нового домена

Далее производим несколько шагов с настройками по умолчанию. В следующем окне установим нижний переключатель, поскольку о DNS мы поговорим позднее (рис. 7).

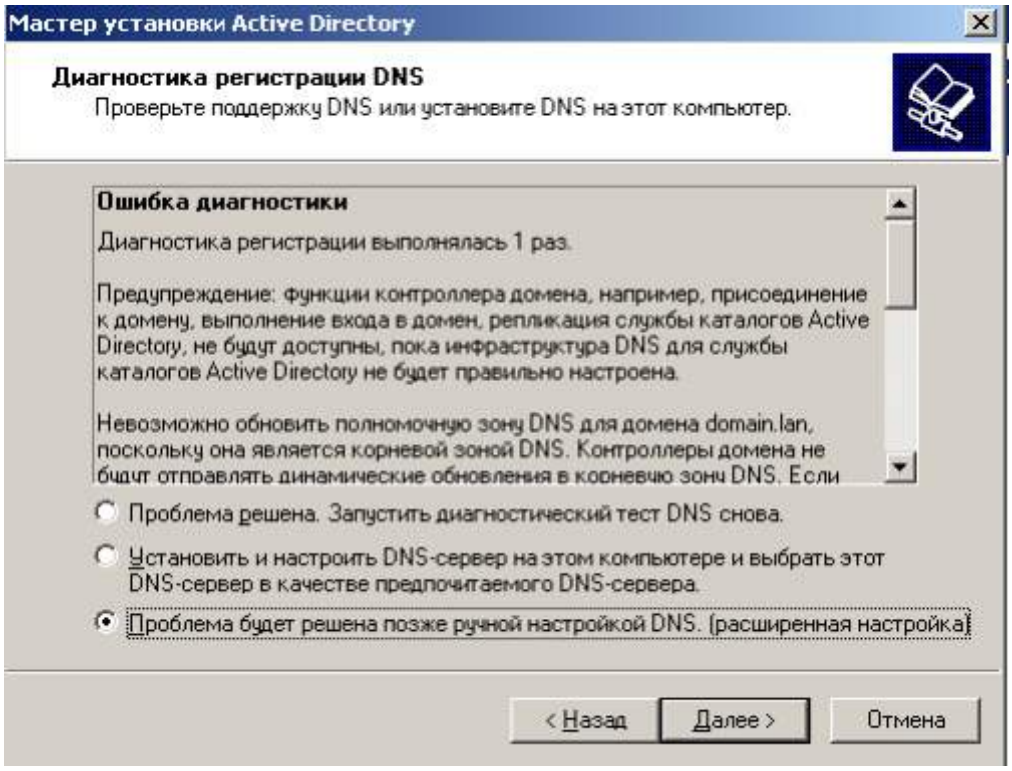


Рис. 7. Диагностика и регистрация DNS

Далее выбираем **Разрешения, совместимые только с Windows 2000 или Windows Server 2008** – рис. 8.

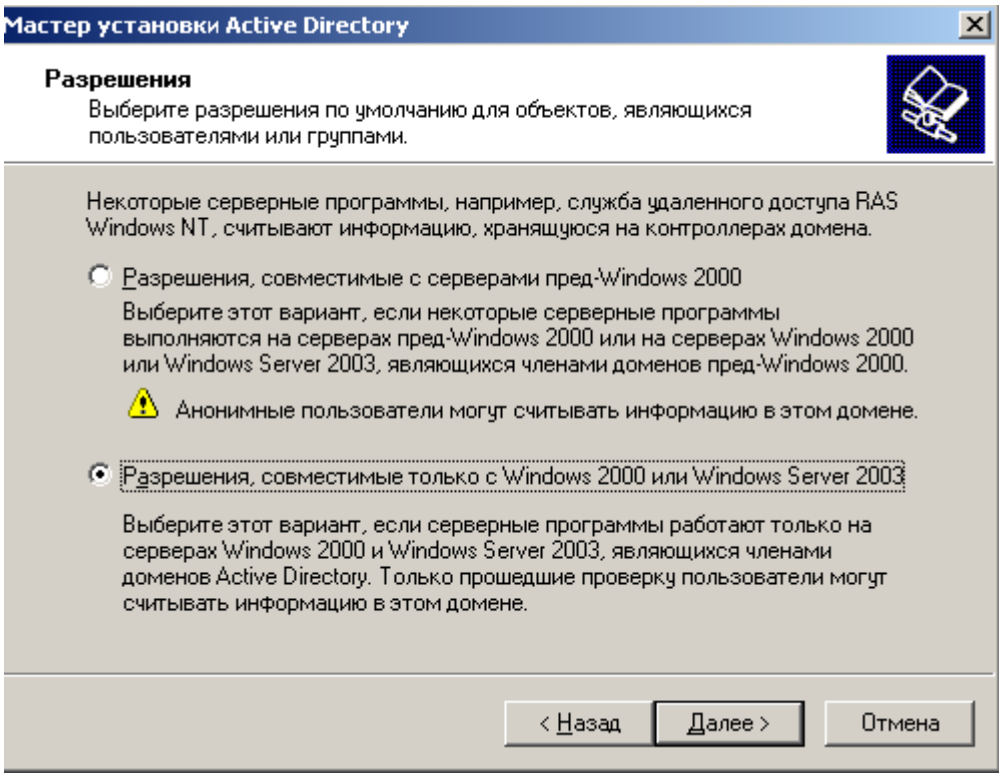


Рис. 8. Выбираем разрешения

Теперь вводим пароль администратора в режиме восстановления, например, тот же, что был при входе в систему - 123456, (рис. 9). Понятно, что простой или пустой пароль допустимы только в учебных целях.

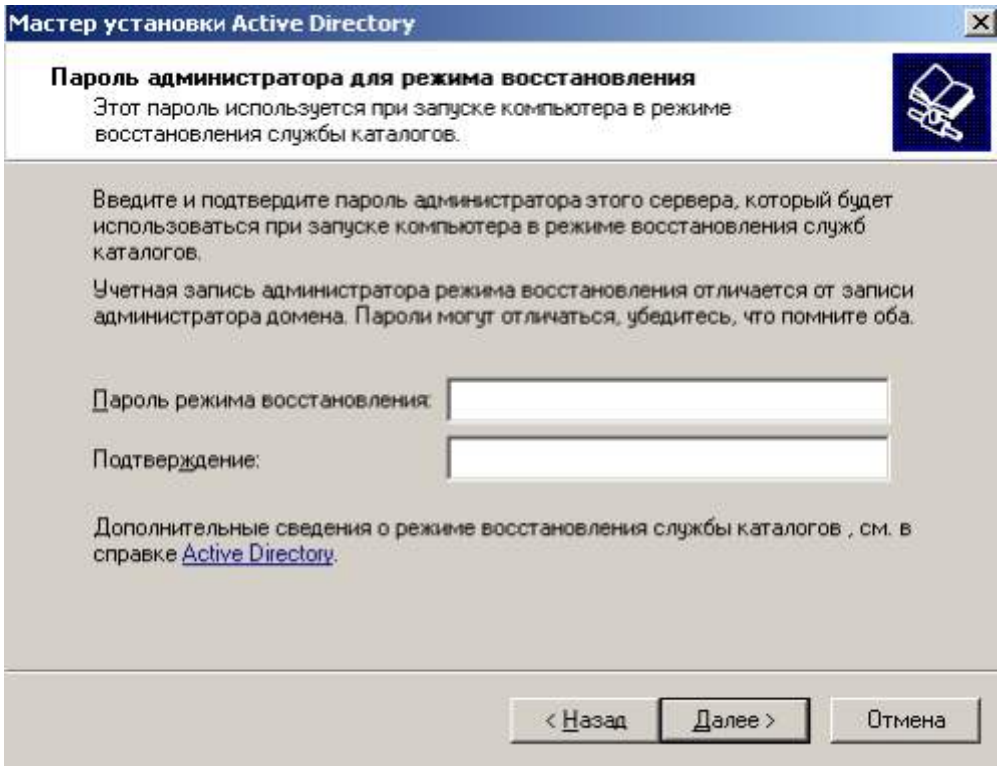


Рис. 9. Задаем пароль режима восстановления

Далее ждем, пока произойдет настройка **Active Dicertory (Активный каталог)** - рис. 10. На этом этапе может понадобиться установочный диск SP2.

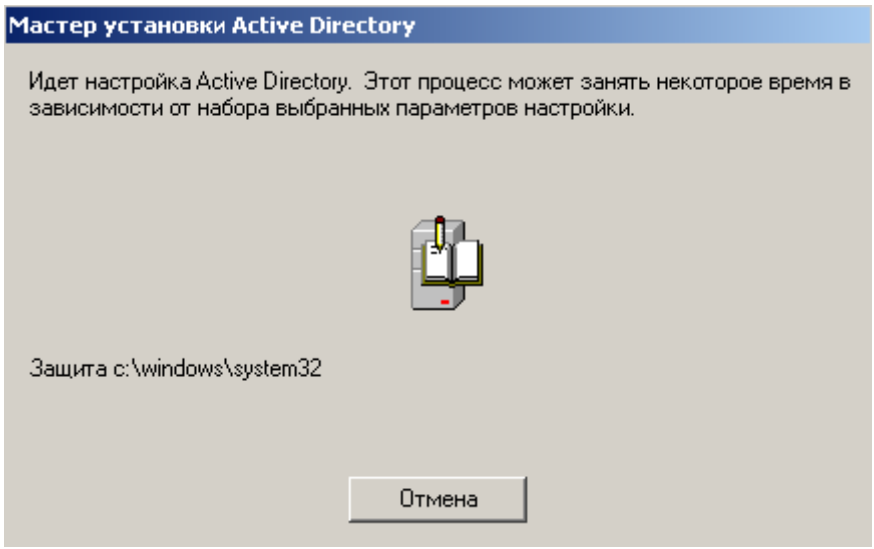


Рис. 10. Идет конфигурирование Active Dicertory

Далее Мастер успешно завершит свою работу следующим окном (рис. 11).

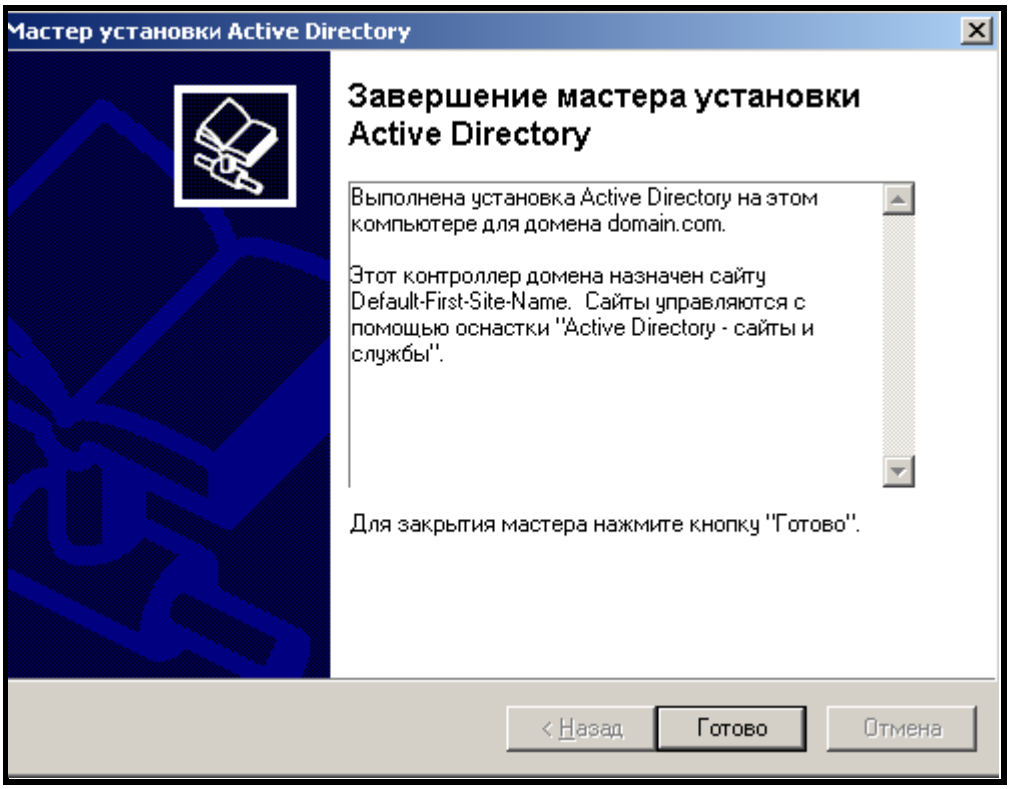


Рис. 11. AD установлена

Работа почти закончена: для домена (domain.lan) active directory установлена, а настройку DNS для этого домена мы сделаем позже.

Примечание

Настроить DNS-сервер означает привязать доменное имя **domain.lan** к IP адресу компьютера, на котором находится ваш сервер.

После перезагрузки мы увидим, что окно входа в систему изменилось

(рис. 12).

Рис. 12. В окне входа в систему появилась строка входа в домен

Далее увидим следующее сообщение (рис. 13).

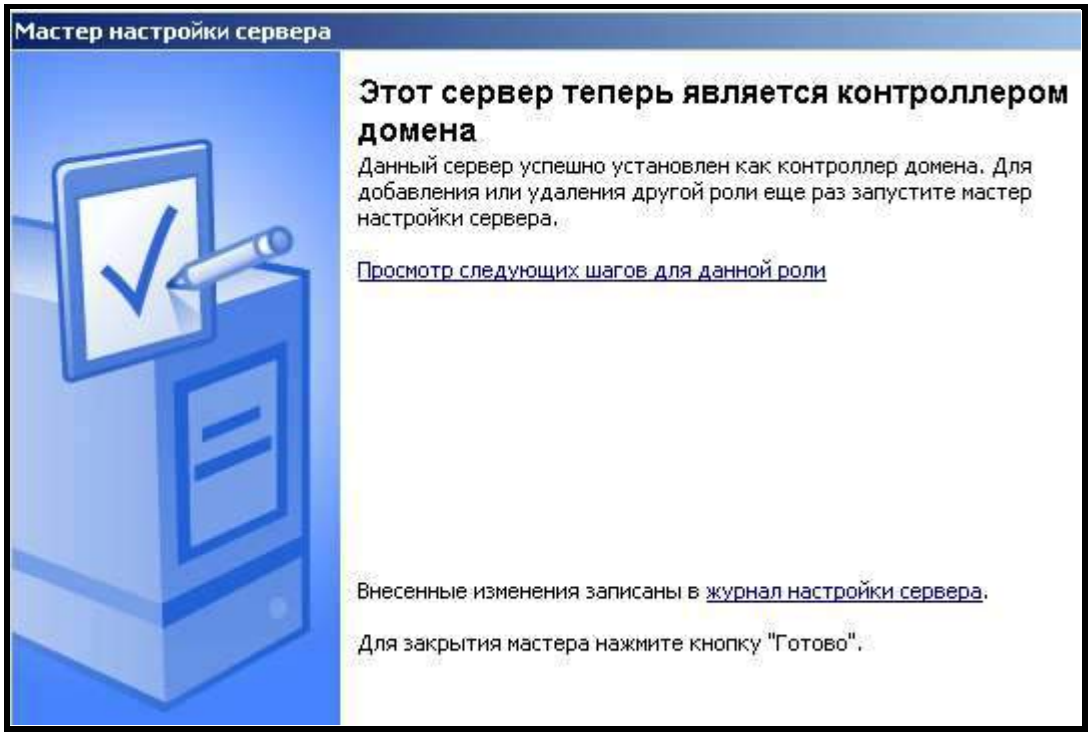


Рис. 13. Настройка роли сервера Контроллер домена завершена
Посмотрим, что изменилось

Выполним **Пуск-Все программы-Администрирование**. Вы увидите, что у нас появилось пять новых служб (рис. 14).

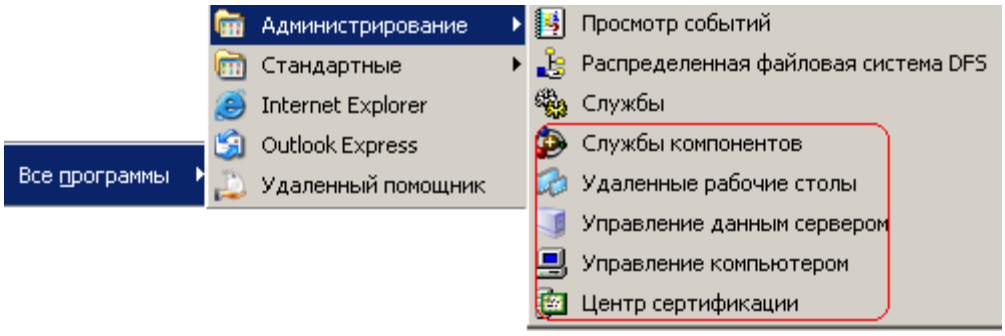


Рис. 14. Красным отмечены новые службы

Войдем в службы компонентов и увидим там наш домен (рис. 15). Доменное имя здесь можно было создать по имени вашей организации, например, NOVGU.LAN или GORGAZ.LAN.

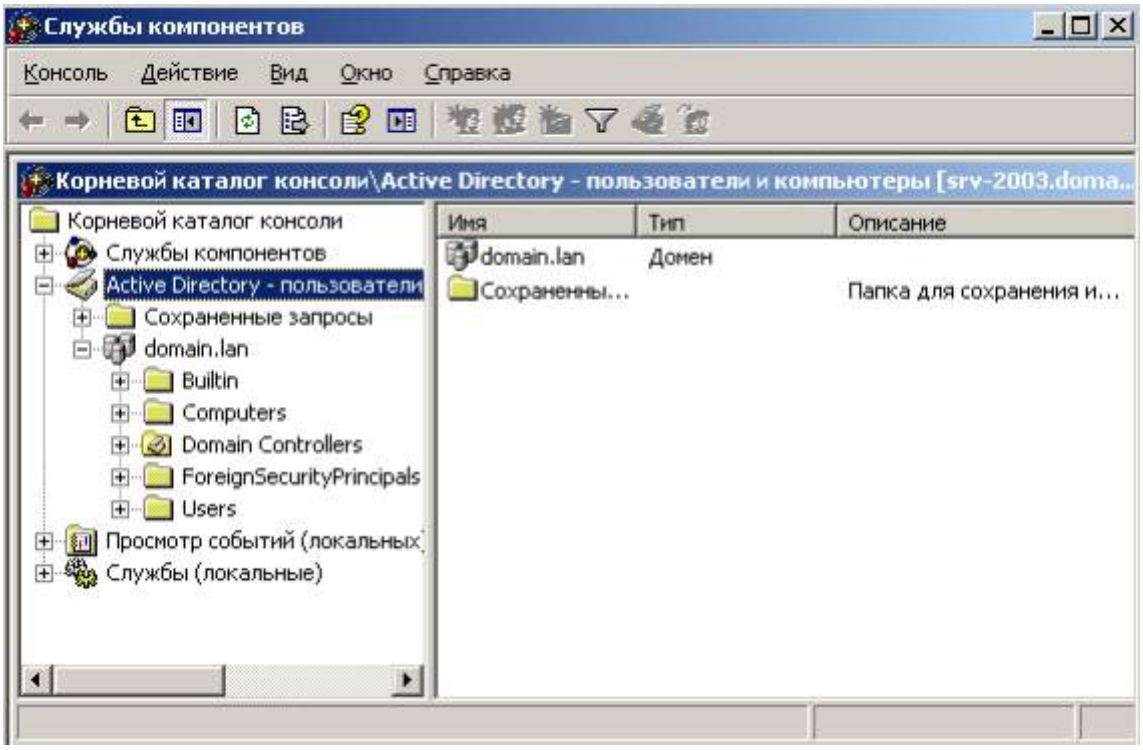


Рис. 15. В AD видим domain.lan

Пока в домене нет компьютеров, но есть пользователи. Дважды щелкнув на учетную запись **Администратор** мы можем задать характеристики данного пользователя (рис. 16).

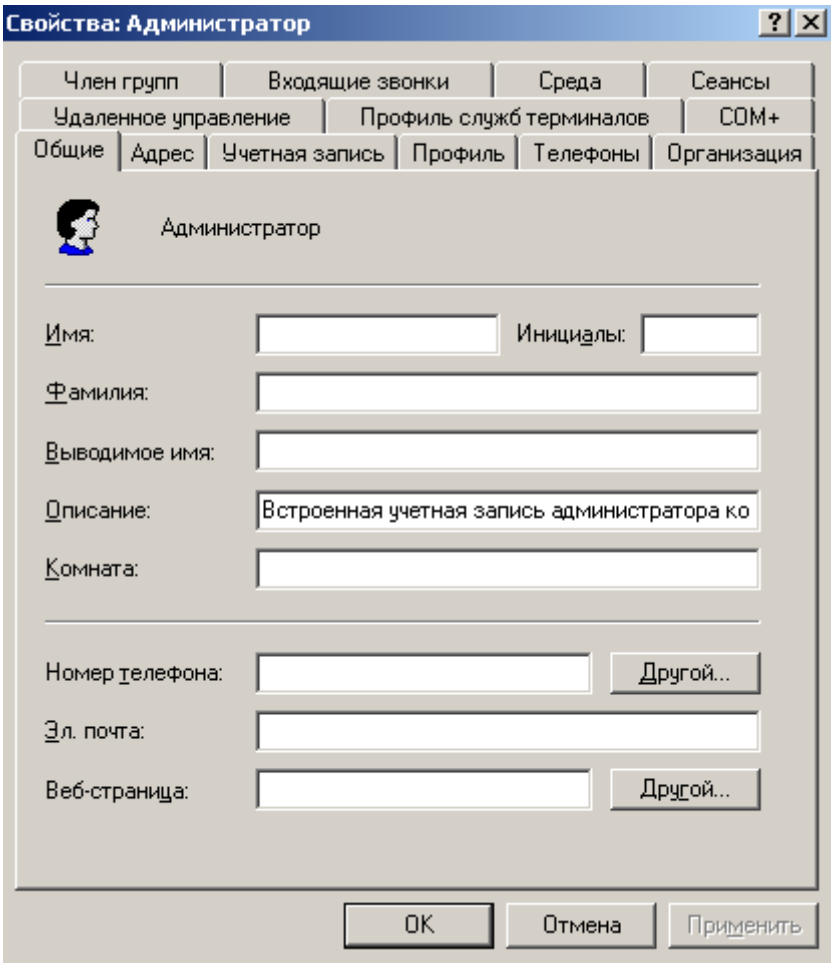


Рис. 16. Окно свойств записи Администратор

Таким образом, номер телефона администратора сети или его почту можно, затем найти из кнопки **Пуск-Поиск-Другие параметры поиска-Принтеры, компьютеры или людей** (рис. 17). Подобным образом заводится информация не только на администратора, но и на других пользователей AD.

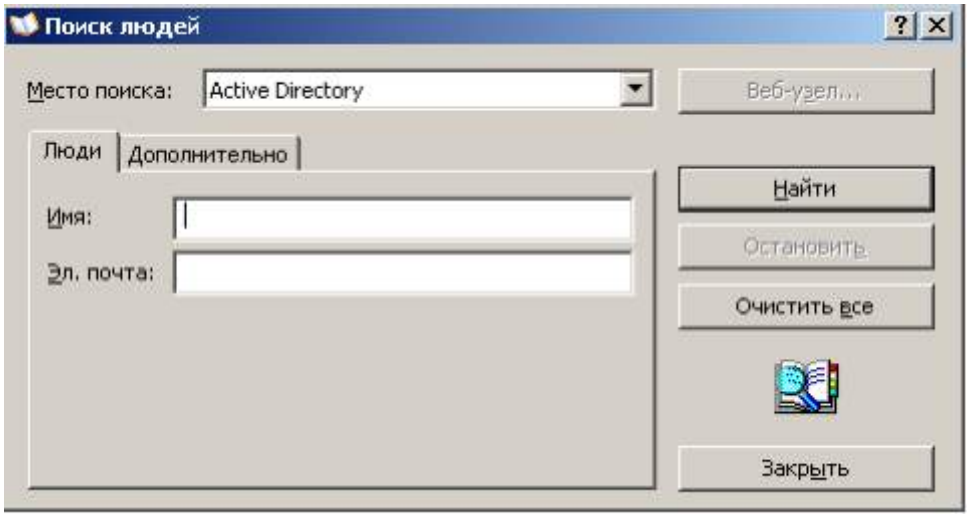


Рис. 17. Окно поиска людей в AD

Домен, дерево доменов, лес и др.

В сети Клиент-Сервер компьютеры могут объединяться в логические единицы, называемые доменами. В одноранговой сети аналогом домена является рабочая группа. Множество доменов образует структуру, похожую на дерево. Каждый домен управляется контроллером домена. Компьютер может входить в состав только одного домена, а доменов может быть несколько. При объединении доменов в лес их конфигурация становится одинаковой (рис. 18).

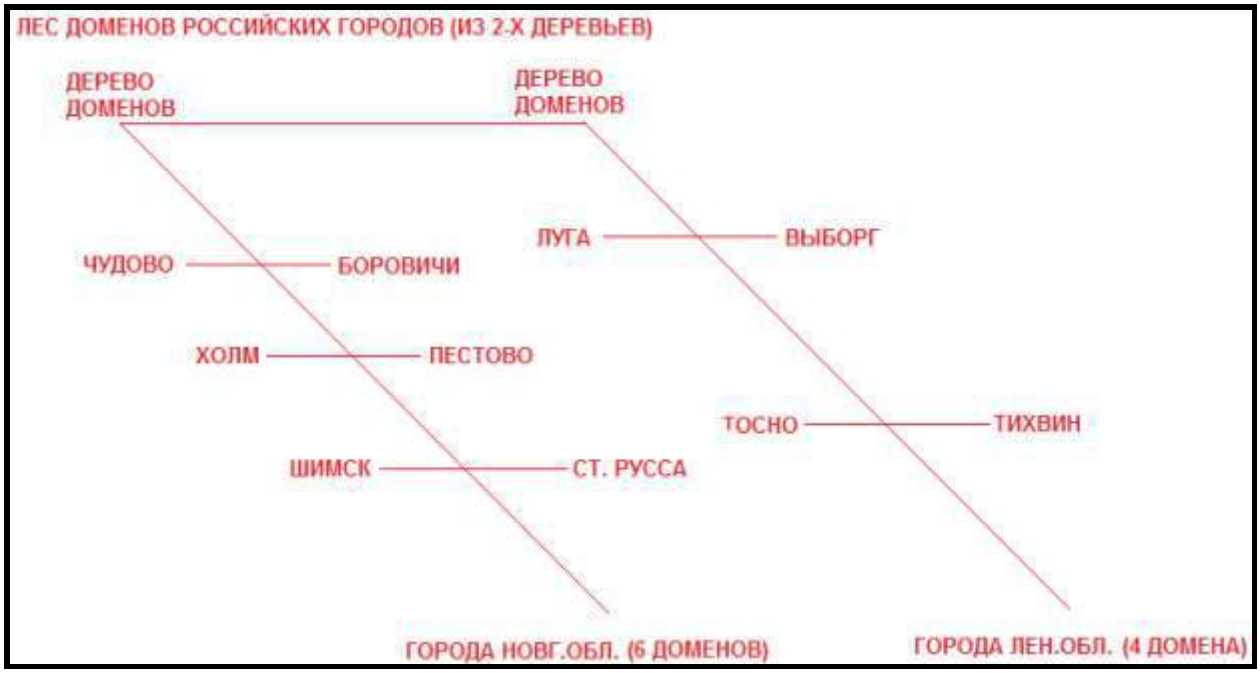
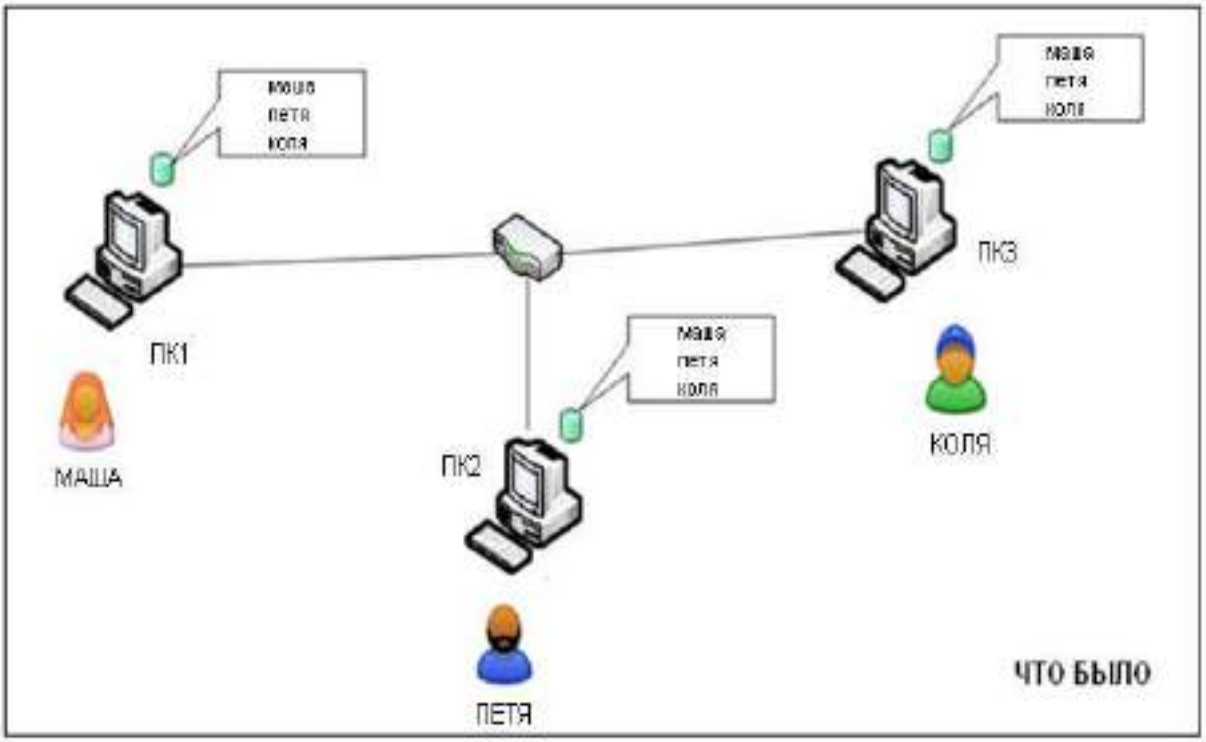


Рис. 18. Пример по аналогии из нашей жизни, дающий представление о лесе доменов

Active Directory (AD-Активный каталог)

AD – справочник о всех объектах сети (пользователях, их паролях etc). Это база данных, содержащая информацию о ресурсах, службах и учетных записях. Для простоты понимания, вы можете представить себе телефонный справочник, содержащий информацию о людях, их телефонах и адресах. На рис. 19 показано как было в локальной сети до использования сервера и **Active Directory (Активный каталог),** и как стало после.



a)Ситуация в сети “До” создания AD

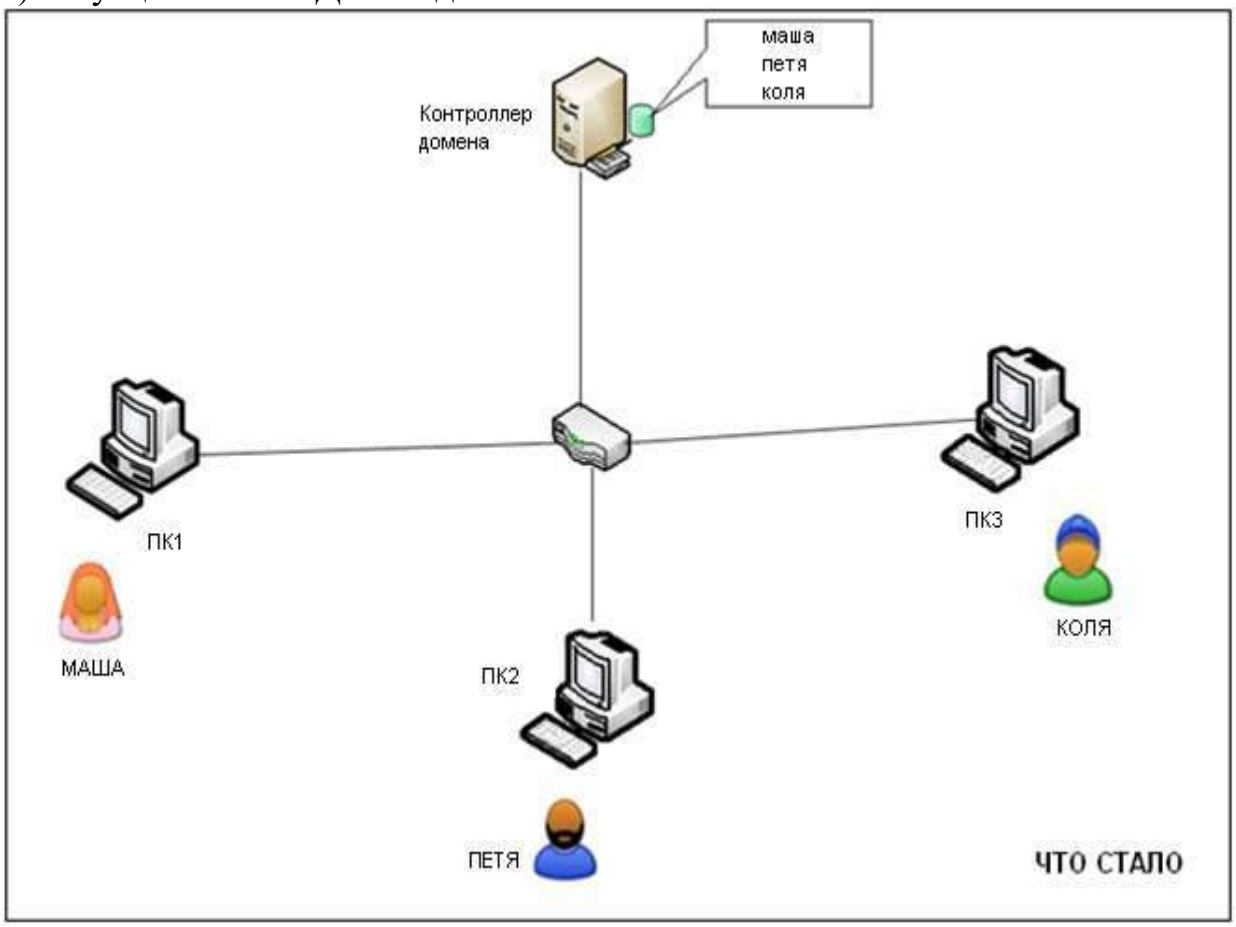


Рис. 19. b)Ситуация в сети “После” создания AD

Как видим из рисунка, "До" – учетные записи пользователя и их ресурсы хранились на локальных ПК. "После" – на сервере. Таким образом, одно из достоинств AD заключается в том, что с появление контроллера домена учетные записи хранятся не на локальных ПК, а на сервере. Поэтому, при поломке одного из ПК пользователь может авторизоваться на любом из локальных ПК и работать, используя ресурсы сервера.

Задание 1. Сколько в лесу (рис. 20) деревьев и доменов?

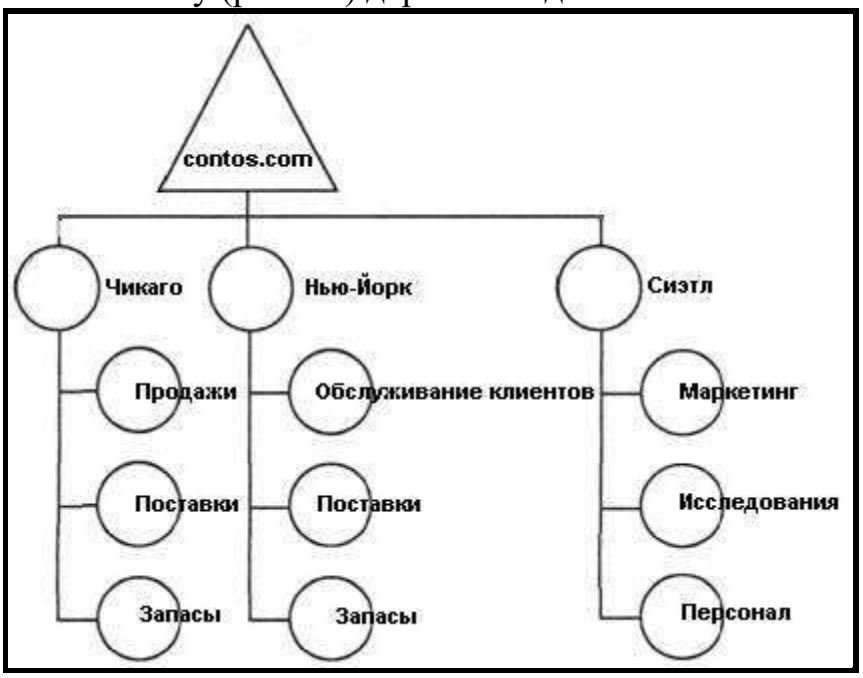


Рис. 20. Пример леса доменов

В качестве примера-подсказки на рис. 21 показан лес из двух деревьев:

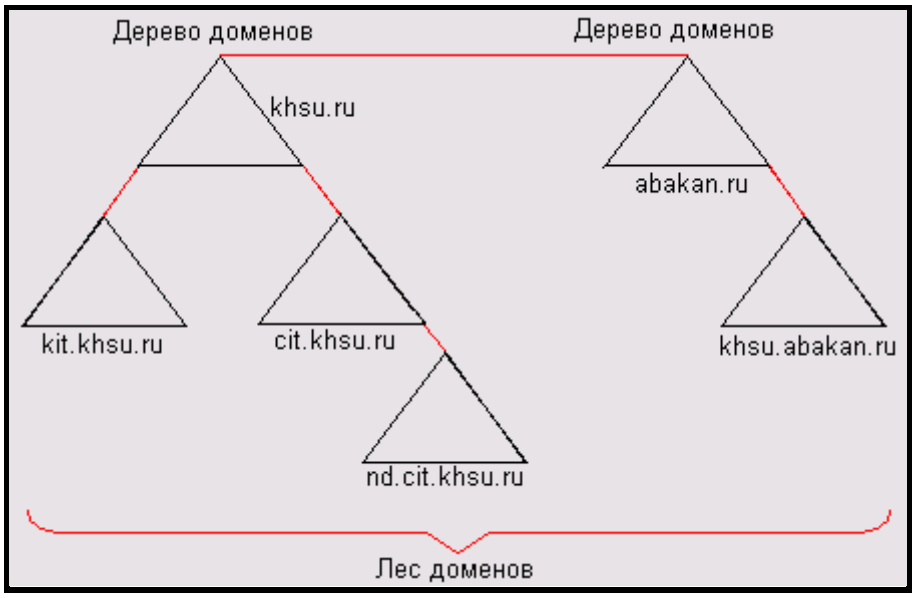


Рис. 21. Один лес, который содержит два дерева доменов

ПРАКТИЧЕСКАЯ РАБОТА №20.
УСТАНОВКА DNS СЕРВЕРА

Цель работы:
Изучить работу по установке DNS сервера

В этой работе мы присвоим серверу роль DNS сервера.

Выбор для сервера роли DNS сервера

DNS (Domain Name System — система доменных имён) — компьютерная система для получения IP-адреса по имени хоста и обратно.

Назначим нашему серверу роль DNS сервера (рис. 1).

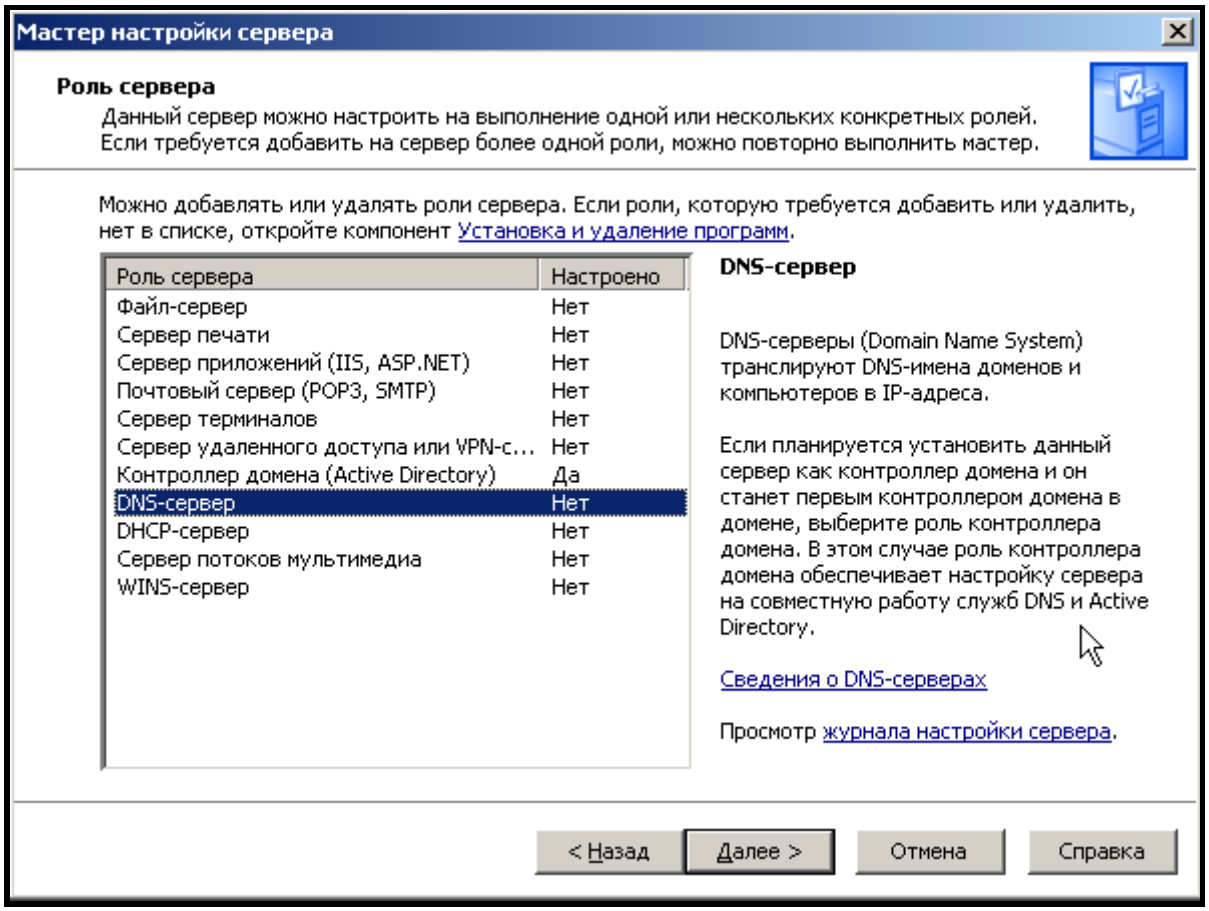


Рис. 1. Мастер настройки сервера-DNS сервер

Далее появиться предложение изменить динамический IP адрес на статический (рис. 2).

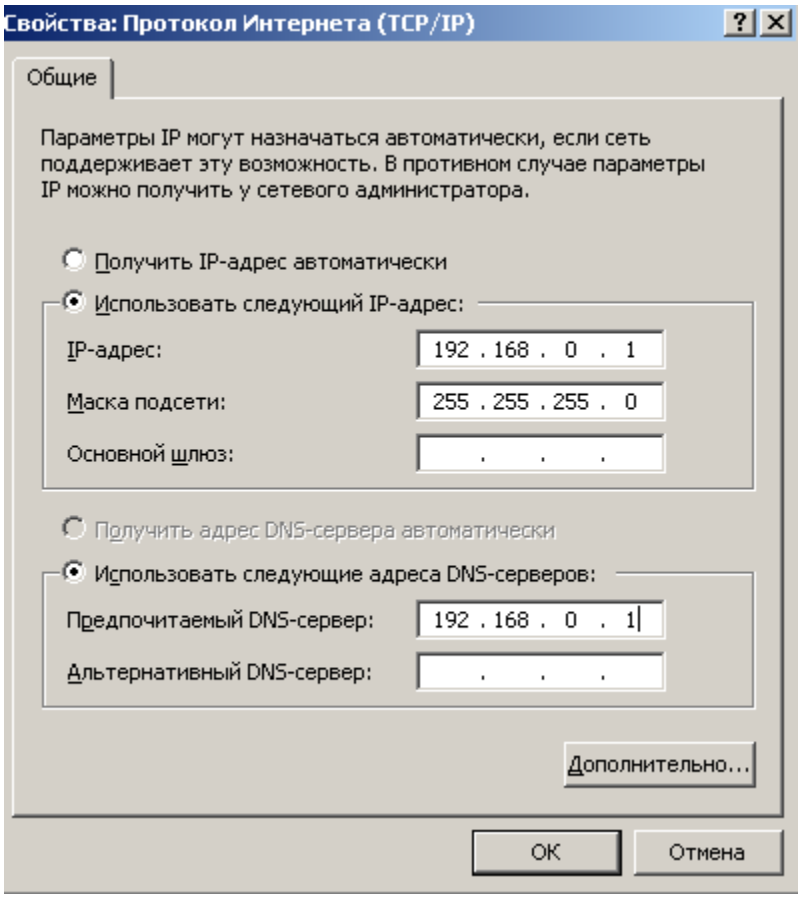


Рис. 2. Задаем серверу статический IP адрес

Далее появится Мастер настройки DNS сервера (рис. 3).

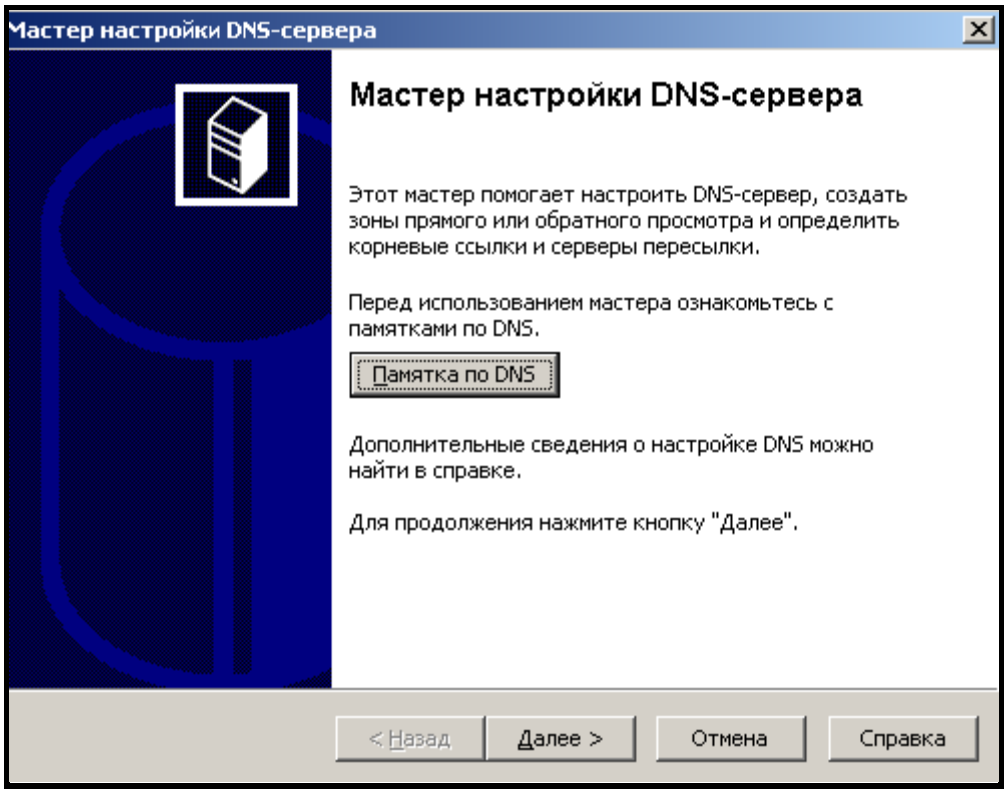


Рис. 3. Окно Мастер настройки DNS сервера

Поскольку сеть у нас небольшая, то установим верхний переключатель (рис. 4).

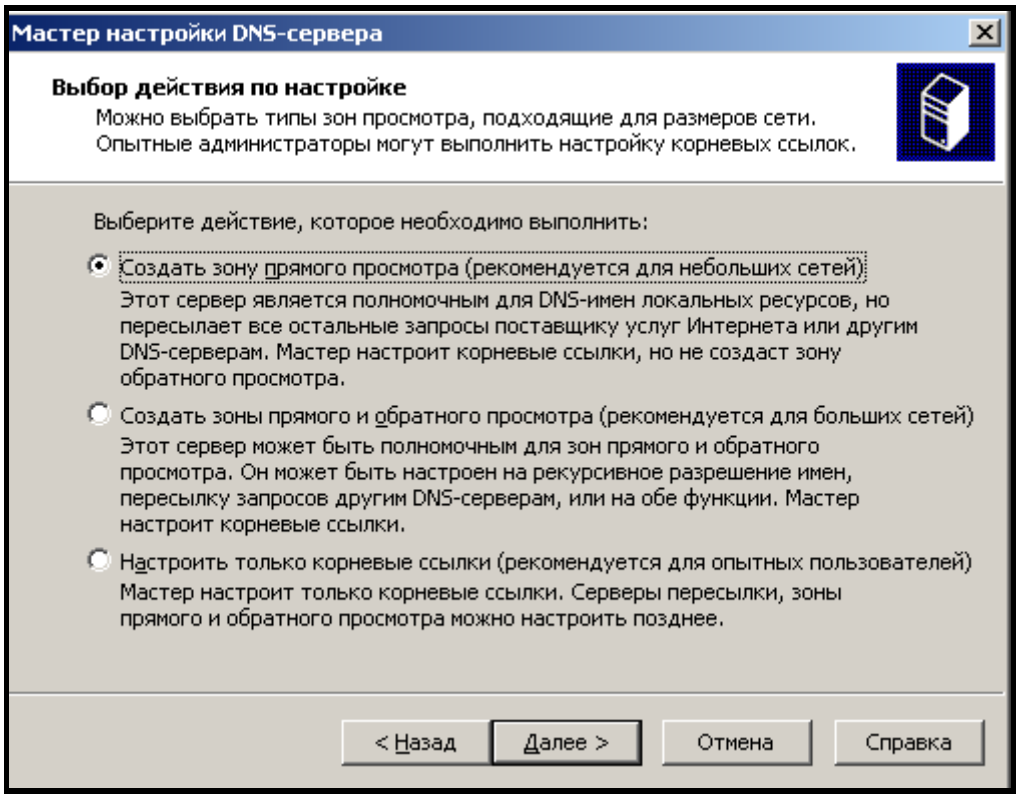


Рис. 4. Создание зоны прямого просмотра

Зону прямого просмотра назовем так же, как и домен – domain.110. Далее исходим из того, что у нас только один DNS сервер, больше пересылать запросы некому (рис. 5).

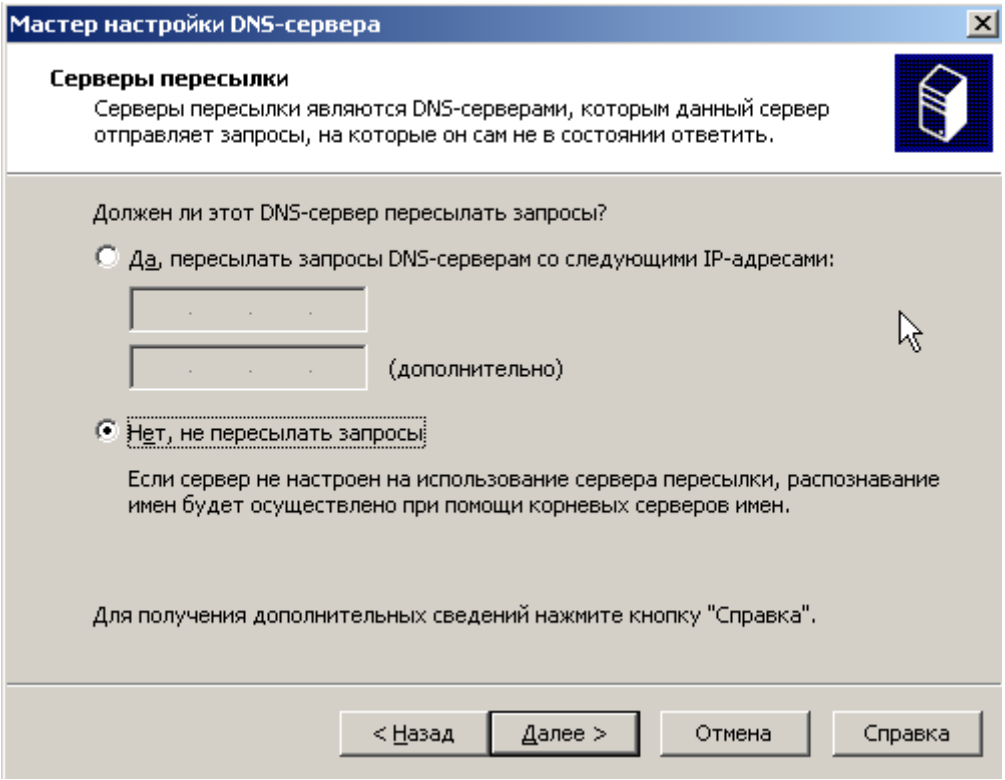


Рис. 5. Активируем нижний переключатель

Настройка сервера завершена (рис. 6).

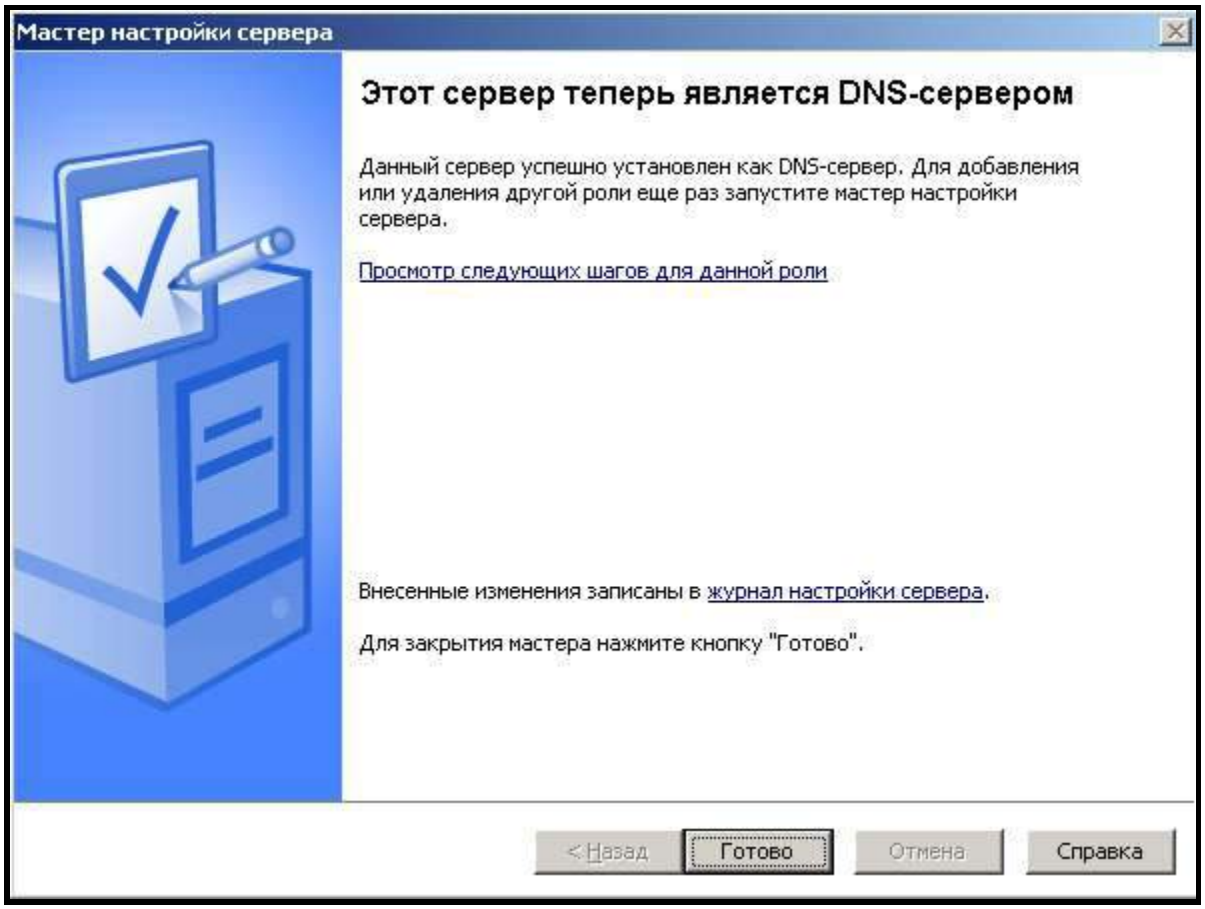


Рис. 6. Сервер получил роль DNS сервера

Выполнив команду, **Пуск-Все программы-Администрирование** мы увидим, что появилась новая оснастка (рис. 7).

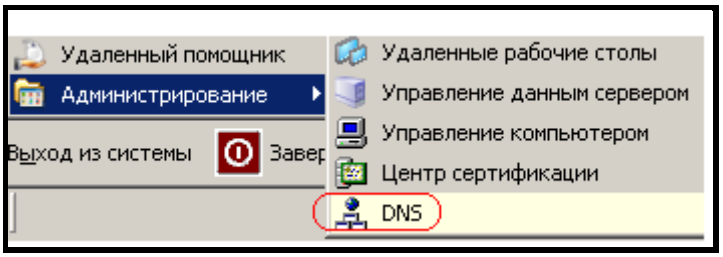


Рис. 7. На рисунке новая оснастка отмечена красным

Откроем ее (рис. 8). Здесь в зоне прямого просмотра вы можете увидеть соответствие имени сервера srv-2003 его IP адресу 192.168.0.1.

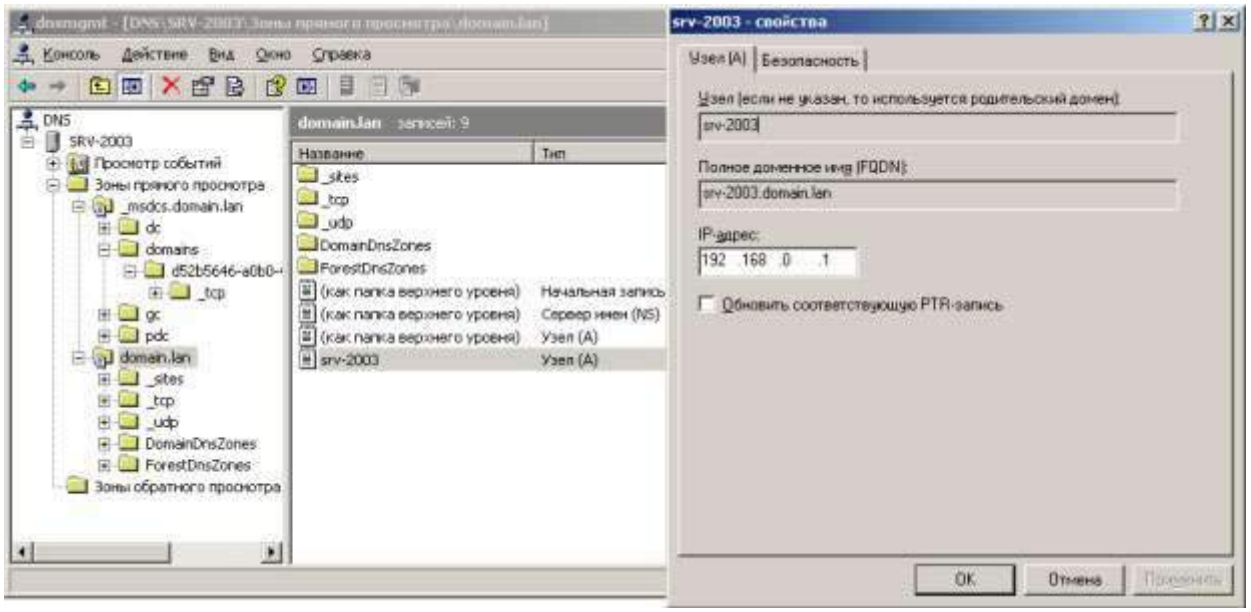


Рис. 8. На рисунке открыта зона прямого просмотра

Создание зоны обратного просмотра

Щелкните на строчку **Зона обратного просмотра** и выберите команду **Создать новую зону** (рис. 9).

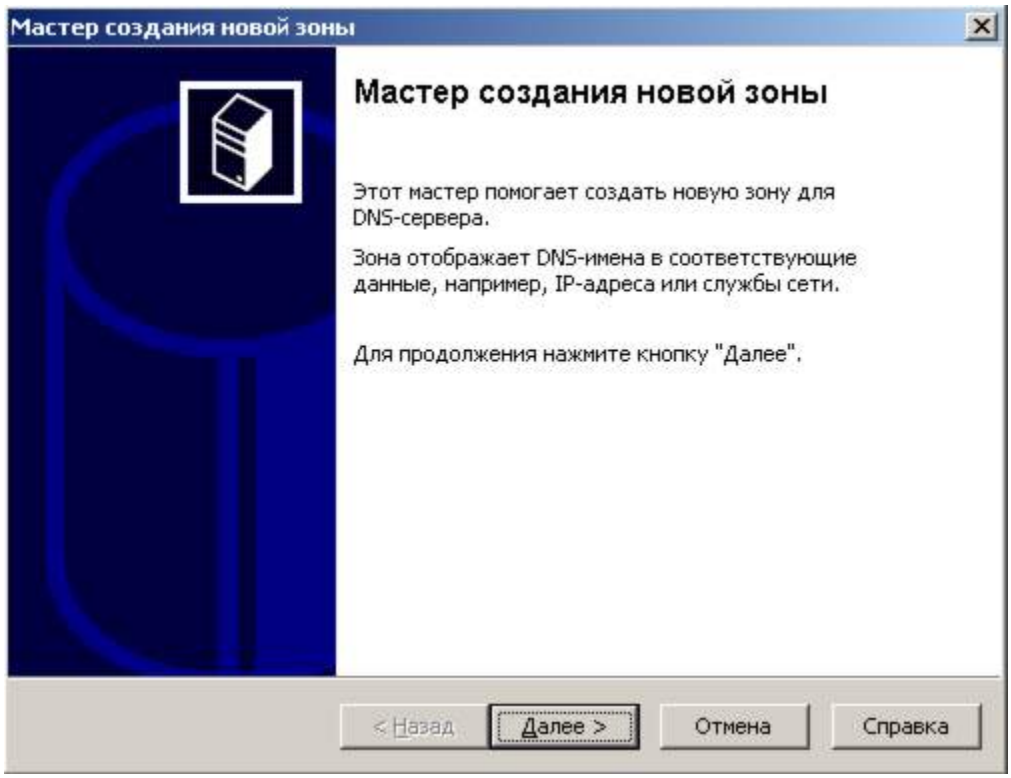


Рис. 9. Окно мастера создания новой зоны

Далее устанавливаем верхний переключатель - рис. 12.

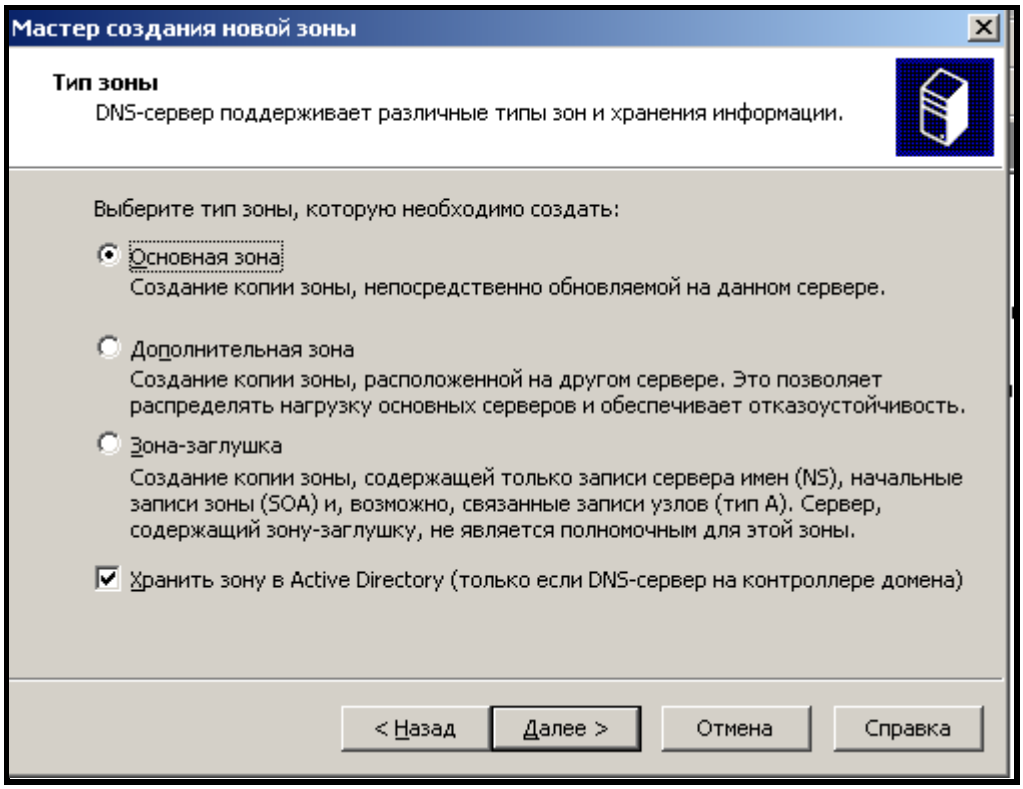


Рис. 10. Устанавливаем переключатель Основная зона

Примечание

Основная зона устанавливается на основной сервер (она - главная), **Дополнительная зона** необходима для резервирования и разгрузки основного сервера. Если загрузка первого DNS сервера велика (или он отключился), то часть запросов можно отправить на второй, альтернативный DNS и отказоустойчивость системы повышается (рис. 11). Зона - заглушка содержит IP адрес сервера, который может обслужить запрос.

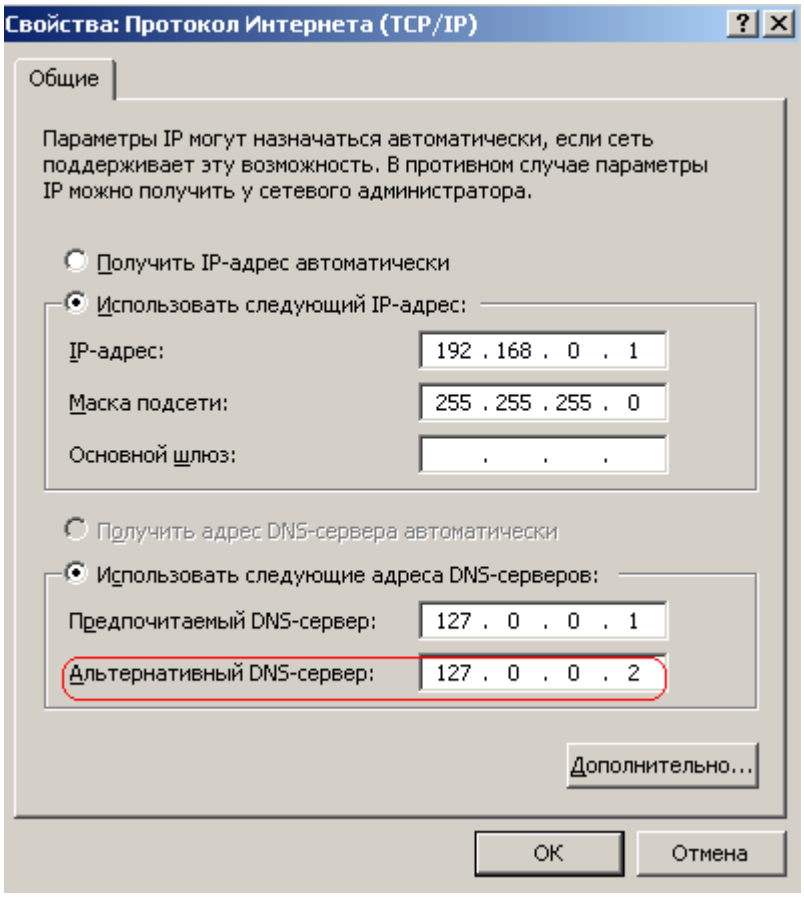


Рис. 11. Пример использования альтернативного DNS сервера

Наша сеть 192.168.0.1 относится к классу сетей С, поэтому значение 192.168.0 мы менять не можем - это и есть код сети (ID) – рис.12.

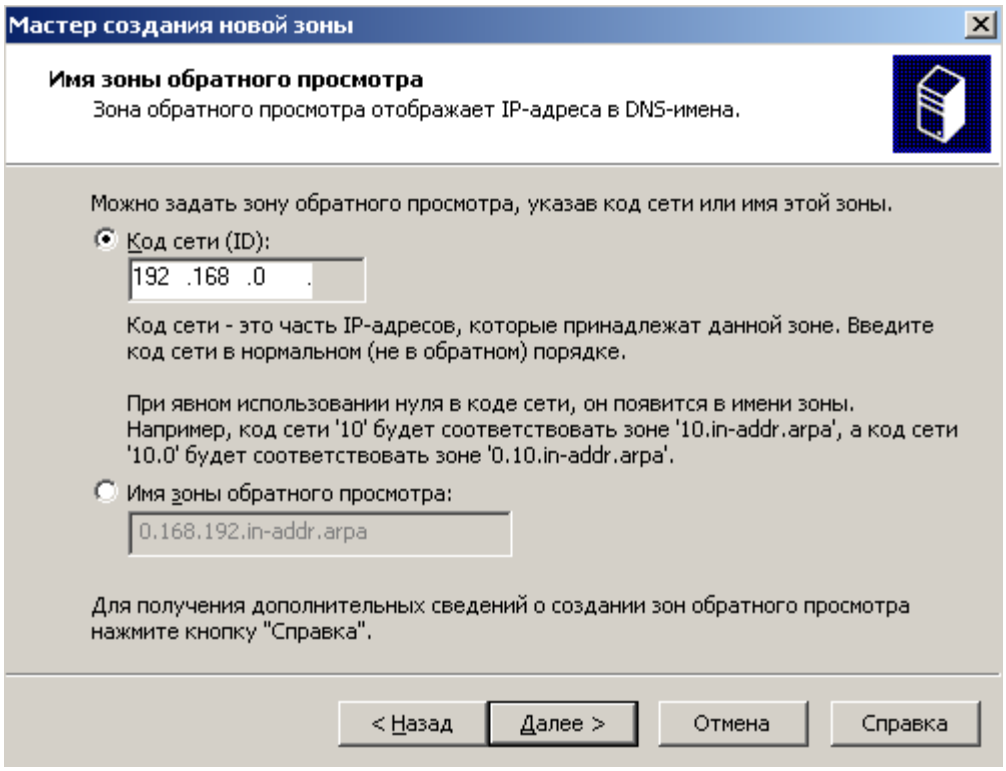


Рис. 12. Задаем код сети

Зона обратного просмотра создана. После подключения первого ПК здесь появится соответствие IP адреса ПК его имени.

Записи ресурсов DNS

Вся DNS состоит из этих RR записей, по которым пользователь может искать ресурсы в сети. Запустим консоль управления DNS и зайдем в зону прямого просмотра (рис. 13).

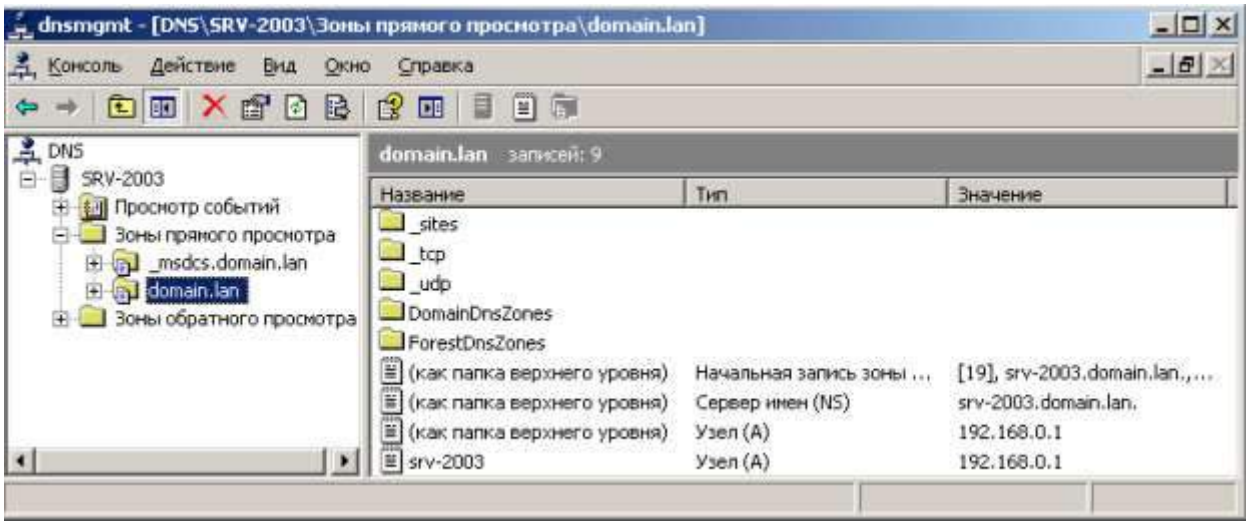


Рис. 13. Зоны прямого просмотра

Выполним двойной щелчок на строчке **Начальная запись зоны** (рис. 14). В данном окне наиболее интересный параметр **Срок жизни (TTL**). Предположим, что компьютер с именем ПК-1 и IP адресом 192.168.0.1 хочет соединиться с именем ПК-2 и IP адресом 192.168.0.2. Он выдает запрос на DNS сервер и тот сообщает, что с компьютер с именем ПК-2 имеет IP адрес 192.168.0.2. Эта запись кэшируется (помещается в память) на **Срок жизни (TTL).** Подобный подход к запросам снижает нагрузку на DNS сервер.

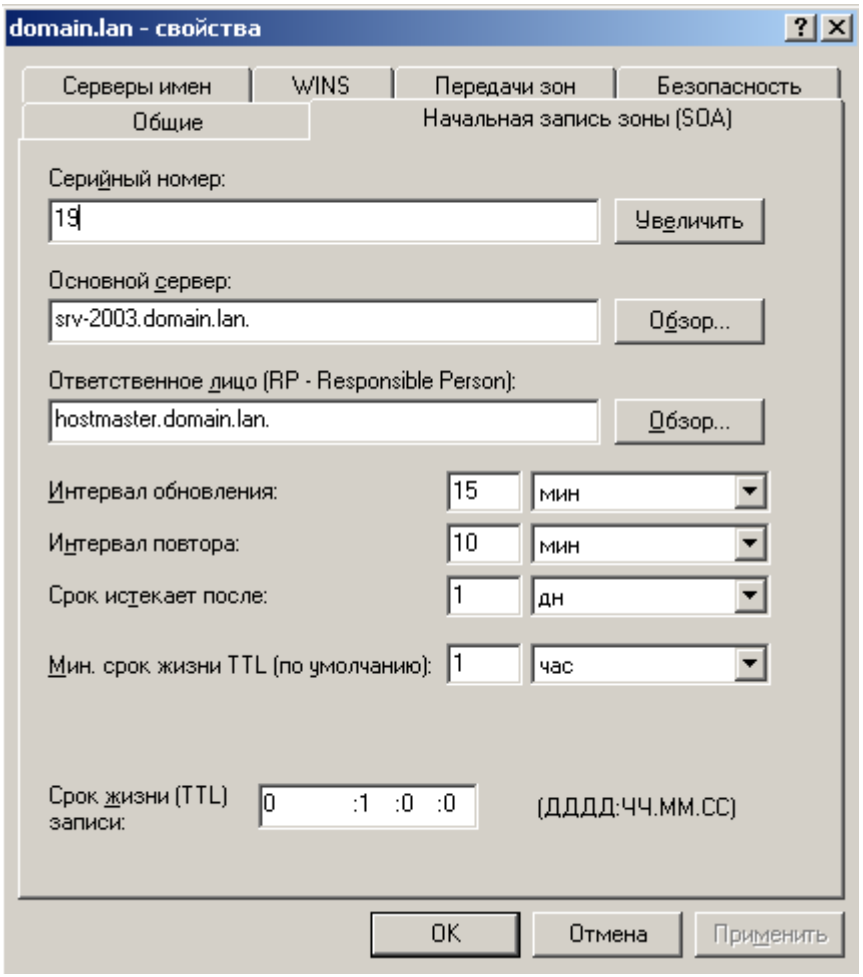


Рис. 14. Вкладка Начальная запись зоны

Теперь выполним двойной щелчок на строчке **Сервер имен** (рис. 15). У нас DNS сервер один, поэтому запись здесь одна. Но, здесь записей может быть столько, сколько имеется DNS серверов.

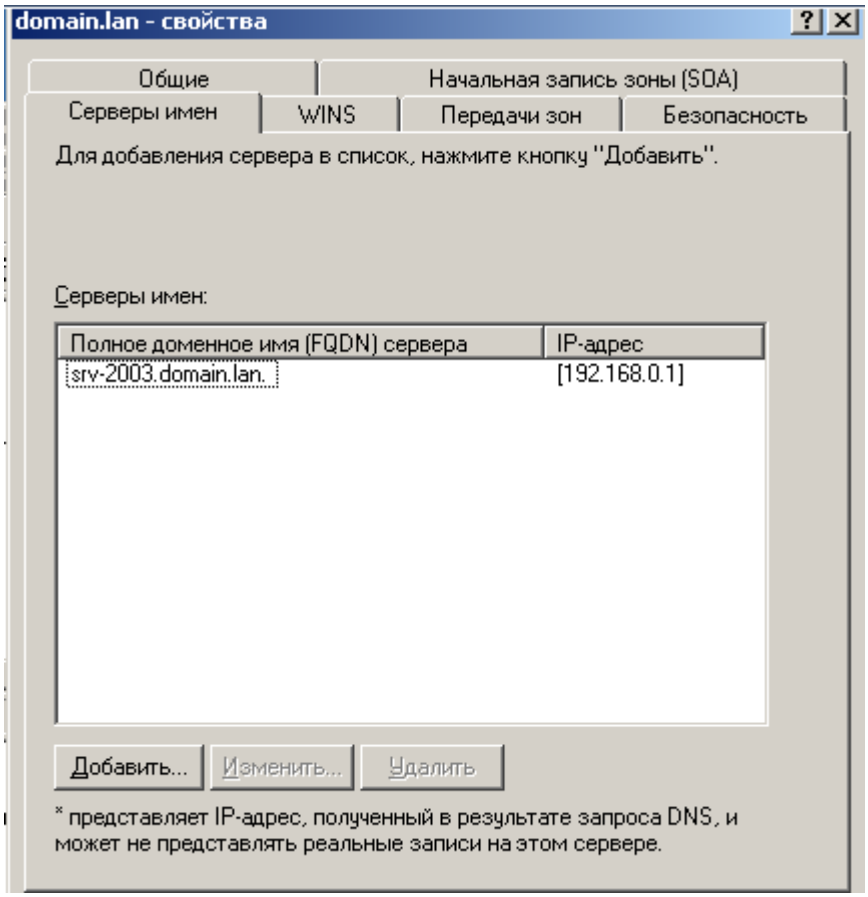


Рис. 15. Вкладка Серверы имен

Выполним двойной щелчок на строчке **Узел А** (рис. 16). Эта запись устанавливает прямое соответствие между именем ПК и его IP адресом.

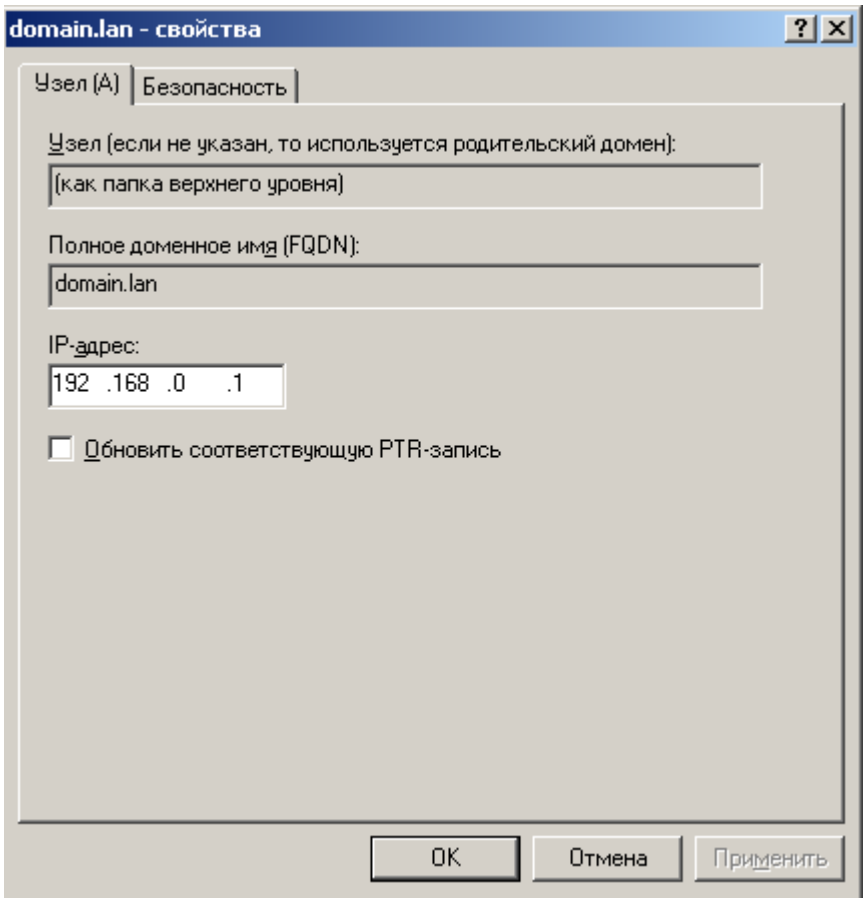


Рис. 16. Вкладка Узел А

Теперь изучим записи зоны обратного просмотра. После перезагрузки ПК здесь будет три записи (рис. 17).

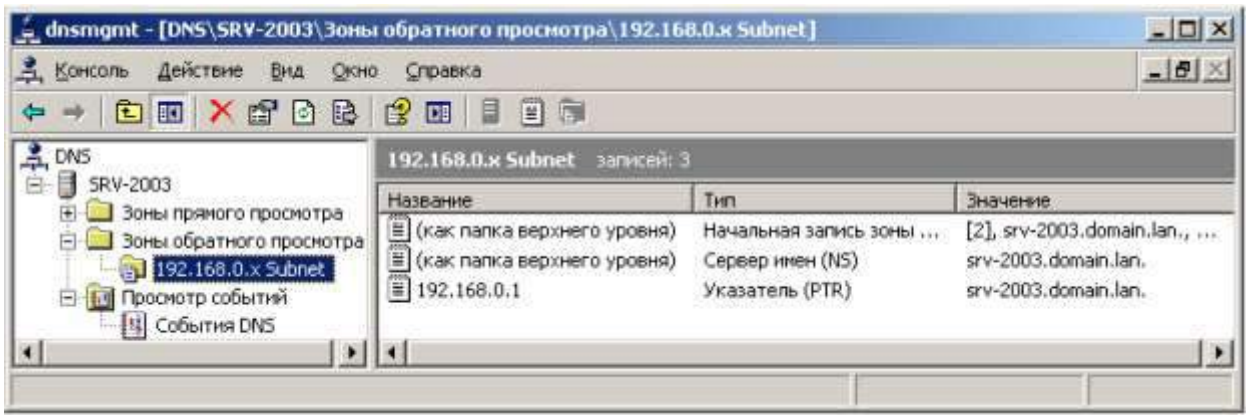


Рис. 17. Записи зоны обратного просмотра

Двойным щелчком мыши зайдем в **Указатель (PTR)** – рис. 18. Как видим, именно здесь задается обратное соответствие IP адреса и имени ПК.

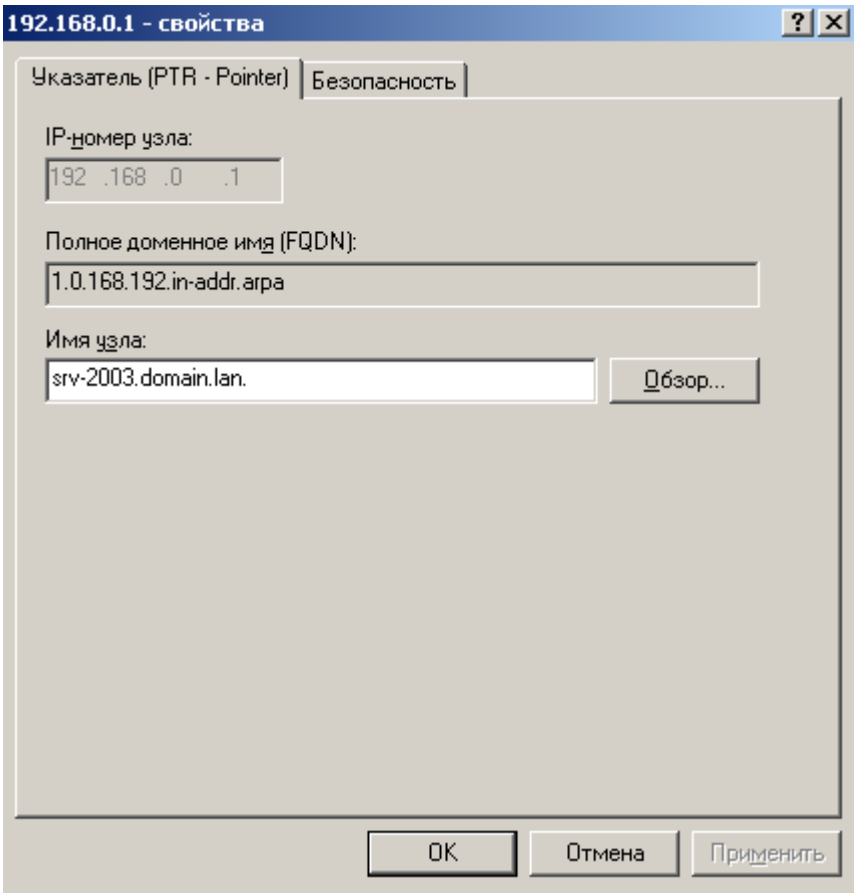


Рис. 18. Вкладка Указатель (PTR)

Проверка работы зон прямого и обратного просмотра

Далее вызовем командную строку и пропингуем наш сервер (рис. 19). Видим, что зона прямого просмотра работает нормально и имени SRV-2003 ставится в соответствие IP адрес 192.168.0.1.

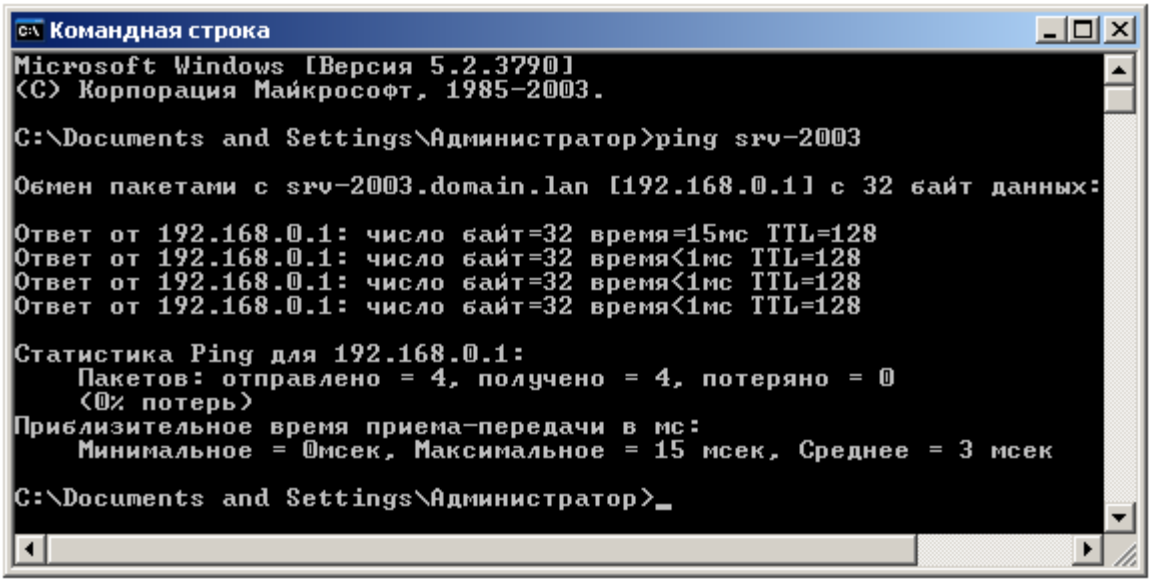


Рис. 19. Окно Командная строка

Если пропинговать не имя, а IP адрес и использовать ключ "-a", то увидим, что зона обратного просмотра также работает хорошо (рис. 20). Обмен данными идет нормально.

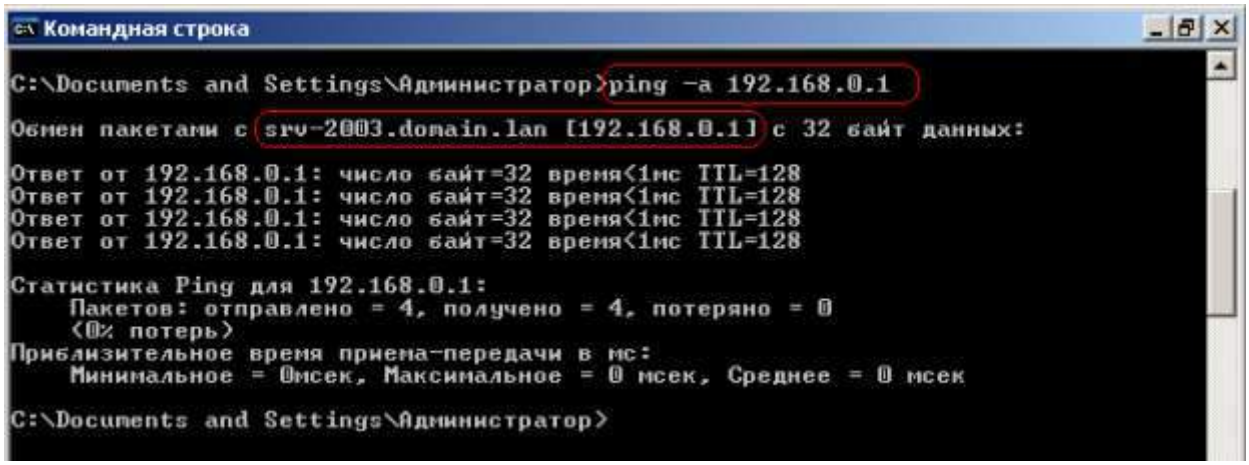


Рис. 20. Зона обратного просмотра работает хорошо

ПРАКТИЧЕСКАЯ РАБОТА №21.
УСТАНОВКА И НАСТРОЙКА СЛУЖБЫ DHCP

Цель работы: Изучить работу по установке службы DHCP

Установим и настроим DHCP сервер, затем проверим его работоспособность.

Установка DHCP сервера

Для того, чтобы добавить компьютер в домен, необходимо для него вручную прописать IP-адрес, маску, основной шлюз, предпочтительный и альтернативный адреса DNS. Это несложно, если в сети мало компьютеров, а если их сотни, то потребуется **DHCP (Dynamic Host Configuration Protocol —** протокол динамической конфигурации **хоста**), который, назначит IP хосту автоматически.

Войдем в **Управление сервером**, нажмем на кнопку **Добавить или удалить роль** и в окне **Мастер настройки сервера** выберем строчку **DHCP сервер** (рис. 1), а затем заполним окно **Имя области** (рис. 2).

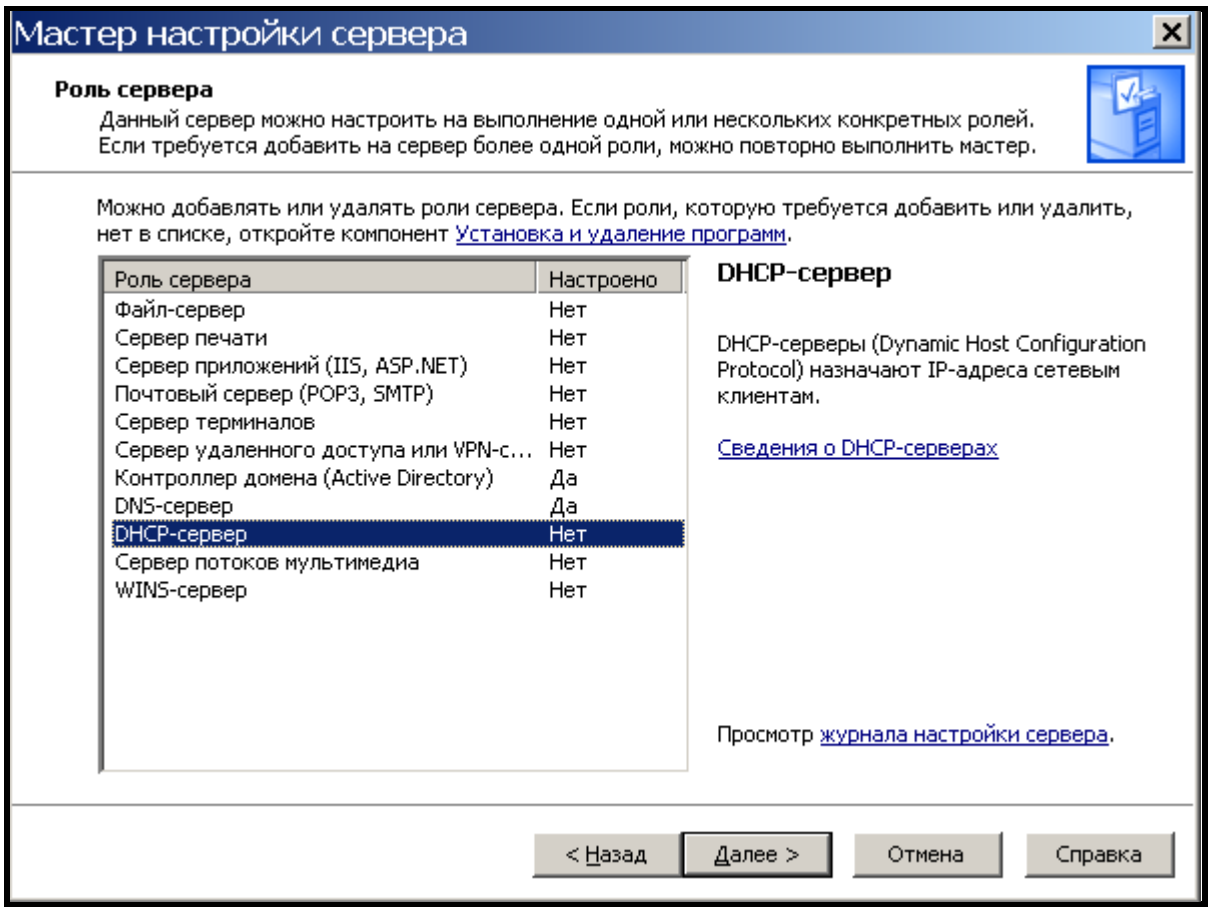


Рис. 1. Задаем серверу роль DHCP сервера

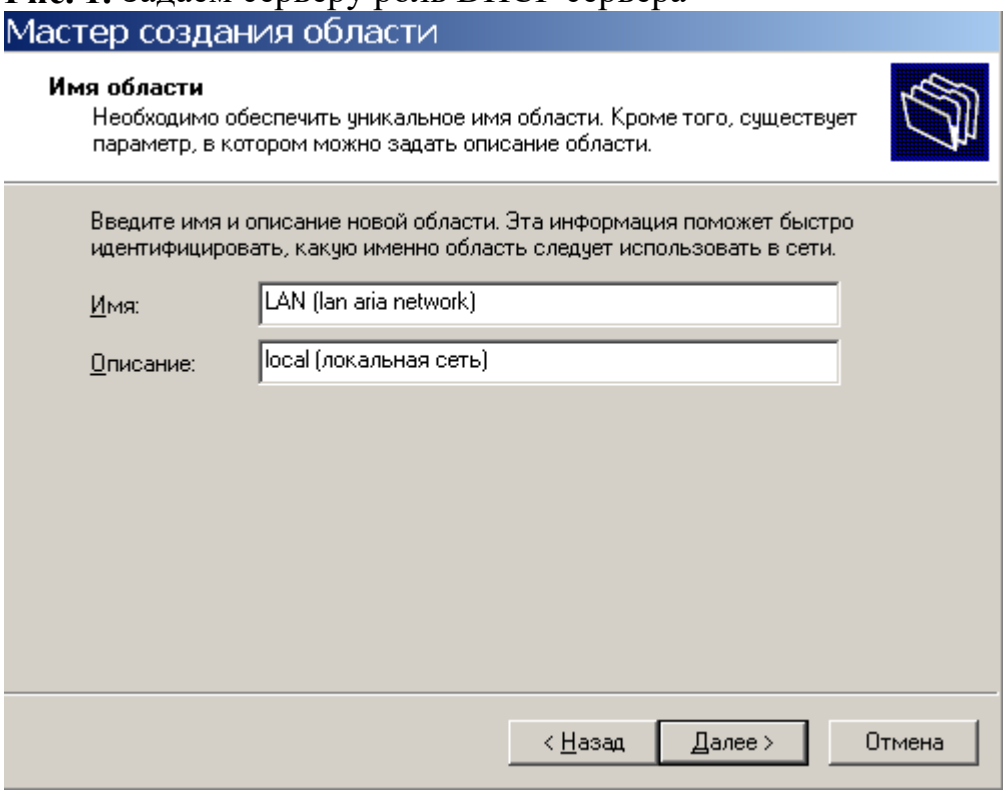


Рис. 2. Задаем имя и описание области для сети

В следующем окне пишем диапазон IP адресов нашей сети, то есть, зададим диапазон в 90 адресов, из этого диапазона будут назначаться IP для наших клиентских ПК (рис. 3).

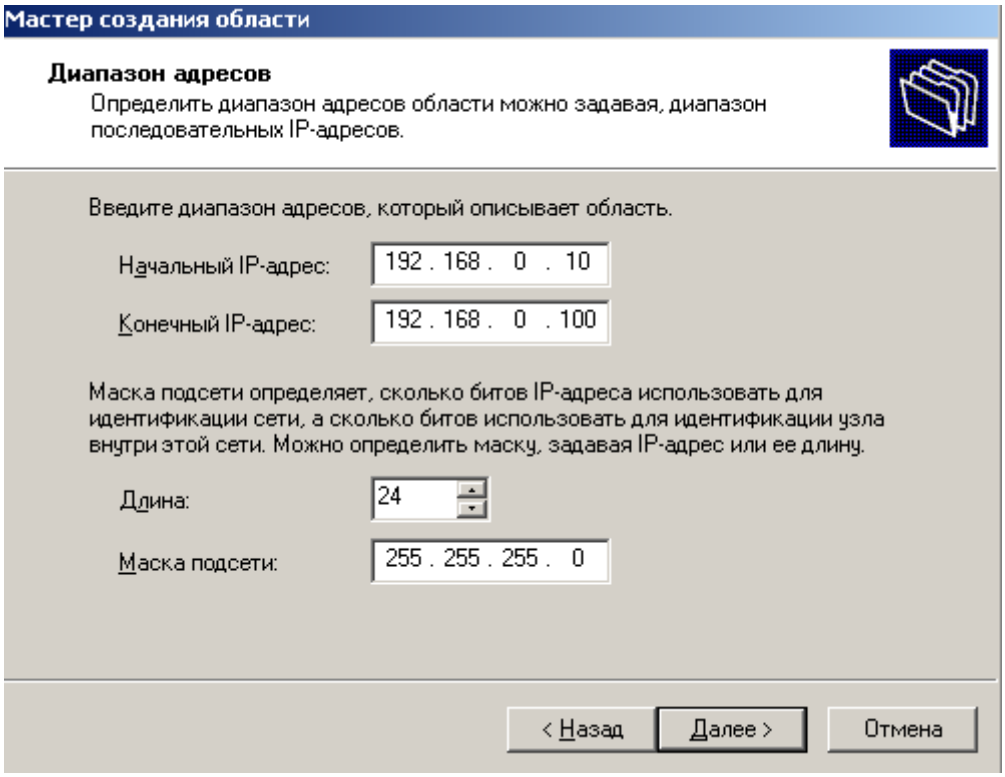


Рис. 3. Задаем диапазон IP адресов для нашей сети

Нажимаем **Далее** в окне **Исключения** можно указать диапазон тех адресов, области из которых IP выбирать нельзя. Давайте в учебных целях в нашем диапазоне 10-100 исключим адреса с 55 по 65 и нажмем на кнопку **Добавить** (рис. 4).

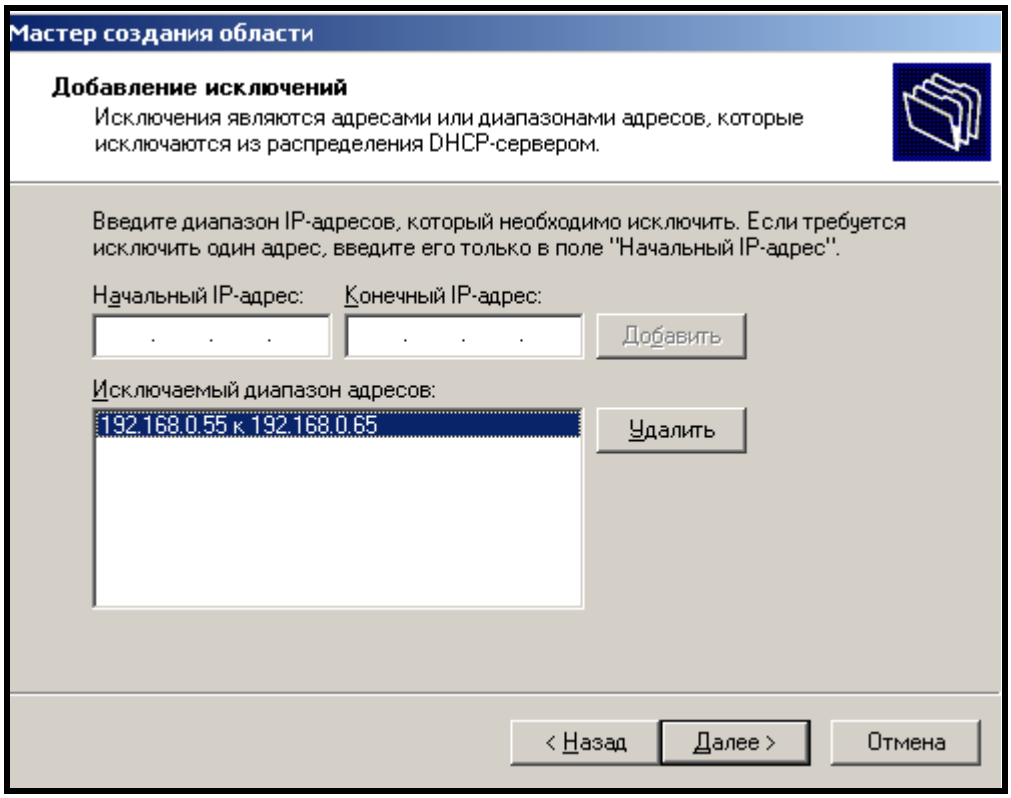


Рис. 4. Задаем исключаемые IP адреса

На следующем шаге задаем срок действия аренды адреса (период резервирования IP адреса) – рис. 5. Здесь цифра непринципиальна, поставьте ее по вашему желанию или оставьте значение по умолчанию.

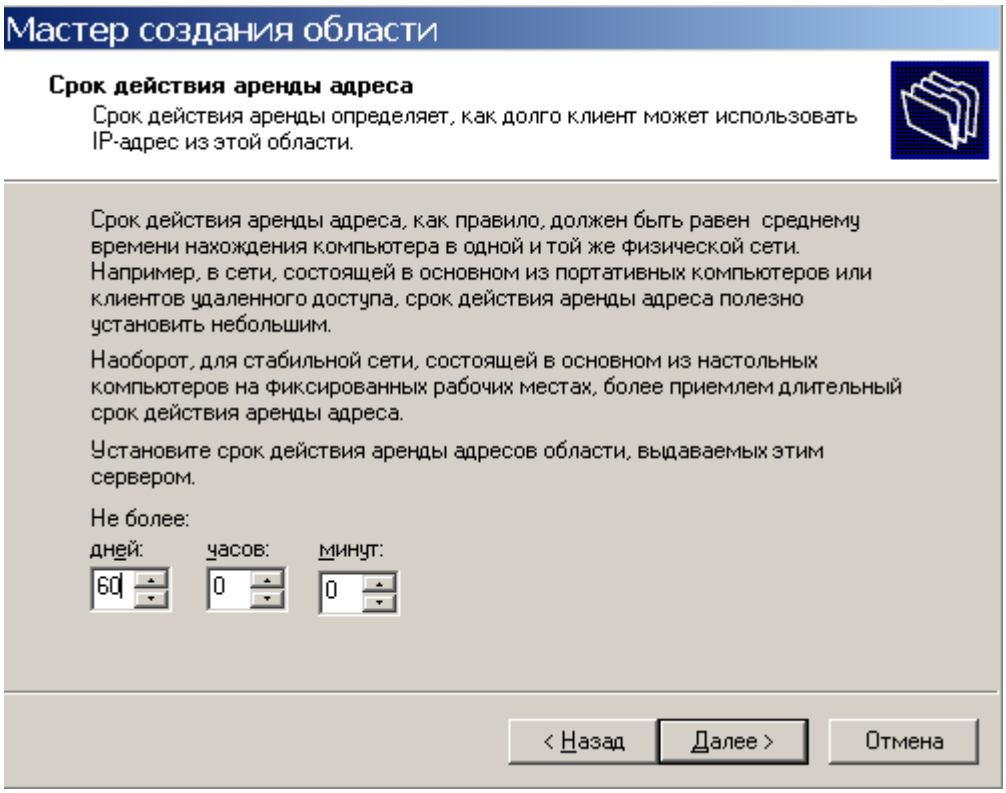


Рис. 5. Выбираем период резервирования IP адреса

Далее пропустим несколько окон с настройками по умолчанию, а в окне **Маршрутизатор** добавим IP адрес нашего сервера кнопкой **Добавить** – рис. 6.>

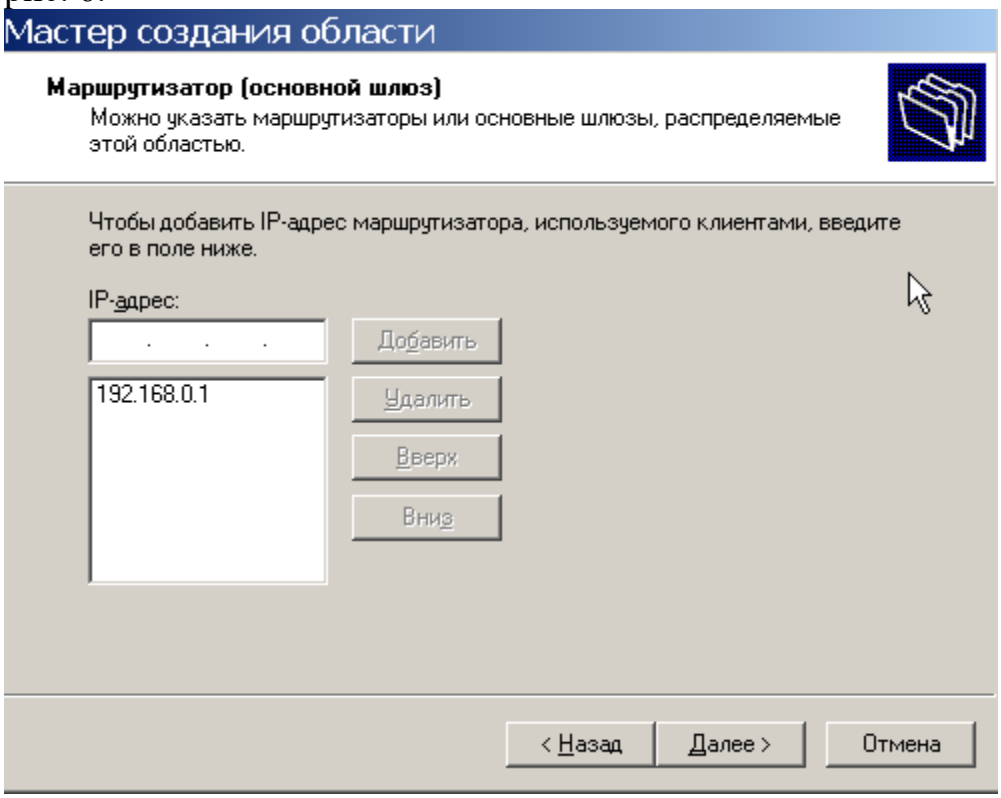


Рис. 6. Задаем IP для маршрутизатора для нашей области IP адресов

Далее вспомним полное имя нашего сервера и пропишем его здесь (рис. 7). Нажмем на кнопку **Добавить**.

Рис. 7.

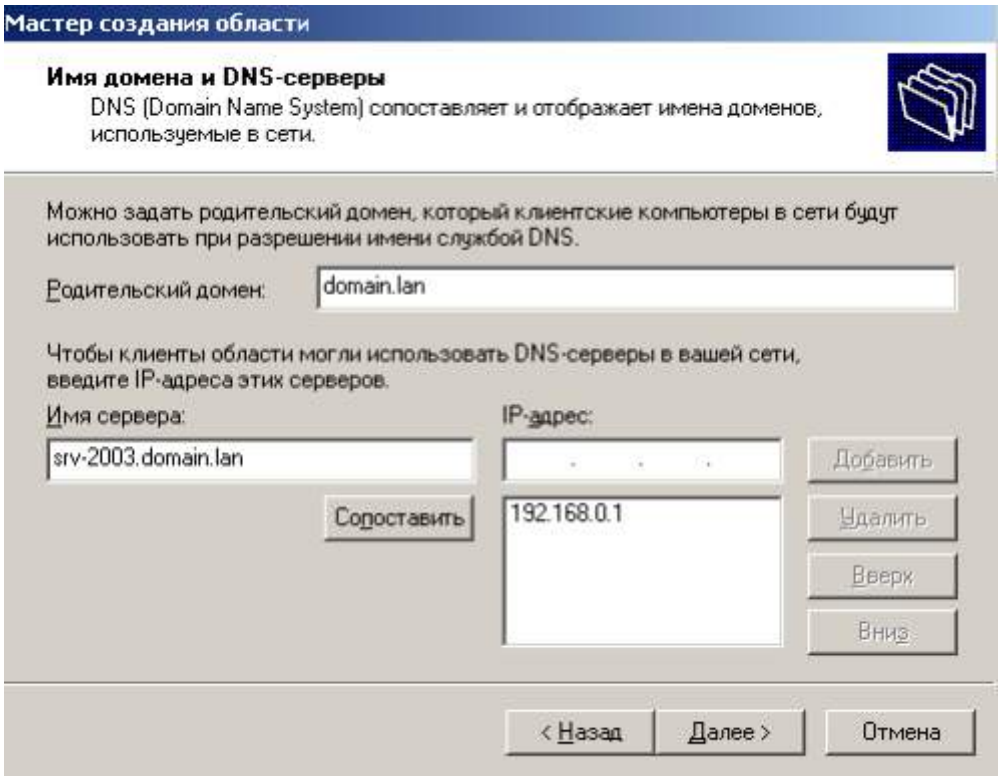


Рис. 8. Задаем адрес для домена и DNS серверов

На следующем шаге окно WINS сервер использовать не будем (это то же, что и DNS, но для старых операционных систем). Теперь активируем переключатель на рис. 9.

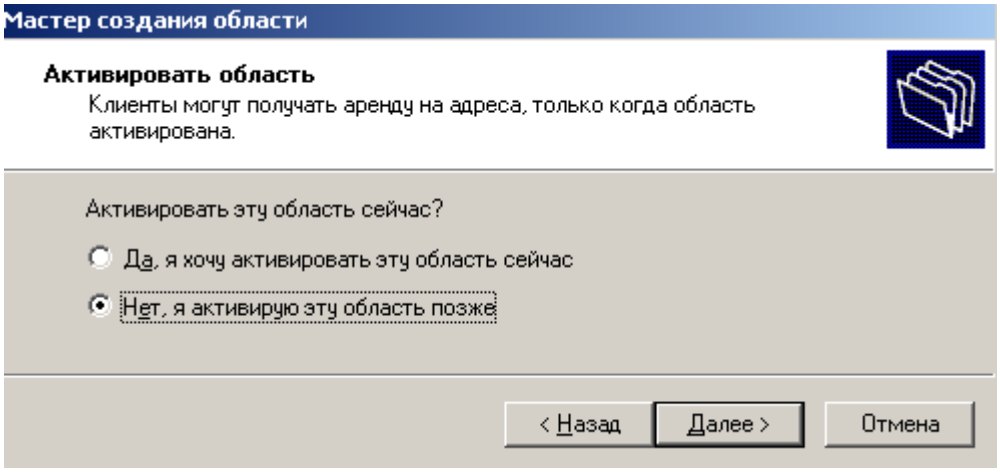


Рис. 9. Активируем область IP адресов

Нажимаем на кнопку **Далее,** затем нажимаем на кнопку **Готово** – рис. 10.

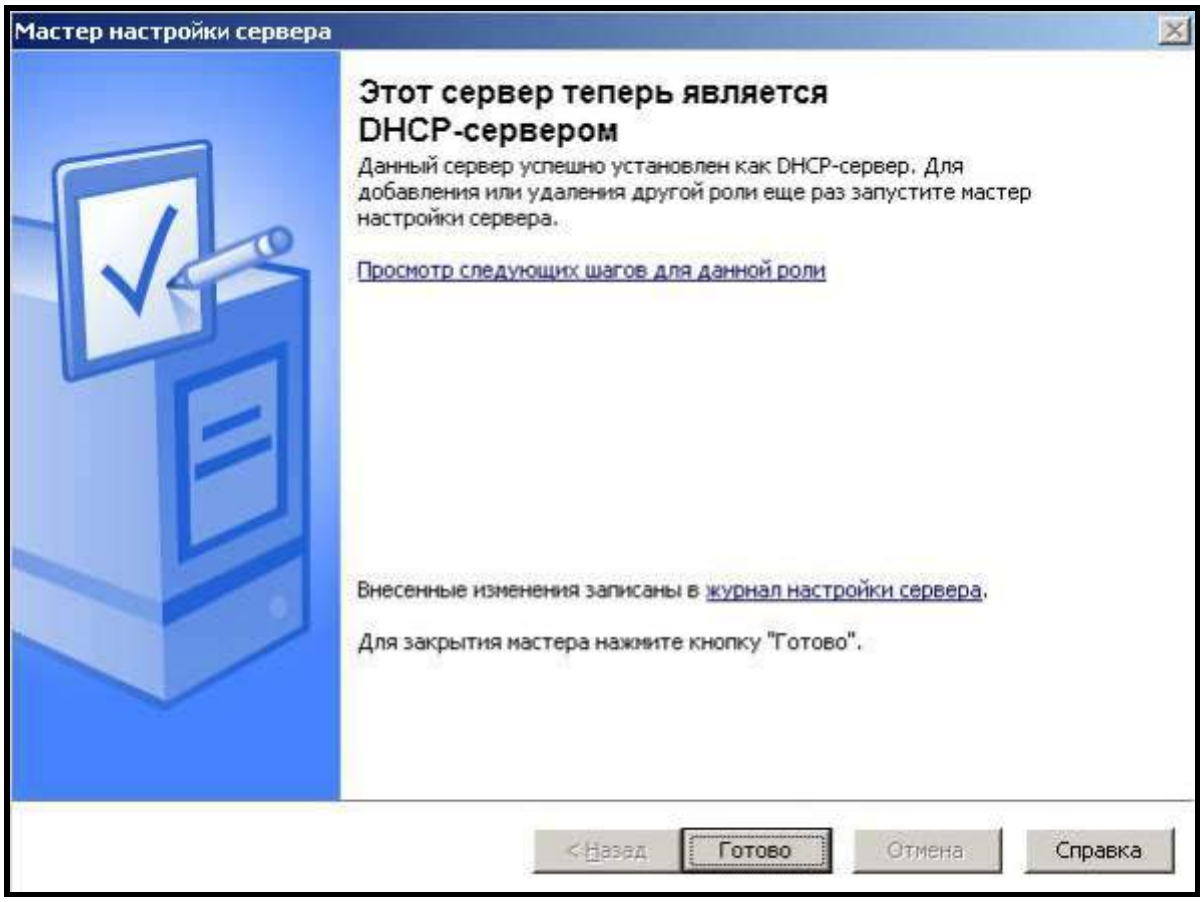


Рис. 10. DHCP сервер успешно установлен

У нас появилась новая оснастка (рис. 11).

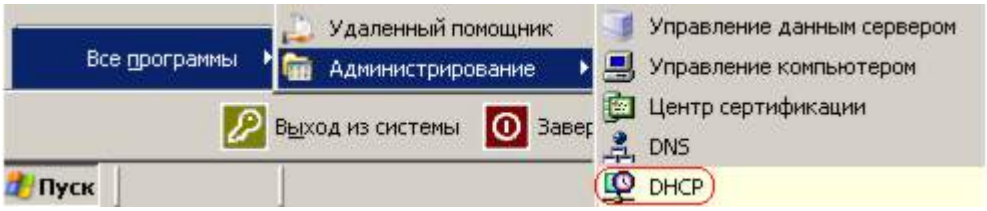


Рис. 11. В администрировании сервера появился новый инструмент

Авторизация DHCP сервера

Пока DHCP сервер не авторизован он не работает. Для авторизации сервера вызовем консоль для его управления. Для этого в окне **Управление данным сервером** выбираем пункт **Управление этим DHCP сервером** или выполняем команду **Пуск-Все программы-Администрирование-DHCP**. Откроется окно, именуемое консолью для управления сервером – рис. 12 и рис. 13.

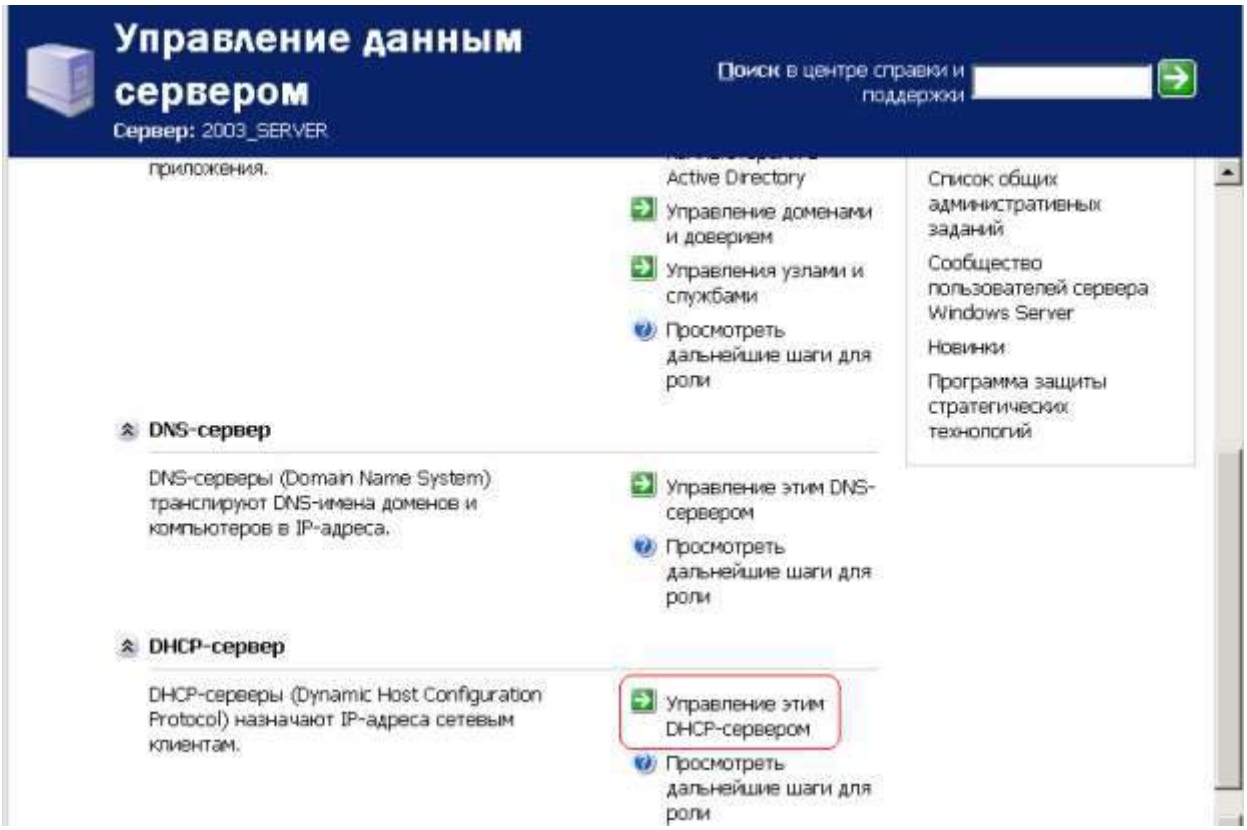


Рис. 12. Выбираем Управление этим DHCP сервером

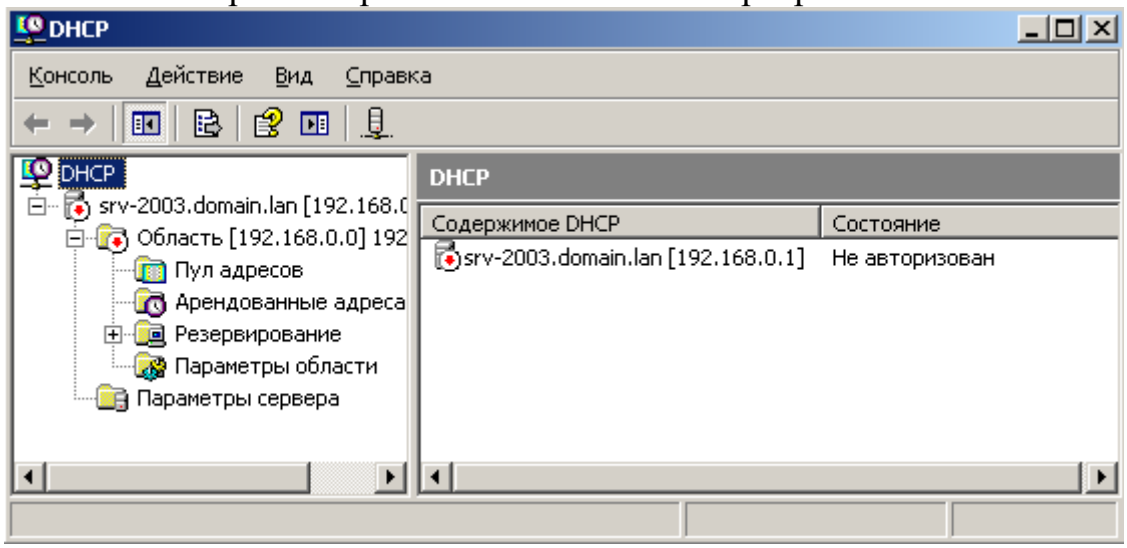


Рис. 13. Красный значок указывает на то, что DHCP-сервер не авторизован

Далее щелкаем правой кнопкой на сервере и выбираем команду **Авторизовать** (рис. 14).

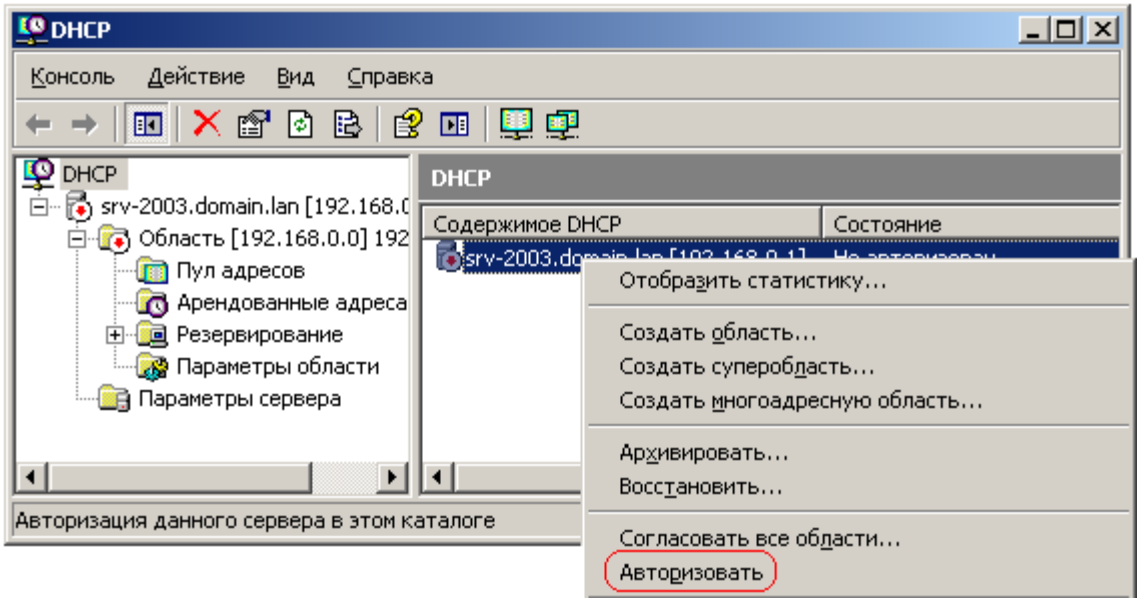


Рис. 14. Команда авторизации DHCP сервера

Значок около сервера станет зеленым - DHCP-сервер начал работать. Но у нас еще не активирована наша область диапазона IP адресов:

Вспомним также, что диапазон IP от 55 до 65 нами запрещен. Нажмем на нее правой кнопкой мыши и выполним команду **Активировать** (рис. 15).

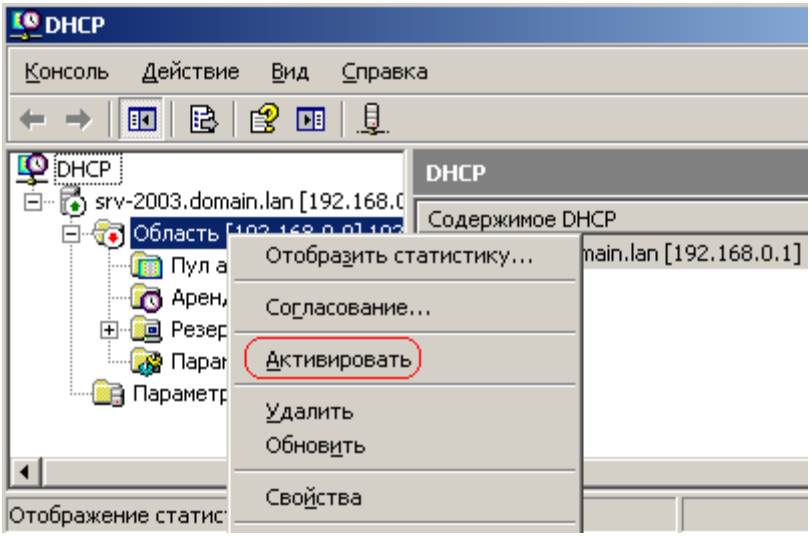


Рис. 15. Активирование заданного нами диапазона IP адресов для клиентских машин

Теперь в пуле адресов видно, какие адрес можно использовать, а какие – нет (рис. 16).

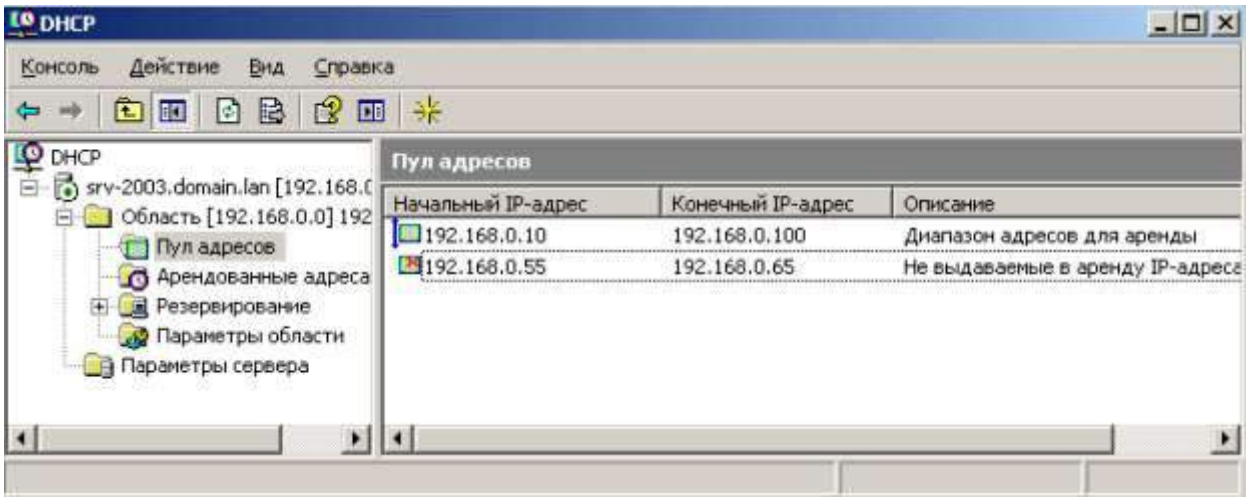


Рис. 16. Показан пул адресов

Проверка работоспособности DHCP сервера

Зайдем на клиенте в его подключение по локальной сети под администратором и увидим его IP адрес (рис. 17). Он настроен вручную (статически).

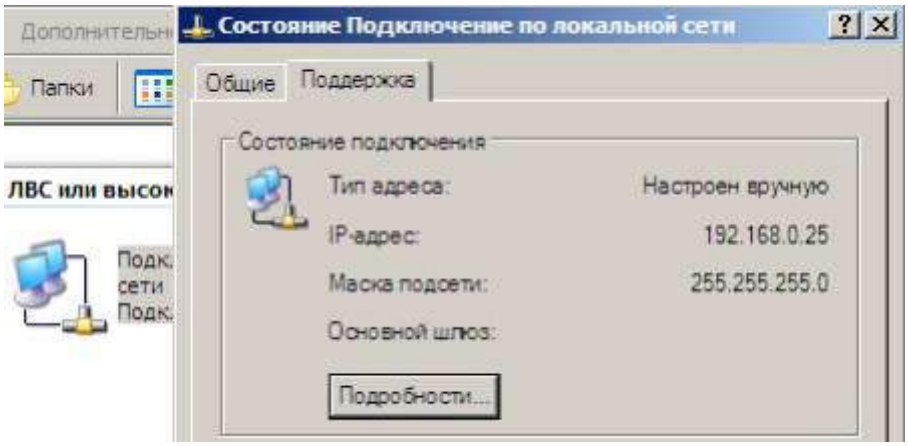


Рис. 17. IP адрес клиента 192.168.0.25

Теперь заходим в свойства IP протокола (рис. 18).

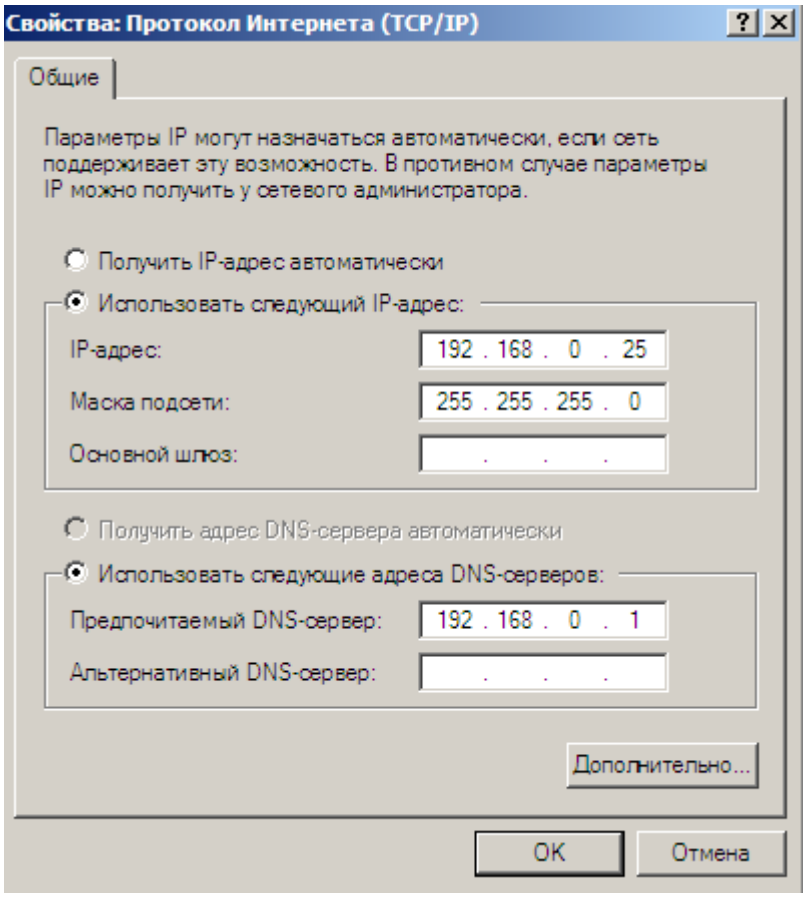


Рис. 50.18. IP адрес клиенту назначен вручную

Здесь мы установим переключатель **Установить IP адрес автоматически** и нажмем ОК. Теперь подключение по локальной сети стало динамическим (рис. 19).

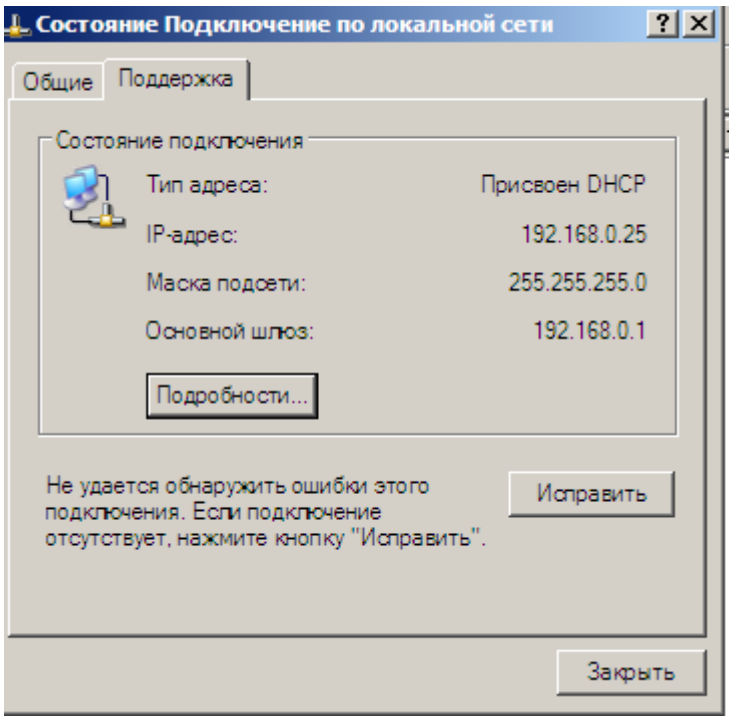


Рис. 19. Теперь IP адрес назначается DHCP сервером

На сервере войдем в арендованные адреса (рис. 20). По истечении срока аренды клиент должен обновить аренду для дальнейшего использования того же адреса или должен будет получить новый IP.

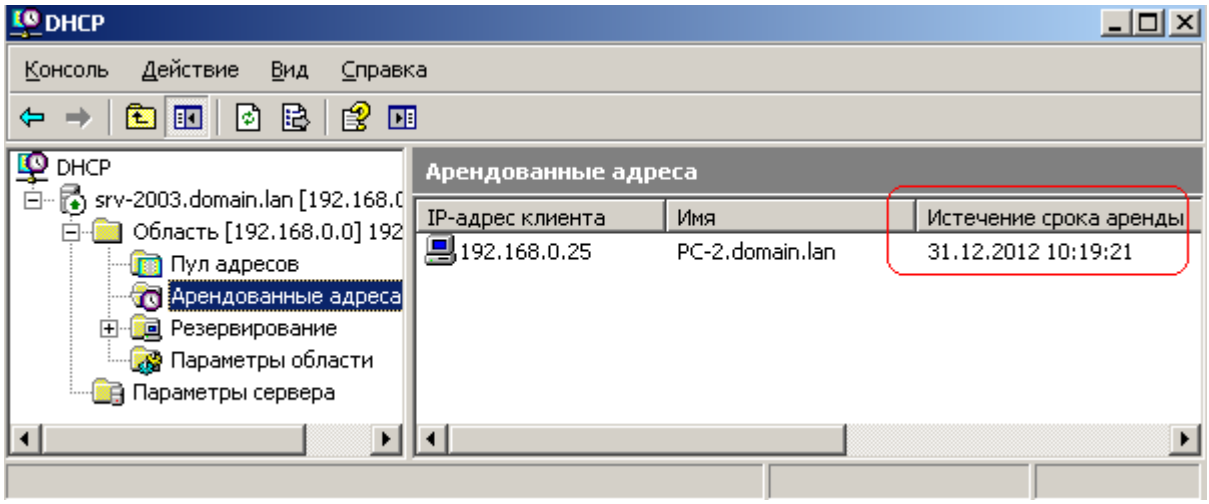


Рис. 20. Консоль DHCP сервера

На сервере вы можете убедиться, что DNS работает нормально и в зоне прямого, и в зоне обратного просмотра (рис. 21).

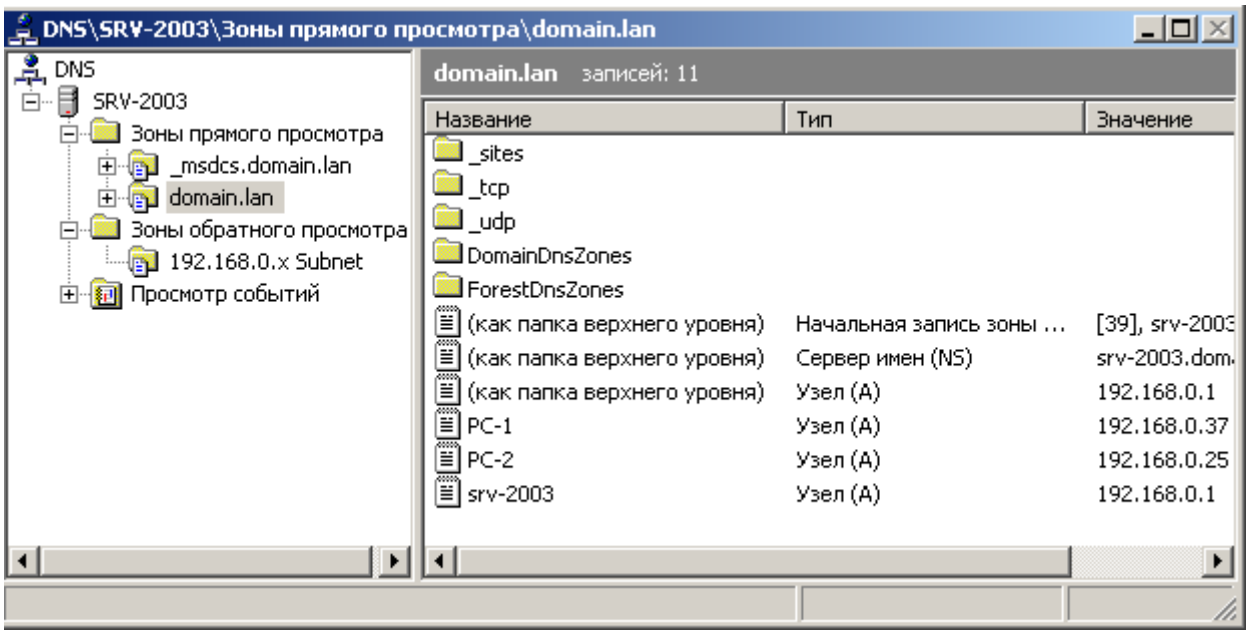


Рис. 21. Все клиенты получили IP адреса из заданного нами диапазона

ПРАКТИЧЕСКАЯ РАБОТА №22.
СОЗДАНИЕ ПОЛЬЗОВАТЕЛЕЙ ДОМЕНА

Цель работы: Изучить работу по созданию пользователей домена

Создадим еще одного пользователя доменом DOMAIN - администратора по фамилии molochkov_vp. При этом метод создания пользователя будет иной, не такой, как мы делали это ранее (другим способом).

Знакомимся с консолью

Консоль MMC (Microsoft Management Console) группирует средства администрирования, которые используются для администрирования компьютеров, служб, других системных компонентов и сетей.

Windows Server 2003 содержит консоль для управления сервером и его компонентами. Иначе говоря, консоль - это специальная панель для выполнения команд и операций, проведения настроек и установок сервера.

Включим сервер, затем на нем выполним команду **Пуск-Выполнить-mmc** появится Консоль1 (рис. 1).

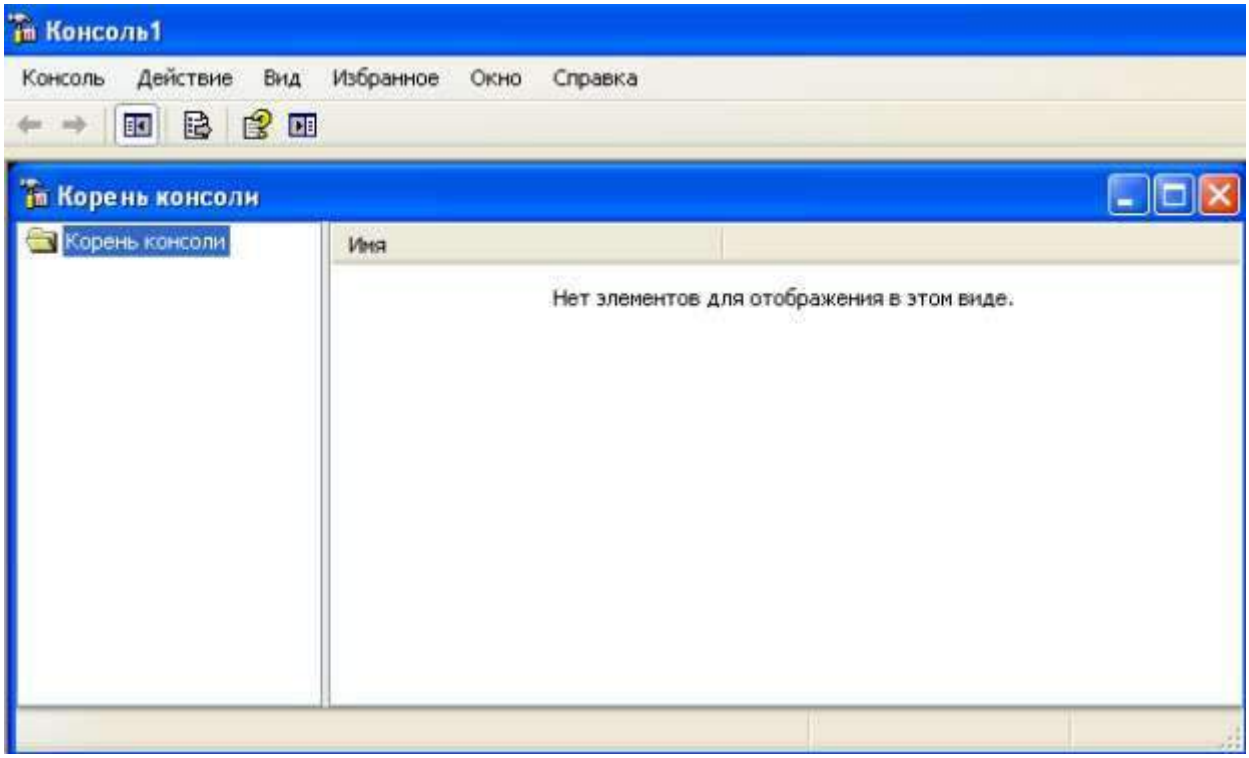


Рис. 1. Консоль1

Выполним команду **Консоль-Добавить или удалить оснастку** и добавим две службы (оснастки), установленные нами ранее – AD и DNS (рис. 2 и рис. 3).

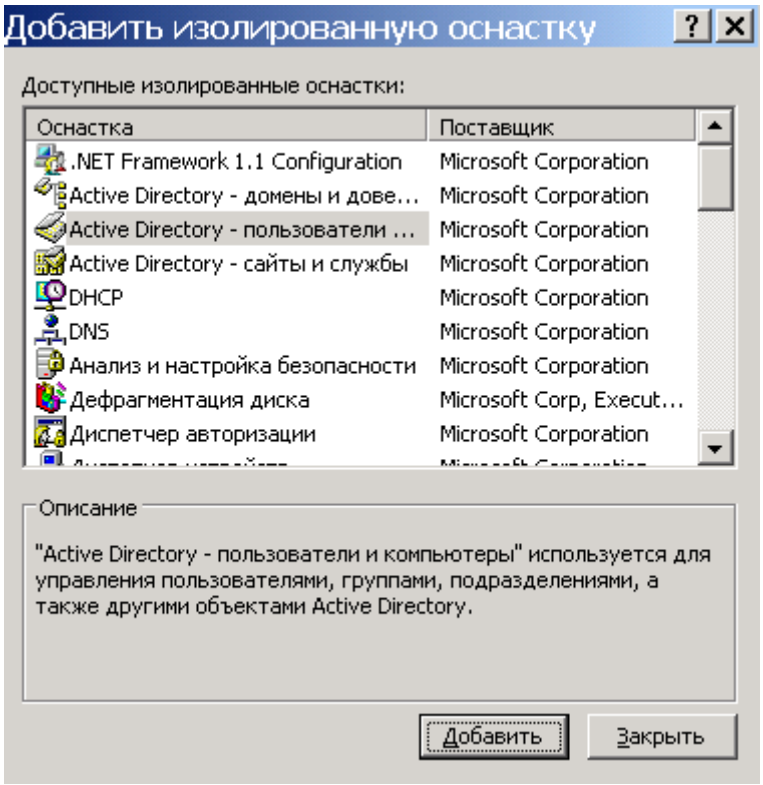


Рис. 2. Окно выбора служб (оснасток)

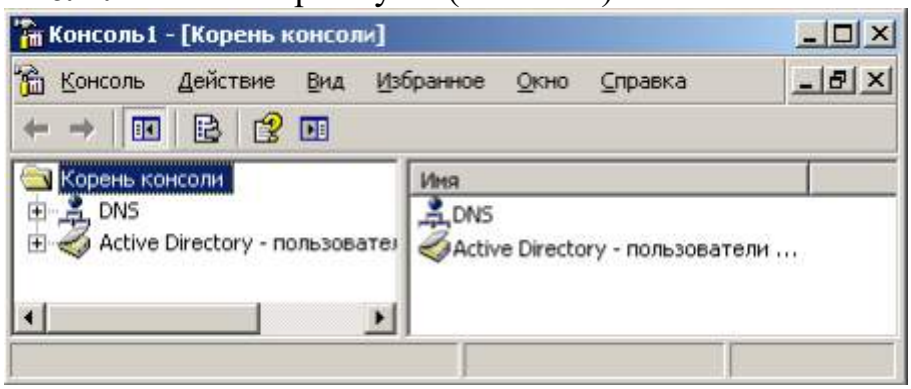


Рис. 3. В консоль мы добавили две службы (оснастки)

Выполняем команду **Консоль-Сохранить, как** и сохраняем консоль

на рабочий стол. Теперь запустим консоль с рабочего стола и откроем **Active Directory**, где увидим наш домен (рис. 4).

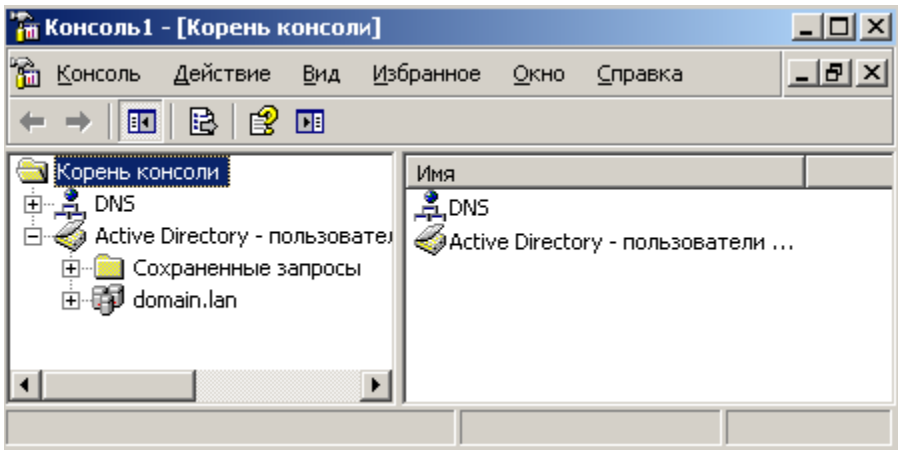


Рис. 4. Видим наш домен (domain.lan)
В домене создаем подразделения, а в них-объекты

Наша цель – создать в домене нового пользователя – **Администратор** с помощью консоли. Для этого в домене правой кнопкой вызовем меню и команду **Создать-Подразделение**, чтобы создать раздел (объект) **Администратор** (рис. 5).

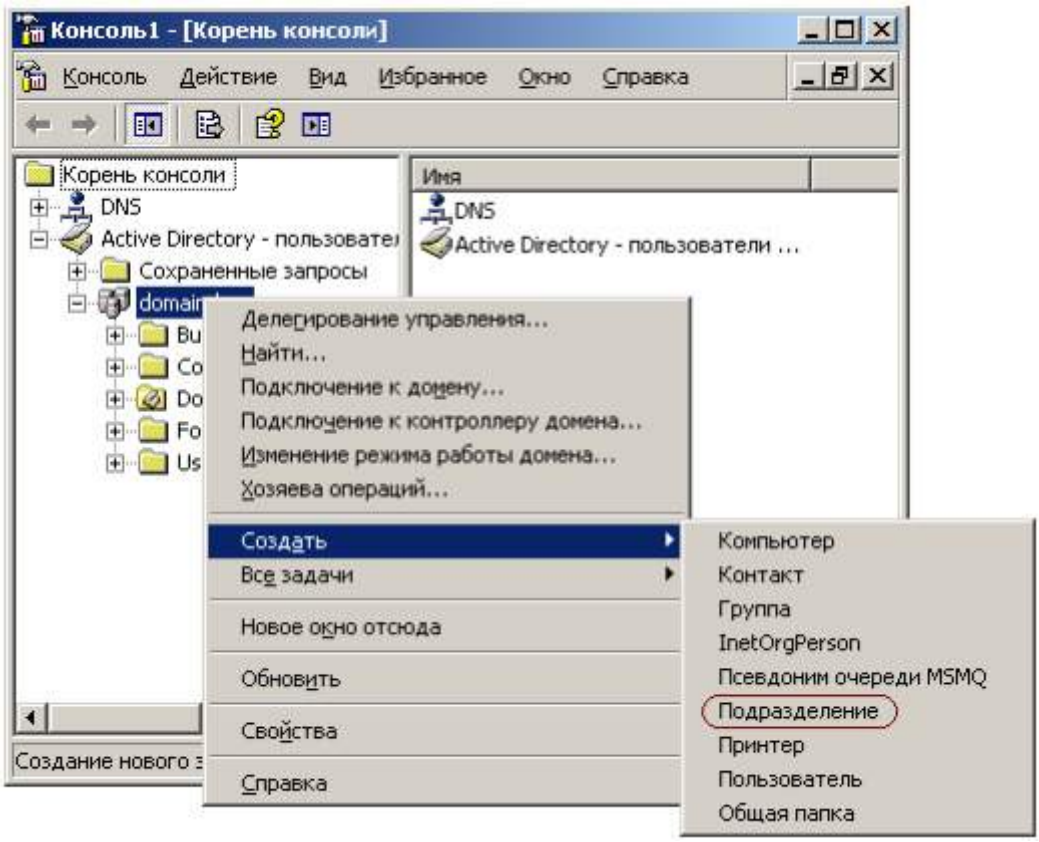


Рис. 5. Создаем подразделение Администратор

Аналогично создадим подразделение **Пользователи** (рис. 6 и рис. 7).

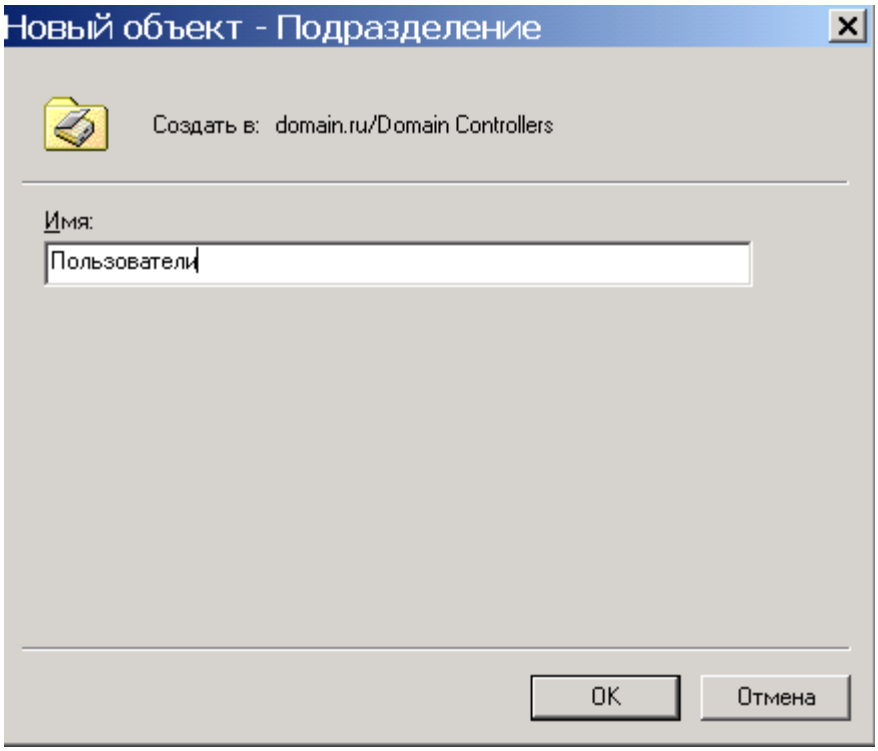


Рис. 6. Имя Пользователи не появится само - его нужно написать

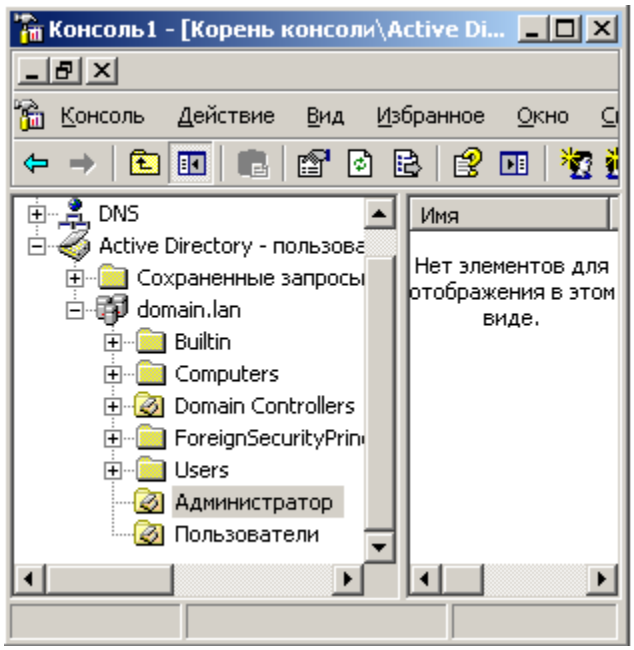


Рис. 7. В Active Directory мы создали два подразделения

Для пользователей в поле справа (**Имя-Тип-Описание)** щелкаем правой кнопкой мыши и выполняем команду **Создать-Пользователь** (рис. 8). Заполняем форму.

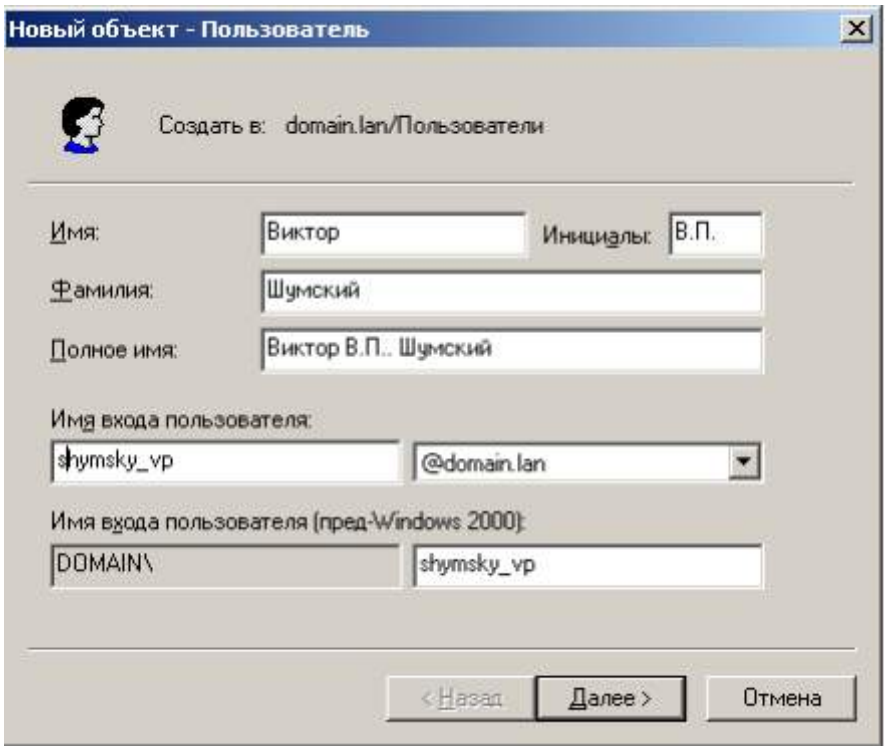


Рис. 8. В домене создаем пользователя

Нажимаем **Далее** и вводим пароль и создаем нового пользователя доменом. Аналогично создаем администратора (рис. 9).

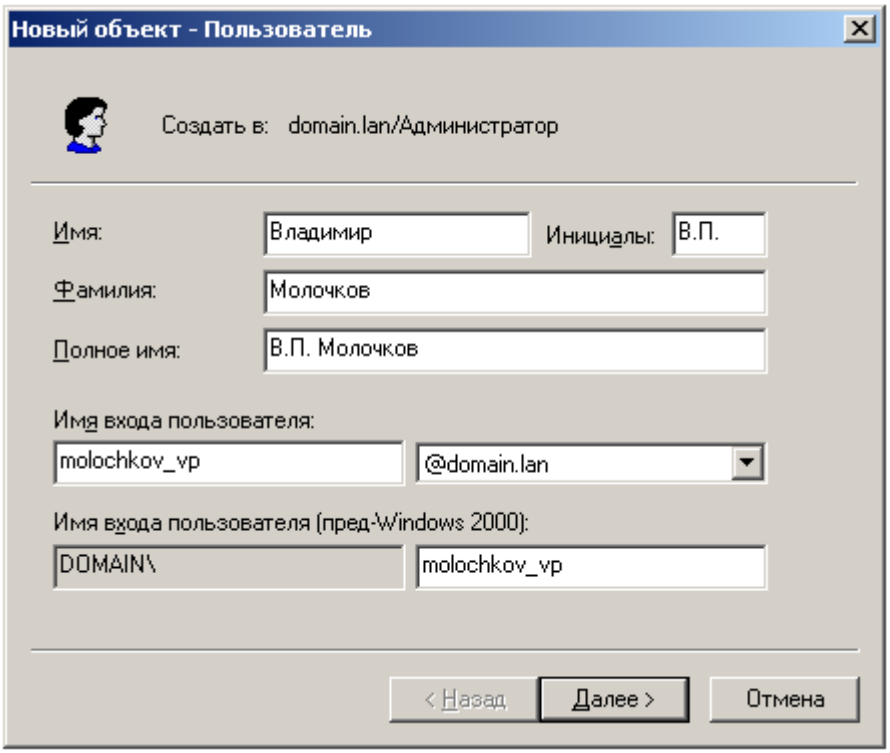


Рис. 9. Создаем администратора

Таким способом мы создадим одного пользователя в разделе **Администратор** и одного пользователя в разделе **Пользователи**. То есть, в домене мы создали

подразделение, а в нем – два объекта. Если теперь дважды щелкнуть на пользователе-администраторе, то мы увидим, что он является членом группы **Пользователи домена** (рис. 10). Второй пользователь (Шумский) – также член группы **Пользователи домена.**

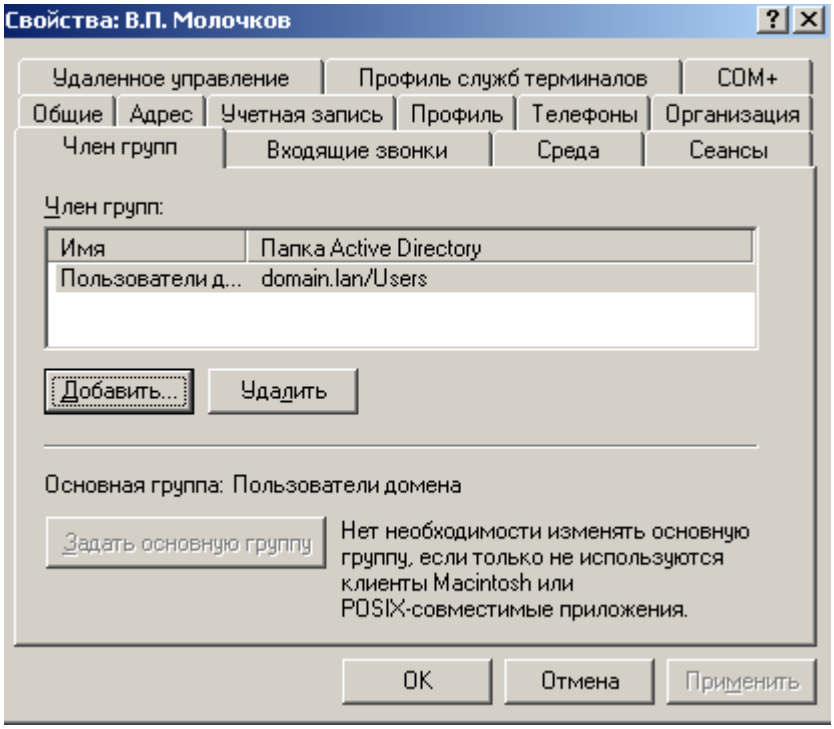


Рис. 10. Молочков является членом группы Пользователи домена

Нажмем в этом окне на кнопку **Добавить** и далее **- Дополнительно-Поиск**, ищем администратора домена, ОК (рис. 11).

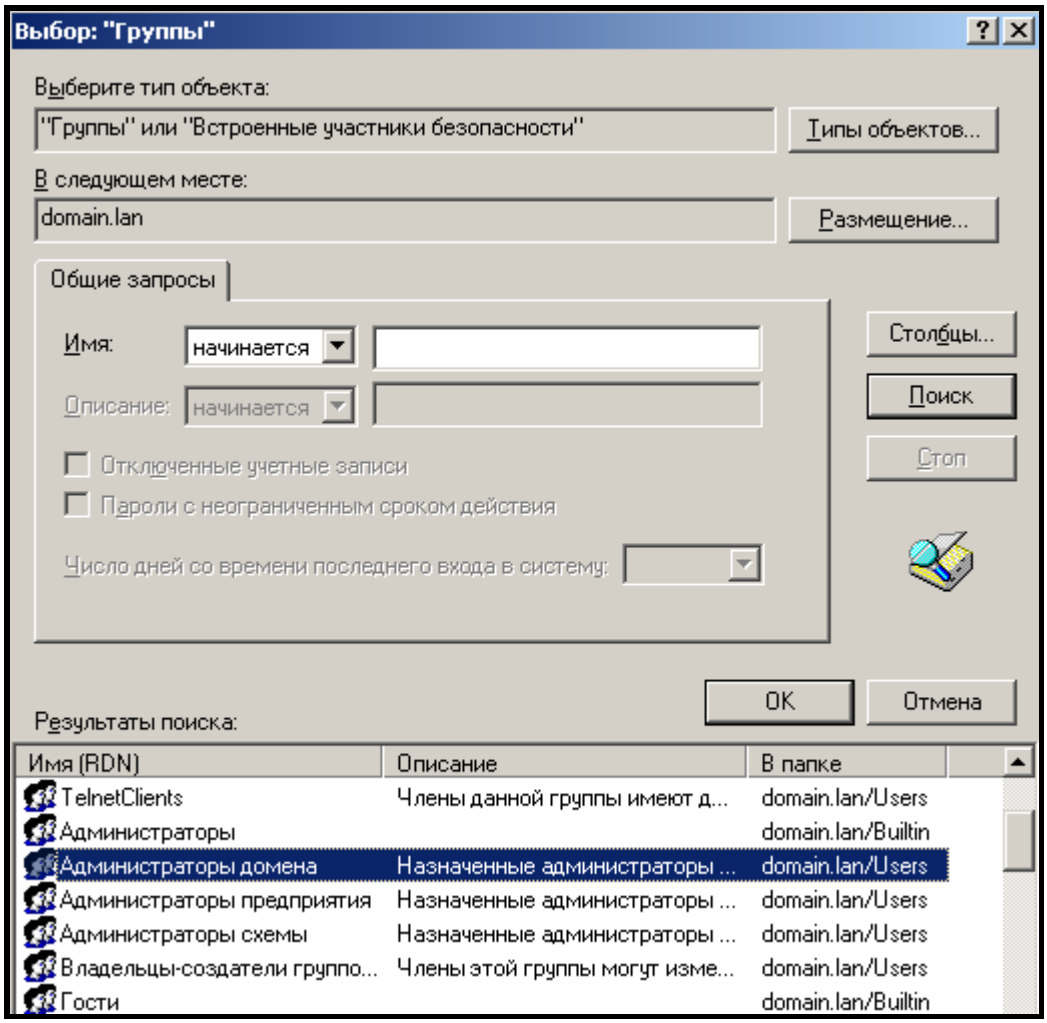


Рис. 11. Выбираем группу администраторы домена

Теперь стаем на строчку **Администраторы домена** и нажимаем на кнопку **Задать основную группу** (рис. 12).

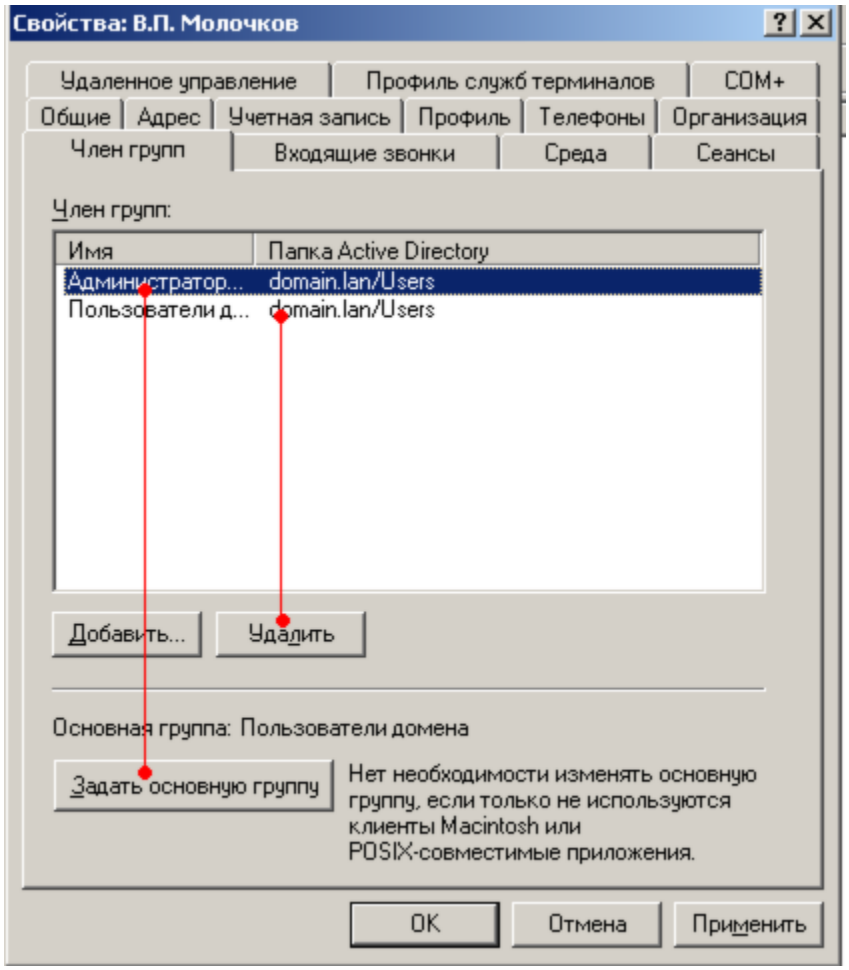


Рис. 12. Основная группа-Администраторы домена

Группу **Пользователи домена** удаляем кнопкой **Удалить** и нажимаем ОК. Теперь, если в консоли щелкнуть на пользователе Молочков, то вы увидите, что он - член группы администраторов домена – рис. 13. Задача решена.

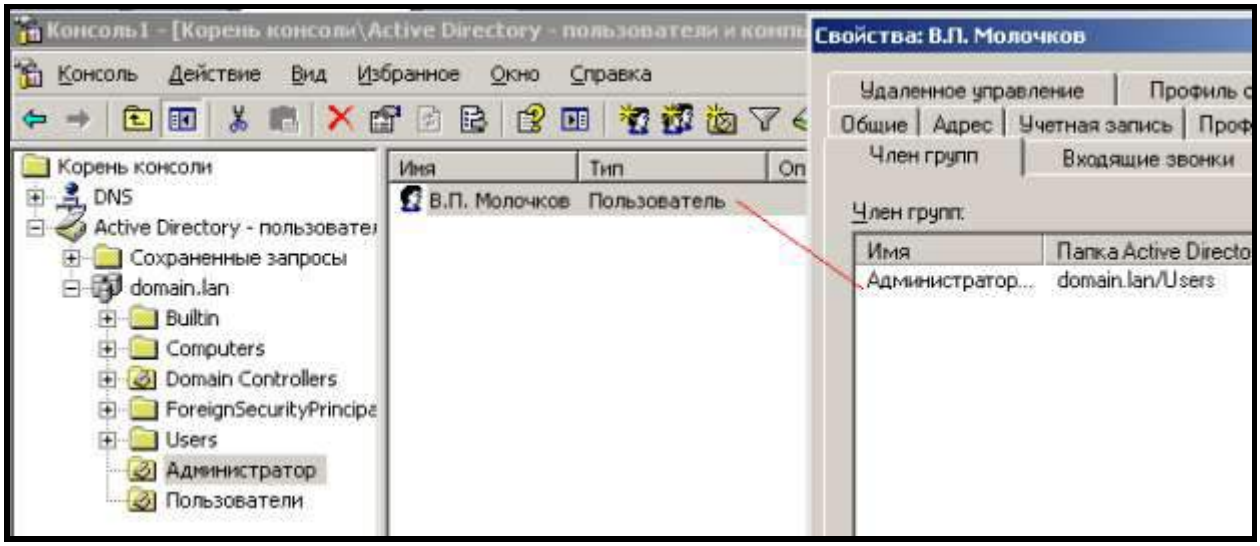


Рис. 13. Молочков - член группы администраторов домена (из пользователей домена он удален)

Ресурсы в локальной сети

На сервере, на диске C:\ создадим две папки: **MUSIC** (только чтение), **VIDEO** (полный доступ) и затем откроем эти ресурсы для доступа пользователям (рис. 14).

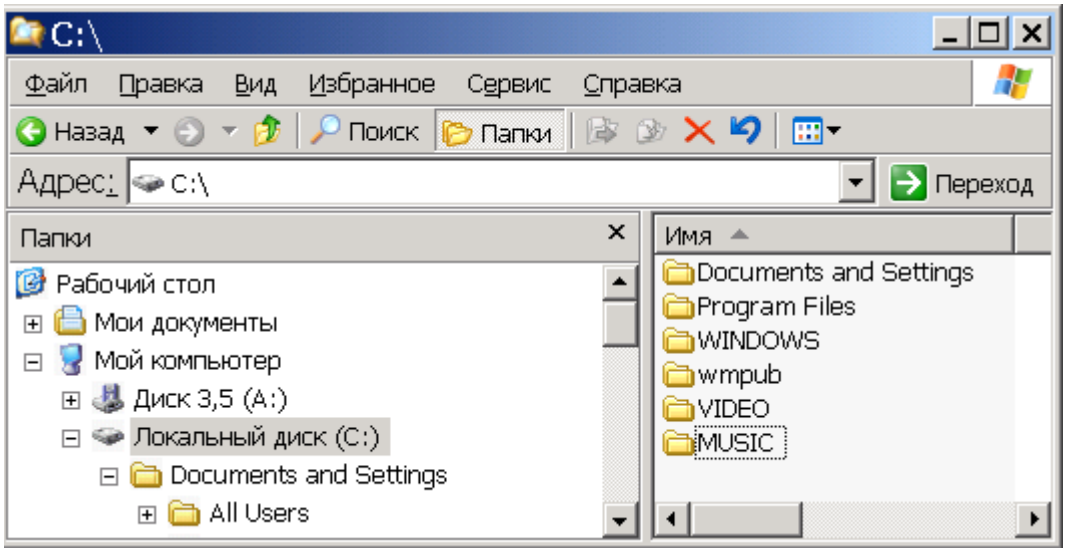


Рис. 14. На диске C:\ созданы две папки

Для назначения папкам требуемых атрибутов щелкнем на ней правой кнопкой мыши и выберем команду **Общий доступ и безопасность.** В данном окне установим переключатель **Открыть общий доступ** (рис. 15).

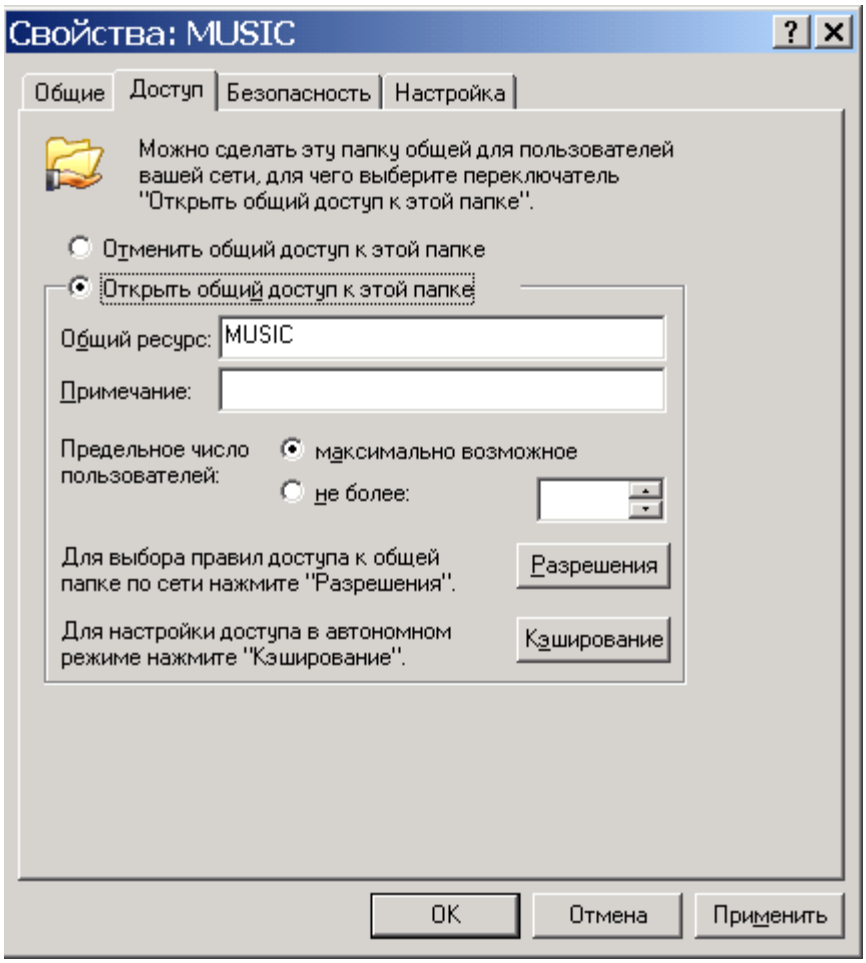


Рис. 15. Окно свойств папки Music

На вкладке **Разрешения** вы можете осуществить поиск пользователей домена и добавить их в пользователи папки MUSIC (рис. 16). Для этого нужно выполнить команды **Добавить-Дополнительно-Поиск** и указать нужного пользователя. Строку **Все** пользователи, стоящую по умолчанию, следует удалить.

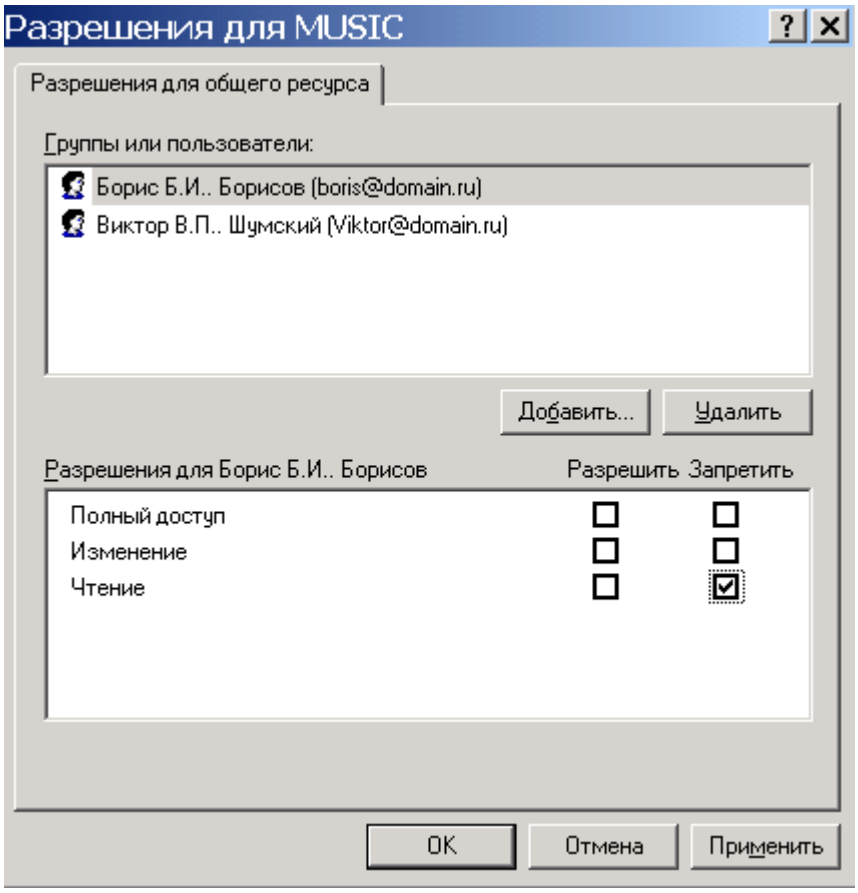


Рис. 16. Добавлены два пользователя с правом чтения папки MUSIC

Таким же образом устанавливается доступ для других папок (рис. 17).

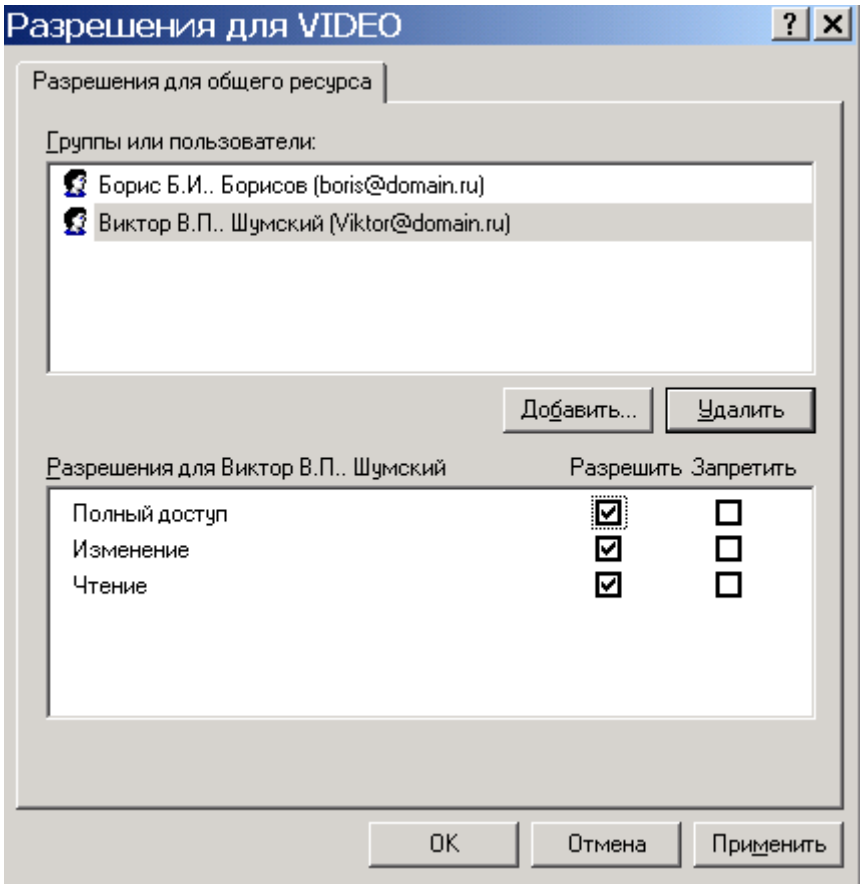


Рис. 17. К папке VIDEO пользователи имеют полный доступ

Перезагрузим и посмотрим, как эти ресурсы будут выглядеть со стороны клиента, для этого войдем в домен под именем пользователя Борисов (рис. 18).

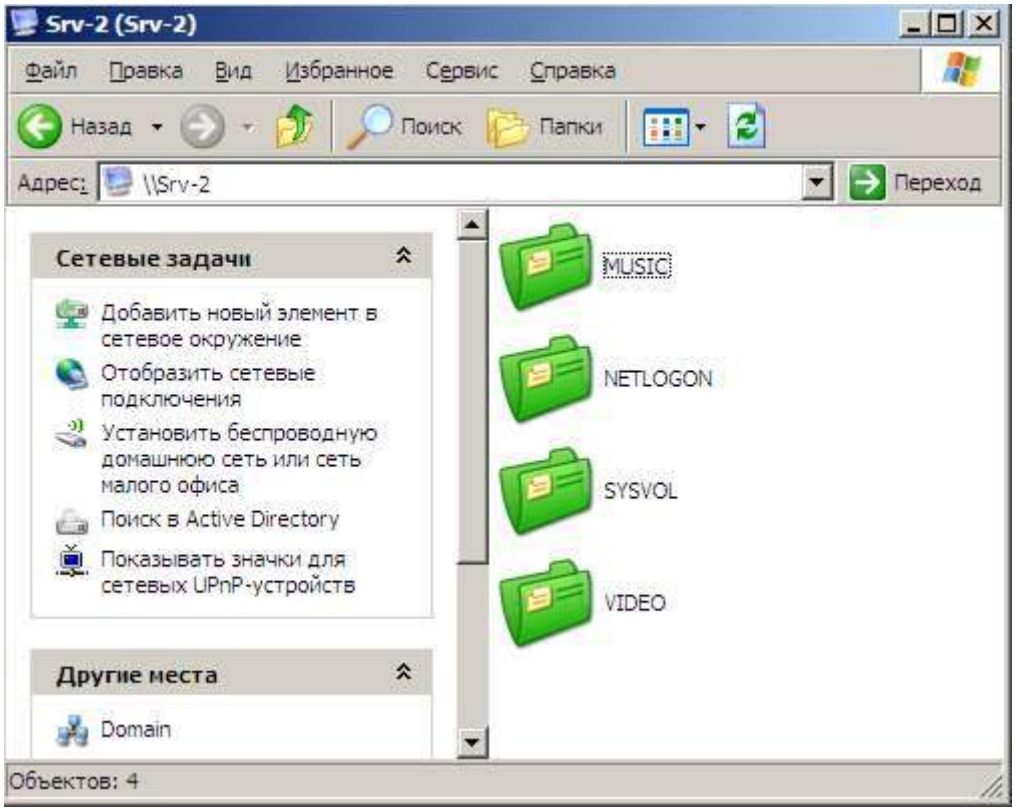


Рис. 18. Вид папок на сервере в сетевом окружении

Как вариант на клиенте можно выполнить команду **Пуск-Выполнить** и **\\Srv-2003**. Мы увидим, что со стороны клиента сетевые ресурсы сервера открыты и он может ими пользоваться согласно назначенным ему разрешениям. Пользователи, не входящие в домен, папки также увидят, но пользоваться ими не смогут (Для компьютеров не входящих в домен папки закрыты).

ПРАКТИЧЕСКАЯ РАБОТА №23-24. АДМИНИСТРИРОВАНИЕ СЕТИ

Цель работы:

Изучить работу по администрированию сети. Составить конспект по основным понятиям администрирования сети.

Основные понятия

1. **Понятие администрирования. Задачи администратора сети**

Основной целью администрирования является приведение сети в соответствие с целями и задачами, для которых она предназначена. Администрирование заключается в контроле за работой сетевого оборудования и управление функционированием сети в целом. Администрирование выполняет администратор сети – специалист, отвечающий за нормальное функционирование и использование ресурсов сети. Если более детально, то администрирование информационных систем включает следующие цели:

- Установка и настройка сети. Поддержка её дальнейшей работоспособности.
- Мониторинг. Планирование системы.
- Установка и конфигурация аппаратных устройств.
- Установка программного обеспечения.
- Архивирование (резервное копирование) информации.
- Создание и управление пользователями.
- Установка и контроль защиты.

Вот выписка должностных обязанностей администратора сети:

1. Устанавливает на серверы и рабочие станции сетевое программное обеспечение.
2. Конфигурирует систему на сервере.
3. Обеспечивает интегрирование программного обеспечения на файл-серверах, серверах систем управления базами данных и на рабочих станциях.
4. Поддерживает рабочее состояние программного обеспечения сервера.

5. Регистрирует пользователей, назначает идентификаторы и пароли.
6. Обучает пользователей работе в сети, ведению архивов; отвечает на вопросы пользователей, связанные с работой в сети; составляет инструкции по работе с сетевым программным обеспечением и доводит их до сведения пользователей.
7. Контролирует использование сетевых ресурсов.
8. Организует доступ к локальной и глобальной сетям.
9. Устанавливает ограничения для пользователей по:
   - использованию рабочей станции или сервера;
   - времени;
   - степени использования ресурсов.
10. Обеспечивает своевременное копирование и резервирование данных.
11. Обращается к техническому персоналу при выявлении неисправностей сетевого оборудования.
12. Участвует в восстановлении работоспособности системы при сбоях и выходе из строя сетевого оборудования.
13. Выявляет ошибки пользователей и сетевого программного обеспечения и восстанавливает работоспособность системы.
14. Проводит мониторинг сети, разрабатывает предложения по развитию инфраструктуры сети.
15. Обеспечивает:
    - сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных);
    - безопасность межсетевого взаимодействия.
16. Готовит предложения по модернизации и приобретению сетевого оборудования.
17. Осуществляет контроль за монтажом оборудования специалистами сторонних организаций.
18. Сообщает своему непосредственному руководителю о случаях злоупотребления сетью и принятых мерах.
19. Ведет журнал системной информации, иную техническую документацию.

2. **Группы пользователей**

Все пользователи сети разделяются по своим полномочиям на группы. Каждая группа может отвечать за выполнение тех или иных задач. Возможно такое определение прав групп пользователей, при котором пользователи имеют все права, необходимые им для выполнения своих функций, но не более того. Полностью все права должны быть только у одного пользователя - администратора (супервизора) сети. Он имеет все права, в том числе может создавать группы пользователей и определять права, которыми они обладают.

Пользователи могут быть членами одновременно нескольких групп. Можно, например, создать новый каталог и разрешить к нему доступ сразу для всех

пользователей сети. При этом вам придется изменять права доступа не для всех пользователей (их может быть несколько десятков), а только для одной группы, что существенно легче. Для каждой лаборатории или отдела имеет смысл создать свою группу пользователей. Если у вас есть пользователи, которым требуются дополнительные права (например, права доступа к каким-либо каталогам или сетевым принтерам), создайте соответствующие группы пользователей и предоставьте им эти права.

Если в сети много рабочих станций, которые находятся в разных помещениях и принадлежат разным отделам или лабораториям, имеет смысл создать группу администраторов сети. Права нескольких администраторов сети определяются системным администратором. Не следует предоставлять администраторам сети всех прав системного администратора. Вполне достаточно, если в каждом отделе или лаборатории будет Один-два администратора, которые обладают правами управления, только работающими в данном отделе или лаборатории пользователями. Если в отделе или лаборатории имеется сетевой принтер или какие-либо другие сетевые ресурсы, у администратора должны быть права на управление этими устройствами. Однако вовсе ни к чему, чтобы администратор одной лаборатории мог управлять сетевым принтером, принадлежащим другой лаборатории. При этом пользователи должны иметь минимально необходимые им для нормальной работы права доступа к дискам сервера.

Таким образом, очевидно, что создание групп пользователей актуально только в больших компьютерных сетях. Если сеть небольшая, то и один человек справится с такими вопросами, как добавление новых пользователей, разграничение доступа к дискам сервера, сетевым принтерам и другим сетевым ресурсам и в создании групп администраторов и обычных пользователей смысла нет.

Задание №1. Выполнить создание группы пользователей

Запускаем на виртуальной машине сервер. Наберем команду **mmc** и добавим в консоль оснастки, с которыми будем работать - **DNS, DHCP, AD-пользователи и компьютеры**. Для этого потребуется команда **Консоль-Добавить или удалить оснастку-Добавить** (рис. 1.

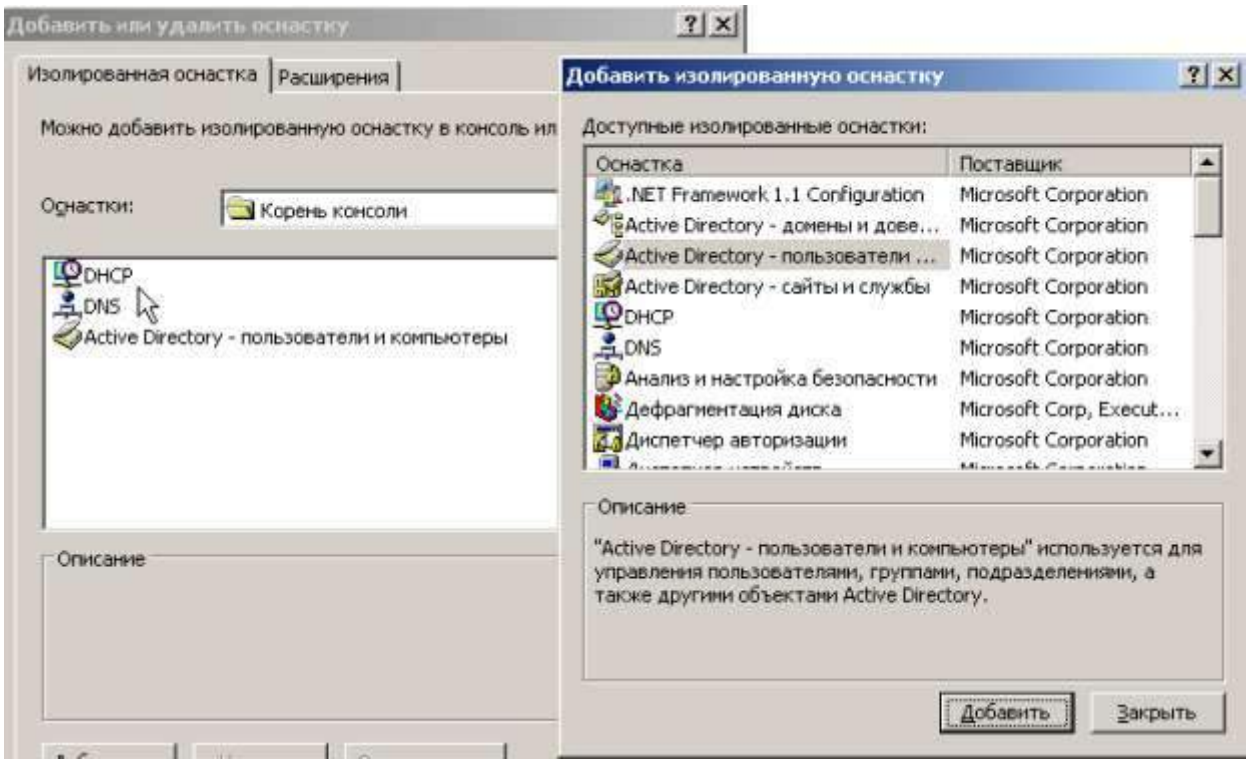


Рис. 1. Создаем консоль с нужными нами оснастками

Теперь в AD щелкните правой кнопкой мыши и выполните команду **Создать-Группа** (рис. 2 и (рис. 3).

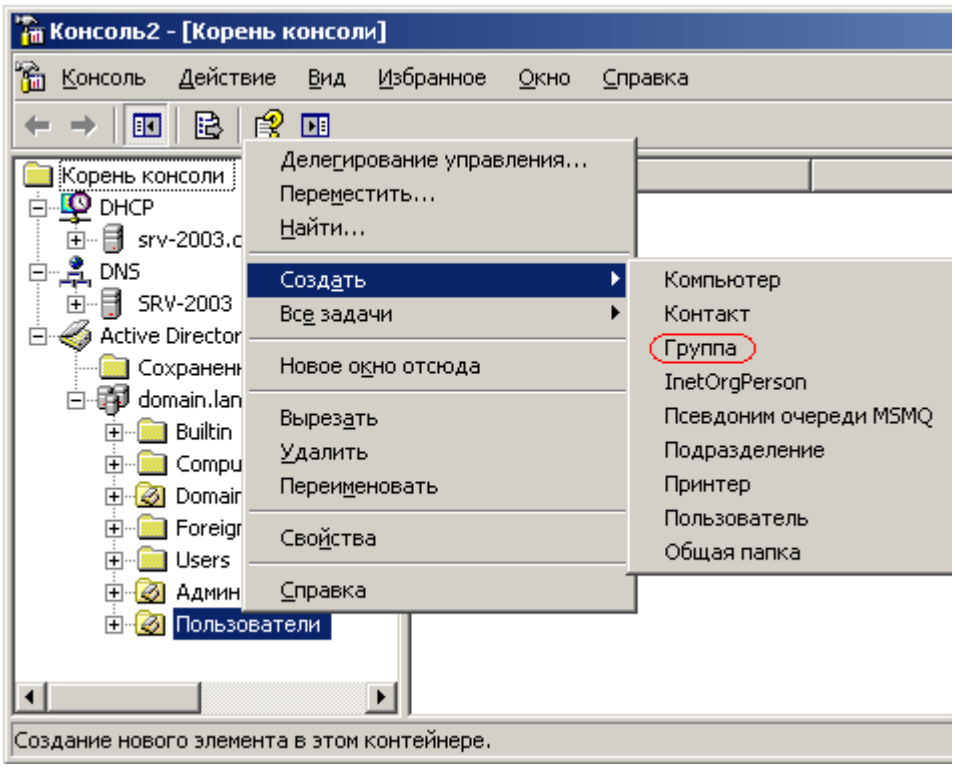


Рис. 2. Создаем группу пользователей

Группа безопасности назначает права доступа к ресурсам сети (администрирует). **Группа распространения** не может заниматься администрированием, она занимается рассылкой сообщений. **Локальная в домене** может содержать в себе пользователя любого домена в лесу, но администрировать эта группа может только в том домене, в котором группа создавалась. **Глобальная** может содержать в себе пользователей из того домена, в котором она была создана, но администрировать они могут любой домен в лесу (если эти домены доверяют друг другу). **Универсальная** может содержать пользователей из любого домена леса, и эта группа может администрировать любой домен в лесу.

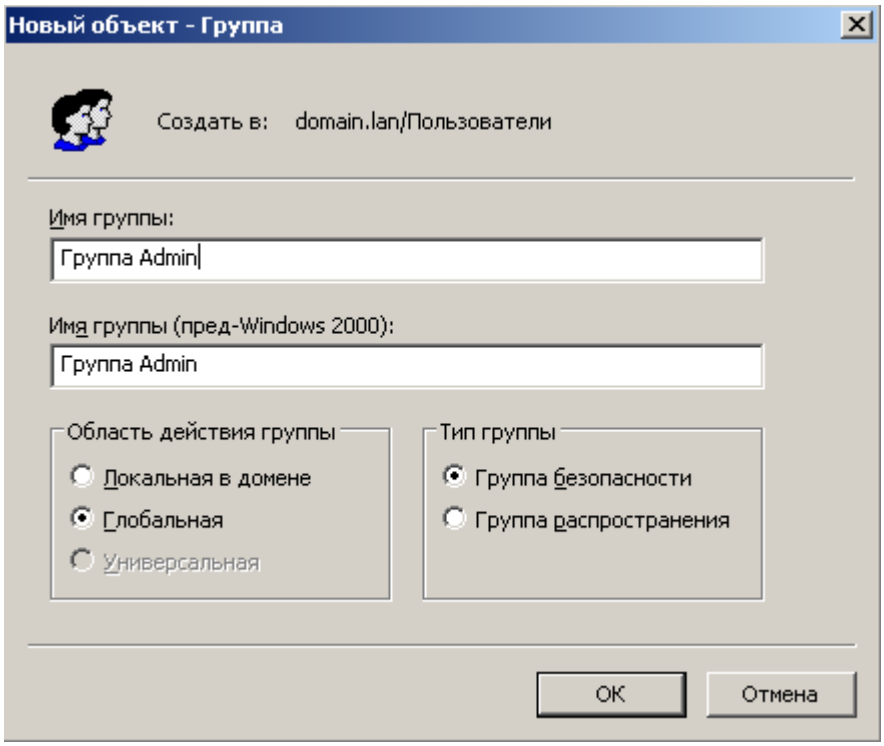


Рис. 3. В этом окне оставим настройки по умолчанию

Группа Admin создана (рис. 4.). Теперь нужно добавить в нее пользователей.

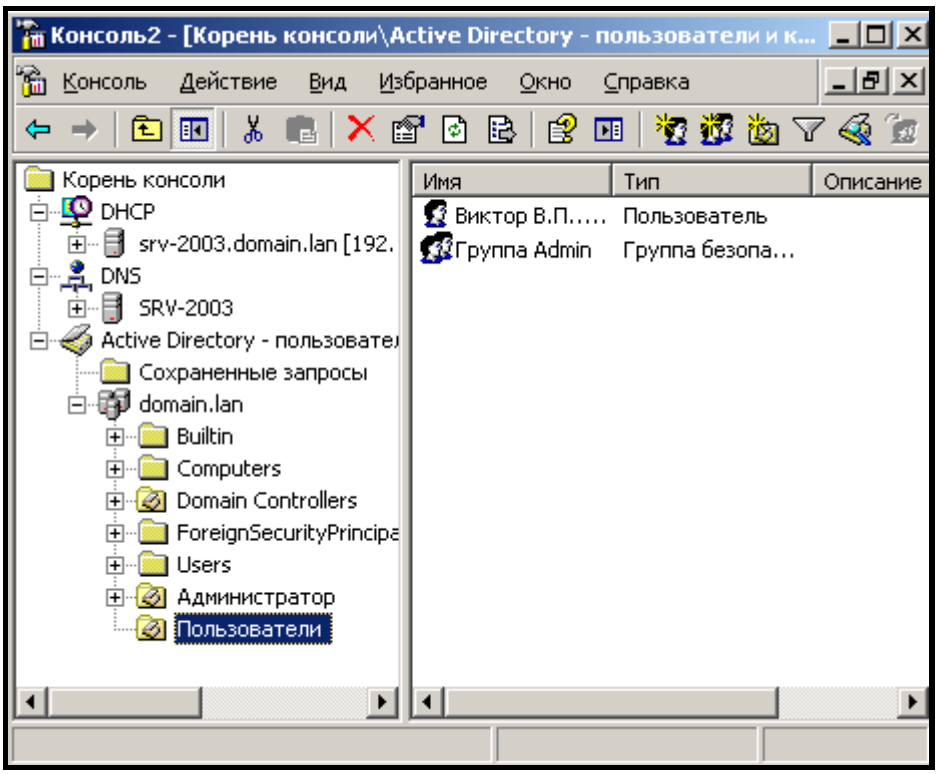


Рис. 4. Группа Admin создана

Щелкнем дважды мышкой на этой группе и на вкладке **Член групп** нажмем на кнопку **Добавить** (рис. 5.

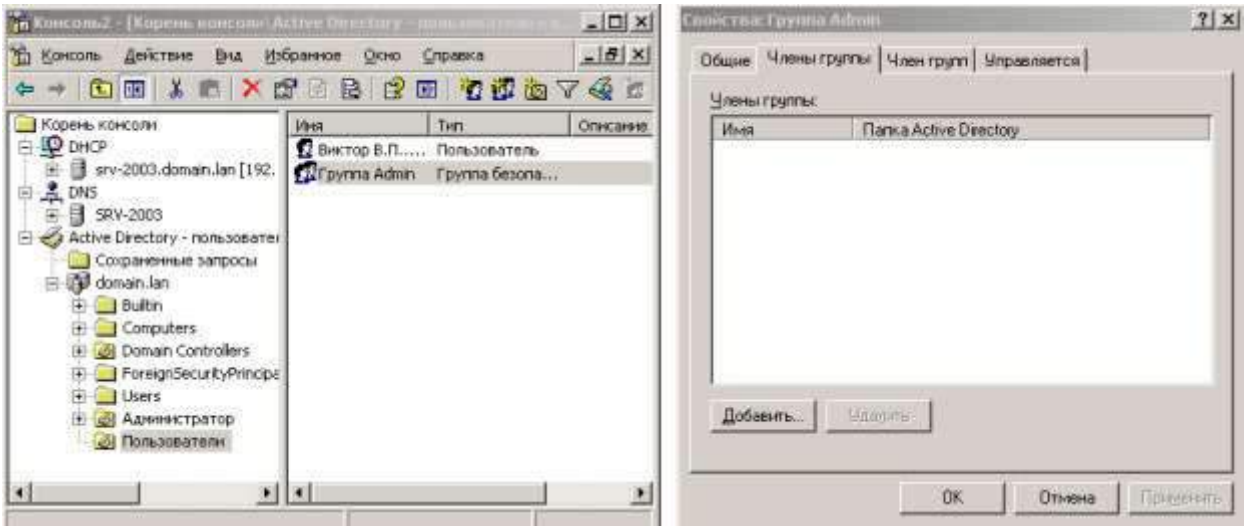


Рис. 5. Активна вкладка Члены группы

Теперь нажмите на кнопку **Дополнительно** и **Поиск** (рис. 6.

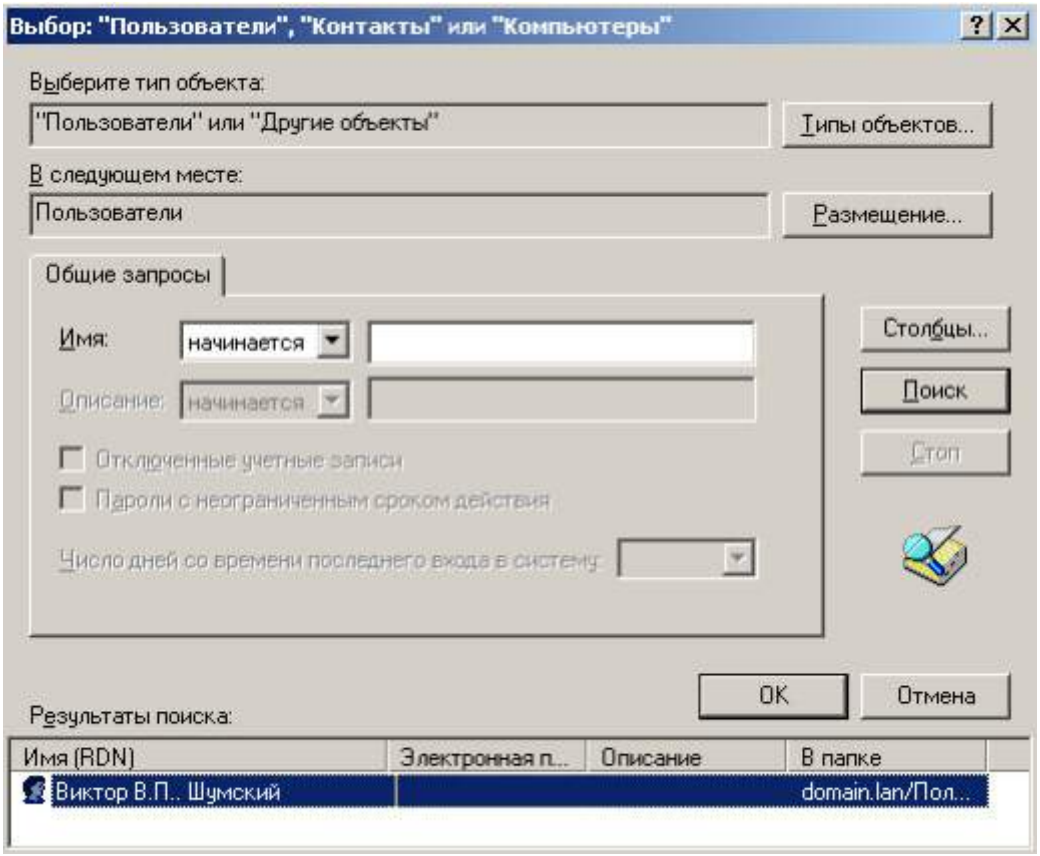


Рис. 6. Виктора Шумского мы добавим в группу Admin кнопкой ОК

Теперь если мы щелкнем мышкой на Виктора Шумского в консоли, то мы увидим в его свойствах, что он является членом сразу двух групп (рис. 7.

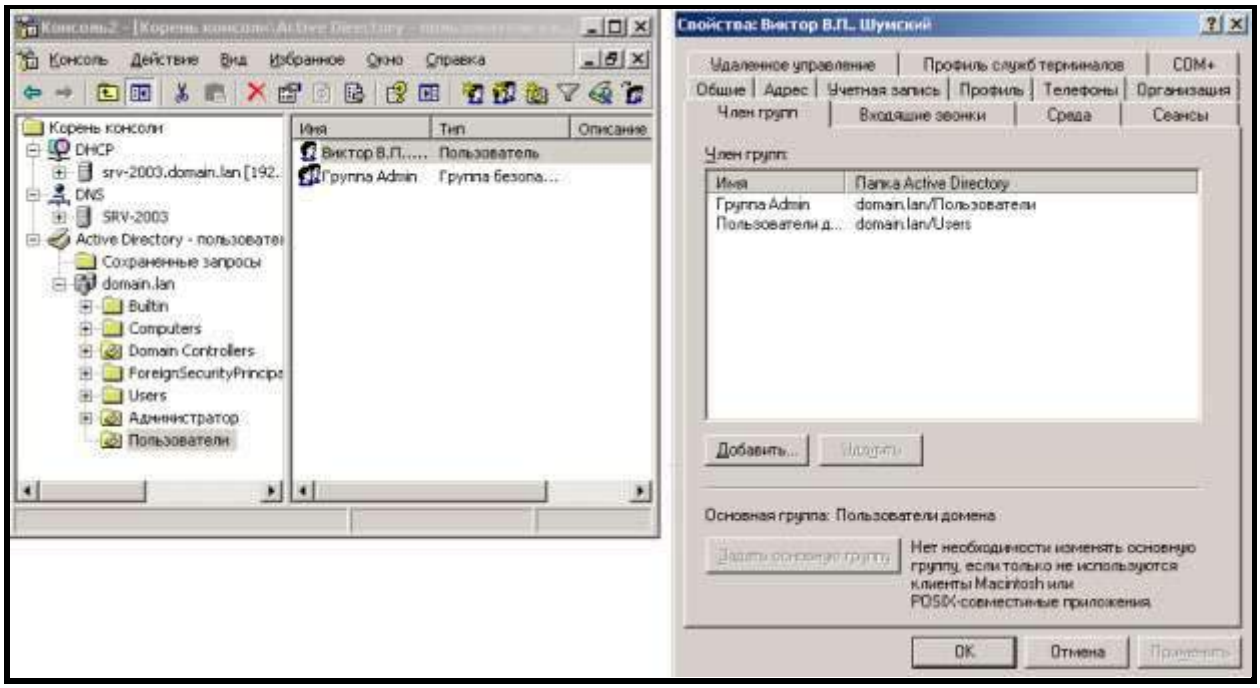


Рис. 7. Виктор член группы пользователей домена и группы Admin

Созданную нами консоль командой **Консоль-Сохранить как** сохраним на рабочий стол.

Задание №2. Выполнить Администрирование групп

Какому-то пользователю можно назначить те или иные права на ресурсы сети. Создадим пользователя **Кондратьева Мария** (kondrateva_mv), который будет управлять группой **Admin**, то есть, назначать им права на ресурсы. В консоли щелкаем правой кнопкой мыши и выполняем команду **Создать-Пользователь** (рис. 8.

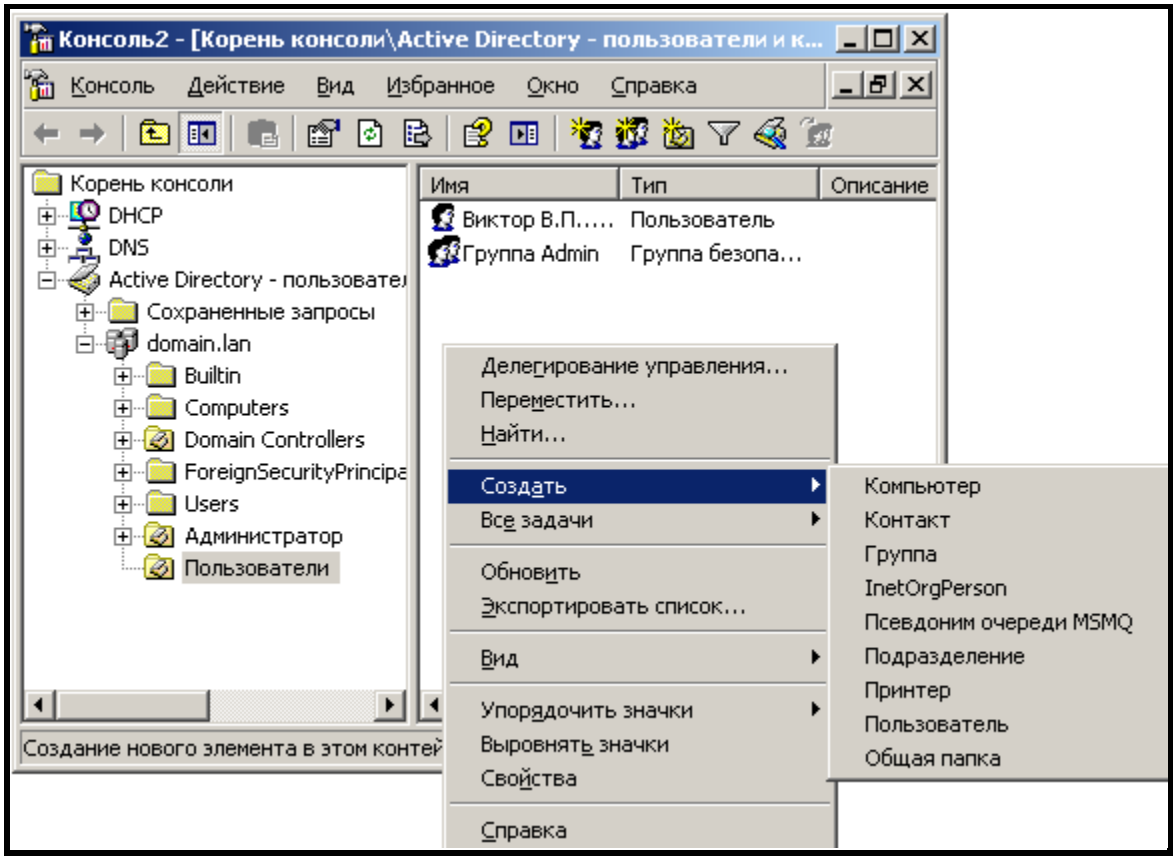


Рис. 8. Создаем нового пользователя

Заполняем форму (рис. 9.

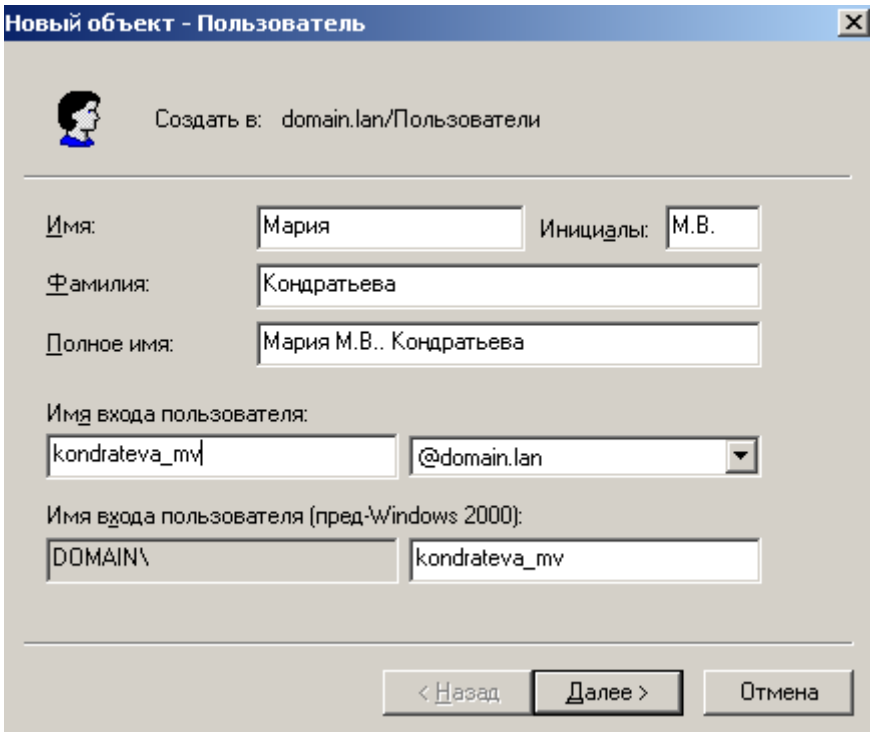


Рис. 9. Вводим данные пользователя

В консоли выполняем команду **Вид-Дополнительные функции**. Далее в консоли заходим в группу **Admin** и активируем вкладку **Безопасность**

(рис. 10.

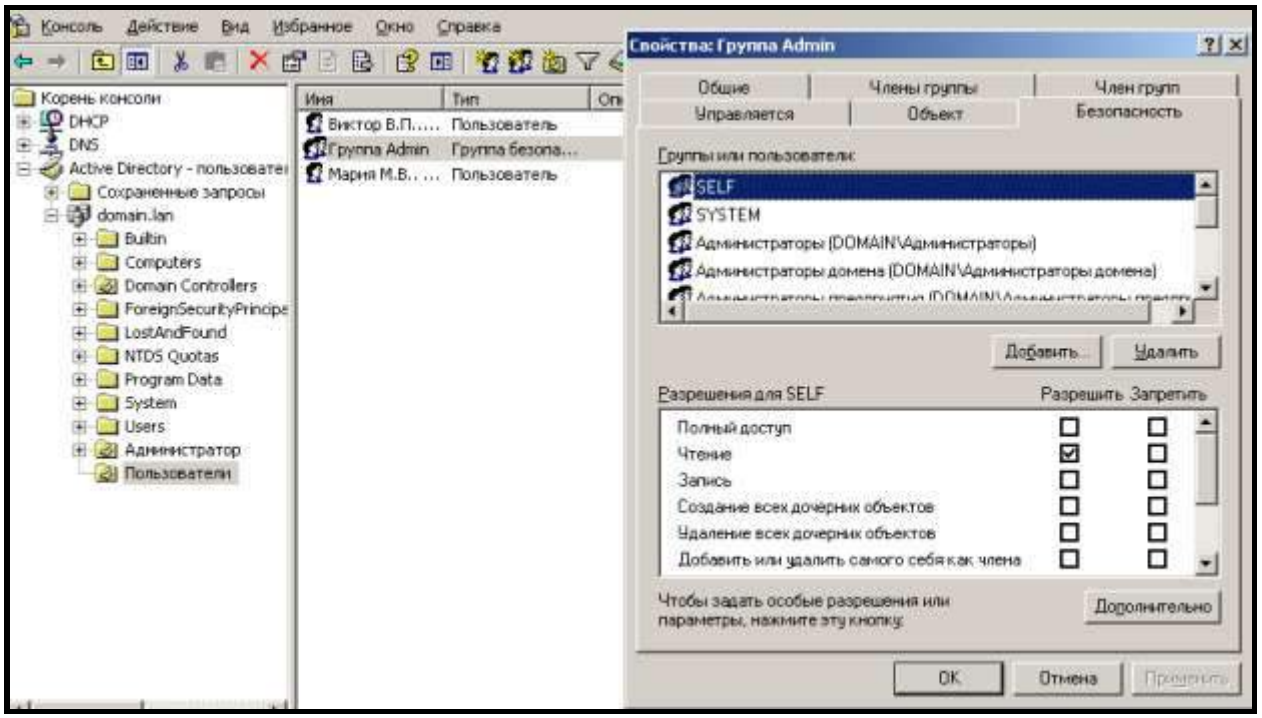


Рис. 10. Окно Свойства группа Admin, вкладка Безопасность

Примечание

Ресурсы хранятся в Active Directory как объекты. Любой объект, с которым связан другой объект, является родительским. В окне на рисунке выше мы видим - дочерний объект. Дочерние объекты в свою очередь могут иметь детей. Хотя родитель может иметь любое количество детей, но ребенок может иметь только одного родителя. Active Directory автоматически выстраивает двусторонние доверительные отношения между родительскими и дочерними доменами в дереве доменов. При создании дочернего домена доверительные отношения автоматически формируются между дочерним доменом и его родителем, что существенно упрощает управление доменами.

Нажимаем на кнопку **Дополнительно-Добавить…Поиск** и добавляем нашего пользователя кнопкой ОК (рис. 11.

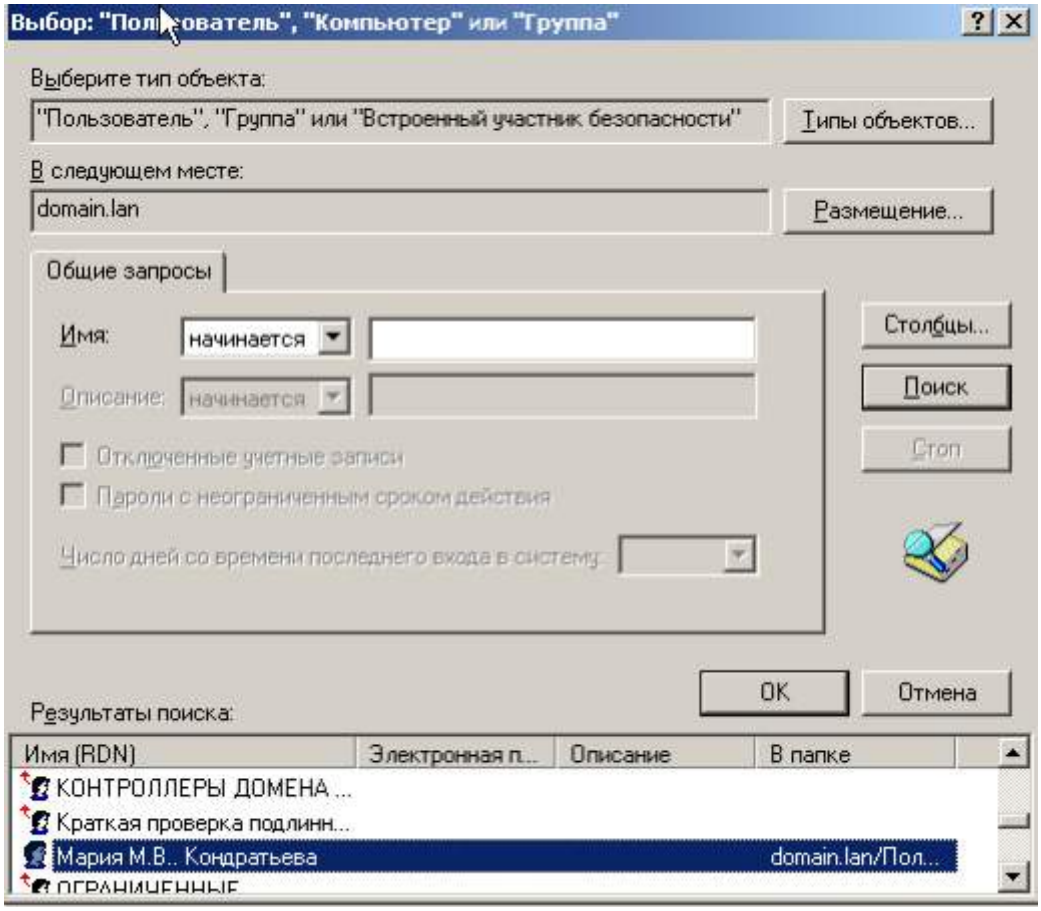


Рис. 11. Выбираем пользователя и нажимаем на кнопку ОК

Теперь зададим, что мы можем разрешить, а что запретить для пользователя (рис. 12.

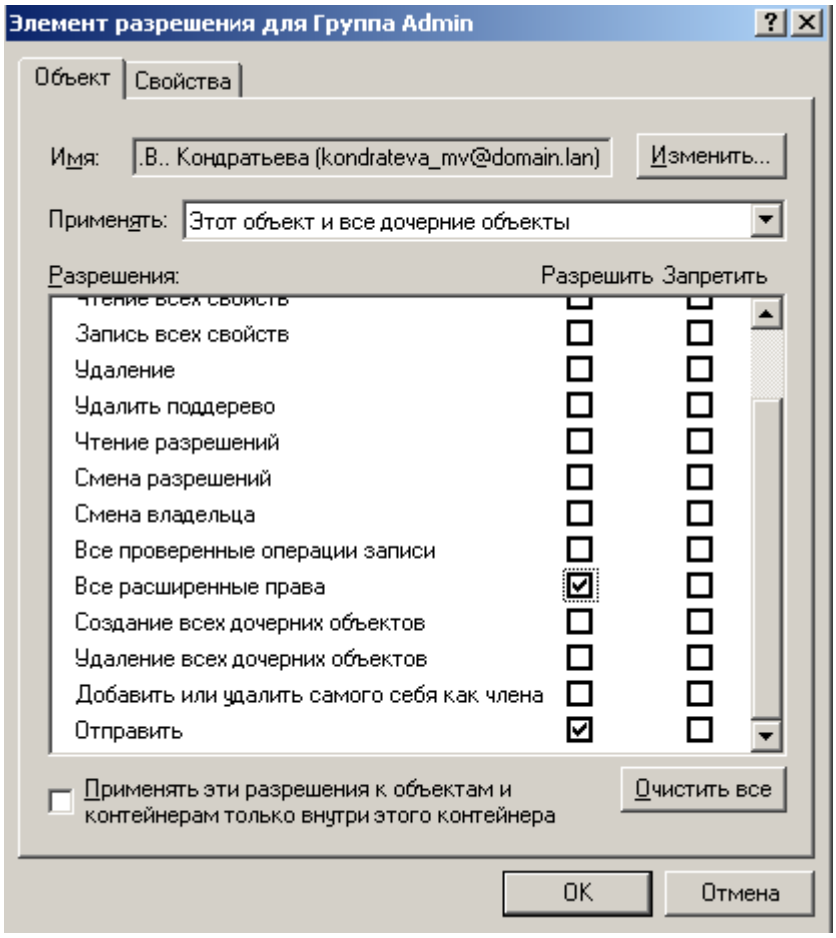


Рис. 12. Определяем права пользователя

Задание №3. Создать групповую политику

Оснастка **Групповая политика** используется для определения параметров политики, которые будут применяться к компьютерам или пользователям.

Групповая политика — это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows. Продуманное применение объектов групповой политики к объектам каталога Active Directory позволяет создавать эффективную и легко управляемую компьютерную рабочую среду на базе ОС Windows.

Изменение групповой политики всех пользователей и ПК

Чтобы увидеть групповую политику домена по умолчанию, зайдем в консоль и, щелкнув в AD на названии домена, вызываем окно свойств домена (рис.13. Эта политика применяется ко всем пользователям и ПК в домене.

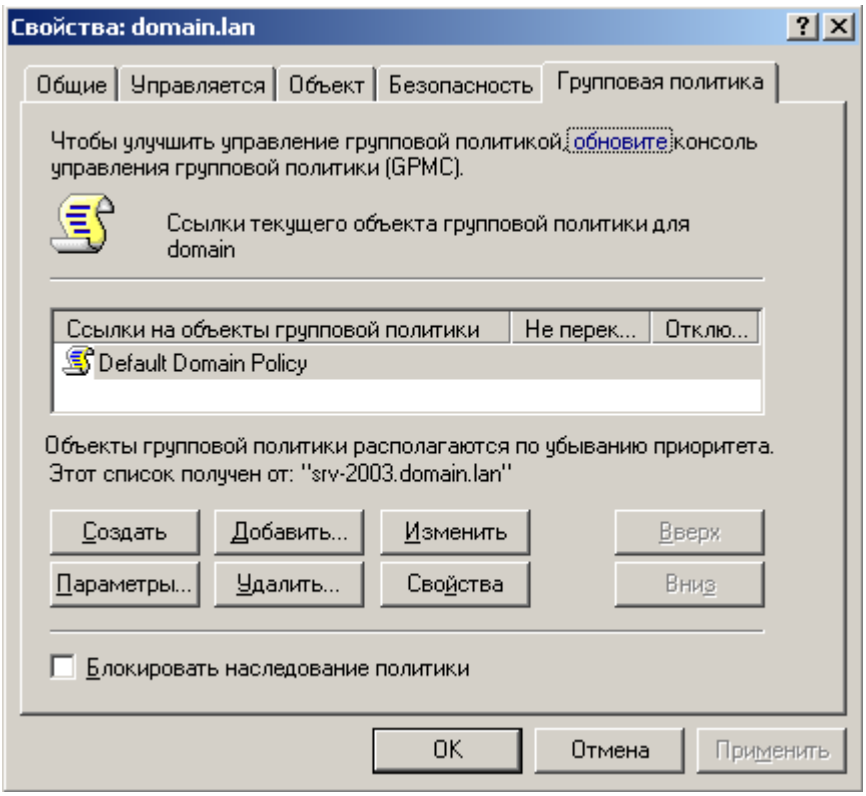


Рис. 13. В окне открыта вкладка Групповая политика

Жмем на кнопку **Изменить** (рис. 14.

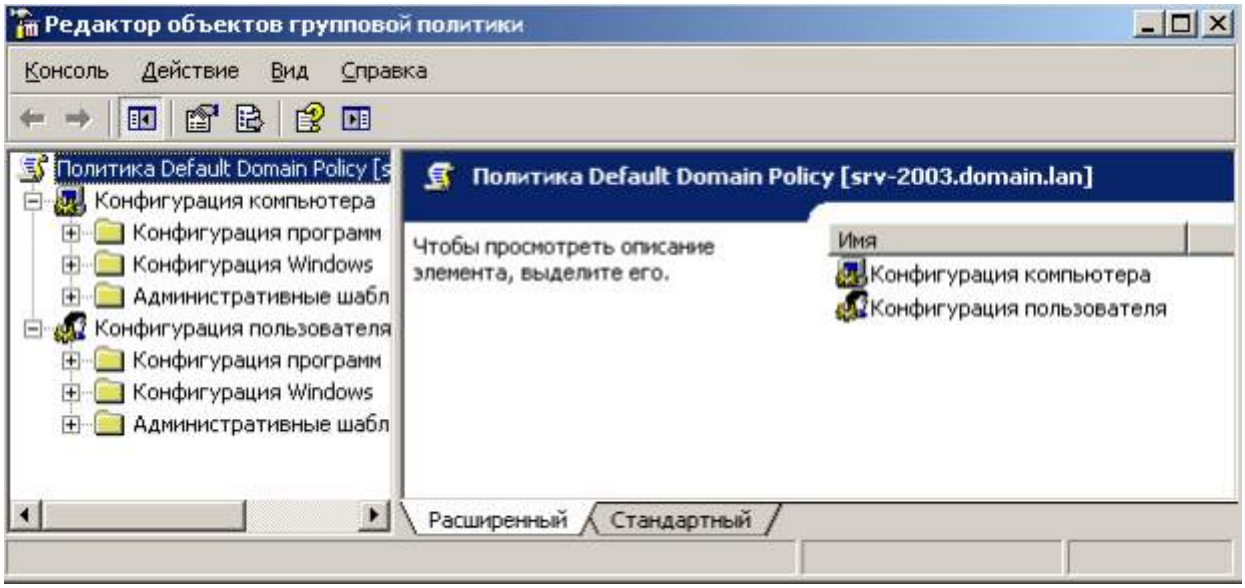


Рис. 14. На рисунке справа мы видим политику компьютера и пользователя

Давайте, например, для всех пользователей домена уберем меню **Справка и поддержка,** а также - **Моя музыка** из меню **Пуск** (рис.15.

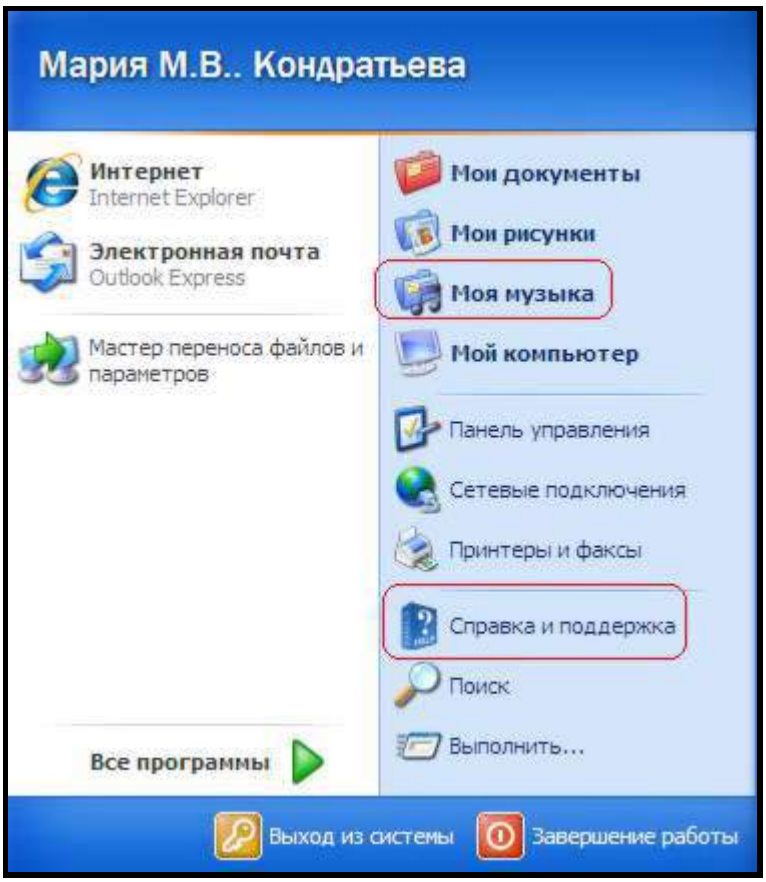


Рис. 15. Отмеченные пункты изначально в меню Пуск присутствуют

Зайдем в **Административные шаблоны** и найдем пункт **Панель задач и меню Пуск**. Находим запись **Удалить значок Моя музыка из главного меню** и задаем переключатель **Включен** (рис. 16. Затем находим запись **Удалить справку из главного меню** и снова устанавливаем переключатель **Включен**.

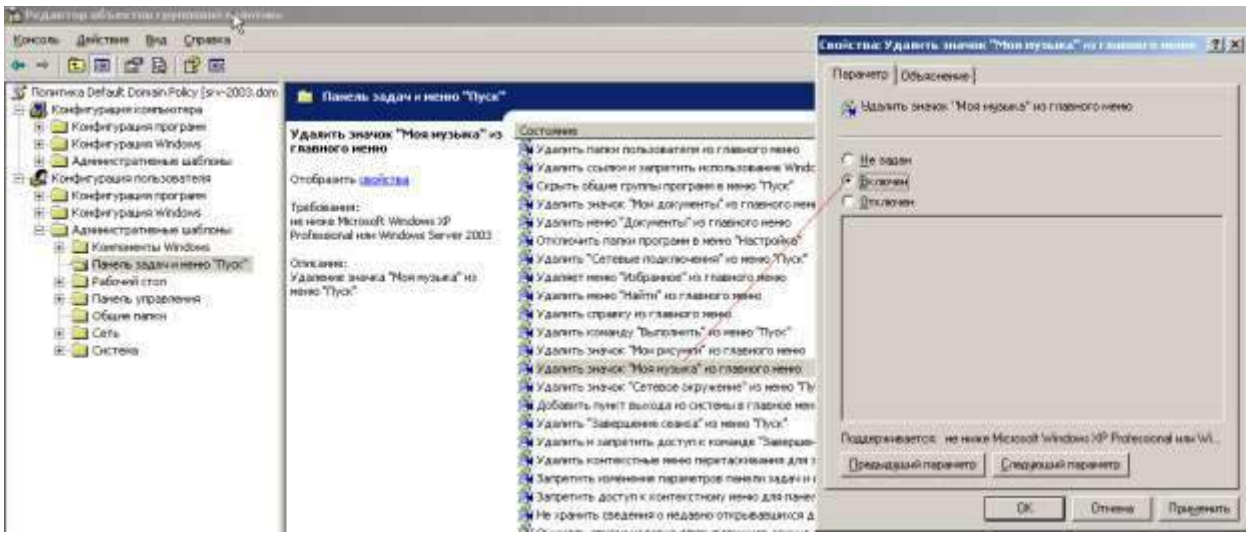


Рис. 16. Меняем два параметра групповой политики по умолчанию

После ОК входим на клиента заново (рис. 17.

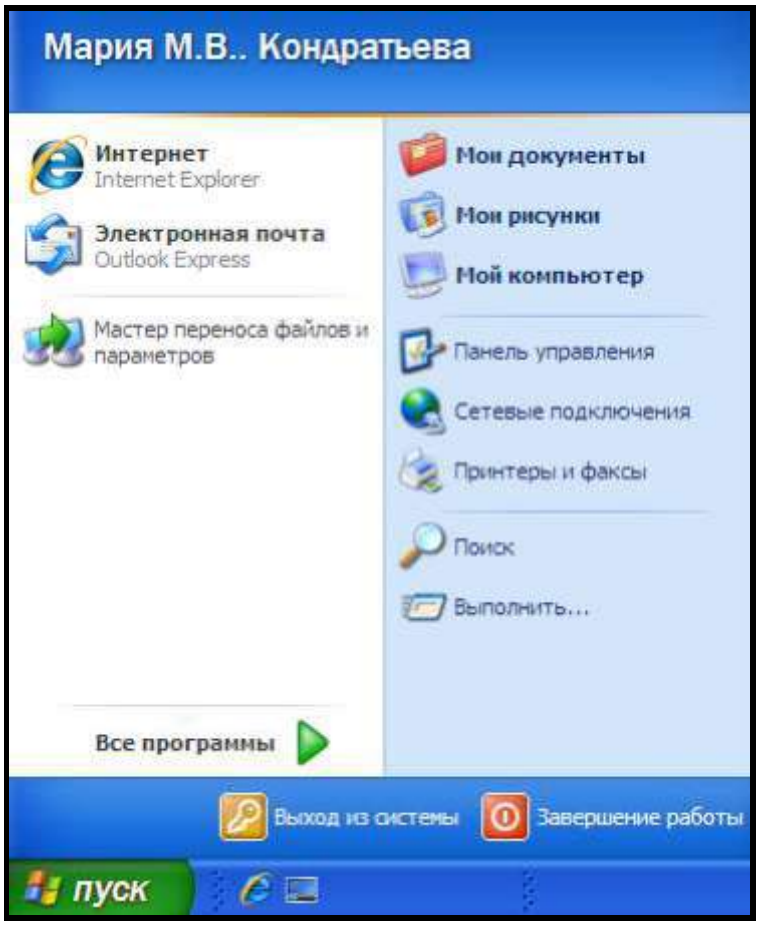


Рис. 17. Меню Пуск изменилось

Таким образом, редактируя групповую политику на сервере, мы можем сразу менять множество параметров на клиентах, что облегчает работу администратора сети.

Вопрос 1. Изменилось ли при данном в примере выше изменении групповой политики всех пользователей и ПК меню Пуск на локальном ПК при входе в него под записью Администратор (рис. 18).

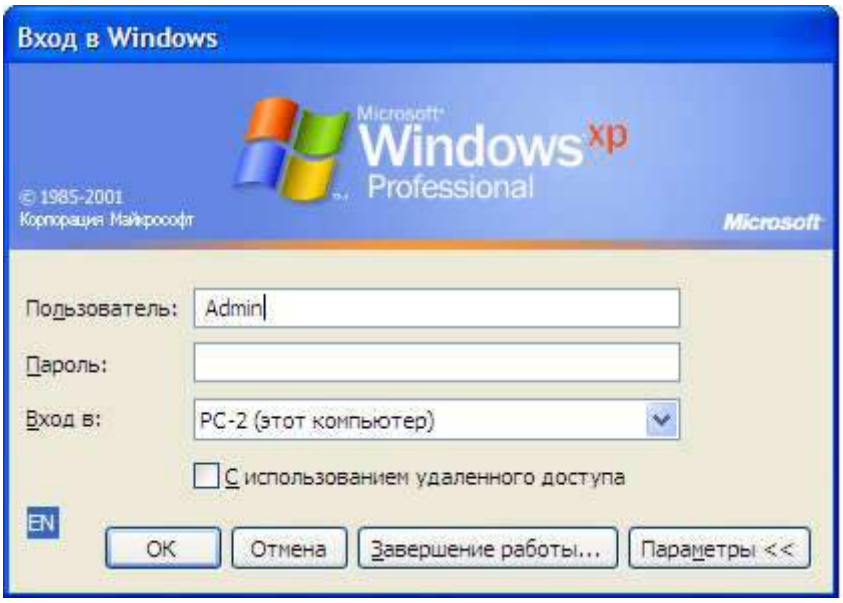


Рис. 18. Входим в локальный ПК под администратором

Правильный ответ – нет.

Вопрос 2. Изменилось ли меню при данном в примере выше изменении групповой политики всех пользователей и ПК меню Пуск на доменный ПК при входе в него под записью Администратор (рис. 19.

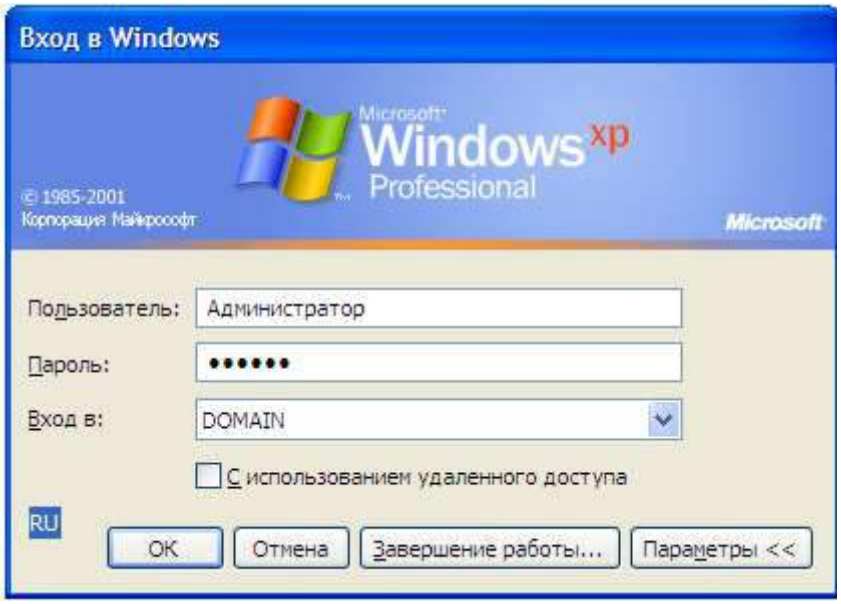


Рис. 19. Входим в доменный ПК под администратором

Правильный ответ – да.

Задание №4. Выполнить изменение групповой политики (ГП) для одного пользователя (не администратора)

Изменим ГП для пользователя домена В.П. Шумский, а именно, запретим ему в рабочее время заниматься видеомонтажом в программе Windows Movie Maker. Сначала создадим политику для него кнопкой **Создать** (рис. 1).

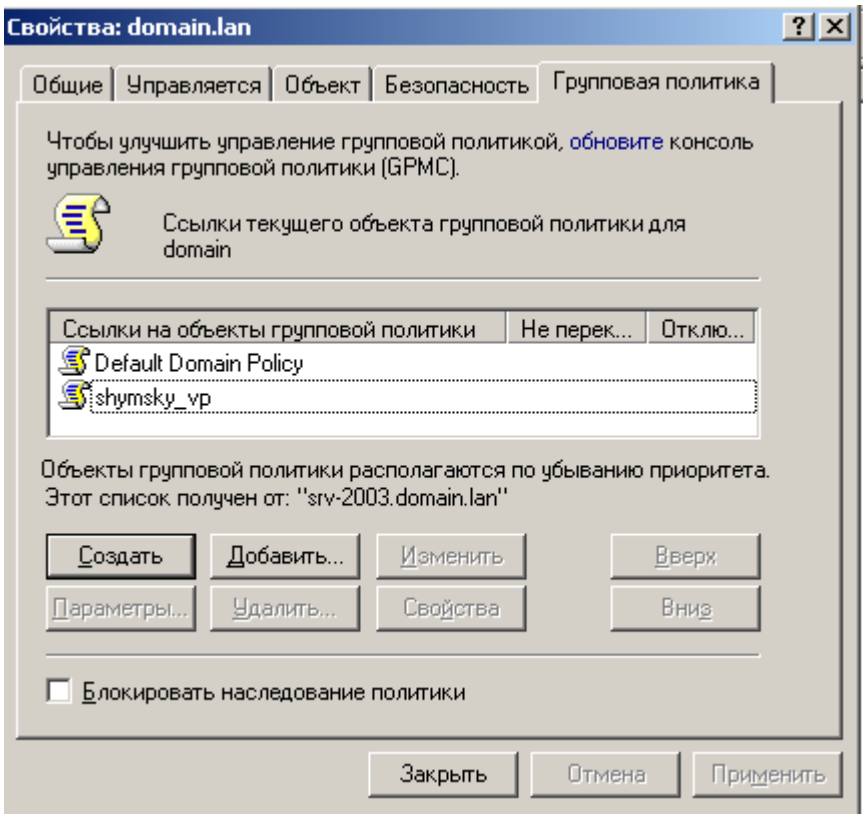


Рис. 1. В данном окне нажмем на кнопку Создать

Далее необходимо, чтобы созданная нами политика не применялась ко всем пользователям. Для этого выделяем пользователя, нажимаем кнопку **Свойства** и переходим на вкладку **Безопасность**, где убираем флажок **Применение групповой политики** для всех пользователей (рис. 2).

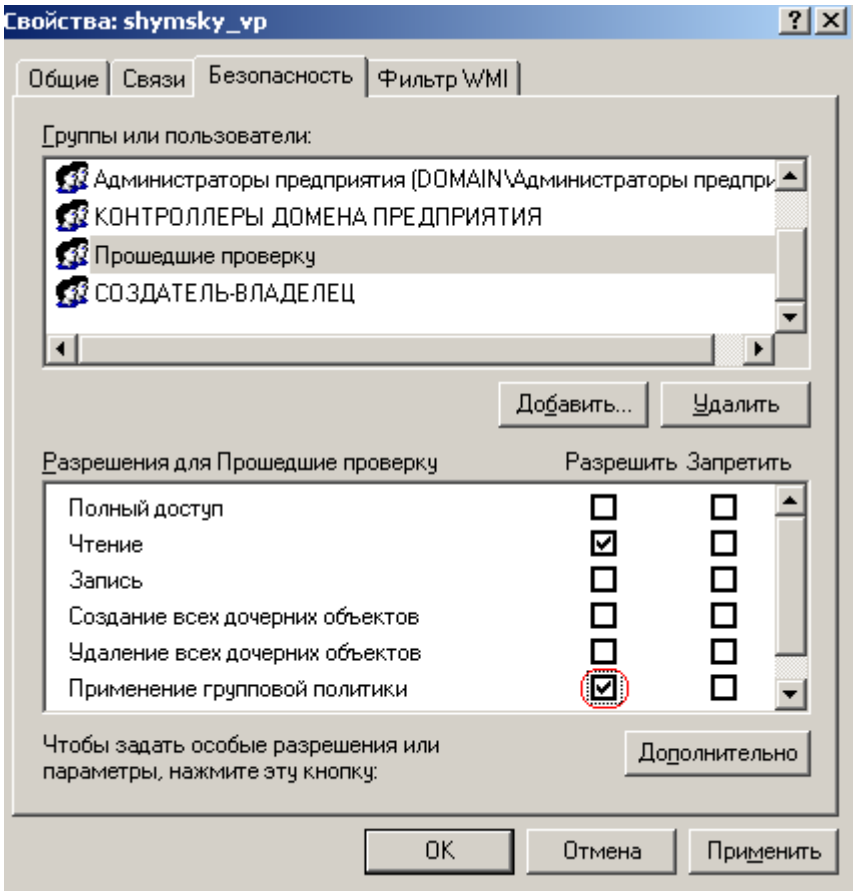


Рис. 2. Выделенный флажок необходимо убрать

Теперь в этом же окне нажмите на кнопку **Добавить**, найдите и добавьте пользователя (рис. 3). Для Шумского нужно разрешить применение групповой политики.

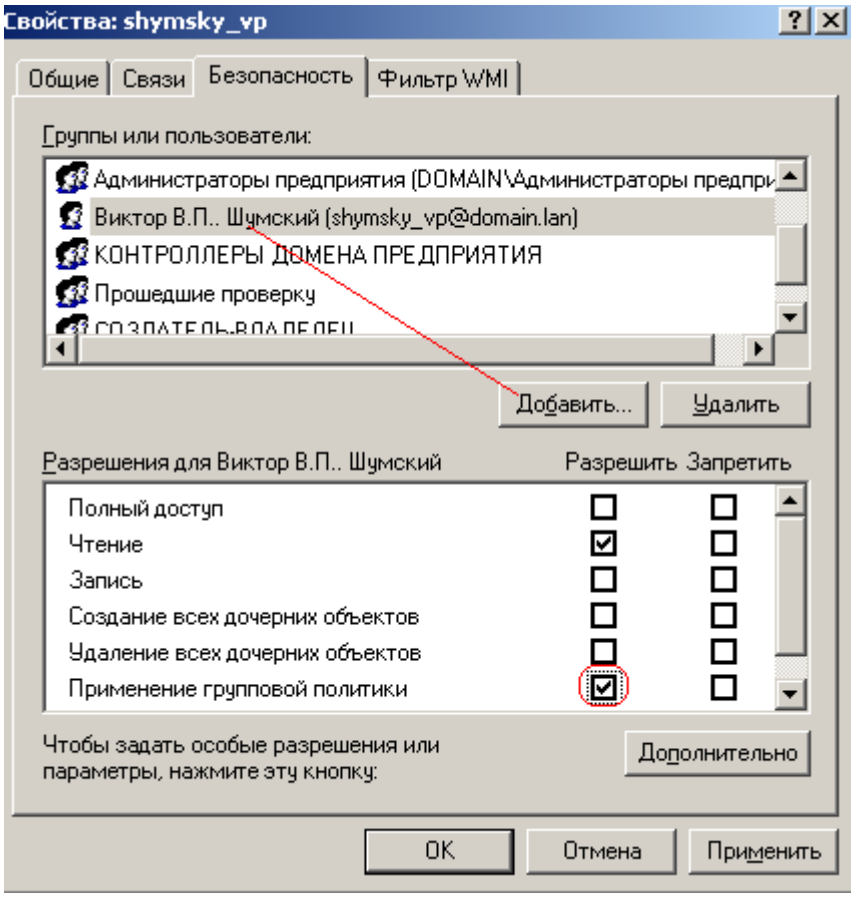


Рис. 3. В.П. Шумский добавлен и к нему будет применена групповая политика

Жмем **Применить**, а затем **Изменить** (рис. 4).

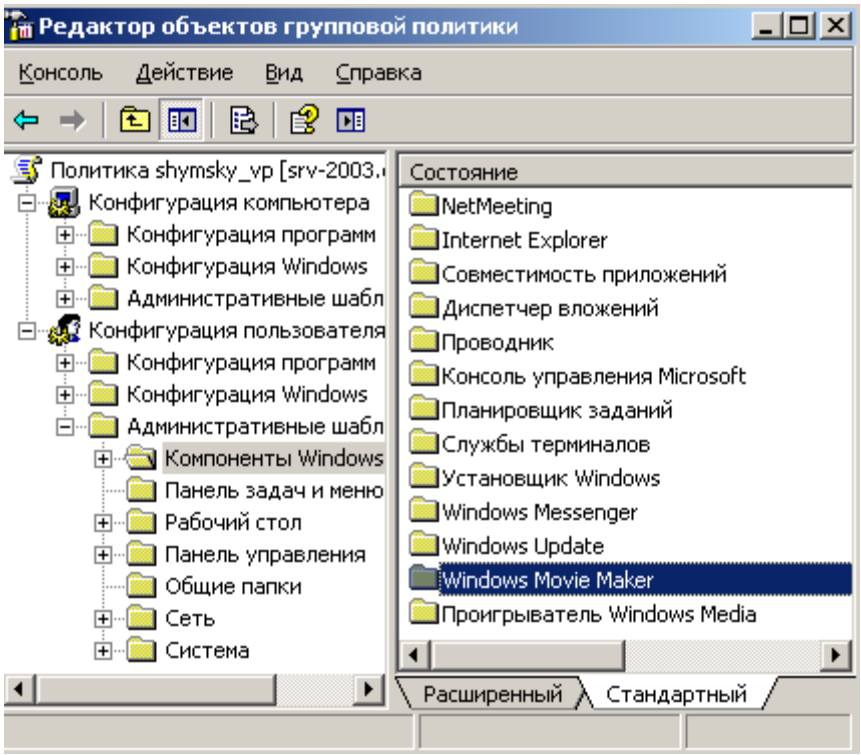


Рис. 4. В компонентах Windows находим Windows Movie Maker

Далее активируем переключатель **Запретить выполнение программы Windows Movie Maker** – рис. 5.

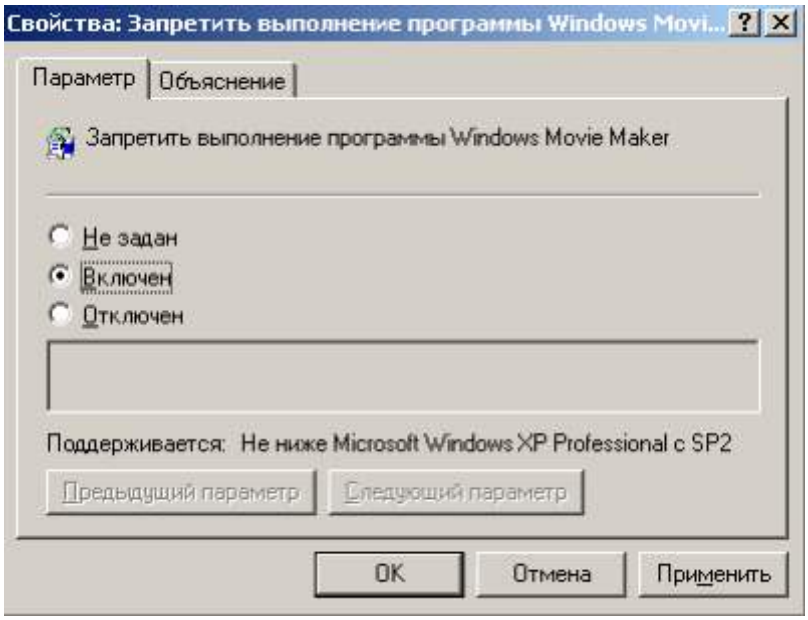


Рис. 5. Активируем средний переключатель

Теперь зайдем в клиента под учетной записью Виктора Шумского (рис. 6).

Рис. 6. Входим в домен

При попытке запустить программу Movie Maker получаем следующее сообщение (рис. 7).

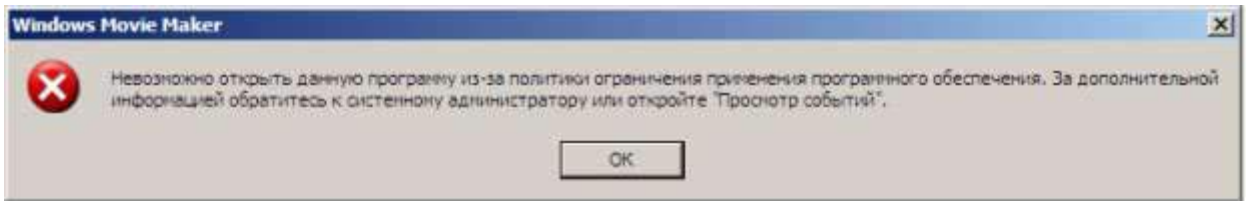


Рис. 7. Групповая политика работает

Наша цель достигнута. Попробуйте зайти в домен под другим пользователем и вы увидите, что программа Movie Maker успешно работает.

Задание №5. Выполнить создание групповой политики для группы пользователей

Ранее мы создали группу пользователей Admin (рис. 8).

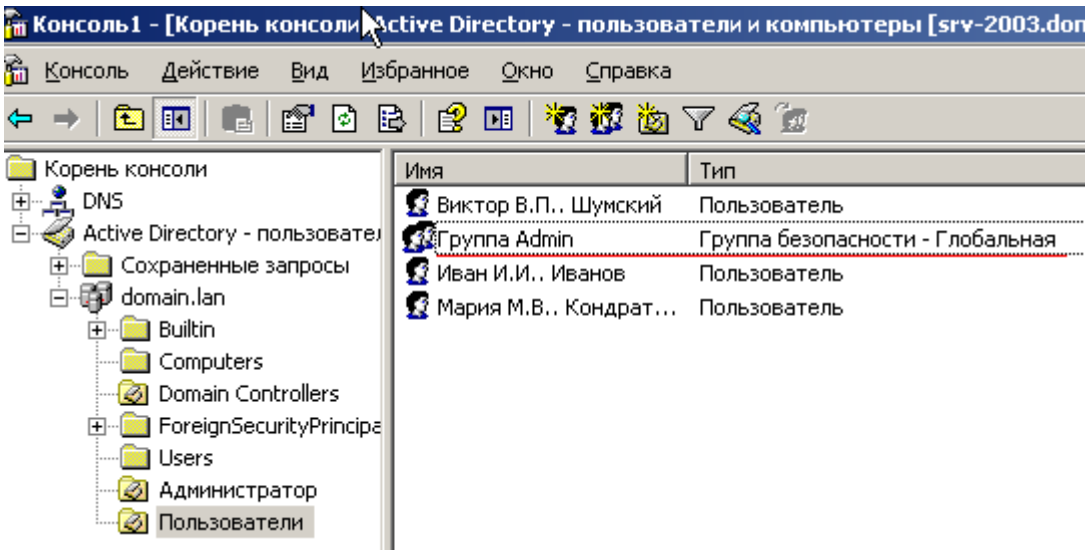


Рис. 8. В AD имеется группа пользователей Admin

Теперь для этой группы пользователей мы создадим групповую политику. Делается это так же, как для отдельного пользователя. Щелкаем на названии домена в AD правой кнопкой мыши, выполняем команду **Свойства-Групповая политика-Создать** (рис. 9).

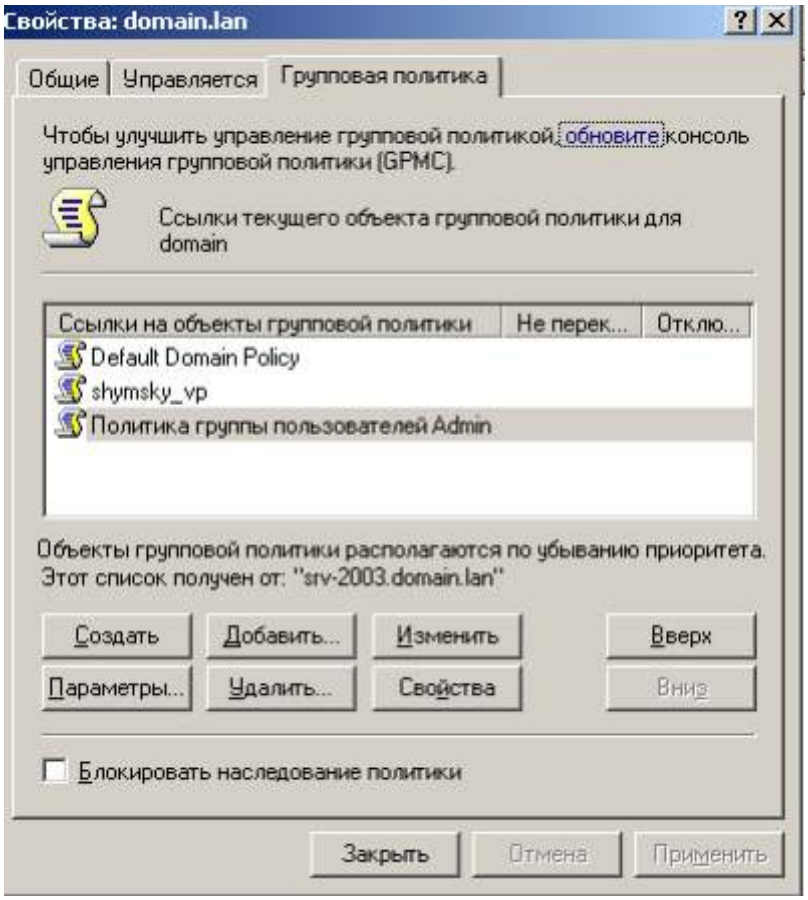


Рис. 9. Создаем политику группы пользователей Admin

Выполняем команду **Свойства-Безопасность** и везде убираем флажок **Применение групповой политики** (рис. 10).

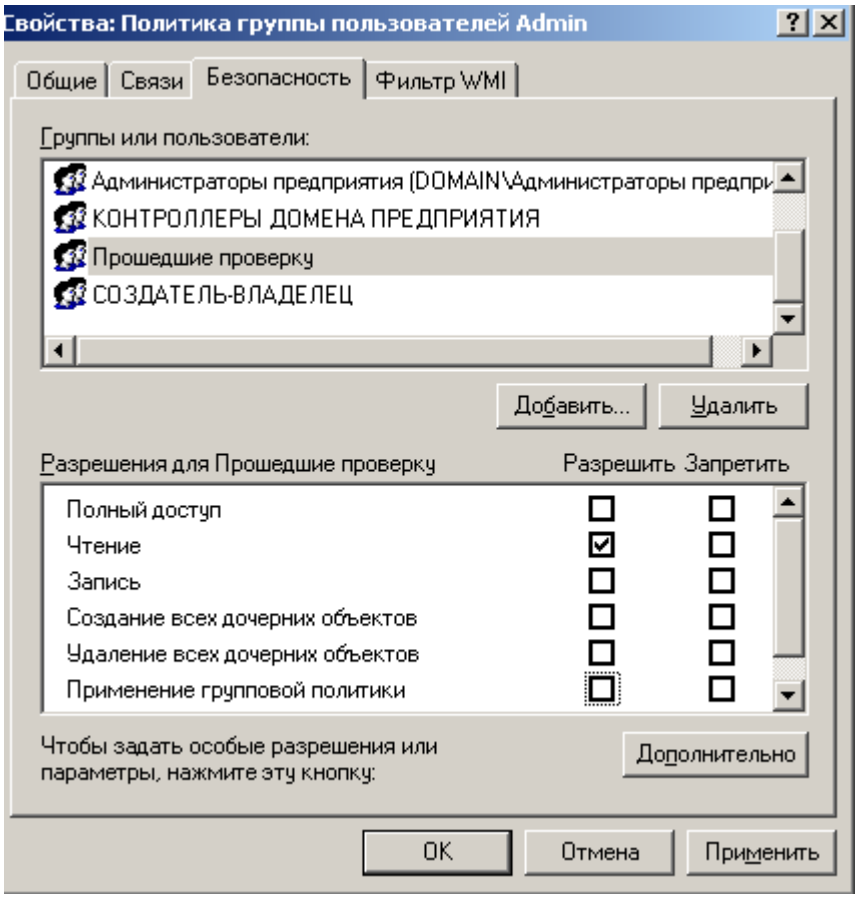


Рис. 10. В данном окне следует для всех групп и пользователей убирать флажок Применение групповой политики

В этом же окне нажимаем на кнопку **Добавить** и кнопкой **Поиск** находим **группа Admin** (рис. 11).

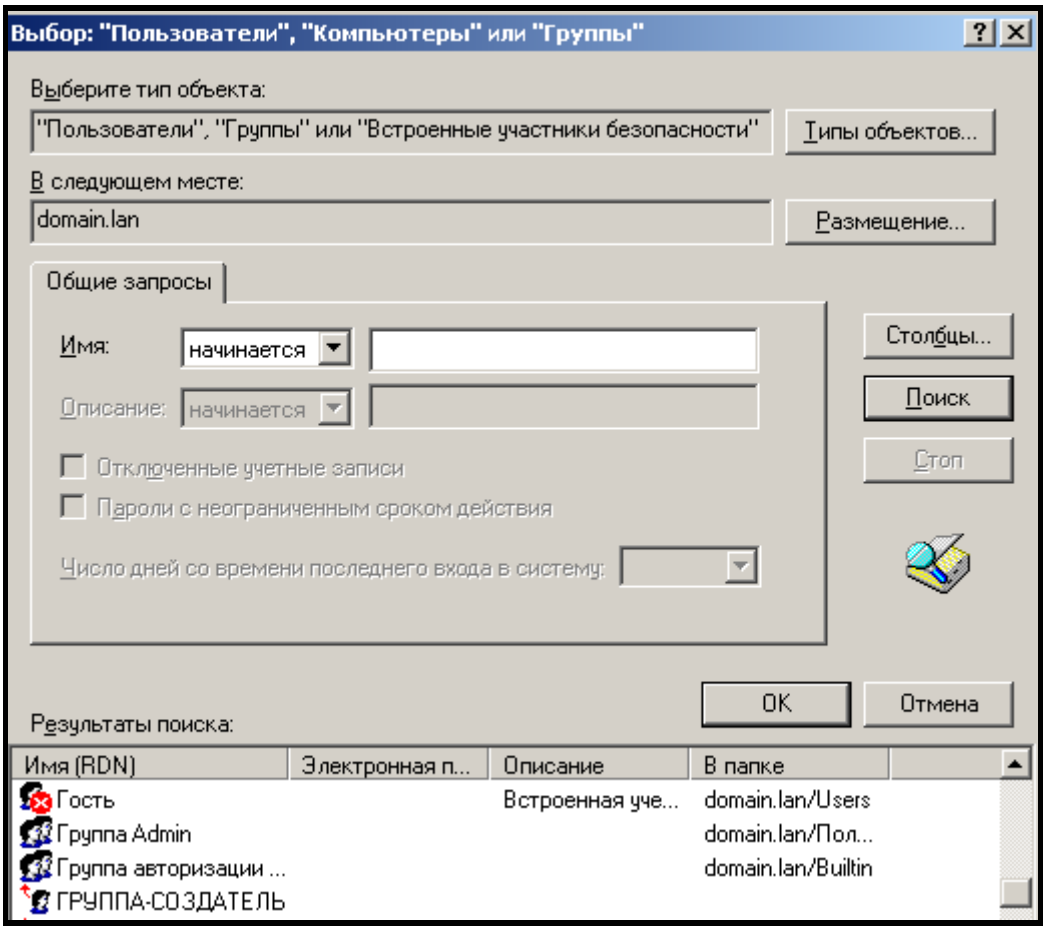


Рис. 11. Здесь нажимаем ОК

Для группы Admin активируем флажок применения групповой политики (рис. 12).

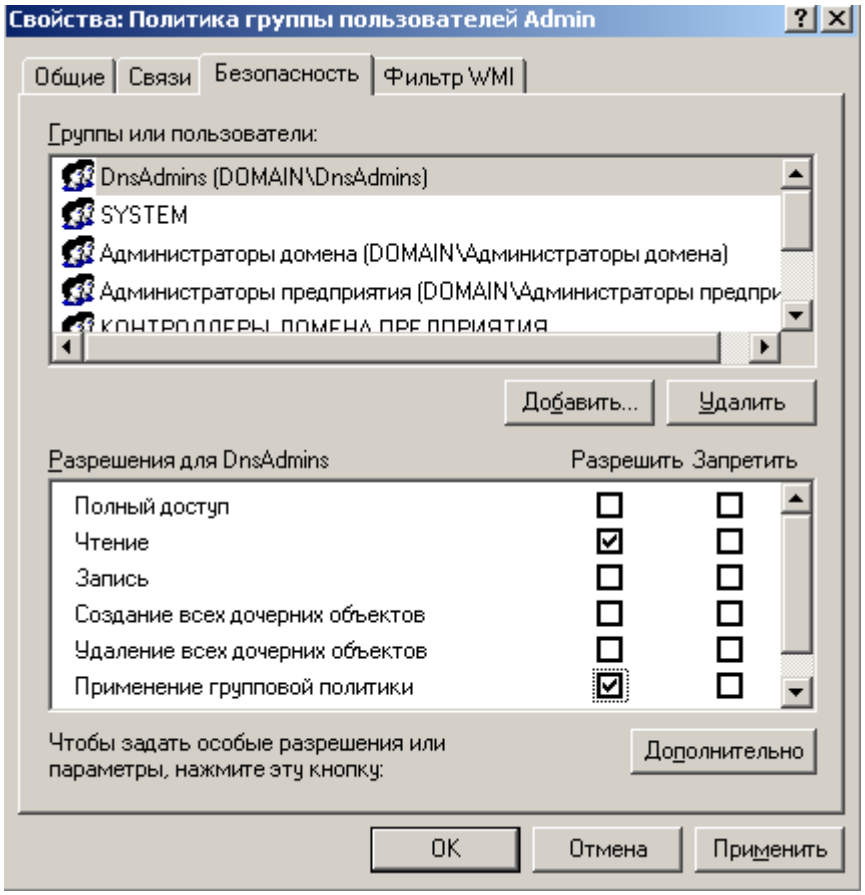


Рис. 12. Admin активируем флажок применения групповой политики

Если теперь войти в группу Admin, то увидим, что пока в ней один член, для которого будет применена групповая политика этой группы. Но кнопкой **Добавить** мы можем добавить сюда других пользователей, и автоматически групповая политика также будет применена и к ним (рис. 13).

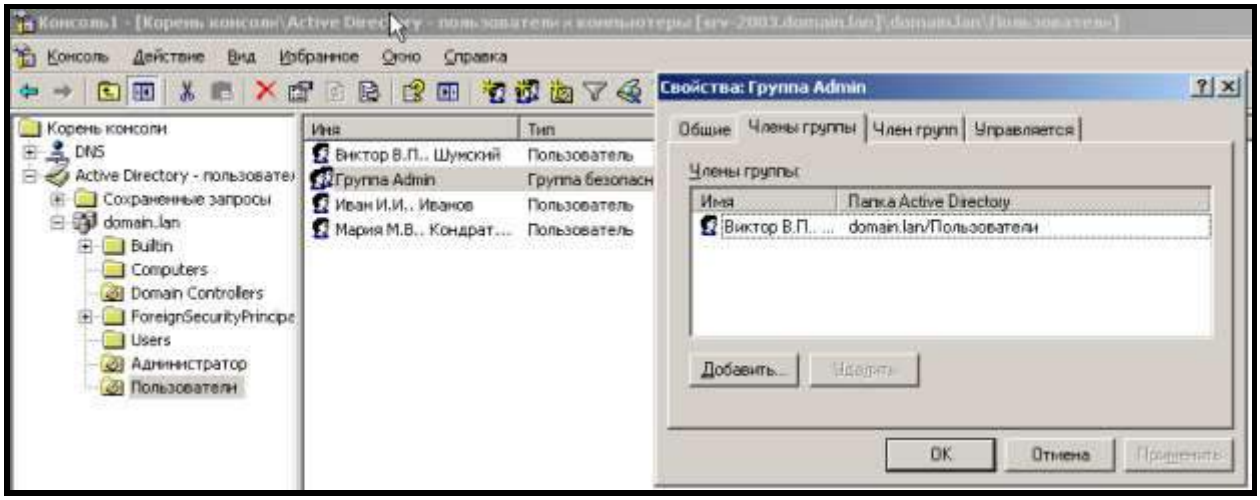


Рис. 13. Окно свойств группы Admin

Примечание

Если групповых политик несколько, то они применяются к пользователям все. Однако приоритетным является верхний уровень (рис. 14).

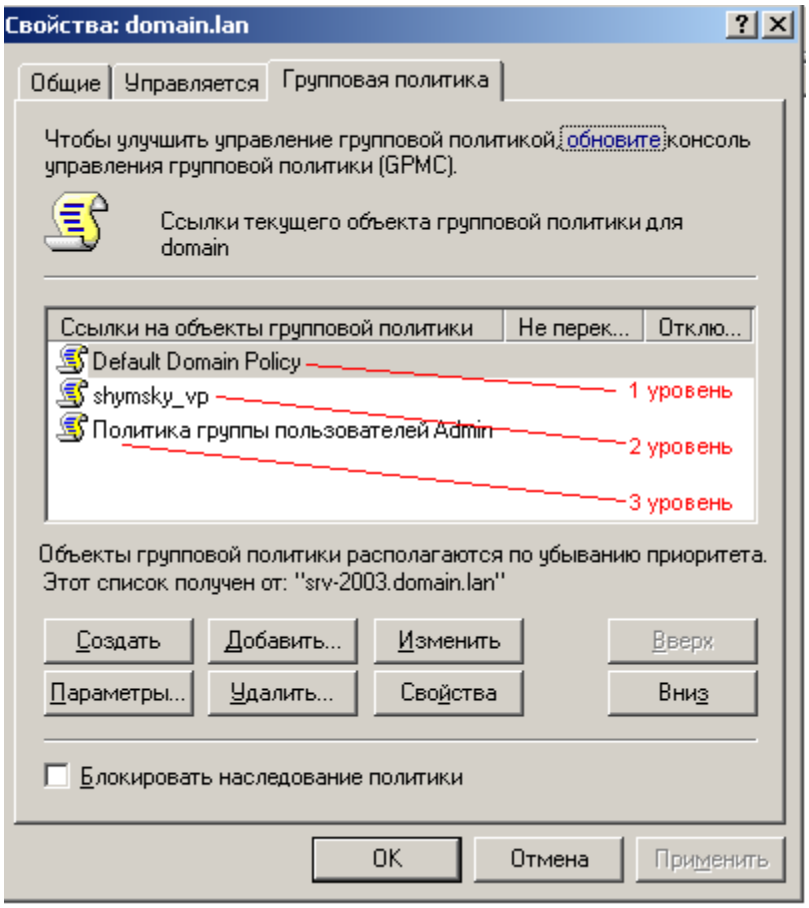


Рис. 14. Уровни приоритета групповых политик

Это означает, что если в политике 3 уровня написано запретить использовать Movie Maker, а в политике 1 уровня написано разрешить использовать Movie Maker, то использование Movie Maker будет разрешено. Однако приоритеты уровней можно изменить кнопкой **Параметры**. Другими словами, если мы нажмем на кнопку **Параметры** и активируем флажок **Не перекрывать**, то политика по умолчанию первого уровня будет изменена политикой 3 уровня и использование Movie Maker будет запрещено (рис. 15).

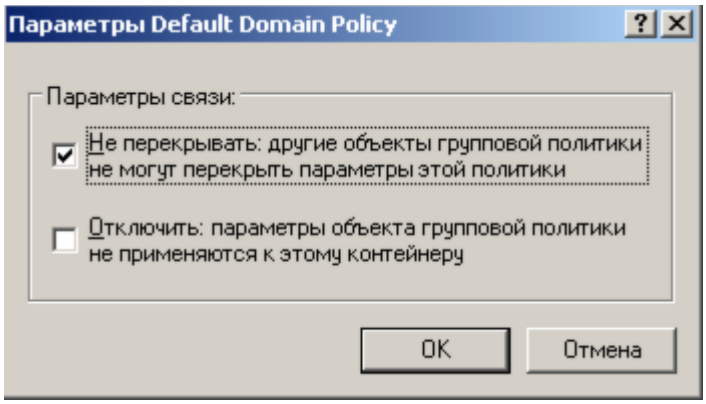


Рис. 15. Окно Параметры связи

Задание №6. Выполнить конфигурирование групповых политик для компьютеров

Когда мы создаем групповую политику для пользователя – она применяется для всех ПК, входящих в домен. При создании групповой политики для компьютеров мы можем запретить ряду пользователей входить в компьютер. Создадим новую групповую политику (рис. 1).

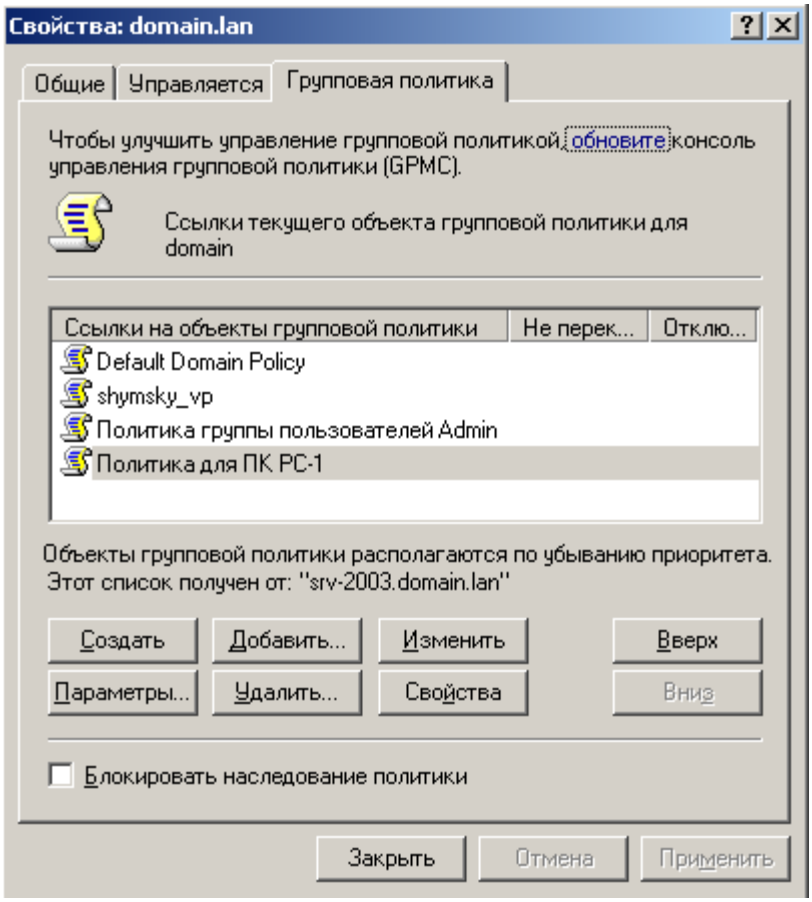


Рис. 1. Создадим Политика для ПК PC-1

Щелкнем мышкой на строчке **Политика для ПК PC-1** дважды и далее раскроем пункты **Конфигурация Windows-Параметры безопасности** (рис. 2).

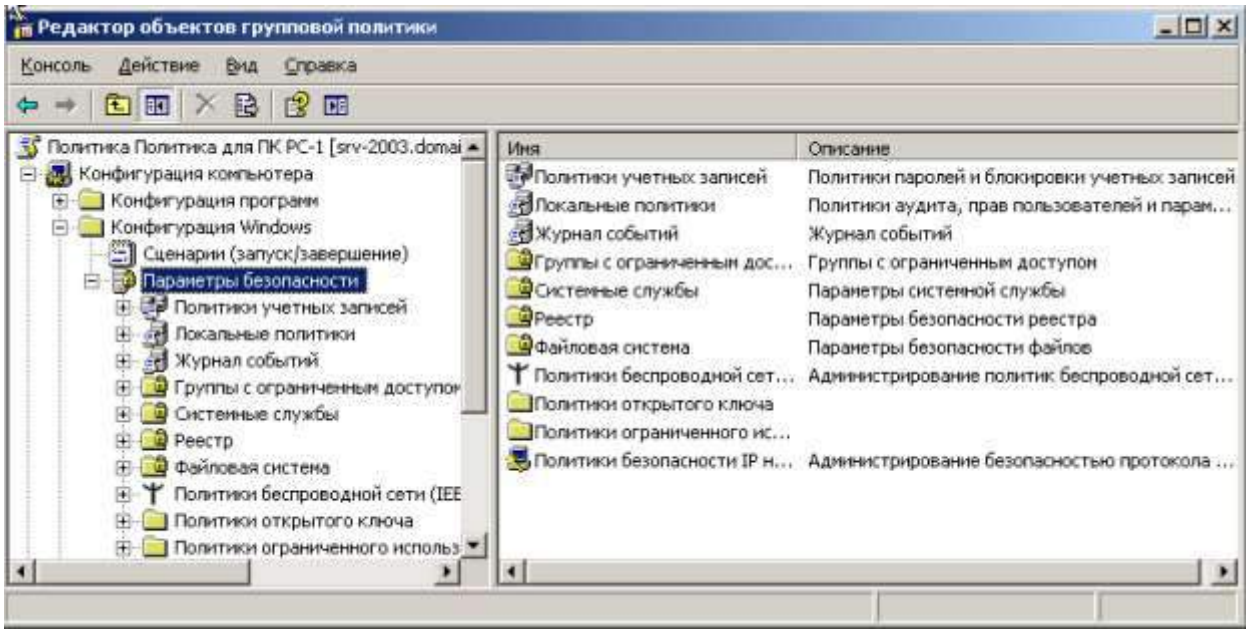


Рис. 2. Окно Редактор объектов групповой политики

Далее ищем **Назначение прав пользователя-Локальный вход в систему** (рис. 3).

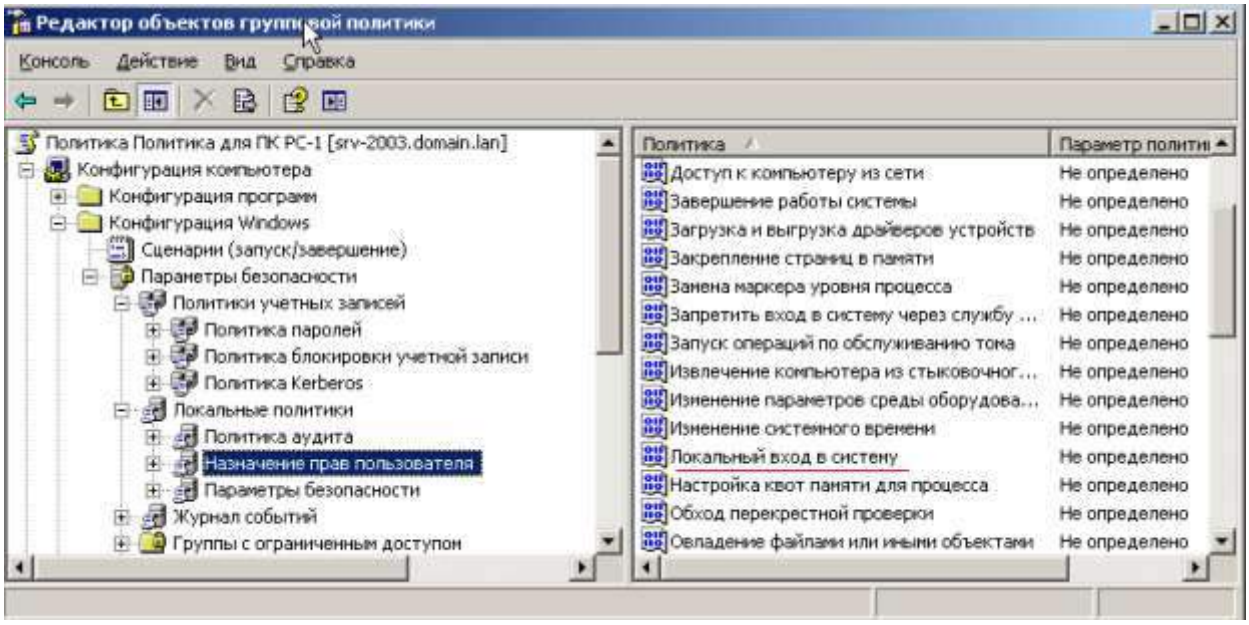


Рис. 3. Ищем запись Локальный вход в систему

Далее активируем флажок, показанный на рис. 4.

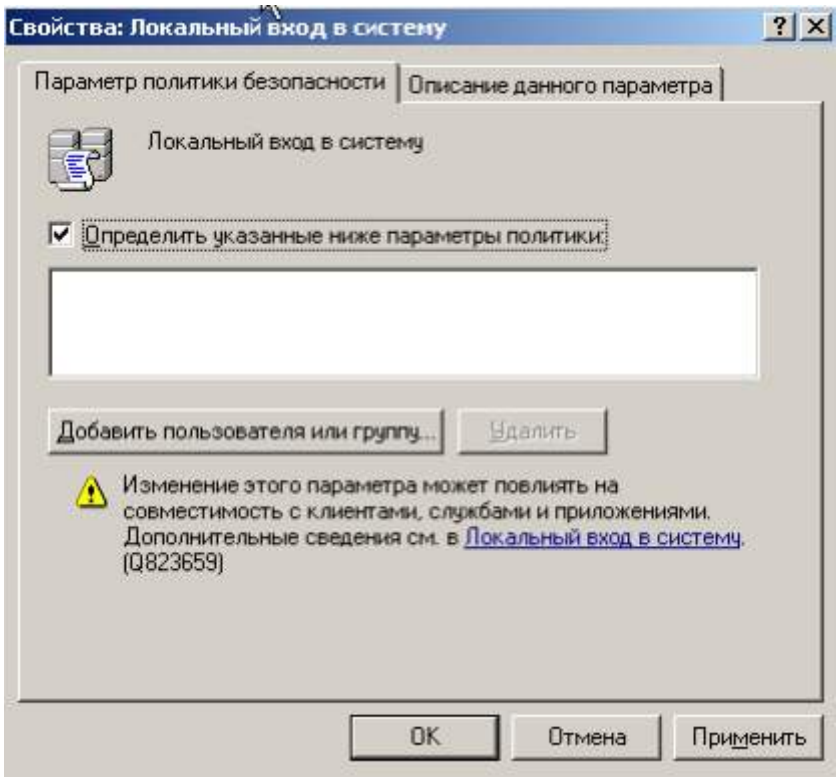


Рис. 4. Окно Свойства: Локальный вход в систему

Кнопкой **Добавить пользователя в группу** задаем пользователей, которым можно заходить в PC-1 (рис. 5).

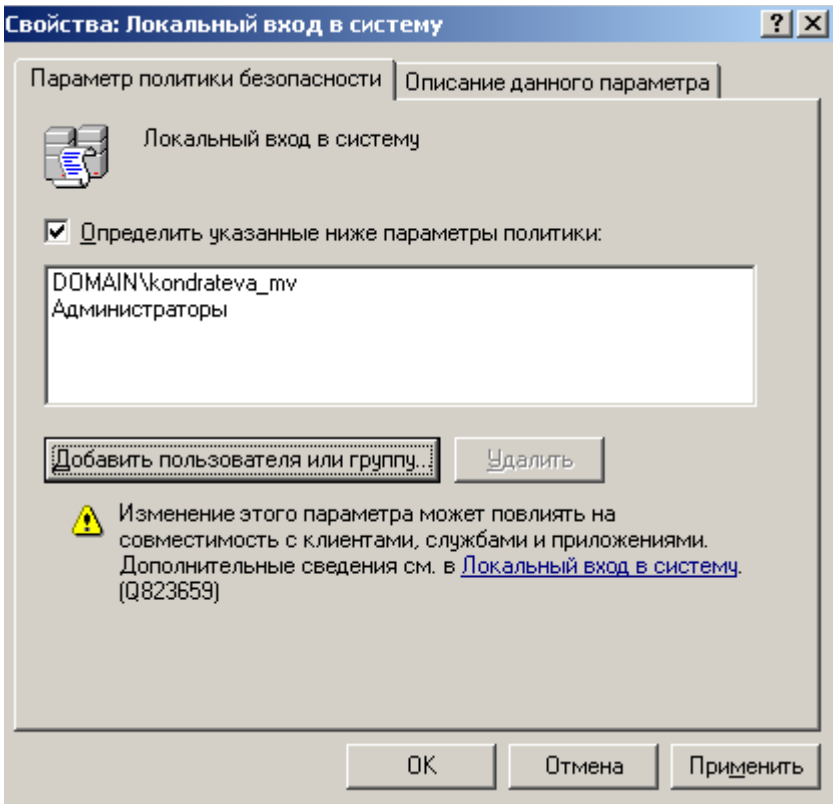


Рис. 5. Мы определили тех, кто может входить в PC-1

В PC-1 обязательно должны заходить администраторы, также мы разрешили вход пользователю Кондратьева М.В. Остальные, даже зная правильный пароль, в этот ПК не войдут. В окне на рис. 6 мы можем указать, для каких ПК данную групповую политику можно применять.

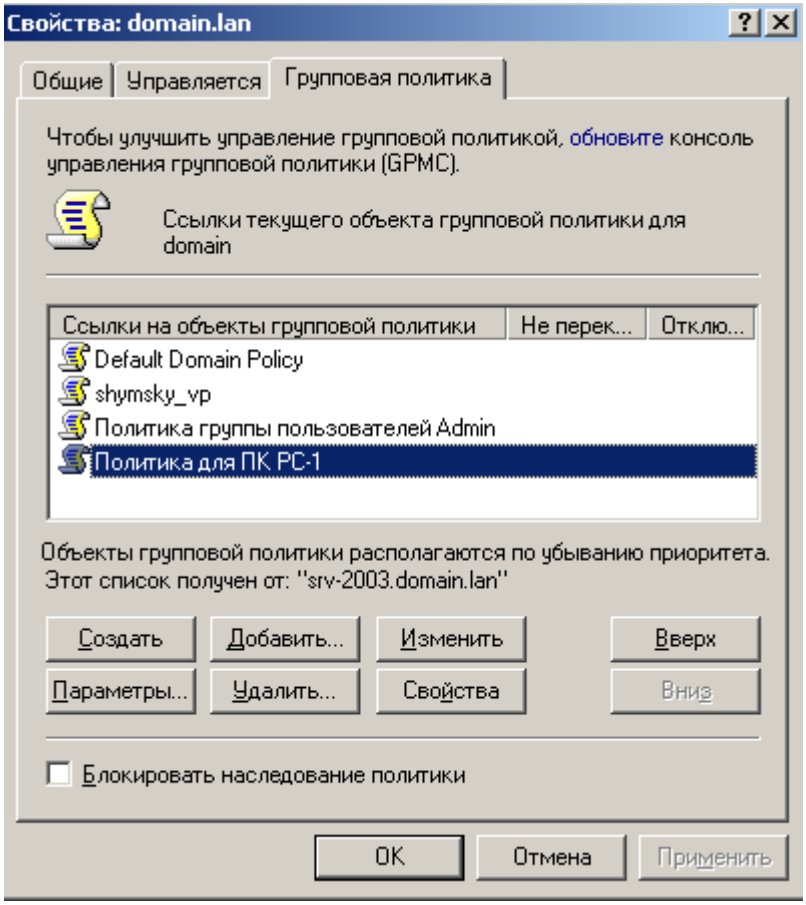


Рис. 6. Выделяем строчку Политика для ПК PC-1

Выполняем команды **Свойства-Безопасность** и убираем галочку **Применение групповой политики** (рис. 7).

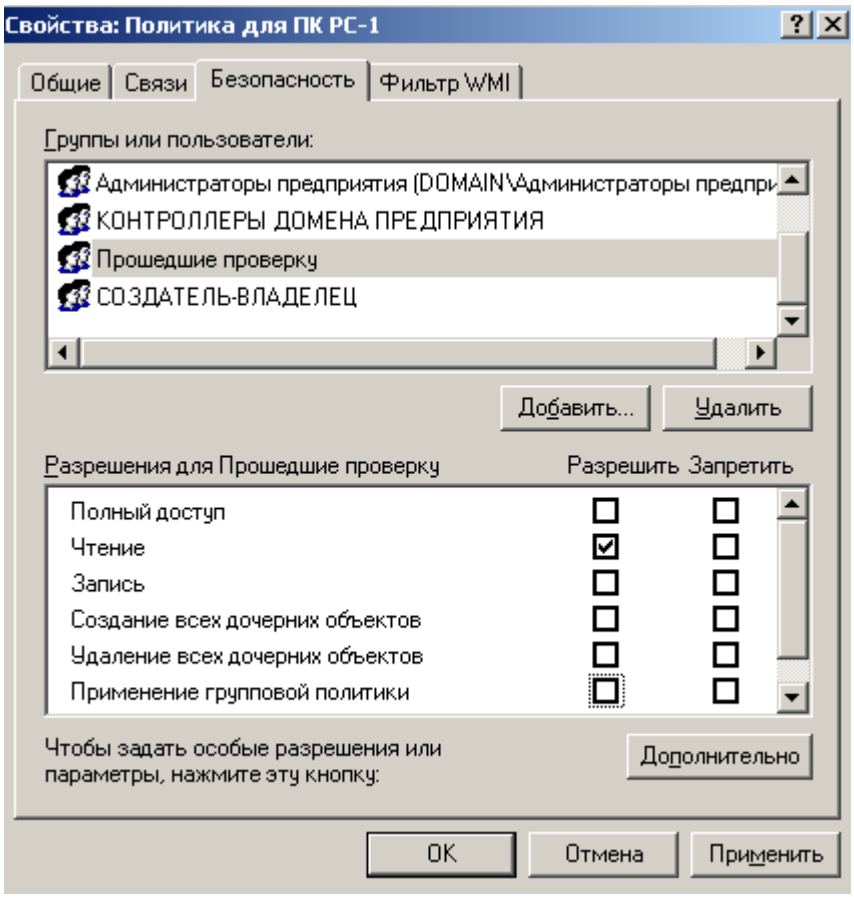


Рис. 7. Убираем галочку Применение групповой политики

Нажимаем **Применить**, затем – **Добавить**. Далее нажимаем на кнопку **Тип объекта** и ставим флажок **Компьютеры** (рис. 8.).

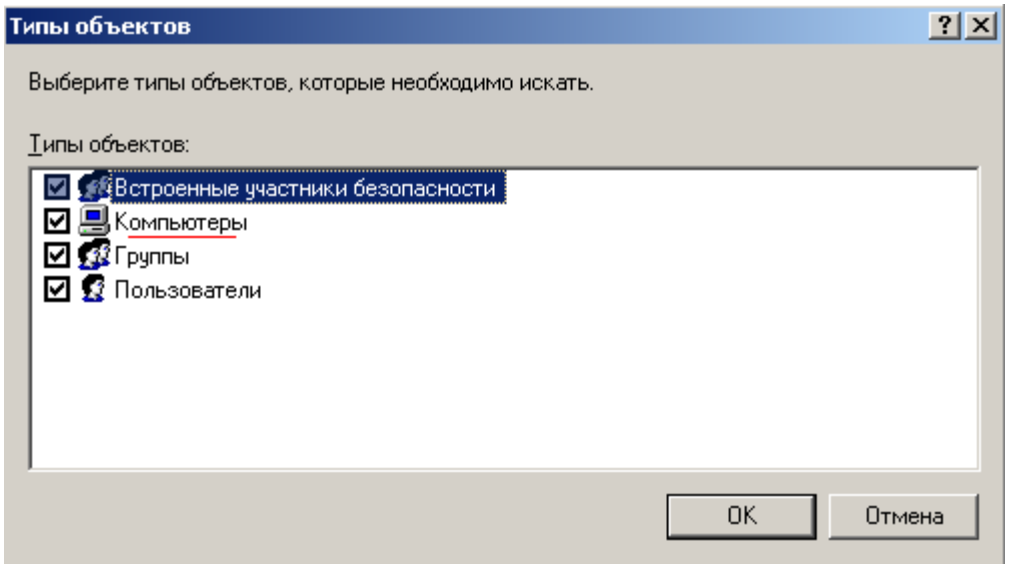


Рис. 8. Активируем флажок Компьютеры

Теперь кнопкой **Поиск** можно найти компьютеры из AD и задать для них сконфигурированную нами групповую политику (рис. 9).

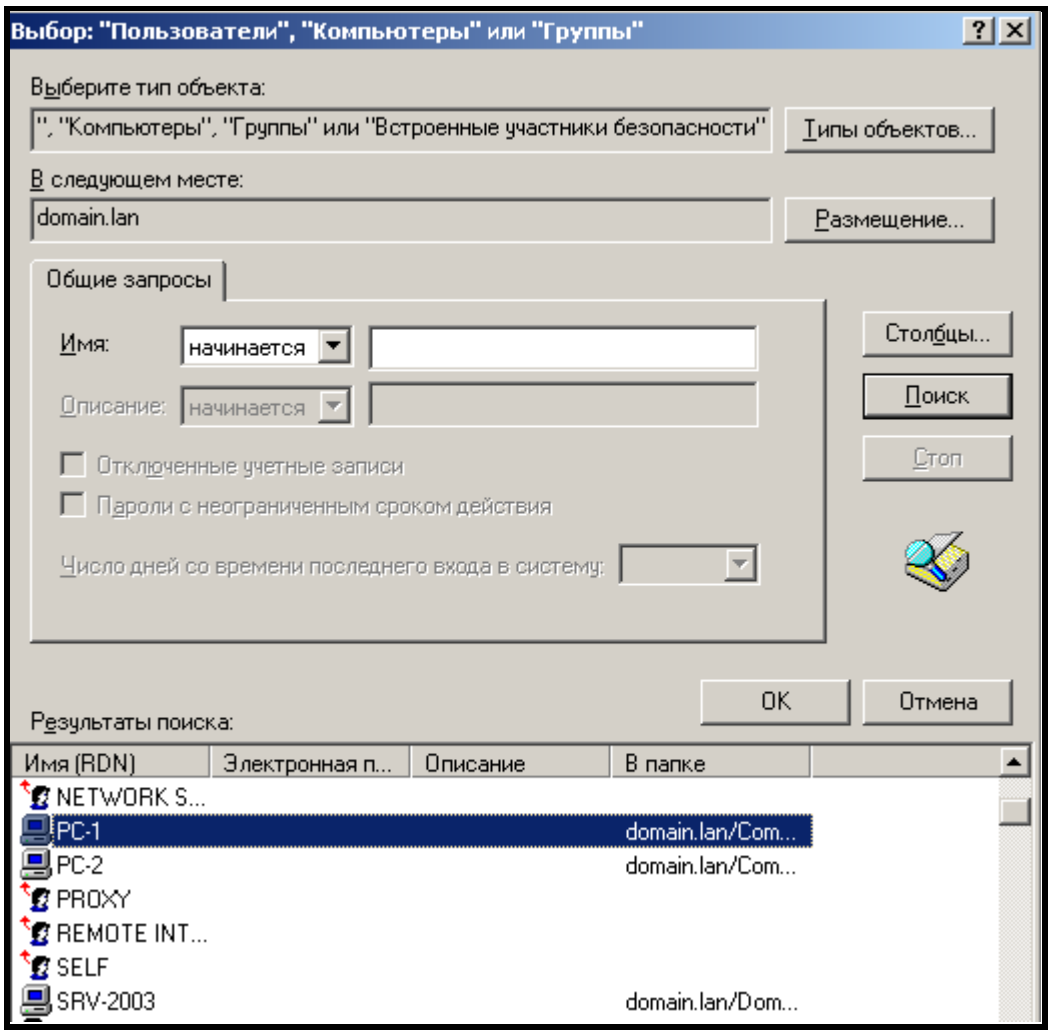


Рис. 9. Находим PC-1

Нажимаем OK и устанавливаем флажок (рис. 10).

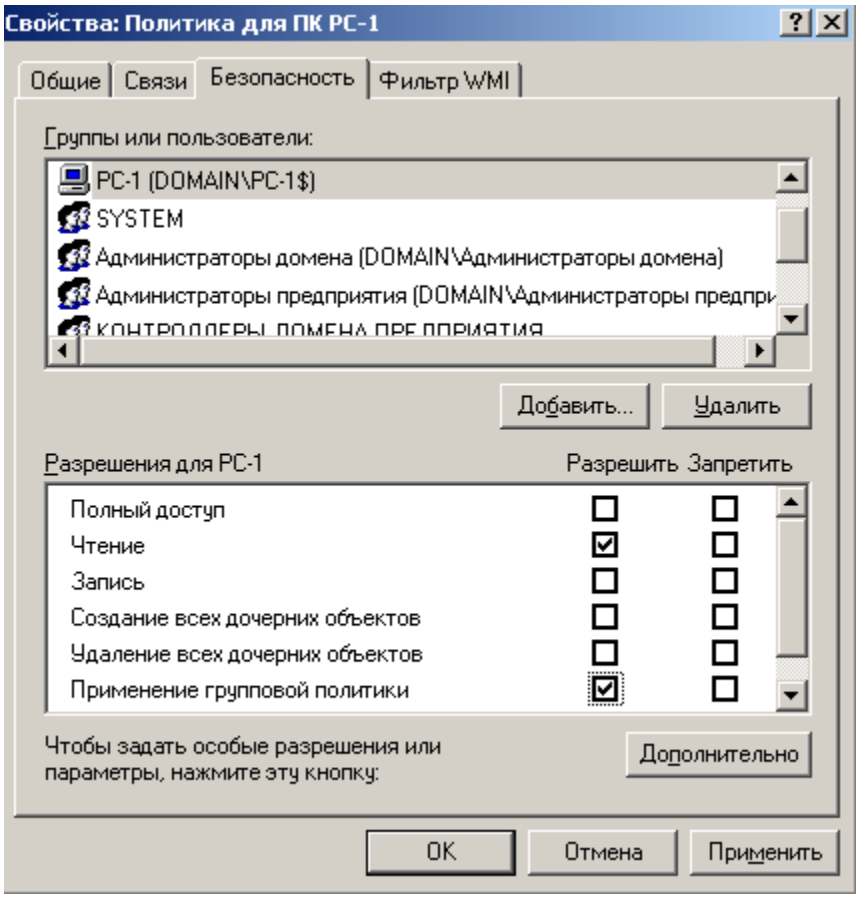


Рис. 10. Активируем для PC-1 флажок Применение групповой политики

Перезагрузите ПК и проверьте результат наших настроек групповой политики самостоятельно.

Итоги. В этой работе мы сделали изменение групповой политики (ГП) для одного (конкретного) пользователя, а также создали групповую политику для группы пользователей. Также научились производить конфигурирование групповых политик для отдельных компьютеров.

ПРАКТИЧЕСКАЯ РАБОТА №25.
ОСНОВЫ РАБОТЫ С VIRTUAL PC 2007. УСТАНОВКА WINDOWS SERVER 2008 НА ВИРТУАЛЬНУЮ МАШИНУ

Цель работы:

Научиться устанавливать Windows Server 2008 на виртуальную машину

Используемое программное обеспечение

Для выполнения данной лабораторной работы понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1, а также дистрибутив операционной системы Windows Server 2008 на DVD-диске или в виде образа DVD-диска (файл с расширением .iso).

В ходе лабораторной работы установим на виртуальную машину операционную систему Windows Server 2008. Работу виртуальной машины упрощенно

иллюстрирует рисунок 1.1. На компьютере устанавливается базовая операционная система, после чего устанавливается программное обеспечение виртуальной машины (ВМ). Оно позволяет установить одну или несколько гостевых операционных систем и запускать в них программы, разработанные для данных ОС. В качестве ПО виртуализации в наших лабораторных работах будет использоваться Microsoft Virtual PC 2007 SP1.

Рис.1. Схема работы виртуальных машин.

Создание виртуальной машины

Из меню Пуск (Программы -> Microsoft Virtual PC) запустим консоль управления виртуальными машинами (рис 1.2). Нажав кнопку **New…**, приступим к созданию новой машины. При создании новой машины надо будет описать расположение ее файлов (файла «машины» с расширением .vmc и файла виртуального жесткого диска с расширением .vhd). Поэтому в запустившемся после нажатия кнопки мастере указываем:- создание новой машины (Create a virtual machine);- имя и расположение файла (если специально не указывается, для выполнения этой лабораторной в классе используем имя S08, и путь D:\VirtPC_доп_лаб\S08; при самостоятельном выполнении работы можно использовать произвольные пути и имена);- тип устанавливаемой операционной системы. Если это ОС разработки Microsoft, будут автоматически выставлены рекомендуемый объем оперативной памяти и виртуального жесткого диска. Поэтому в окне выбора ОС вместо значения по умолчанию ―Other‖ выберите из выпадающего списка Windows Server 2008;- в следующих окнах мастера согласимся с предлагаемым объемом выделяемой машине оперативной памяти (512 MB); укажем, что надо создать новый виртуальный жесткий диск (A new virtual hard drive), проверим путь D:\VirtPC_доп_лаб\S08, поменяем предлагаемое название файла диска ―S08 Hard Disk.vhd‖ на более короткое ―S08.vhd‖ и уменьшим предлагаемый размер с 65 Гб до 40Гб. Размер и имя можно оставить и по умолчанию, изменение настроек предлагается «чтобы потренироваться». Тут надо отметить, что при использовании данного мастера файл виртуального диска создается

минимального размера и увеличивается по мере надобности, т.е. сразу 40 Гб не потребуется.

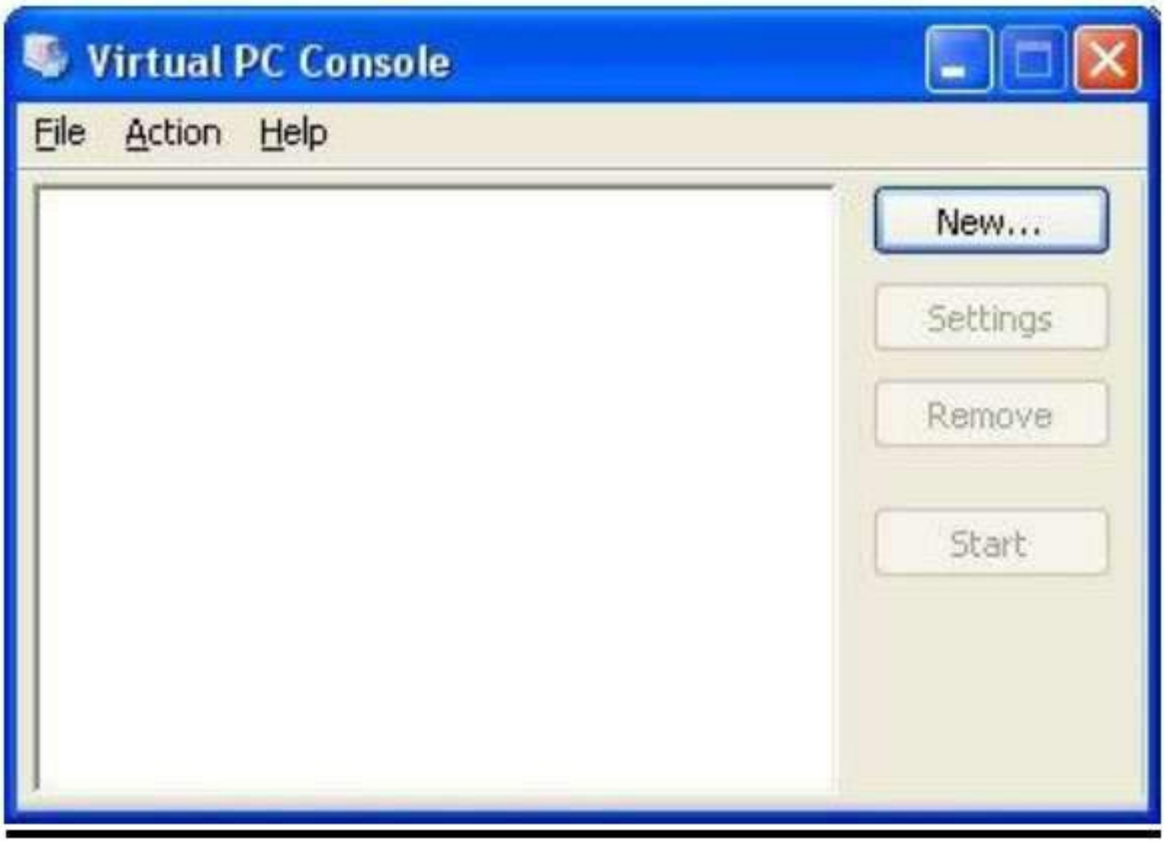


Рис.2. Консоль управления виртуальной машиной.

После сделанных настроек в окне консоли (рис.1) появится новая виртуальная машина, которую можно запустить, выделив ее и нажав кнопку Start. При этом может появиться сообщение об ошибке «The virtual machine could not be started because there was not enough memory available on the host» - виртуальная машина не может быть запущена, потому что недостаточно памяти. Это произойдет, например, если на компьютере установлено меньше 1 Гб оперативной памяти или в момент запуска виртуальной машины запущено много других программ. В последнем случае, проблема может быть решена завершением работы временно ненужных запущенных программ. Если же мало физической памяти, то через настройки виртуальной машины (кнопка Settings в консоли) можно попробовать несколько уменьшить размер памяти, выделяемой виртуальной машине. Но надо помнить, что минимально рекомендуемый объем памяти для Windows Server 2008 – это 512 МБ и сильно урезать его без потери работоспособности ОС не получится. Среди прочих настроек виртуальной машины хотелось бы отметить параметры сети (рис. 3). Выбрав раздел «Networking», можно указать число адаптеров виртуальной машины, а также параметры для каждого адаптера. В частности, можно указать, какой сетевой адаптер физического компьютера будет задействоваться виртуальной машиной. Для локальных соединений (в рамках одного компьютера) можно выбрать тип Local only. А для первого сетевого адаптера также можно указать тип Shared networking. В этом случае используется механизм трансляции сетевых адресов NAT, виртуальный сетевой адаптер получает адрес из

зарезервированного диапазона 192.168.x.y и может «обращаться» к внешним узлам, используя базовую ОС, как NAT устройство. Этот вариант позволит, например, получить из виртуальной машины доступ в Интернет, если на «физической» машине используется dial-up соединение. Пока остановимся на конфигурации с одним сетевым адаптером и типом соединения Shared networking.

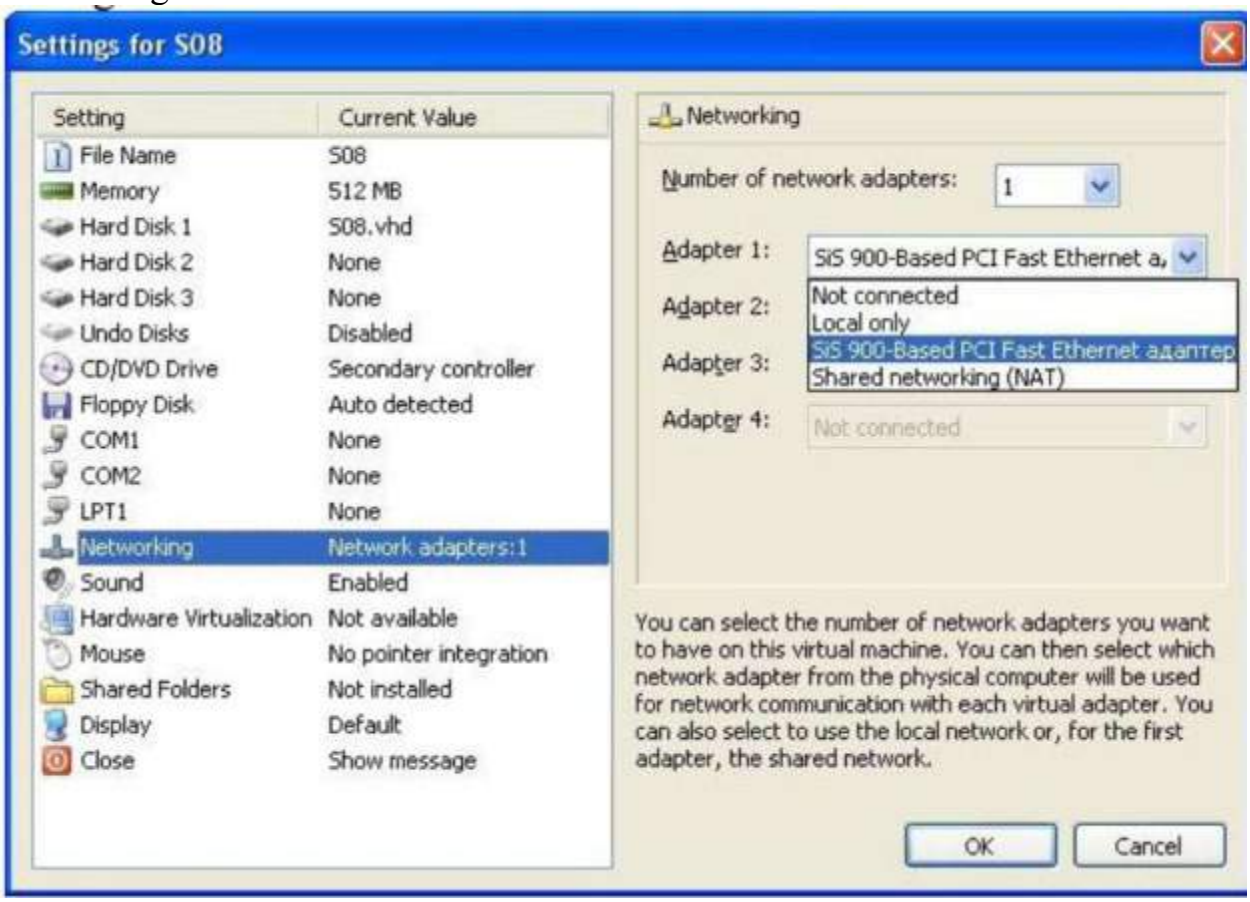


Рис. 3. Настройка сетевых адаптеров виртуальной машины.

Установка Windows Server 2008

Следующая задача – установить операционную систему на виртуальную машину. Если Ваш дистрибутив Windows Server 2008 находится на DVD диске, то установите его в привод и запустите подготовленную виртуальную машину кнопкой **Start** на консоли виртуальных машин. После сообщения с просьбой нажать любую клавишу для подтверждения загрузки с CDROM начнется установка. В случае, когда используется файл *.iso с образом дистрибутивного диска, последовательность действий будет несколько отличаться. Запустите виртуальную машину и в меню CD выберите пункт «Capture ISO image» (подключить образ диска), после чего укажите расположение файла с образом диска и при необходимости перезапустите машину (меню Action, пункт Reset). Итак, установка началась. Для имеющих опыт установки операционных систем Microsoft, процесс установки Windows Server 2008 особых сложностей представлять, скорее всего, не будет. Первое окно мастера установки позволяет выбрать язык, региональные настройки и раскладку клавиатуры. Дальше, в зависимости от версии дистрибутива, будет предложено ввести серийный

номер (который, в частности, и укажет какую версию Windows Server 2008 надо устанавливать) или сразу будет показано окно выбора устанавливаемой операционной системы. Дело в том, что с одного и того же дистрибутивного диска может быть установлен Windows Server 2008 в версиях Standard, Enterprise или Datacenter. Каждая из трех версий может быть установлена в режиме полной установки (Full) или установки основных компонентов (Server Core). Режим Server Core – одно из новшеств, появившихся в операционной системе Windows Server 2008. Он позволяет путем отказа от установки средств графического администрирования и ряда модулей операционной системы получить «специализированную» конфигурацию сервера для выполнения ряда функций (файловый сервер, контроллер домена и т.д.), более защищенную и требующую меньшего внимания администратора. Для наших лабораторных работ устанавливаем версию Enterprise (Full installation) и отмечаем галочкой «I have selected the edition of Windows that I purchased» (Выбрана приобретенная версия Windows). Далее интерес представляет окно выбора раздела для установки. В нем будет отображаться диск виртуальной машины (если помните, мы его задавали размером 40 Гб). Если нажать на ссылку Drive options (Advanced) появятся дополнительные команды, позволяющие в частности, разбить диск на разделы. Нужно отметить, что Windows Server 2008 можно установить только в раздел отформатированный в NTFS. Создайте два логических диска размером 30 Гб (на который будет устанавливаться операционная система) и 10 Гб. В процессе установки операционная система несколько раз перезагрузится. В самом конце будет выдан запрос на установку пароля администратора. Чтобы в дальнейшем было удобнее работать, предлагается на всех устанавливаемых в классе виртуальных машинах назначить пароль **Serv08Saiu** (по-английски, с соблюдением указанной очередности больших и малых букв). Для первого входа пользователя понадобится знание следующих команд.

Команды виртуальной машины

Вместо сочетания клавиш «Alt+Ctrl+Del» надо нажимать «правый Alt+Del».

«Правый Alt+Enter» – переключение между обычным и полноэкранным режимом. Захваченный виртуальной машиной указатель мыши освобождается нажатием на правую клавишу Alt и выводом курсора из окна виртуальной машины. После установки расширений (см. ниже) эти действия больше не понадобятся, и указатель мыши будет свободно перемещаться между окном виртуальной машины и остальной областью экрана.

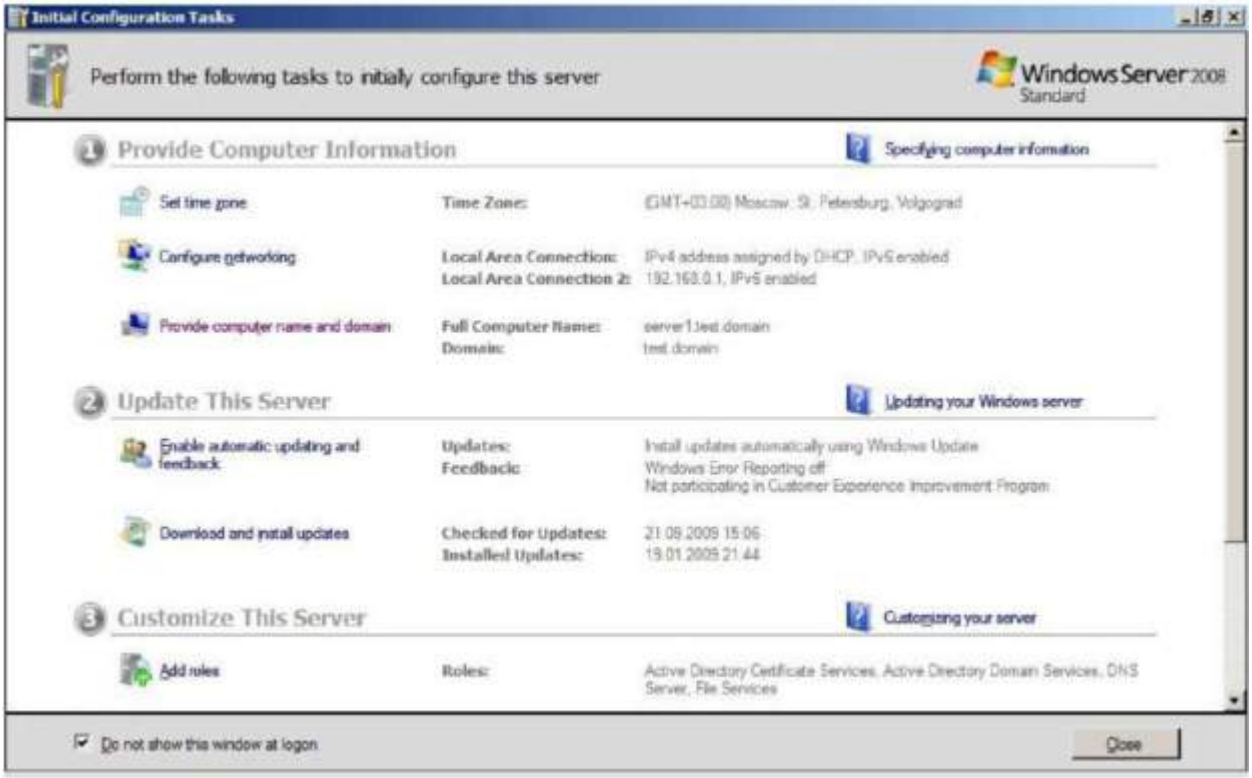


Рис 4. Окно Initial Configuration Tasks.

После первого входа в систему пользователь увидит окно начальной настройки системы Initial Configuration Tasks. Выглядит оно примерно так, как представлено на рис. 1.4. В нем в секции 1 (Provide Computer Information) проверьте, правильно ли выставлен часовой пояс: для нас это (GMT+03:00) Москва, Санкт-Петербург, Волгоград. Кроме того, в разделе Provide computer name and domain вы увидите автоматически сгенерированное имя компьютера и рабочую группу Workgroup. Рабочую группу пока оставим как есть, а имя изменим на **S08**. Итак, мы подготовили виртуальную машину с Windows Server 2008, которую назвали **S08**, и назначили учетной записи **Administrator** пароль **Serv08Saiu**. Последнее задание данной лабораторной – установить на наш сервер расширения, которые добавят некоторые удобства в работе с виртуальной машиной. В частности, это передача данных между базовой ОС и гостевыми через буфер обмена, возможность подключения папки на диске «физической» машины в качестве сетевого диска виртуальной машины, возможность свободного перехода указателя из области окна виртуальной машины в область рабочего стола базовой ОС и т.д. В меню Action окна виртуальной машины выберите пункт Install or Update Virtual Machine Additions (установите или обновите расширения виртуальной машины). Если виртуальная машина загружена и пользователь совершил вход, то в CDROM виртуальной машины будет автоматически подключен «псевдообраз» диска с инсталляционным пакетом расширений. Останется только согласиться с автоматическим запуском программы setup и дождаться окончания установки.

ПРАКТИЧЕСКАЯ РАБОТА № 26.
УПРАВЛЕНИЕ ЗАГРУЗКОЙ WINDOWS SERVER 2008. ДОБАВЛЕНИЕ РОЛЕЙ. УСТАНОВКА ПЕРВОГО КОНТРОЛЛЕРА ДОМЕНА.

Цель работы:
Научиться управлять загрузкой Windows Server 2008, выполнять добавление ролей, устанавливать контроллер домена.

Используемое программное обеспечение
Для выполнения данной лабораторной работы понадобится установленный на виртуальную машину Windows Server 2008.

Параметры загрузки. Утилита bcdedit. Утилита System Configuration
Начнем выполнение работы со знакомства с новыми инструментами управления загрузкой операционной системы. В Windows Server 2003 (также как и в предыдущих версиях клиентских и серверных операционных систем семейства Windows NT) использовался загрузчик NT loader, который считывал настройки из файла boot.ini. Вот пример такого файла:
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems] multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional RU" /noexecute=optin /fastdetect
Изменять файл (и параметры загрузки) можно было прямо в текстовом редакторе. В Windows Vista и Windows Server 2008 используется новый диспетчер загрузки Windows Boot Manager. Параметры загрузки теперь хранятся в бинарном файле конфигурации (Boot Configuration Data – BCD) расположенном в скрытой системной папке с именем \boot на диске, с которого загружается операционная система. Для работы с BCD используется утилита командной строки bcdedit. Некоторые параметры доступны из графической утилиты конфигурирования System Configuration и окна System в панели Управления. Начнем с рассмотрения графических утилит.
Отройте Панель управления (*Start-> Control Panel*), при необходимости переключитесь к классическому виду (*Classic View*) и откройте окно *System*. В нем перейдите по ссылке *Advanced System Setting* и в разделе *Startup and Recovery* нажмите кнопку *Settings*. В появившемся окне (рис.1) можно увидеть список загружаемых операционных систем, выбрать операционную систему, загружаемую по умолчанию, установить интервал ожидания выбора пользователем системы для загрузки. Следующая утилита – это *System Configuration* (запускается из раздела *Administrative Tools* главного меню). На вкладке boot (рис.2.) можно увидеть и изменить дополнительные параметры, например, указать что в определенном варианте загрузки надо вести протокол загрузки (флажок Boot log). Кнопка Advanced options позволяет ограничить число процессоров, используемых ОС, объем оперативной памяти и установить

некоторые параметры, необходимые для отладки.

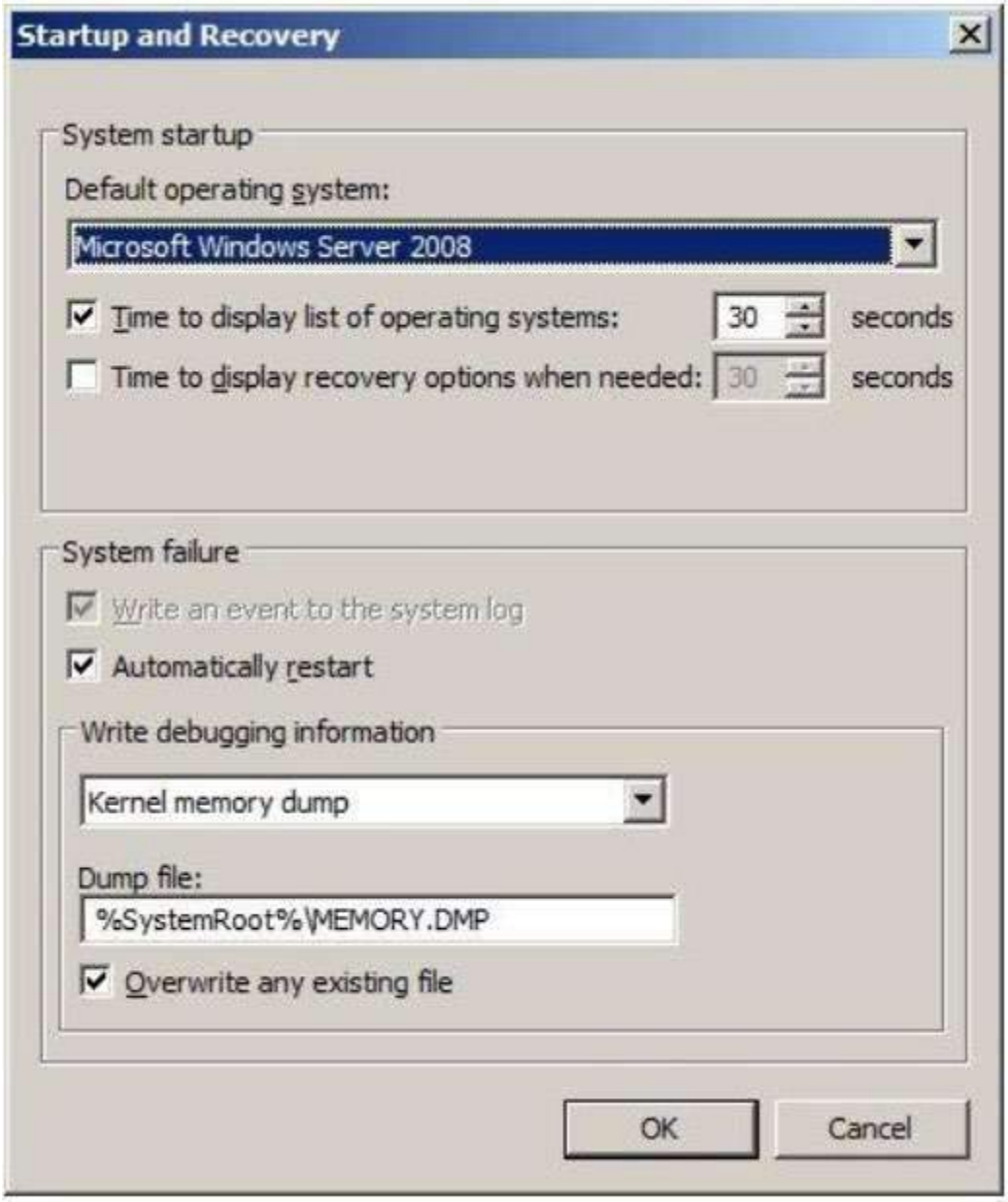


Рис.1. Окно Startup and Recovery.

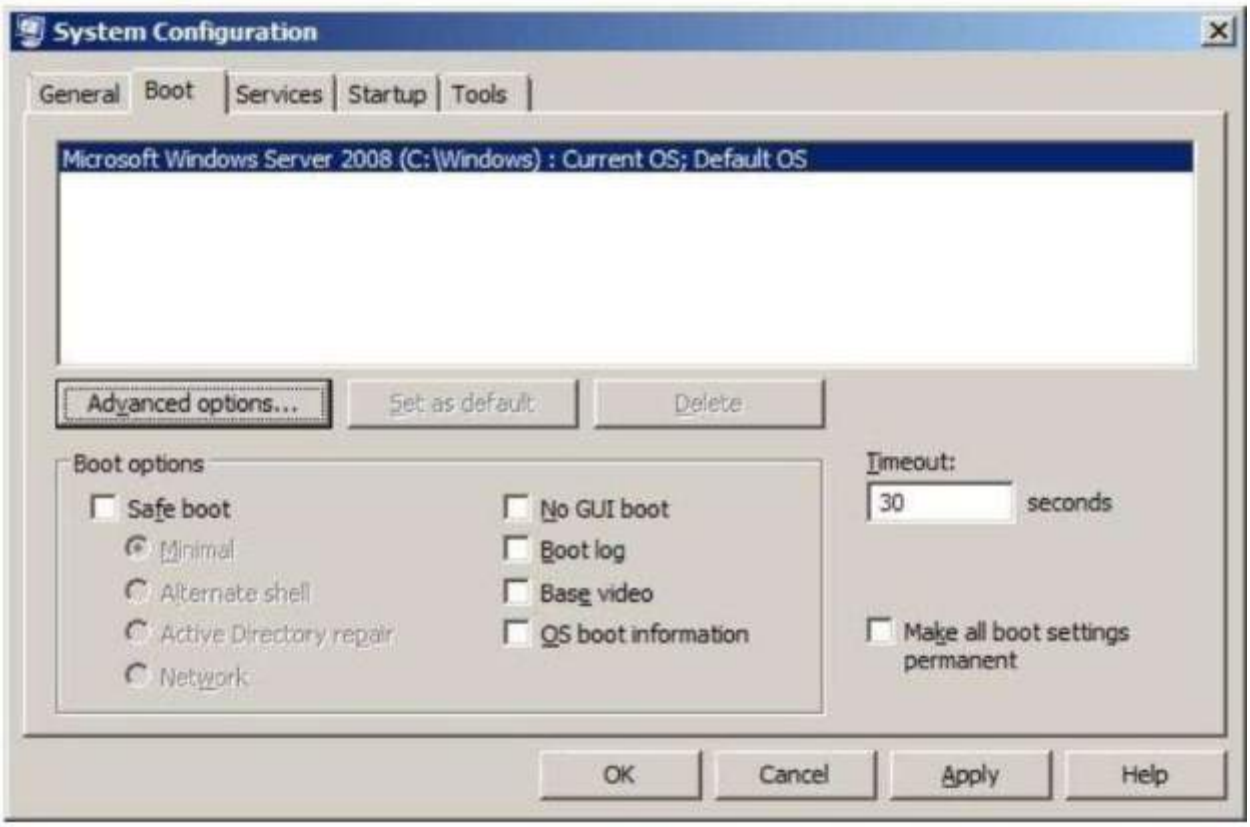


Рис.2 Вкладка Boot окна утилиты System Configuration.

Но создавать новые варианты загрузки можно только с помощью утилиты командной строки bcdedit. Запустим ее (Start->Command Prompt -> bcdedit.exe). При запуске без ключей будет выведена информация о текущей конфигурации, например, следующего вида:

Windows Boot Manager
---
identifier {bootmgr}
device partition=C:
description Windows Boot Manager
locale en-US
inherit {globalsettings}
default {current}
displayorder {current}
toolsdisplayorder {memdiag}
timeout 30

Windows Boot Loader
---
identifier {current}
device partition=C:

path	\Windows\system32\winload.exe
description Microsoft Windows Server 2008	

locale	en-US
inherit {bootloadersettings} osdevice partition=C:	
systemroot	\Windows
resumeobject {51c6bea1-e439-11dd-bb9b-ed314082ca2a}	
nx	OptOut

Здесь видно, что в файле содержатся две записи – одна для самого диспетчера загрузки (Windows Boot Manager), другая – для операционной системы Windows Server 2008. Запуск bcdedit.exe /? позволит получить краткую справку по ключам команды. Вот некоторые из них:

/enum	Отображает список всех имеющихся в BCD файле записей. Запуск утилиты без ключей эквивалентен запуску "bcdedit /enum ACTIVE"
/v	Отображает идентификаторы записей в полном виде, вместо использования «хорошо известных» идентификаторов. Например, вместо идентификатора{current} будет что-нибудь вида {51c6bea0-e439-11dd-bb9b-ed314082ca2a}
/copy	Копирует запись
/create	Создает новую запись
/delete	Удаляет запись
/export	Экспортирует содержимое файла BCD в указанный файл
/import	Восстанавливает содержимое BCD из указанного файла
/set	Устанавливает

	значения параметра для записи

Теперь сделаем следующее.
1. Создадим копию файла BCD в файл bccopy в корне диска C:
bcdedit.exe /export "C:\bccopy"
Убедимся, что в отличие от boot.ini при открытии файла в текстовом редакторе осмысленного текста мы не увидим.
2. Добавим к файлу копию записи с идентификатором {current}и назовем ее test08 bcdedit.exe /copy {current} /d "test08"
Убедимся, что новая запись появилась.
3. Чтобы было быстрее, из утилиты System Configuration для созданного варианта загрузки укажем, что нужно выполнить загрузку в безопасном режиме (Safe boot, переключатель minimal). Перезагрузимся, протестируем работу настройки.
4. Командой bcdedit.exe /import "C:\bccopy"
вернем файл BCD в начальное состояние.

Роли и компоненты

Сейчас у нас имеется установленная операционная система Windows Server 2008, но для того, чтобы использовать ее для выполнения некоторой серверной функции надо установить роль (role). Роль включает одну или несколько служб (role services), необходимых для выполнения определенной функции. Например, File Services (файловые службы) или Web-server (IIS). Когда роль объединяет несколько служб, то могут устанавливаться или все сразу, или отдельные службы. Дополнительная функциональность может быть получена путем установки программных модулей, называемых компонентами (feature). Пример компоненты – это SMTP Server. Роли и компоненты могут быть как независимыми, так и взаимосвязанными. Добавить или удалить роли и компоненты можно с помощью оснастки Server Manager (Start -> Administrative tools ->Server Manager). Окно оснастки представлено на рис.3. Если выделить узел Roles, то увидим список установленных ролей. Добавлять или удалять роли можно, перейдя по ссылкам Add Roles или Remove Roles соответственно. Добавьте роль File Services (не устанавливая дополнительных служб, таких как DFS и т.д.). Теперь наш сервер сможет выполнять роль файлового сервера. Работе с файловыми ресурсами будет посвящена отдельная лабораторная работа. Сейчас же стоит отметить только, то что в данном случае никакого

дополнительного конфигурирования после установки роли не потребовалось.

Рис.3. Окно административной оснастки Server Manager.

Задача лабораторной работы – сделать наш сервер контроллером домена Windows. Для этого понадобится установить роль Active Directory Domain Services и выполнить настройку параметров домена. Домен Windows логически объединяет несколько компьютеров для того, чтобы можно было их централизованно администрировать. Примером административной задачи может быть создание такой учетной записи, чтобы пользователь мог входить под ней на любой компьютер своего подразделения организации. В этом случае, чтобы такую запись завести только один раз (а не на каждом компьютере), нужно вести единую базу данных с информацией о пользователях и компьютерах. Подобная база называется каталогом, а разработанная Microsoft служба каталога – Active Directory. Серверы, на которых работает служба и которые, в частности, выполняют проверку пользователей с доменными

учетными записями, называются контроллерами домена.

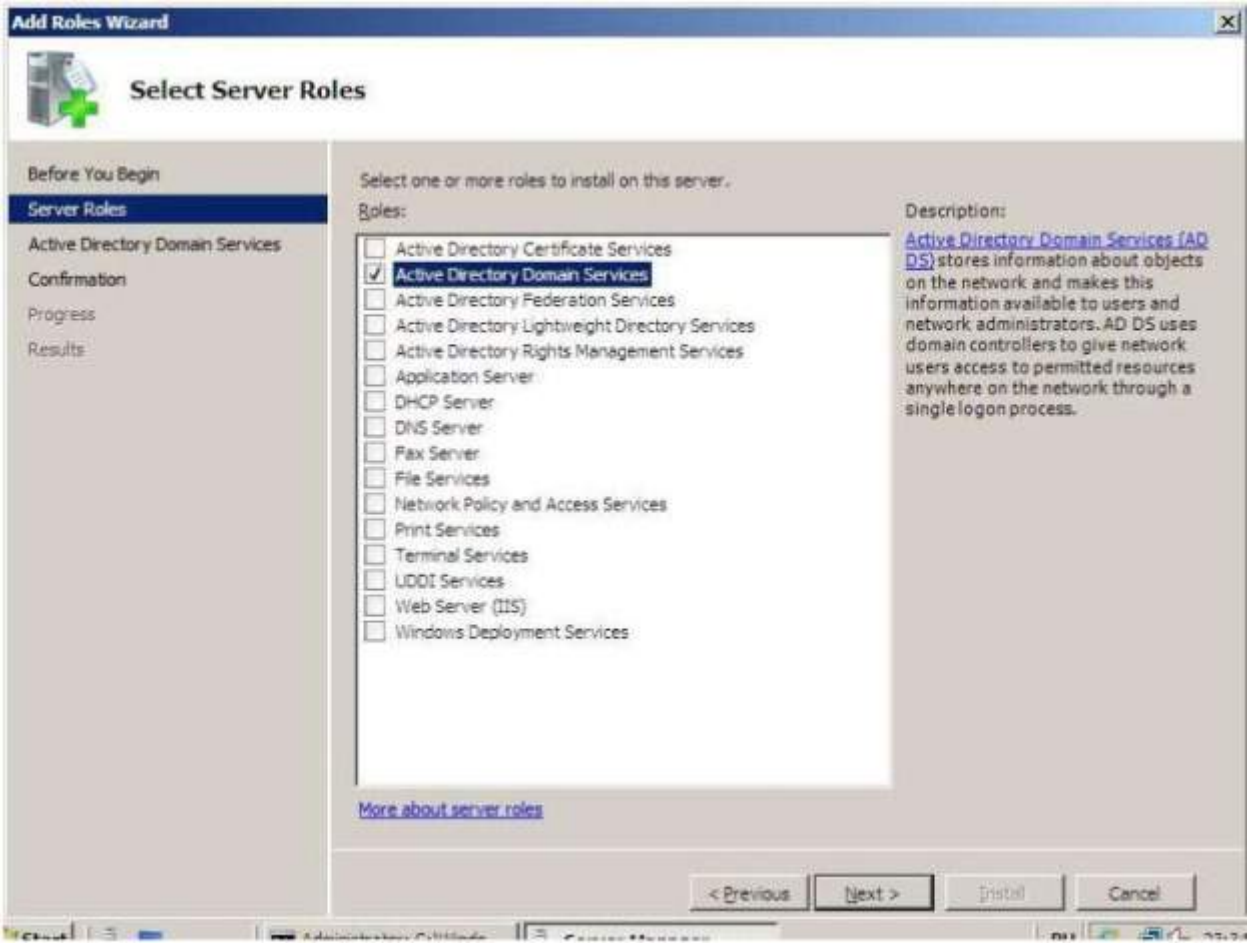


Рис. 4. Добавление роли Active Directory Domain Services.

Из оснастки Server Manager добавляем роль Active Directory Domain Services (рис.4). Когда роль добавлена, потребуется произвести начальное конфигурирование нового контроллера. Делается это запуском утилиты dcpromo из основного меню (Start- >Run…-> dcpromo) или по ссылке, которая появится в окне Server Manager после установки роли.

Рис.5. Создание нового домена в новом лесе.

Для понимания дальнейшего надо ввести несколько понятий. Как мы уже разобрались, информация об объектах сети хранится в каталоге. Для этого сначала создаются определения объектов, которые помещаются в служебную структуру, называемую схема каталога. Если хотим создать объект нового типа, нужно сначала поместить в схему его определение. Совокупность доменов, использующих единую схему каталога и общую конфигурацию, называют лесом доменов (forest). В окне мастера, представленном на рисунке 5, мы указываем, что создаем новый лес, т.е. мы конфигурируем первый контроллер первого (корневого) домена в нашей организации. В следующем окне мастера (рис.6) запрашивается имя домена. Обычно имена соотносятся с доменными именами Интернет (например, ftk.spbstu.ru), но для наших лабораторных будем использовать имя **SAIU_Test**.

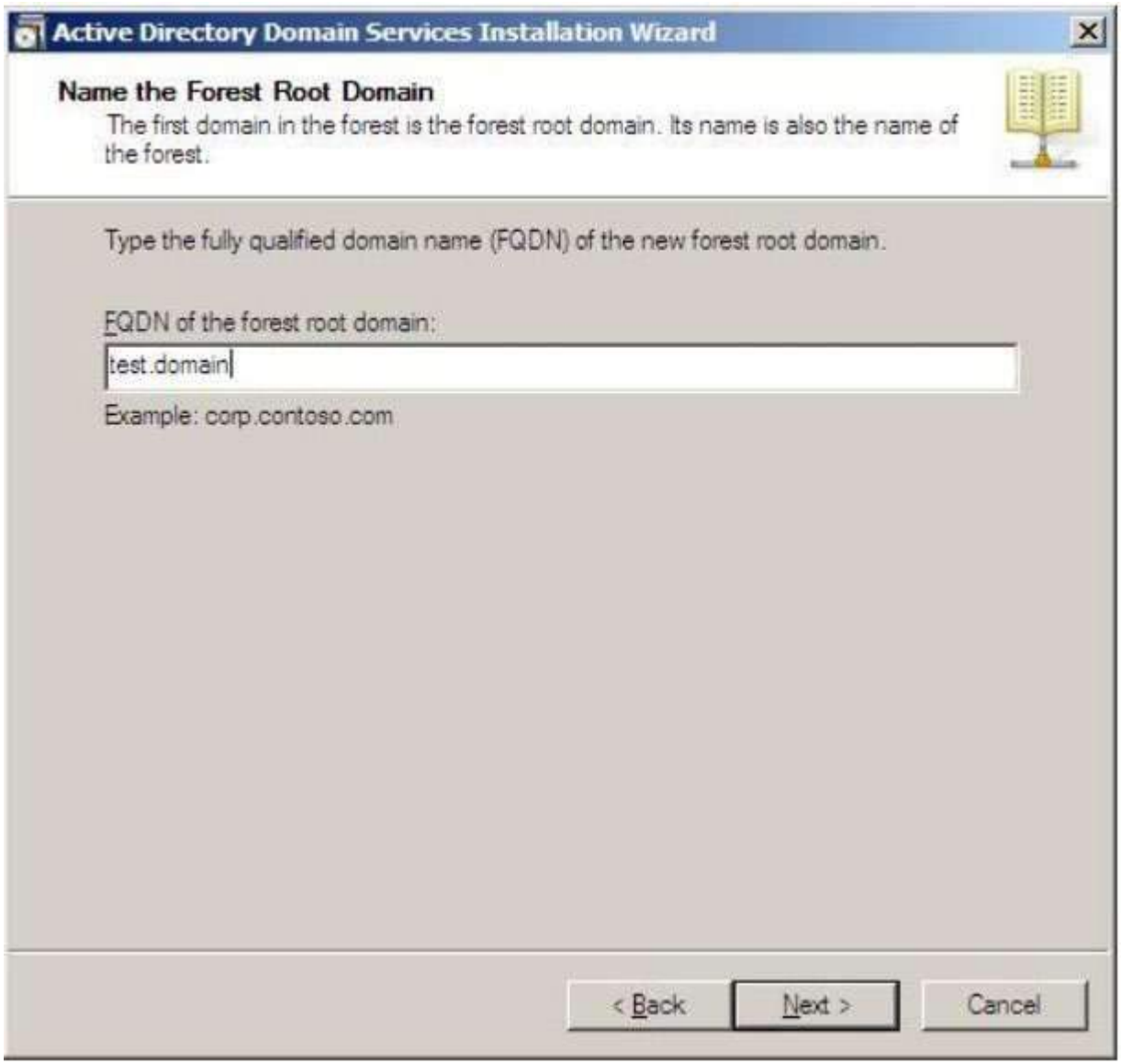


Рис.6. Вводим имя домена.

Далее, так как в нашей виртуальной сети пока нет DNS сервера, мастер предложит установить DNS сервер (рис.2.7). Служба DNS используется для разрешения доменных имен компьютеров в ip-адреса (например, имени www.ftk.spbstu.ru сопоставляется адрес 195.19.212.13). В домене Windows клиентские компьютеры с помощью DNS получают информацию о контроллерах домена (более подробно об этом в следующих лабораторных), поэтому хотя бы один DNS сервер необходим.

Рис. 7. Установка DNS сервера.

Следующее окно позволяет выбрать функциональный уровень домена. Если выбрать уровень Windows Server 2008, то мы получим поддержку всех новых функций, но в роли контроллеров домена смогут выступать только компьютеры с Windows Server 2008 (и, наверное, более новых ОС после их появления). Наоборот, выбор уровня Windows 2000 позволит использовать контроллеры с более старыми версиями серверных ОС (Windows 2000 Server, Windows Server 2003), но не даст использовать некоторые возможности, имеющиеся только в Windows Server 2008. Для лабораторных выберем уровень Windows Server 2008.

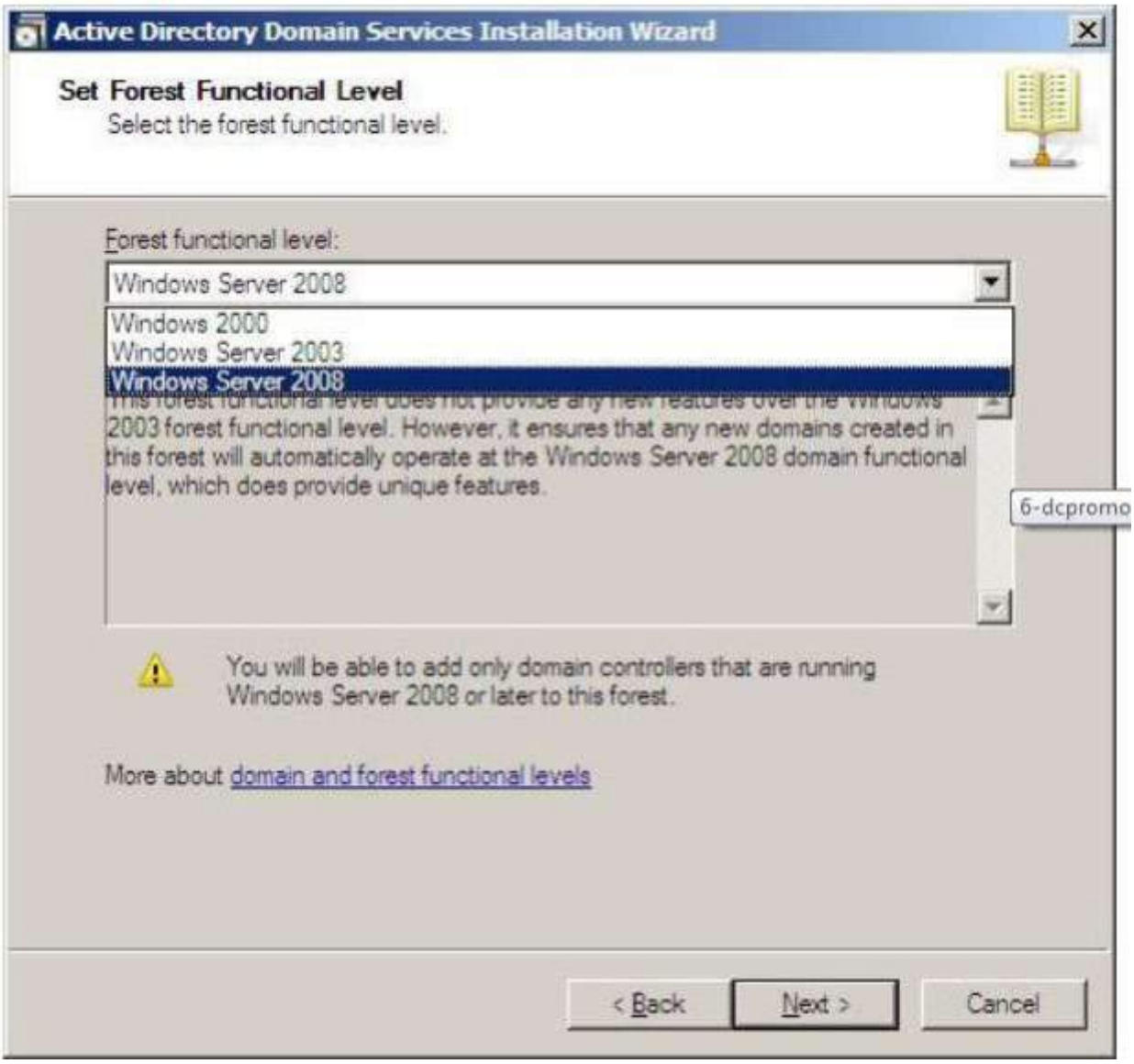


Рис. 8. Выбор функционального уровня домена.

Следующее окно мастера позволяет выбрать расположение базы каталога, файлов журнала и служебного каталога SYSVOL (в нем, в частности, хранятся политики и скрипты, запускающиеся при входе пользователя в домен). Можно согласиться с настройками по умолчанию. В конце надо будет задать пароль для доменной учетной записи **Administrator** (пусть это снова будет **Serv08Saiu**) и перезагрузить нашу виртуальную машину. После перезагрузки зайдите под учетной записью **Administrator**. Последнее задание – создание нового пользователя. Для этого надо запустить административную оснастку Active Directory Users and Computers (Start-> Administrative Tools-> Active Directory Users and Computers) или можно получить к ней доступ из окна Server Manager, как показано на рис.9. Раскройте узел, соответствующий нашему домену, перейдите на контейнер Users и вы увидите список созданных автоматически стандартных групп и учетных записей. В контекстном меню выберите создание нового пользователя (New->User) пусть имя учетной записи будет **Labos**, пароль **Lab0s123** (имя и фамилию пользователя придумайте

сами). Укажите, что пользователю не надо менять пароль при первом входе. Когда учетная запись создана, попробуйте войти под ней на сервер. Должно появиться сообщение, что действующая политика не позволяет это сделать. Дело в том, что настройки по умолчанию не позволяют обычным пользователям локально входить на контроллер домена. Созданная учетная запись нам понадобится на следующей лабораторной работе, когда мы добавим в домен рабочую станцию.

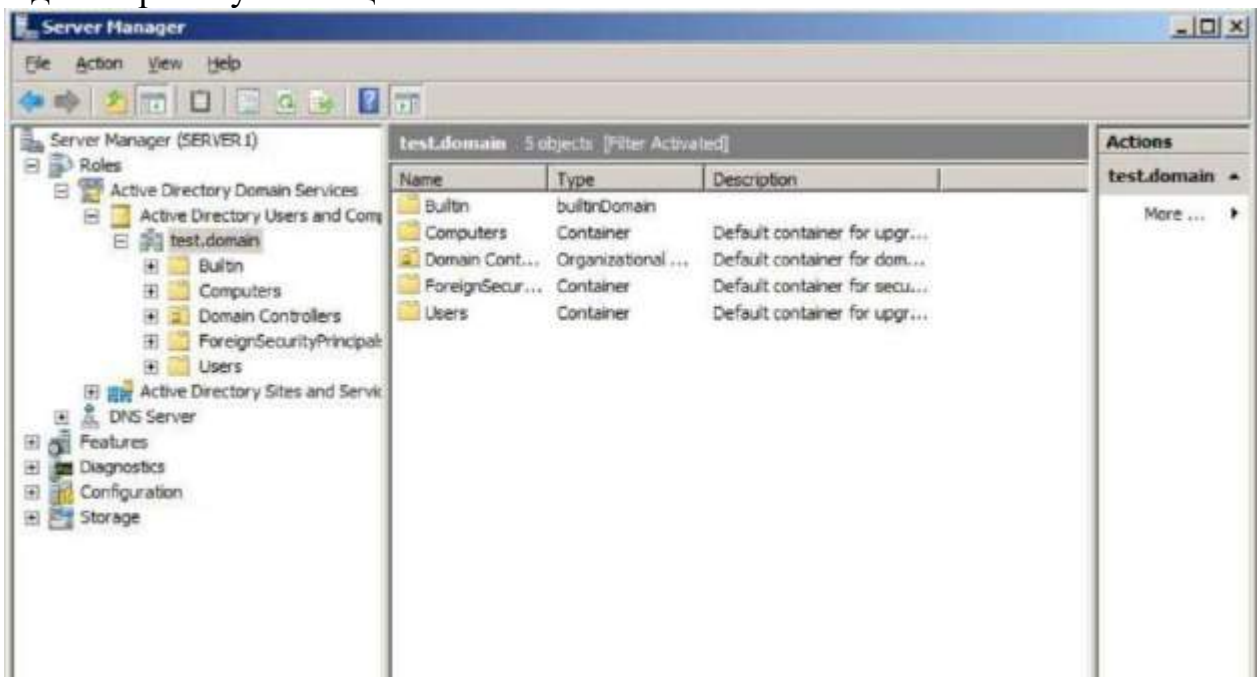


Рис.9. Управление доменными учетными записями.

ПРАКТИЧЕСКАЯ РАБОТА № 27.

ОСНОВЫ АДМИНИСТРИРОВАНИЯ ДОМЕНА WINDOWS: ДОБАВЛЕНИЕ КОМПЬЮТЕРА В ДОМЕН, РАБОТА С УЧЕТНЫМИ ЗАПИСЯМИ И ГРУППАМИ

Цель работы:
Научиться выполнять администрирование домена, добавлять компьютер в домен, выполнять работы с учетными записями и группами.

Используемое программное обеспечение
Для выполнения данной лабораторной работы понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1 и 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista. В ходе работы виртуальная машина с Windows Vista будет добавлена в домен, доменным контроллером которого выступает Windows Server 2008.
Настройка параметров сети для виртуальных машин

Для выполнения работы нам понадобится настроить параметры сетевых подключений виртуальной рабочей станции и сервера. В случае если компьютер, на котором выполняется лабораторная работа, не позволяет одновременно запустить две виртуальные машины (сервер и рабочую станцию), то для выполнения лабораторной понадобятся два компьютера, подключенные к сети. Эту конфигурацию и рассмотрим. Сначала, до запуска виртуальных машин, сделаем настройки, указывающие, что виртуальная машина будет использовать физический сетевой адаптер. В консоли управления Virtual PC 2007 в свойствах виртуальной машины найдем пункт Networking и выберем для использования один из сетевых адаптеров нашего компьютера (рис.1).

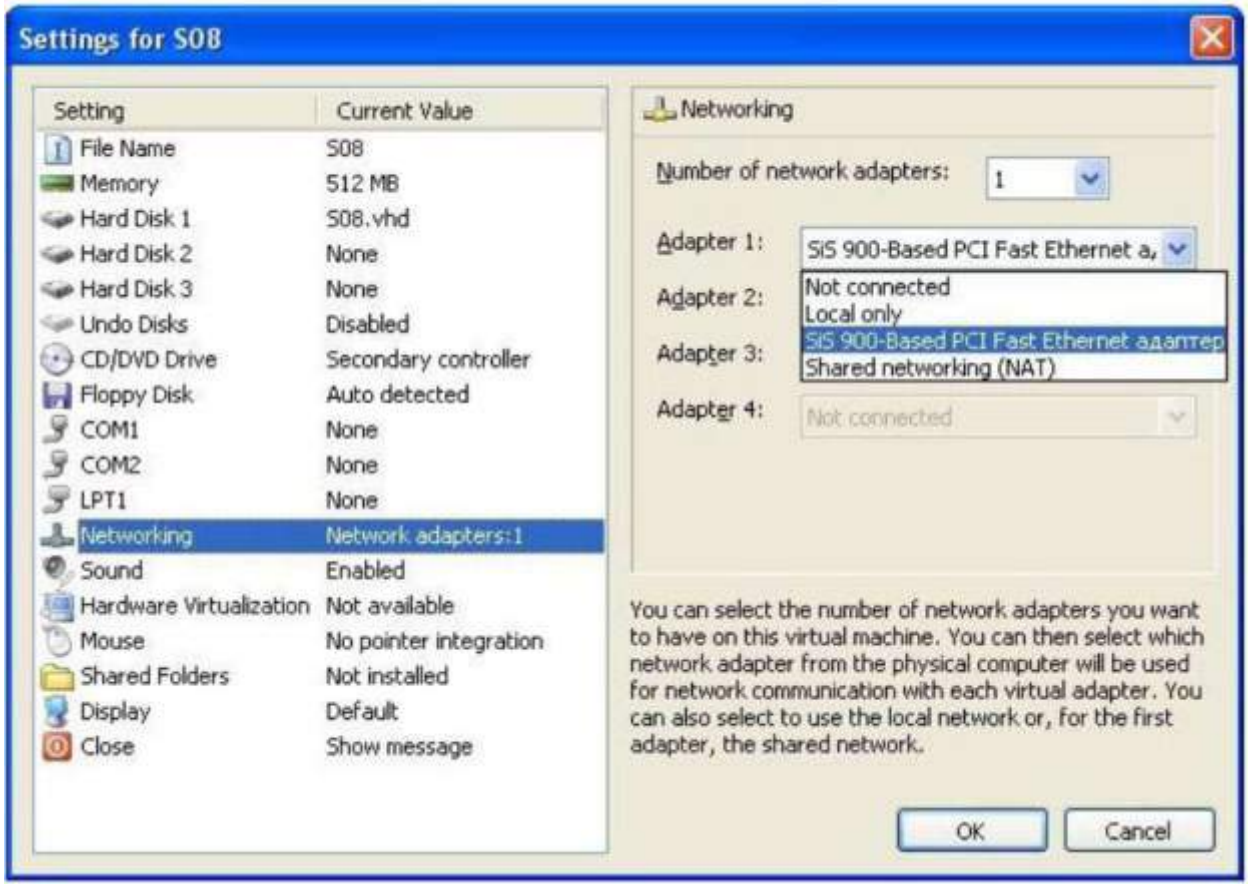


Рис.1. Выбор «физического» сетевого адаптера в свойствах виртуальной машины.

После этого разделимся на пары, на одном компьютере каждой пары запускается виртуальная машина с Windows Server 2008, сконфигурированном для работы в качестве контроллера домена (у нас он назвался S08). На другом компьютере запускаем виртуальную машину с Windows Vista (в нашем классе машина называется Vista_dop). Входим с правами администратора. Для S08 это учетная запись **Administrator** с паролем **Serv08Saiu**. Для Vista_dop учетная запись **Adm** с паролем **123qwe**. На виртуальных машинах настроим протокол TCP/IP v4 таким образом, чтобы сервер смог взаимодействовать с рабочей станцией, не мешая проведению лабораторных другими парами. Для этого, откроем параметры сетевого подключения на рабочей станции и сервере.

Например, таким образом Start->Control Panel->(при необходимости переключаемся к классическому виду Classic View) Network and Sharing Center -> ссылка Manage Network Connections (Пуск-> Панель управления-> Центр управления сетями и общим доступом->Управление сетевыми подключениями). Находим наше подключение (оно должно быть единственным), открываем его свойства, находим протокол TCP/IP v.4 и кнопкой Properties открываем окно настроек для этого протокола (рис.2).

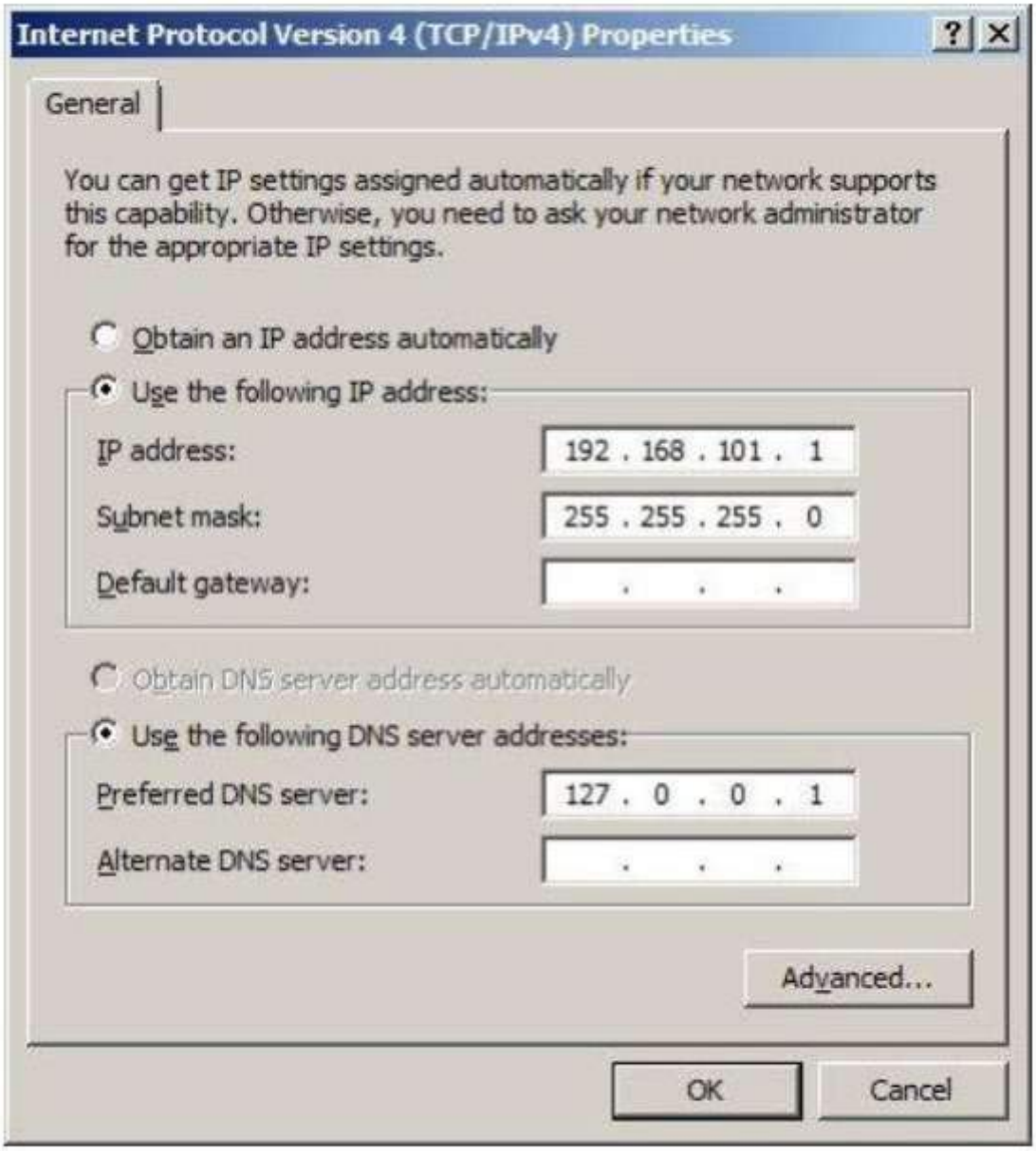


Рис.2. Настройка параметров TCP/IP.

Переключателями укажите, что настройка параметров будет осуществляться вручную (переключатель Use the following IP address). Для сервера зададим: Ip адрес 192.168.1уу.1 , где уу –двузначный порядковый номер компьютера в классе (192.168.101.1 для первого); маска 255.255.255.0; шлюз - <оставляем пустым> DNS 127.0.0.1 Для рабочей станции, которая будет подключаться к данному серверу: Ip адрес –192.168.1уу.2, где уу – номер, такой же как у сервера (192.168.101.2 для рабочей станции, подключающейся к серверу с адресом 192.168.101.1); маска – 255.255.255.0; шлюз – 192.168.1уу.1; DNS –

192.168.1уу.1. 19 Таким образом, у нас сервер и рабочая станция и сервер окажутся в одной ip-сети, а другие пары «сервер - рабочая станция» – в других. Чтобы проверить правильностьсделанных настроек с рабочей станции выполните команду ping 192.168.1уу.1 (уу - в зависимости от номера пары, например ping 192.168.101.1) если будет получен ответ, то все сделано правильно, сервер доступен. Итак, у нас в одной сети есть сервер-контроллер домена и рабочая станция, в домен пока не включенная. Перед выполнением следующих заданий проверьте на рабочей станции состав групп Администраторы и Пользователи (Пуск->Панель управления- >(классический вид) Администрирование -> Управление компьютером -> Локальные пользователи и группы). На сервере откроем оснастку администрирования Active Directory Users and Computers (Start->Administrative tools) и убедимся, что в контейнере Computers ничего нет. Кстати, а где сам сервер S08, он же член домена?! Контроллеры домена находятся в контейнере Domain Controllers. Теперь, администрируя рабочую станцию, добавим ее в домен. Для этого откроем Панель управления, переключимся к классическому виду и запустим инструмент *Система*.

В открывшемся окне найдите раздел *Имя компьютера, имя домена, параметры рабочей группы*, выберите ссылку *Изменить параметры*. В открывшемся окне на вкладке Имя компьютера нажмите кнопку *Изменить*. И укажите, что теперь компьютер включен в домен (он у нас называется saiu_test). Для завершения этой операции понадобится логин и пароль учетной записи, обладающей правами добавлять пользователей в домен. Это учетная запись Administrator. Чтобы явно указать, что учетная запись доменная, используйте полное имя в виде saiu_test\Administrator. После добавления в домен рабочую станцию надо перезагрузить. В это время проверьте на сервере, что в домене появился новый компьютер. Войдите на рабочую станцию сначала под доменной учетной записью **Labos** (пароль **Lab0s123** – эту запись мы создавали на прошлой лабораторной работе), потом под локальной записью **Adm**. Посмотрите, как изменился состав локальных групп Пользователи и Администраторы. На сервере откройте оснастку *Active Directory Users and Computers*. В контейнере *Users* найдите учетную запись **Labos**. Откройте ее свойства (в контекстном меню пункт Properties), на вкладке *Account* найдите кнопку *Logon Hours ...* (рис.3). Отредактируйте параметры таким образом, чтобы время выполнения лабораторной работы не попадало в период, разрешенный для входа пользователя. Попробуйте на рабочей станции зайти под пользователем **Labos**.

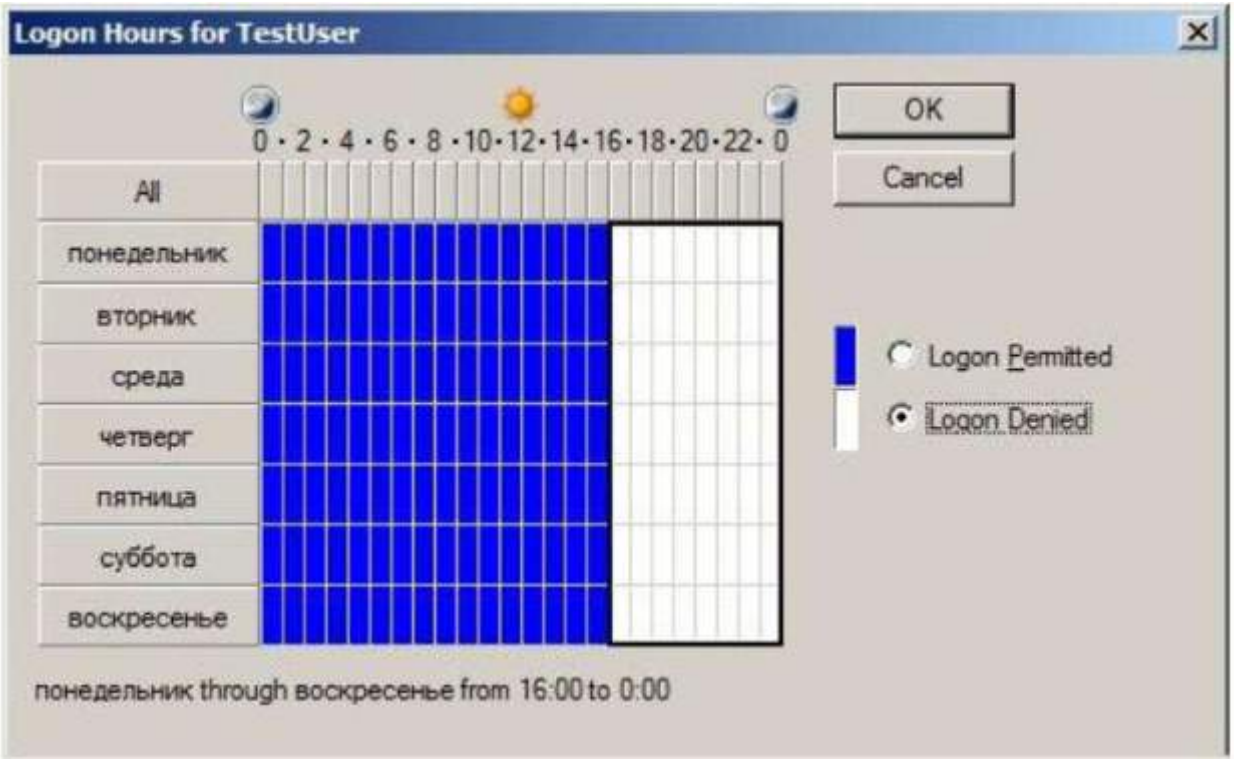


Рис.3. Редактирование расписания работы пользователя.

Теперь сделайте расписание таким, чтобы пользователь Labos мог входить в домен в это время. Но ограничьте перечень компьютеров, на которые может входить пользователь (вкладка Account кнопка Logon to…) и исключите рабочую станцию Vista_dop. Проверьте работу настройки. Верните назад сделанные изменения. При необходимости, поменяйтесь в паре и проделайте лабораторную работу для другого сочетания сервер-рабочая станция.

ПРАКТИЧЕСКАЯ РАБОТА № 28.
АДМИНИСТРИРОВАНИЕ ФАЙЛОВОГО СЕРВЕРА

Цель работы:
Научиться выполнять администрирование файлового сервера

Используемое программное обеспечение

Для выполнения данной лабораторной работы Вам понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1. А также 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista.

Дополнительная настройка виртуальных машин

В ходе выполнения лабораторной работы нам понадобится добавить диски к виртуальной машине. Для этого в консоли Virtual PC нужно выделить виртуальную машину и кнопкой Settings открыть ее параметры. Найдите список жестких дисков и на месте отсутствующего диска (надпись «None») с помощью мастера, запускаемого нажатием кнопки Virtual Disk Wizard, создайте новый диск. Процедура достаточно понятна и не требует особых пояснений.

При выборе типа диска оставьте настройку по умолчанию Dynamically expanding (динамически увеличивающийся). Для выполнения работы понадобится подключить два диска размером по 10 Гб.

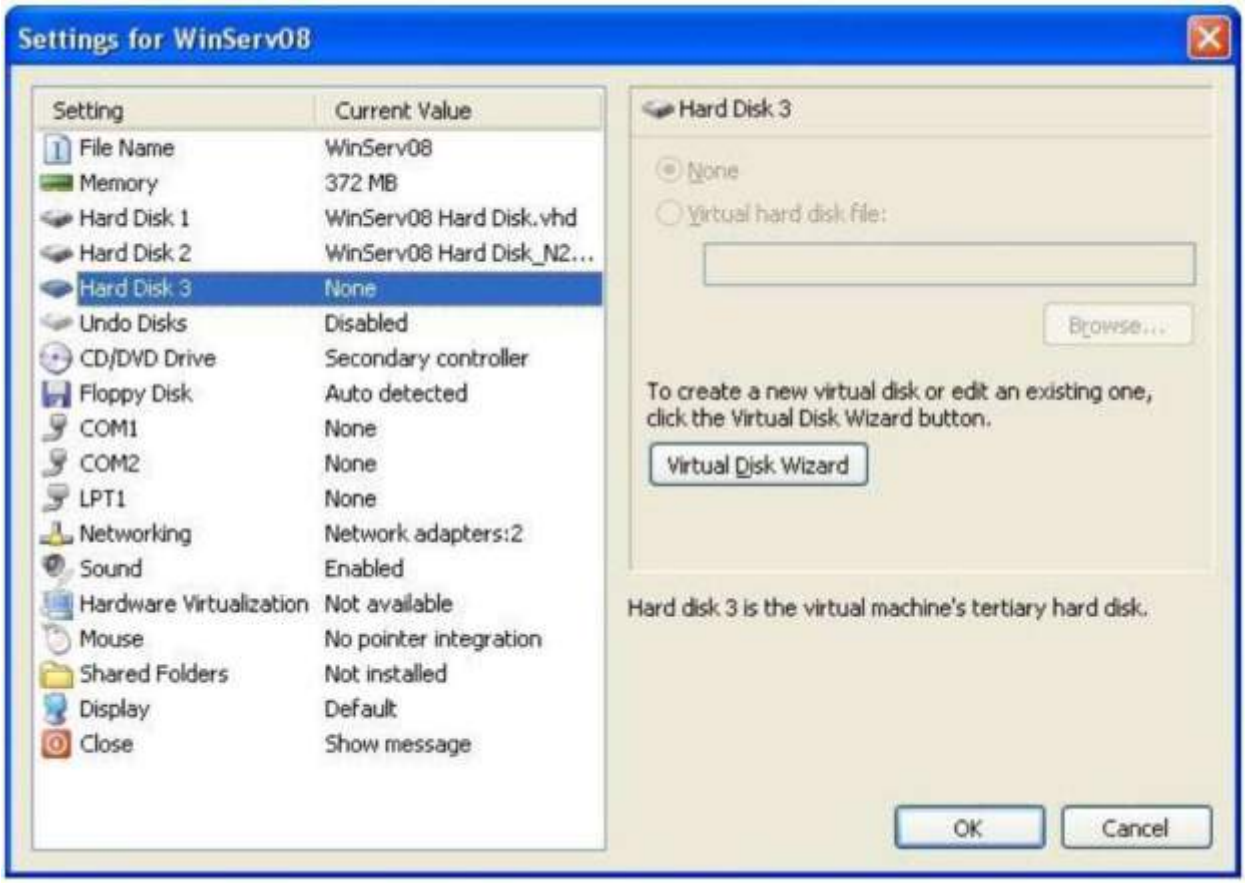


Рис.1. Окно параметров виртуальной машины.

Также иногда требуется подключить к виртуальной машине папку с «физического» компьютера. В виртуальной машине она будет отображаться как сетевой диск, что позволить осуществлять обмен файлами. Для этого в параметрах уже запущенной виртуальной машины надо зайти в раздел Shared Folders (рис.4.2) и, нажав кнопку Share Folder подключить к виртуальной машине выбранную папку.

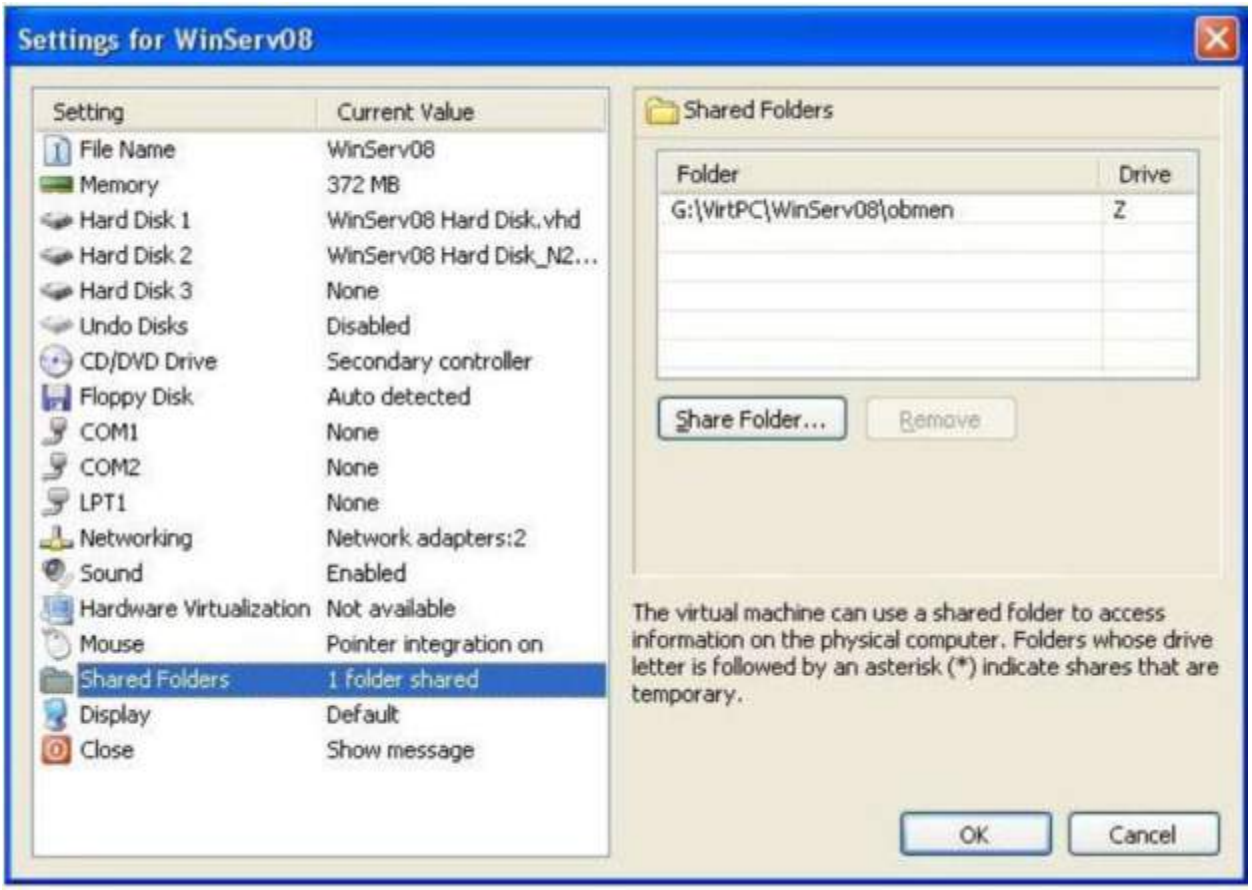


Рис.2. Подключение папки к виртуальной машине.

Управление дисками

Теперь рассмотрим ряд вопросов, связанных с организацией дискового пространства в Windows Server 2008. Для работы с дисками запустим оснастку Server Manager и в ней откроем узел Storage и там Disk Management (рис.3).

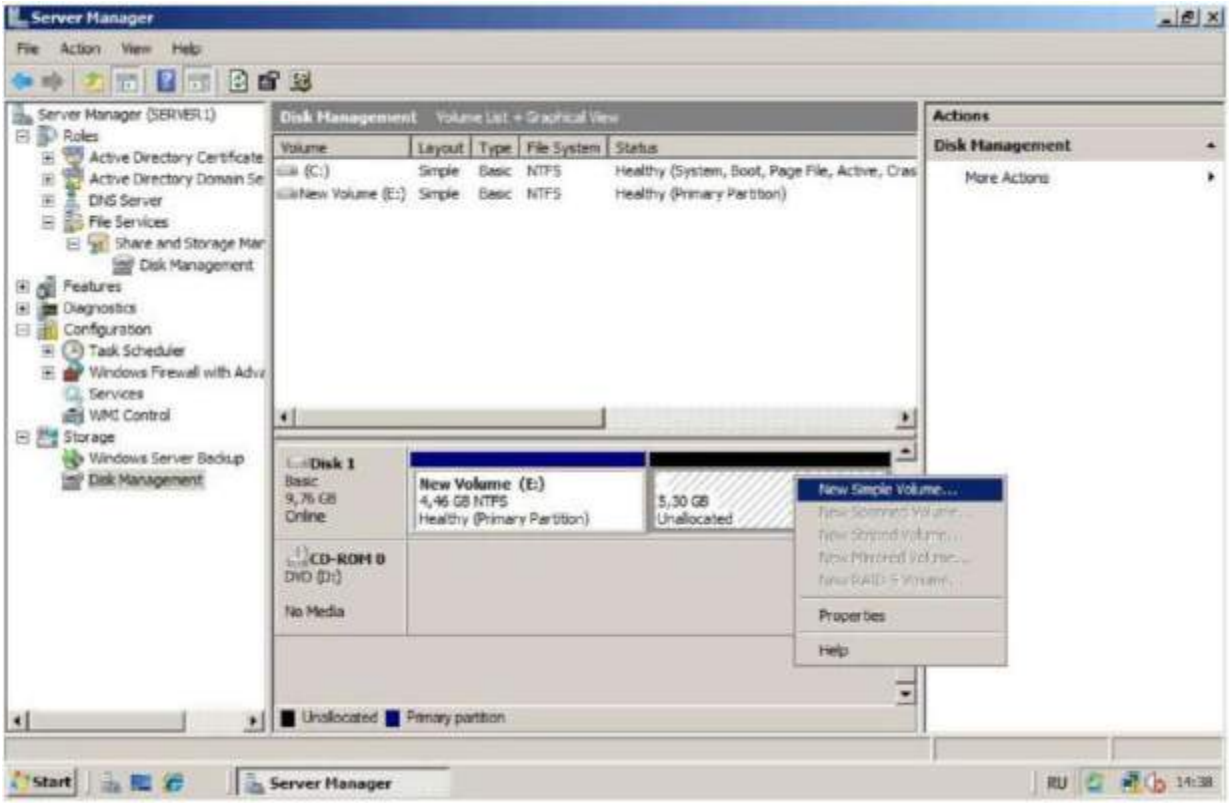


Рис.3. Окно оснастки Disk Management.

Если Вы добавили два новых виртуальных диска (см. предыдущий раздел), то при открытии Disk Management появится окно с предложением подключить новые диски к системе и выбрать их тип - MBR или GPT. Диски типа MBR («обычные» для персональных компьютеров на безе процессоров Intel и совместимых) могут иметь размер до 2 терабайт и поддерживают до 4 разделов на логический диск. Новый тип GPT используется для дисков большего объема и позволяет создавать до 128 разделов. Для нашей лабораторной работы выберем тип MBR. Посмотрите на созданный при установке операционной системы диск. Если Вы внимательно выполнили первую лабораторную работу, то сейчас должны увидеть физический диск с типом Basic, логическим диском C: на 30 гигабайт, куда установлена операционная и система, и примерно 10 гигабайтами свободного пространства. Теперь в свободной области диска создадим новый раздел. Для этого в контекстном меню (рис.3) выберем пункт New Simple Volume, укажем, что все свободное место отводится под раздел, назначим букву (например, D:) и выберем форматирование в файловую систему NTFS (при этом размер кластера – Allocation Unit Size – лучше оставить по умолчанию, а метку тома можно изменить на более информативную, например, TEST DATA). Таким образом, мы создали второй основной раздел на диске типа basic. В предыдущих версиях Windows Server оснастка Disk Management также позволяла создавать и расширенные разделы (extended partition). В начале основного раздела находится загрузочный сектор (boot sector) и с него может загружаться операционная система. Расширенный раздел загрузочного сектора не содержит, но может быть разделен на несколько логических дисков (основной раздел содержит только один логический диск).

Windows Server 2008 поддерживает работу с расширенными разделами, но создавать их можно только с помощью утилиты командной строки diskpart.exe. Говоря о новых возможностях Disk Management, нужно отметить возможность уменьшить (shrink) или увеличить (extend) размер существующего раздела диска. Для выполнения этих операций надо щелкнуть на изображении раздела правой клавишей мыши и из контекстного меню выбрать соответствующую операцию. Расширить раздел на базовом диске можно только в том случае, если непосредственно за ним есть неразмеченная область диска. Теперь перейдем к рассмотрению динамических дисков. Новые возможности, предоставляемые данным типом дисков – создание одного логического диска на нескольких физических, создание массивов дисков (RAID от англ. Redundant Array of Independent Disks массив независимых дисков с избыточностью). Итак, у нас в виртуальной машине появились два новых диска. По умолчанию они имеют тип Basic. Но их можно преобразовать в тип Dynamic воспользовавшись контекстным меню, появляющимся при щелчке правой клавишей мыши по названию диска (рис.4). Безопасно преобразовать к динамическому типу можно любой базовый диск (в том числе, уже размеченный и содержащий данные). Обратное преобразование оснастка Disk Management осуществить не позволяет. Преобразуем два новых диска к типу Dynamic. На одном из них создадим новый том (тип Simple Volume), занимающий все пространство диска, пусть он будет обозначен буквой E:. На новом логическом диске создайте какие-нибудь папки или файлы. Теперь предположим, что понадобилось увеличить объем логического диска. Для этого задействуем второй «физический диск»: в оснастке Disk Management щелкните правой клавишей мыши на изображении диска E:, в контекстном меню выберите пункт Extend Volume и с помощью мастера добавьте все пространство второго диска к тому E:. Обратите внимание, что после этой операции тип тома с «простого» (simple volume) изменился на «составной» (spanned volume). Эта конфигурация позволяет более гибко управлять дисковым пространством, но не обладает отказоустойчивостью. Убедимся в этом на следующем примере.

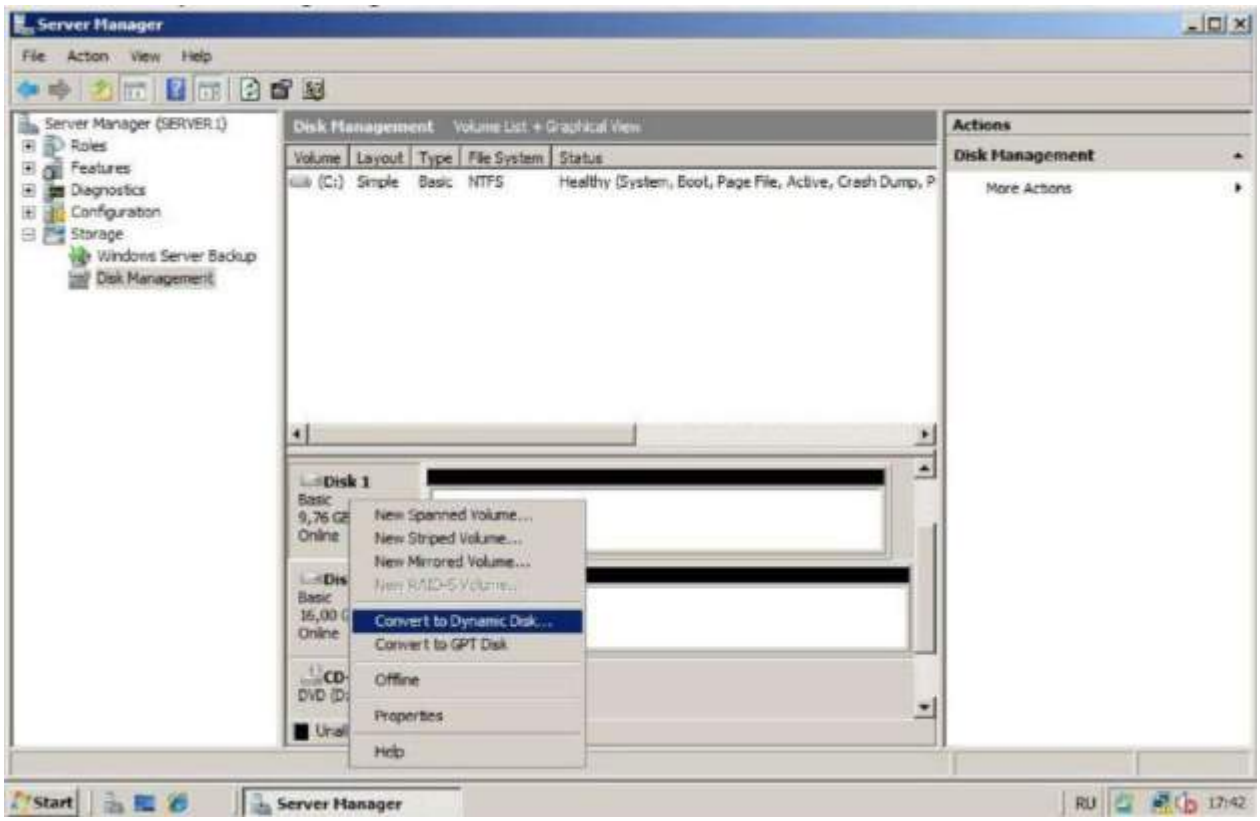


Рис.4. Изменение типа диска с basic на dynamic.

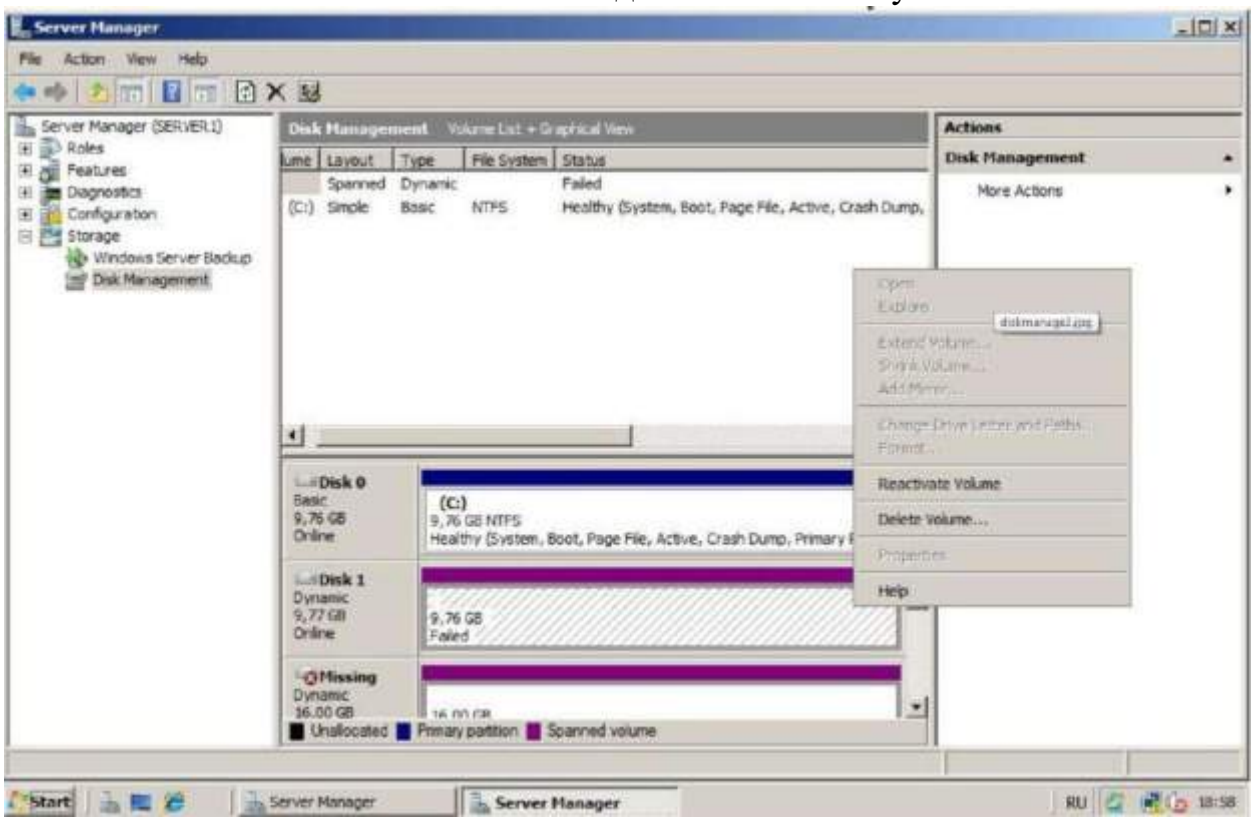


Рис.5. Имитируем отказ одного из дисков в составном томе.

Сначала проверим, что созданные нами папки и файлы остались на диске E:. Теперь выключим виртуальную машину и отключим третий виртуальный диск (на первом у нас операционная система и раздел для данных, а второй и третий диски занимал динамический том). После очередной загрузки виртуальной

машины увидим, что диска, созданного нами на динамическом томе, в проводнике нет. Если открыть оснастку Disk Management, то увидим, что составной том неработоспособен (рис.5). Его можно удалить, чтобы использовать дисковое пространство на работоспособном физическом диске. Но это не позволит получить доступ к хранившимся там файлам. Кроме рассмотренных простого и составного тома, при использовании нескольких физических дисков можно создавать следующие типы томов: - чередующийся (stripped) – соответствует RAID 0, в массив объединяются несколько физических дисков, записываемые файлы делятся на блоки, которые поочередно записываются на различные диски. За счет этого повышается скорость работы (операции распараллеливаются между несколькими физическими устройствами), но снижается надежность, т.к. выход из строя одного диска приводит к недоступности всех данных; - зеркальный или зеркалируемый (mirrored) – соответствует RAID 1, в массив объединяются два диска, содержимое которых будет идентично - данные записываются одновременно на оба. При отказе одного из дисков, данные могут быть считаны со второго. Но плата за большую надежность – избыточность, т.к. для пользователя доступно только 50% суммарного пространства дисков, входящих в массив; - RAID 5 – так называемый чередующийся массив с переходящим контролем чѐтности; в массив объединяют 3 или более диска, данные записывают блоками, на все диски кроме одного: на него пишутся контрольные суммы для блоков. Все диски по очереди используются для записи данных и контрольных сумм. При отказе одного из дисков все данные можно восстановить по содержимому оставшихся. В этом случае обеспечивается отказоустойчивость и избыточность ниже, чем в случае RAID 1. Важно отметить, что обычно в серверных системах RAID-массивы организуются с помощью аппаратных RAID-контроллеров. Программные реализации дополнительно загружают центральный процессор и поэтому менее предпочтительны. Для учебных целей на месте разрушенного составного тома создадим зеркальный. Для этого выключим виртуальную машину, снова создадим третий виртуальный диск и загрузимся. На двух дисках создадим зеркальный том и запишем на него какие-нибудь файлы. Выключим виртуальную машину и отключим один из дисков. Снова загрузимся. Как и в предыдущем случае, в проводнике диск виден не будет. Но с помощью оснастки Disk Management (в меню почти таком же, как на рис.5) можно для сбойного тома выбрать опцию Remove Mirror и из неработающего зеркального тома получить работоспособный обычный. Только будьте внимательны при выборе диска, исключаемого из массива. Исключить надо отказавший диск (а не оставшийся работоспособным) иначе данные будут потеряны! А если нужно восстановить «зеркало», то вместо выбывшего из строя, надо установить еще один диск и использовать его для восстановления.

Квоты и сетевые папки

Для продолжения лабораторной работы нам понадобится только один логический диск (далее будем называть его E:), не считая того, где расположена операционная система. Остальные можно удалить или оставить для каких-то еще экспериментов Предположим, нам нужно разместить на сервере файлы пользователей нашего домена. И для этого будем использовать диск E:. Зачастую при администрировании файлового сервера возникает необходимость отслеживать, сколько дискового пространства используется каждым из пользователей и, при необходимости, ограничивать это значение. Сделать это позволяет механизм дисковых квот. В проводнике откройте окно свойств диска E: (Start->Computer щелчок правой клавишей на диске E:, пункт Properties в контекстном меню). Перейдите на вкладку Quota и отметьте флажок Enable quota management, установите какую-нибудь небольшую квоту (например, 1 Мб) и пороговое значение для предупреждения администратора (оно должно быть не больше размера квоты, а чаще берется чуть меньше) (рис.6). Просмотреть текущее использование дисковых квот можно, нажав на кнопку Quota Entries.

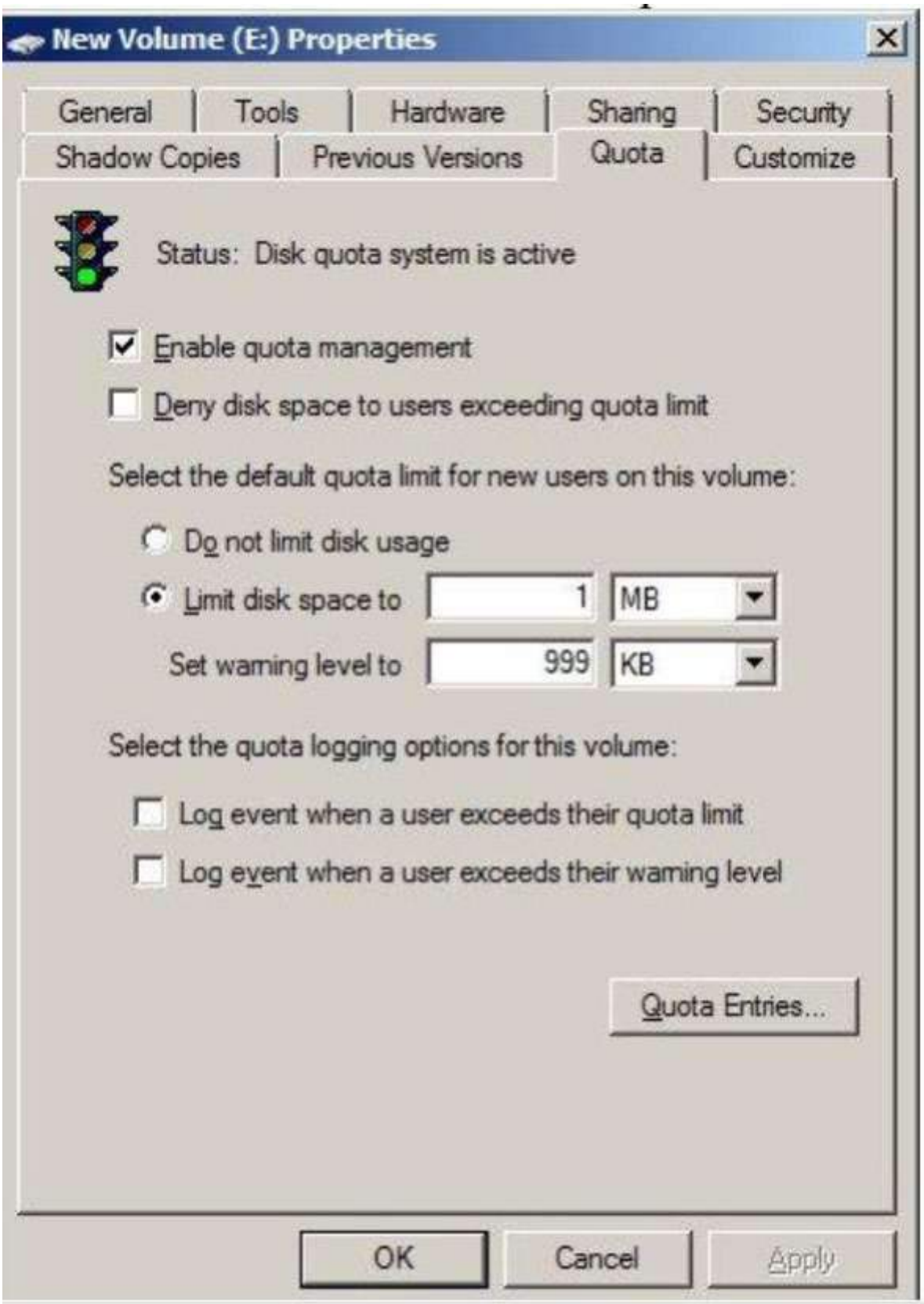


Рис.6. Настройка квот для диска.

Для дальнейшего выполнения лабораторной работы проверьте, чтобы на сервере была установлена роль File Services (это делалось в ходе лабораторной работы №2). Если роли нет, добавьте ее. Теперь создадим на диске E: папку и предоставим ее в общий доступ. Для этого откроем свойства папки и перейдем

на вкладку Sharing (рис.7). Для более точной настройки общего доступа вместо кнопки Sharing нажмите Advanced Sharing. Отметьте переключатель Share this folder и введите имя общей папки (по умолчанию, подставляется такое же, как имя папки на диске). Если понадобится создать папку, которая не будет отображаться в «Сетевом окружении», то в конце ее имени ставится знак $. Но в нашем случае этого не требуется.

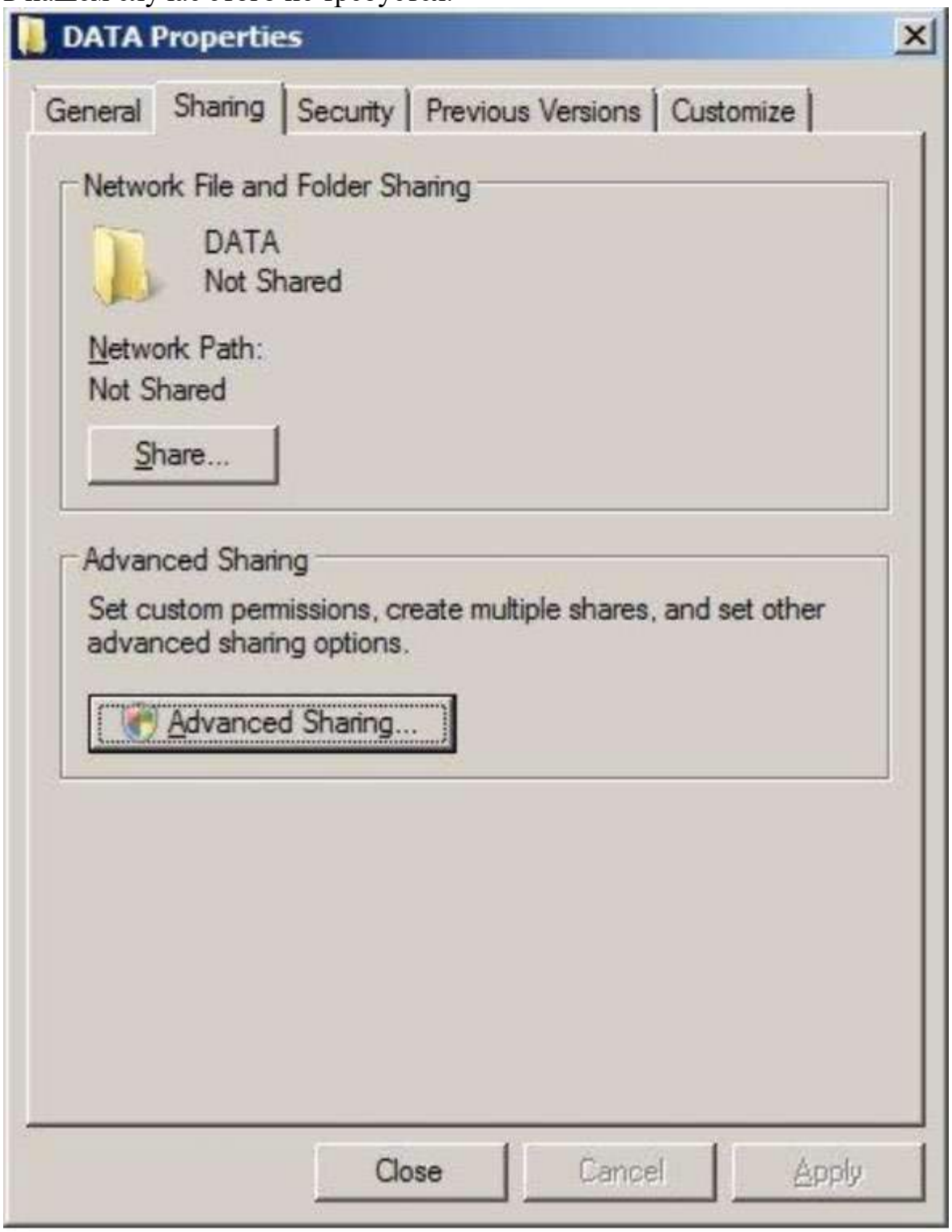


Рис.7. Настройка общего доступа для папки.

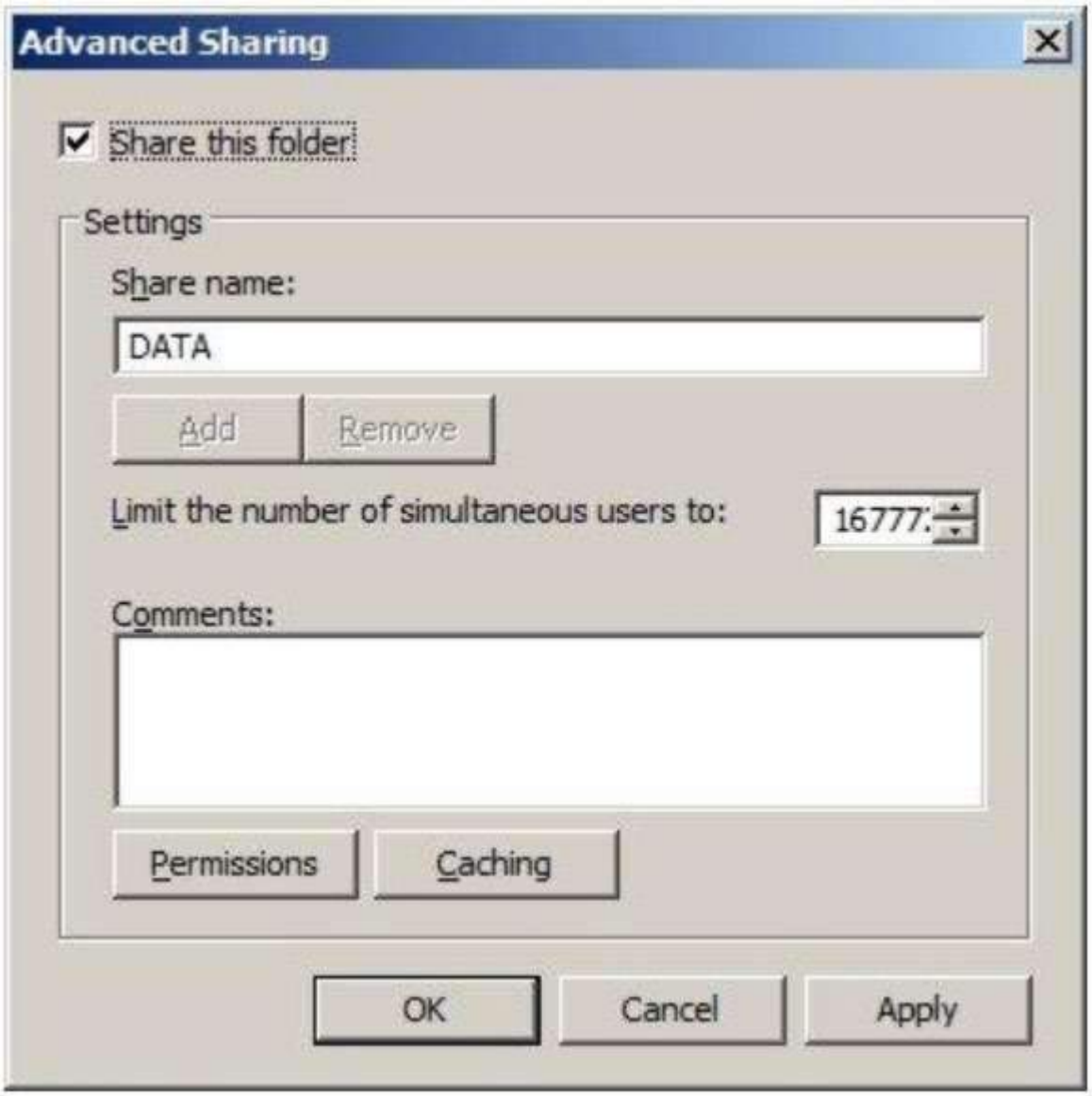


Рис.8. Настройка общего доступа к папке (продолжение).

Теперь нажмите кнопку Permissions, чтобы отредактировать разрешения для пользователей. Вы увидите, что группа Everyone имеет разрешение на чтение (Read). Добавим в список (кнопка Add) доменного пользователя Labos и дадим ему полный доступ к файлам папки (разрешение Full Control). Тут надо отметить, что на файловой системе NTFS также устанавливаются разрешения на работу с файлами и папками (их можно просмотреть в свойствах файла или папки на вкладке Security). При доступе к папке локально, работают только разрешения NTFS. При доступе к папке через сеть срабатывают и разрешения NTFS, и разрешения на общий доступ (итоговое разрешение – наименьшее из двух).

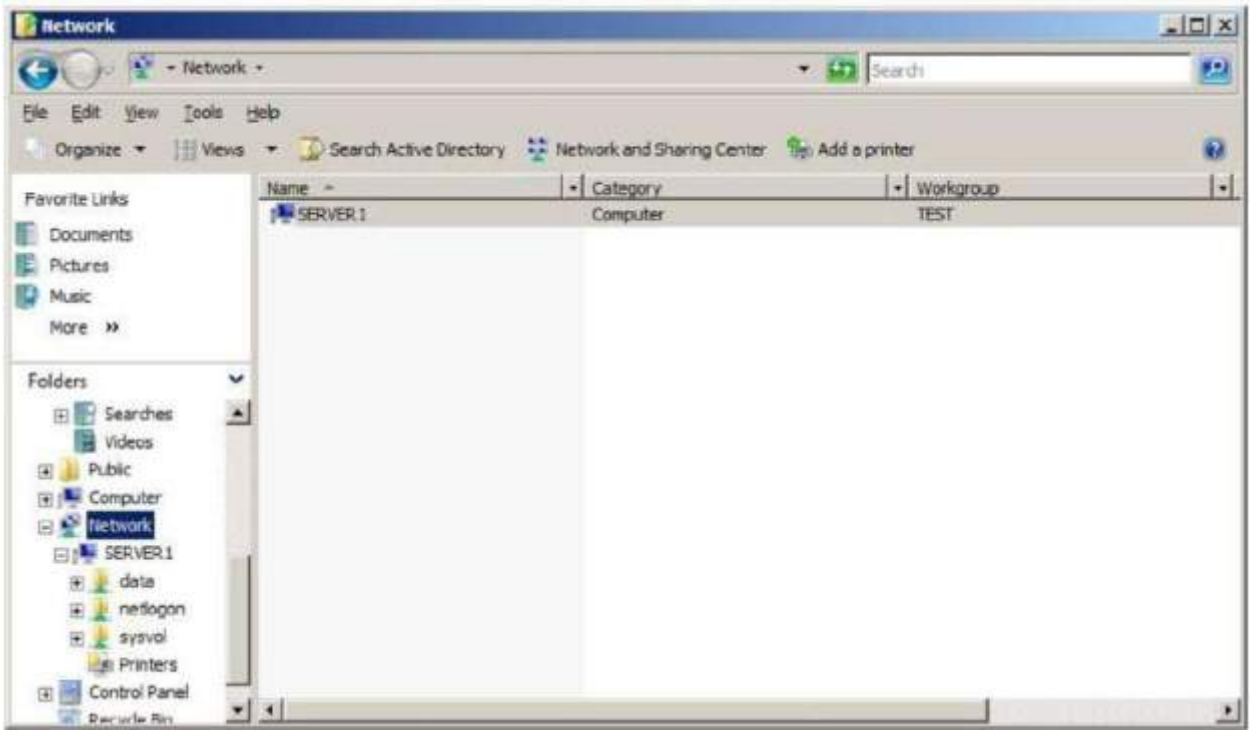


Рис.9. Поиск папки в сети.

Теперь запускаем рабочую станцию с операционной системой Windows Vista (как и при выполнении лабораторной работы № 3 в нашем учебном классе делимся парами – на одном компьютере Windows Server, на другом – входящая в этот домен рабочая станция). На рабочую станцию заходим под учетной записью Labos и запускаем Windows Explorer. Открываем узел Network (рис.9), находим наш сервер и открываем сетевую папку. Записываем в нее несколько файлов, чтобы их суммарный размер был больше 1 Мегабайта. На сервере откроем информацию об использовании квот (кнопка Quota Entries рис.6). Там Вы должны увидеть, что пользователь Labos превысил лимит. Но пока ему писать файлы на диск не запрещается. Срабатывает так называемая мягкая (soft) квота, которая позволяет проинформировать администратора. Если в настройках квот (рис.6) отметить переключатель Deny disk space to users exceeding quota limit, то будет установлена жесткая (hard) квота и пользователь не сможет больше записывать файлы на этот диск. Установите жесткую квоту, проверьте ее работу.

ПРАКТИЧЕСКАЯ РАБОТА № 29.
АДМИНИСТРИРОВАНИЕ ФАЙЛОВОГО СЕРВЕРА ПРОДОЛЖЕНИЕ)

Цель работы:
Научиться выполнять администрирование файлового сервера

Используемое программное обеспечение
Для выполнения данной лабораторной работы понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1. А

также 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista.

Управление общими папками

Ознакомимся с рядом инструментов, упрощающих администрирование файлового сервера. Первая задача – получение информации обо всех папках на компьютере, предоставляемых в общий доступ. Ее можно решить с помощью оснастки Shared Folders, входящей в состав оснастки Computer Management (Start->Administrative Tools- > Computer Management, рис.5.1). Как видно на рисунке, в папке Shares можно просмотреть список имеющихся на сервере папок с общим доступом, их расположение, число текущих подключений пользователей. Открыв свойства папки, можно просмотреть разрешения, опубликовать папку в каталоге Active Directory (если сервер входит в домен), установить максимальное число одновременных подключений (по умолчанию ставится максимально допустимое, зависящее от типа лицензии сервера).

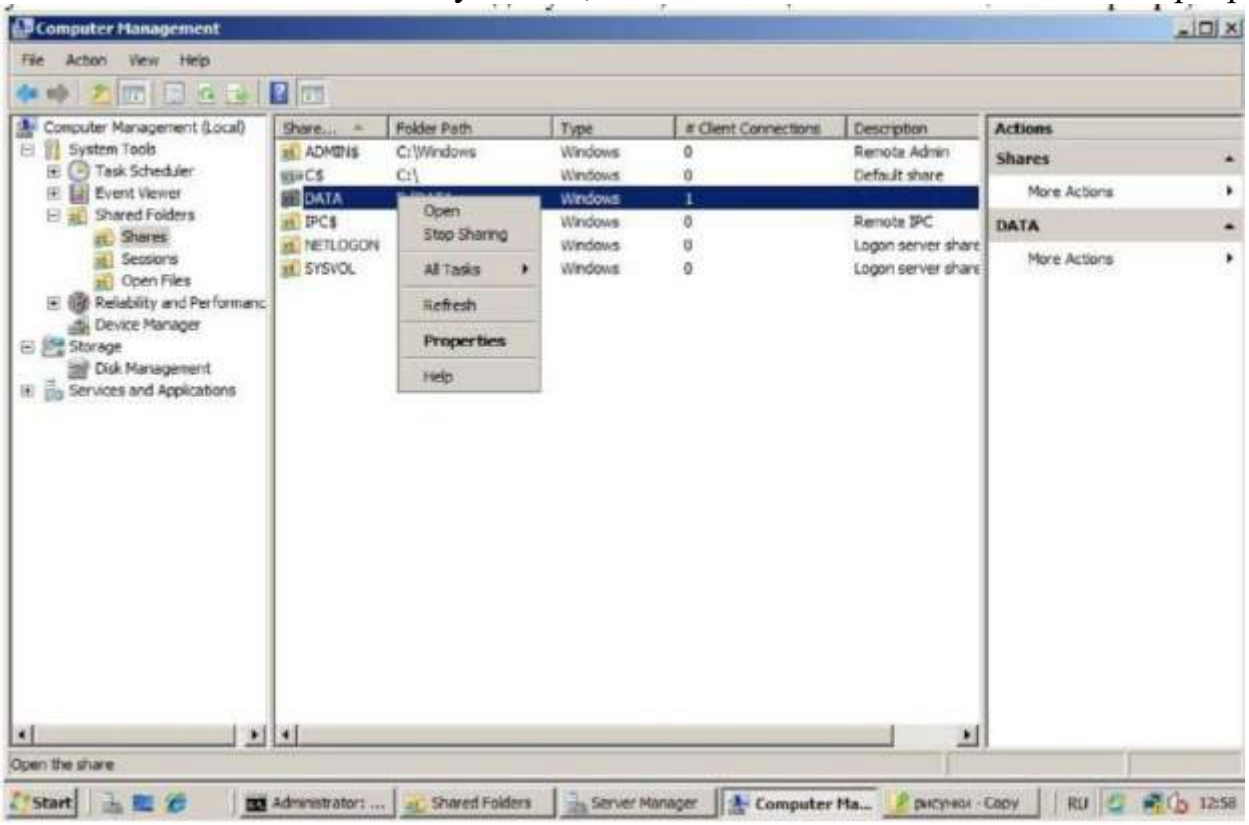


Рис.1. Оснастка Shared Folders.

Информацию о текущих сессиях (какие пользователи подключены, число открытых файлов и т.д.) и открытых файлах можно получить, открыв папки Sessions и Open Files оснастки Shared Folders.

***Задание**. Откройте оснастку Shared Folders, просмотрите информацию о папках с общим доступом.*

Из командной строки получить информацию о папках в общем доступе позволяет команда net share. Ее запуск без дополнительных параметров приведет к получению списка всех имеющихся папок: C:\Users\Administrator>net share Share name Resource Remark

---
C$ C:\ Default share IPC$ Remote IPC
ADMIN$ C:\Windows Remote Admin
DATA E:\DATA
NETLOGON C:\Windows\SYSVOL\sysvol\test.domain\SCRIPTS
Logon server share
SYSVOL C:\Windows\SYSVOL\sysvol Logon server share
The command completed successfully.

Подробную информацию о папке можно получить, запустив команду net share имя_папки. С помощью net share также можно предоставлять общий доступ к папке, отменять его, менять параметры, т.е. делать все те операции, которые ранее проделывались нами средствами с графическим интерфейсом. Просмотреть список папок, предоставляемых в общий доступ удаленным компьютером можно с помощью команды net view.

Например: C:\Users\Administrator>net view \\server1 Shared resources at \\server1
Share name Type Used as Comment

DATA Disk NETLOGON Disk Logon server share SYSVOL Disk Logon server share
The command completed successfully.

Задание. *Запустите рабочую станцию (виртуальную машину с ОС Windows Vista). С помощью команды net view просмотрите с нее список папок предоставляемых в общий доступ сервером S08. Сравните со списком, который возвращает команда net share, выполненная на сервере. По справке найдите ключ команды net view, который позволит получить полный список папок.*

Папку, предоставляемую другим компьютером в общий доступ, можно подключить в качестве сетевого диска. Это можно сделать из окна Windows Explorer, найдя в разделе Network нужный компьютер, открыв список предоставляемых в общий доступ папок и в контекстном меню нужной папки, выбрав пункт Map Network Drive (рис.2). В открывающемся после этого окне можно выбрать букву для обозначения сетевого диска, отметить, надо ли подключать диск при следующем сеансе работы в системе (по умолчанию – «да»), если подключение к сетевому ресурсу нужно проводить от имени другой учетной записи, можно ввести имя пользователя и пароль. Отключить сетевой диск можно, выбрав в его контекстном меню пункт Disconnect. Аналогичные действия из командной строки можно выполнить с помощью команды net use. Например, net use F: \\server1\data подключит в качестве сетевого диска F: папку data с компьютера server1. А net use F: /delete отключит сетевой диск F:.

***Задание**. На рабочей станции подключите папку с сервера в качестве сетевого диска.*

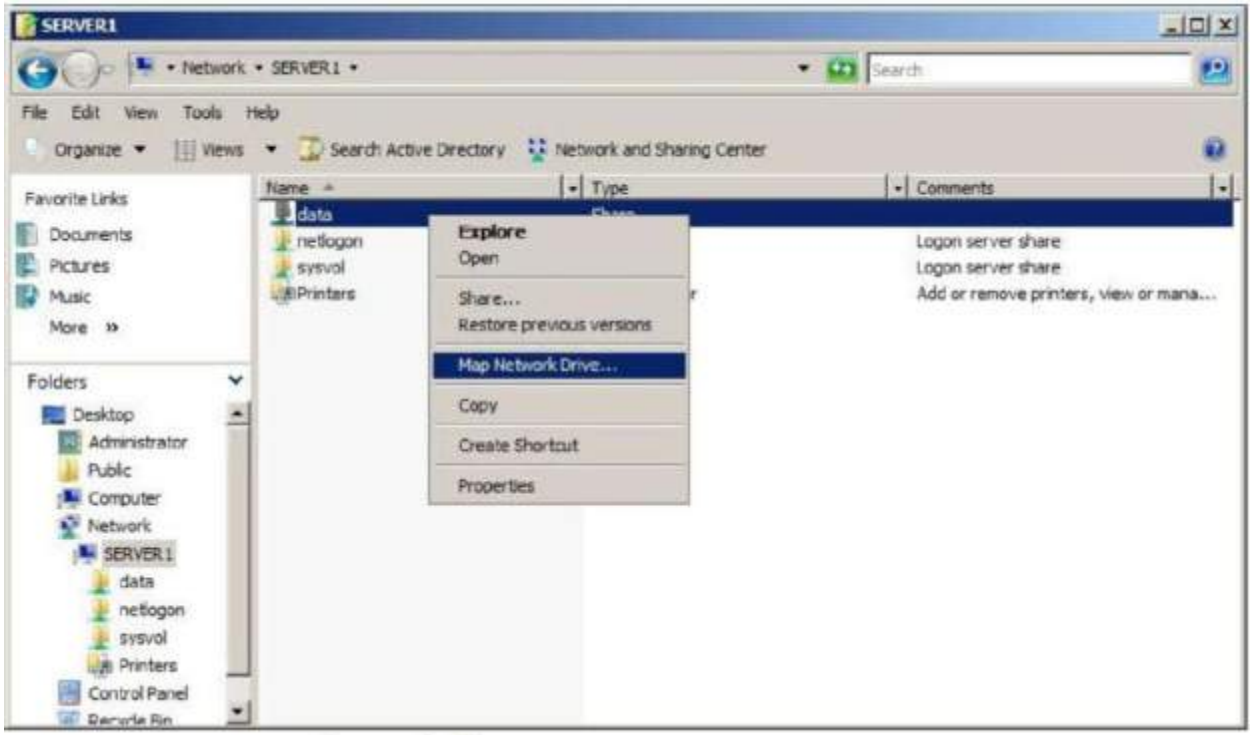


Рис.2. Подключение сетевого диска.

Теперь познакомимся с дополнительными средствами администрирования файлового сервера. С помощью File Server Resource Manager можно, например, устанавливать квоты на отдельные папки или ограничить перечень типов файлов, которые пользователь может хранить на сетевом диске. Это средство добавляется как отдельная служба роли File Services. Запустите Server Manager, откройте узел Roles и в нем узел File Services (рис.3). Проверьте, установлена ли служба File Server Resource Manager. Если не установлена, добавьте ее. При добавлении службы появится запрос, состояние каких дисков будет отслеживать данная служба (рис.4). Нас будет интересовать диск, выделяемый для хранения файлов пользователей сети. На рисунке 4 это диск E:. Также выводится список формируемых отчетов, который можно откорректировать, нажав кнопку Options. Следующее окно мастера установки File Server Resource Manager позволяет указать путь к папке, где будут храниться генерируемые отчеты. При необходимости, можно сконфигурировать автоматическую отправку отчетов администратору по электронной почте.

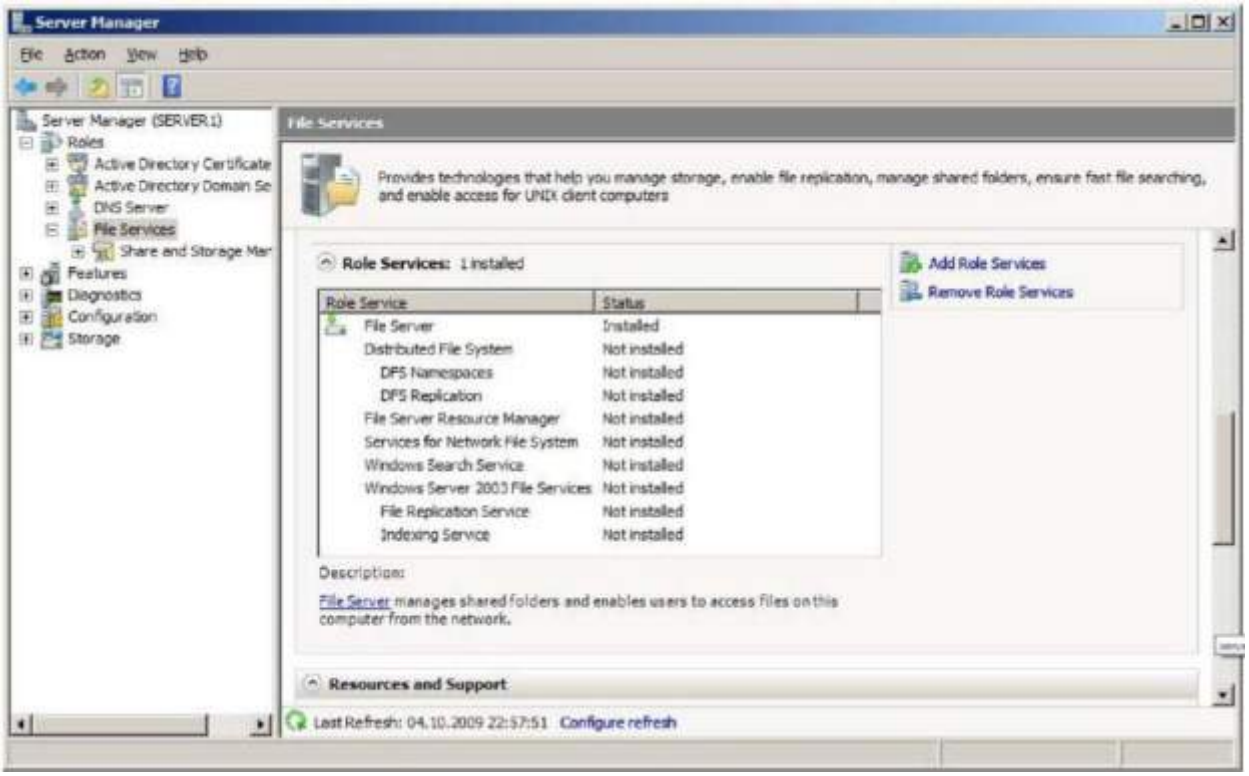


Рис.3. Набор служб роли File Services.

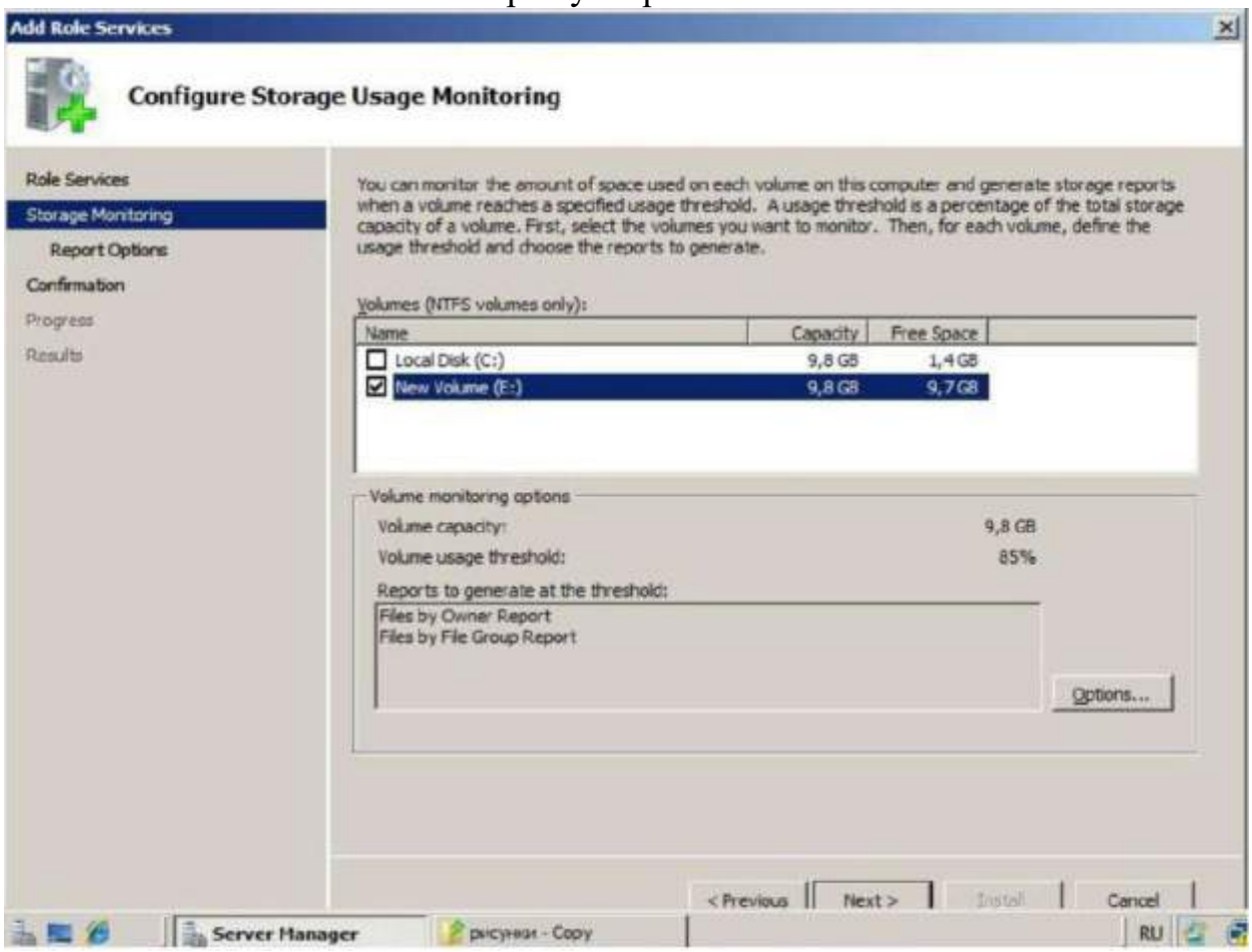


Рис.4. Установка службы File Server Resource Manager.

***Задание**. Добавьте оснастку File Server Resource Manager. Выполните настройку и поверку квот и ограничений на содержимое в соответствии с приводимым ниже описанием.* После установки в разделе Administrative Tools появится оснастка File Server Resource Manager (рис.5). В оснастке есть три узла – Quota Management (позволяет устанавливать квоты на папки или диски), File Screening Management (позволяет определить, какие файлы нельзя записывать в папки) и Storage Reports Management (для работы с отчетами). Начнем с создания квоты на папку. Чтобы результаты выполнения предыдущей работы не оказывали влияния, проверьте, чтобы в свойствах выбранного для экспериментов диска были отключены квоты на диск. Раскроем узел Quota Management (рис.5), в нем две папки – квоты и шаблоны квот. Предустановленные шаблоны (с квотами 100, 200, 500 MB) нам для эксперимента не подойдут – слишком большие квоты. Поэтому создадим квоту, не используя шаблон. Выделим папку Quotas и в контекстном меню выберем создание новой квоты (Create Quota…). Установим на папку, предоставляемую в общий доступ, жесткую квоту в 10 MB (рис.6), т.к. готового шаблона у нас нет, надо выбрать в окне Define custom properties и, нажав кнопку Custom Properties … , определить размер и тип квоты. На основе заданных параметров можно будет создать новый шаблон (это будет предложено в следующем окне мастера), но для наших целей это не обязательно.

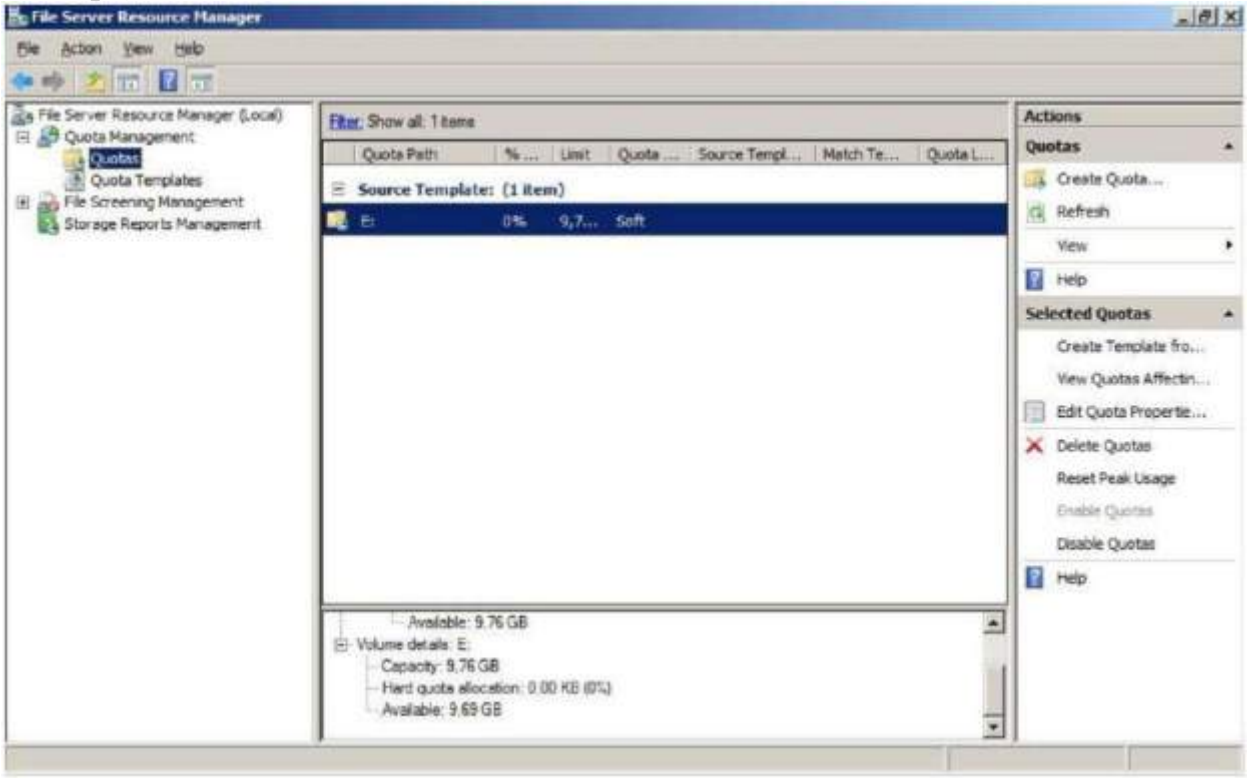


Рис.5. Оснастка File Server Resource Manager.

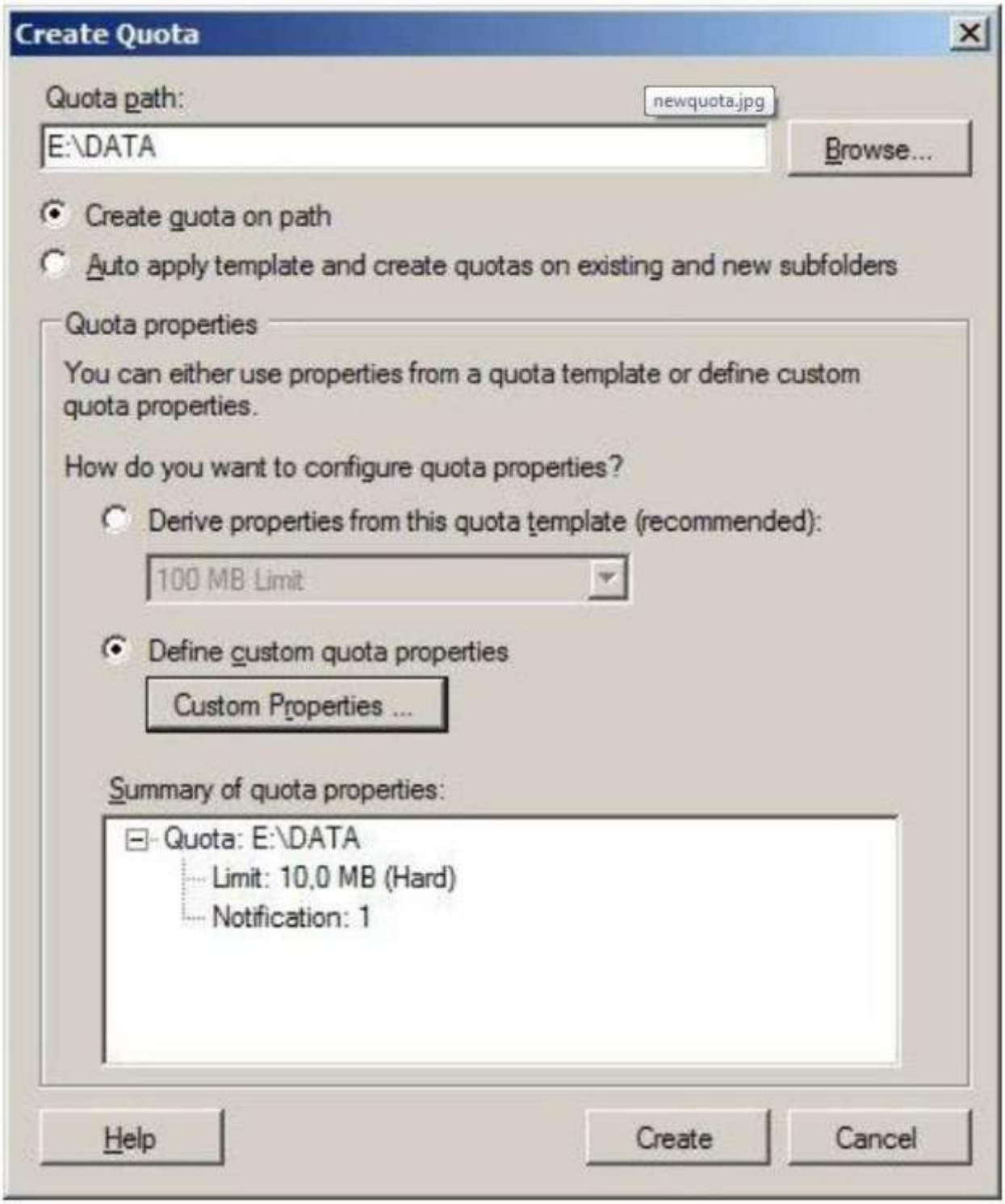


Рис.6. Создание квоты на папку.

С рабочей станции под учетной записью Labos запишите в общую папку на сервере (подключенную как сетевой диск) какие-нибудь файлы до срабатывания квоты. Обратите внимание, если в Windows Explorer открыть свойства сетевого диска, то его размер будет равным установленной квоте. Работая на сервере под учетной записью Administrator, попробуйте записать в предоставляемую в общий доступ папку какие-нибудь файлы. Должна сработать квота, не позволяющая это сделать. Данный пример показывает разницу между квотами на диск, которые мы устанавливали в предыдущей работе, и квотами, создаваемыми с помощью File Server Resource Manager. В

первом случае, квота устанавливается для каждого пользователя индивидуально, во втором – для папки, не зависимо от того, какие пользователи туда записывают файлы. Очистим папку от записанных файлов (чтобы квоты не срабатывали). Снова откроем оснастку File Server Resource Manager, теперь нас будет интересовать узел File Screening Management. Здесь можно создать ограничение по типу записываемых на диск (в папку) файлов. Например, если файловый ресурс предназначается только для хранения документов, можно запретить запись туда мультимедийных и исполняемых файлов.

Просмотрите список предустановленных шаблонов. Воспользуемся шаблоном Block Image Files, чтобы запретить запись в нашу папку файлов изображений. На его основе создадим новое ограничение (рис.7,8). Попробуйте сначала с сервера, потом с рабочей станции записать картинку в папку. Убедитесь, что ограничение работает. И закончим знакомство с оснасткой File Server Resource Manager созданием отчета.

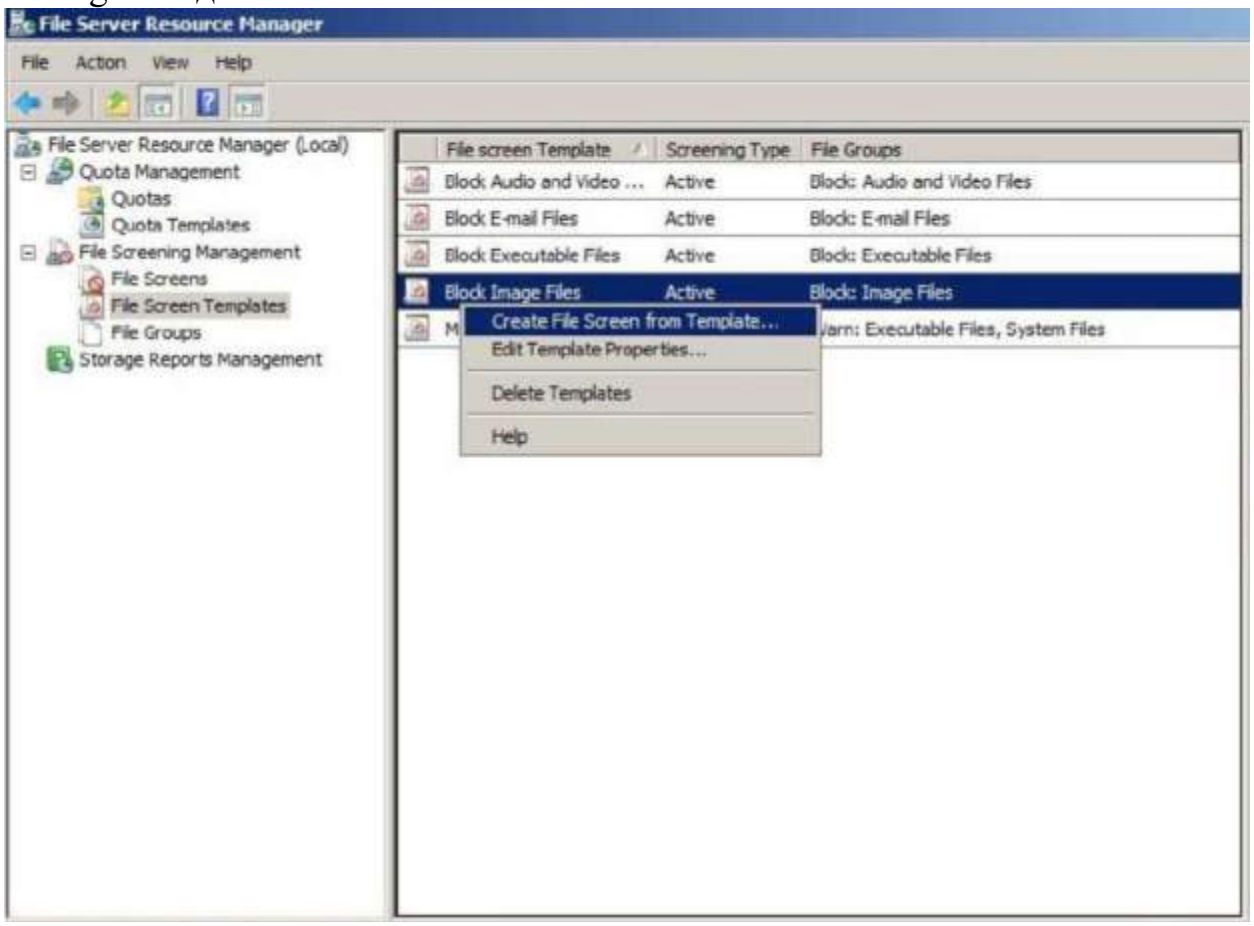


Рис.7. Создание ограничение на содержимое на базе шаблона.

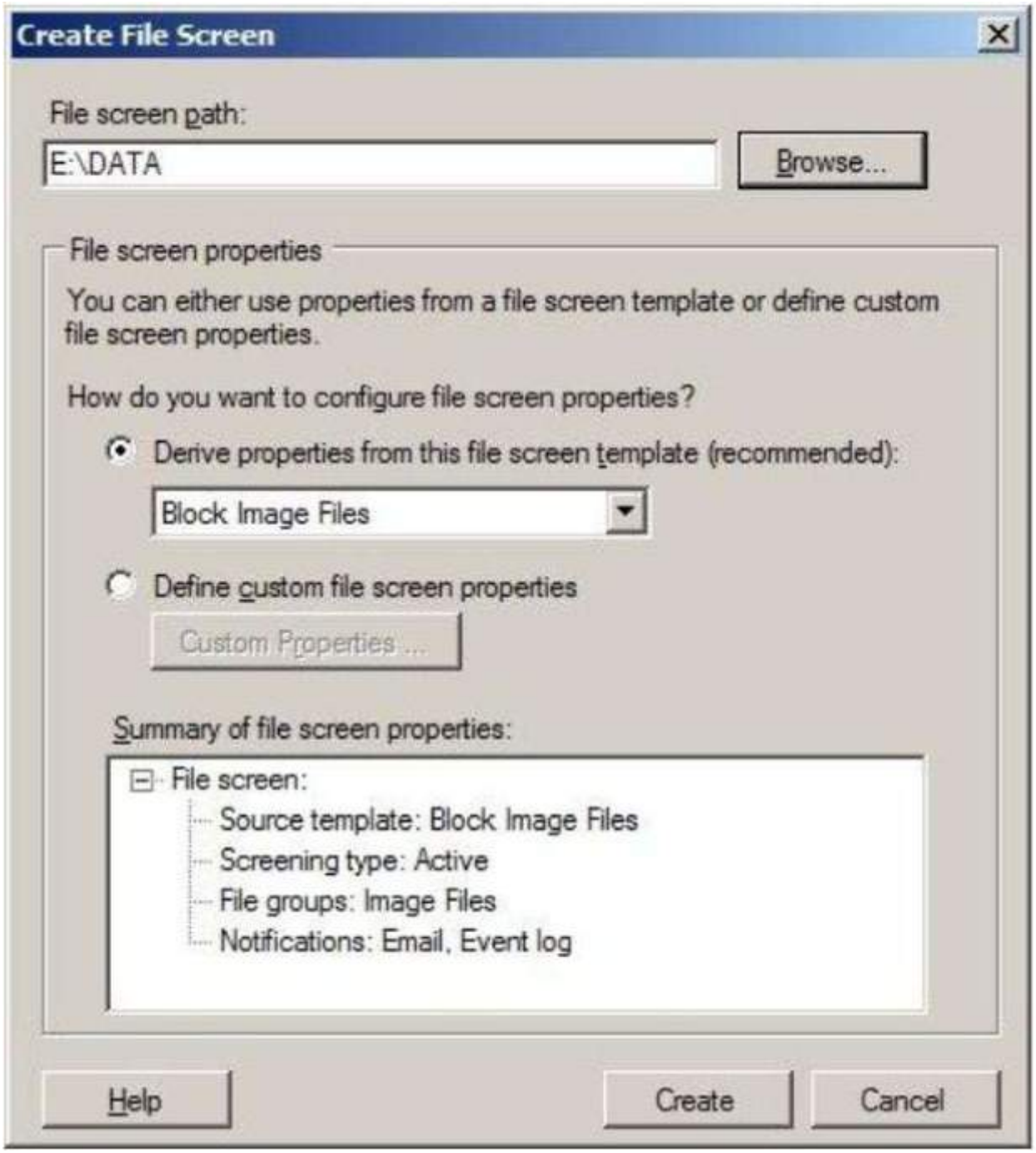


Рис.8. Создание ограничение на содержимое на базе шаблона (продолжение).

Снова запишем в нашу папку какие-нибудь файлы. В оснастке перейдите на узел Storage Reports Management, щелкните на нем правой клавишей и выберите в контекстном меню Generate Reports Now…

В открывшемся окне выберите папку, для которой будет создаваться отчет, и типы отчетов (нас будет интересовать использование квот – рис.9). В следующем окне подтвердите, что нужно сгенерировать отчет и отобразить «прямо сейчас», и после создания отчет будет открыт в браузере.

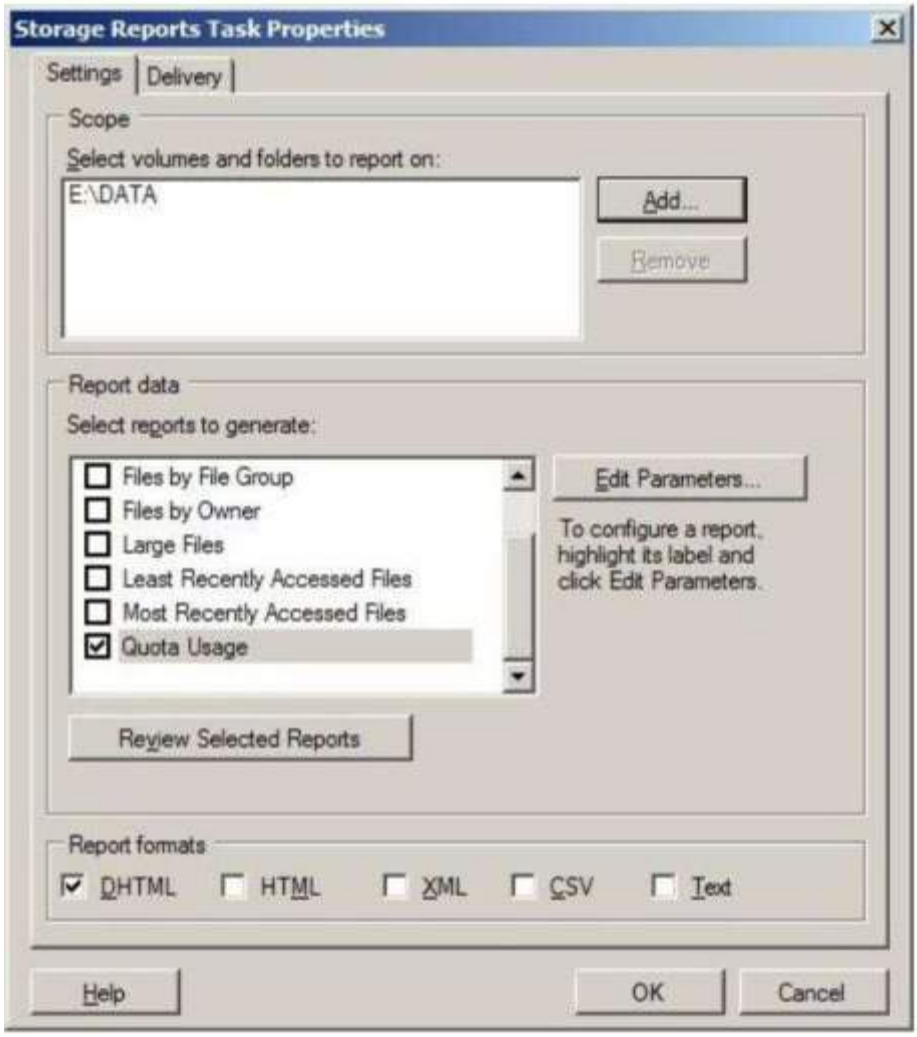


Рис.9. Задание параметров отчета.

ПРАКТИЧЕСКАЯ РАБОТА № 30.
АВТОНОМНЫЕ ФАЙЛЫ. СЛУЖБА DFS

Цель работы:
Научиться работать с автономными файлами.

Используемое программное обеспечение
Для выполнения данной лабораторной работы Вам понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1.

Автономные файлы
В ходе выполнения предыдущей работы мы разобрались, как можно подключить предоставленную в общий доступ папку в качестве сетевого диска. Но при настройках по умолчанию, как только пользователь отключится от сети, файлы на этом диске станут для него недоступны.

Задание. *Создайте на сервере папку и запишите в нее текстовый файл. Предоставьте папку в общий доступ, дайте все права на нее пользователю labos и подключите ее к рабочей станции в качестве сетевого диска (командой*

net use или из графического интерфейса). Откройте файл с рабочей станции (зайдя под учетной записью labos), внесите в него изменения, закройте файл. Отключите виртуальную машину от сети (Пуск->Панель управления -> Центр управления сетями и общим доступом-> Управление сетевыми подключениями) - рис.1. Убедитесь, что файлы с сетевого диска недоступны. Снова подключите виртуальную машину к сети.

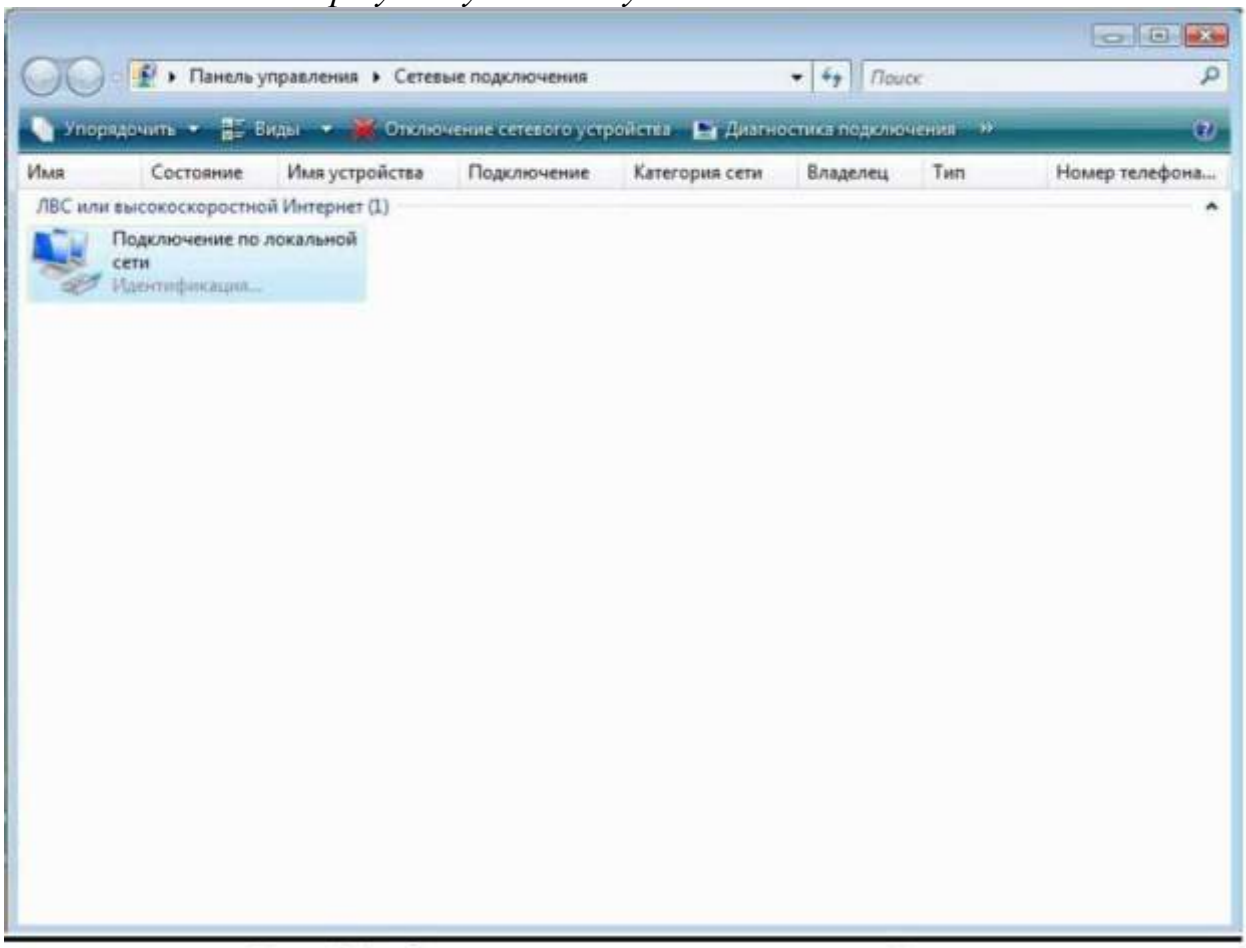


Рис.1. Отключение сетевого устройства.

Теперь на сервере посмотрим на свойства папки, предоставляемой в общий доступ. На вкладке Sharing нажмите кнопку Advanced Sharing и там кнопку Caching. Появится окно с настройками параметров кэширования (рис.2). При настройках по умолчанию, явно указанные пользователем файлы из предоставляемой в общий доступ папки будут ему доступны, когда он отключен от сети. Второй вариант – все открываемые файлы и папки будут доступны. Третий – кэширование отключено. Оставим настройку по умолчанию и разберемся, как же работает механизм кэширования файлов. Рис.2. Настройка параметров кэширования. Работа с так называемыми автономными файлами, организуется следующим образом. Если настройки на сервере и клиенте позволяют, выбранные файлы с сетевого диска записываются в локальный кэш (специальную область дискового пространства) на компьютере клиента и становятся ему доступны, даже если компьютер отключен от сети. С настройками на стороне сервера мы разобрались, теперь посмотрим, что можно настроить на клиенте.

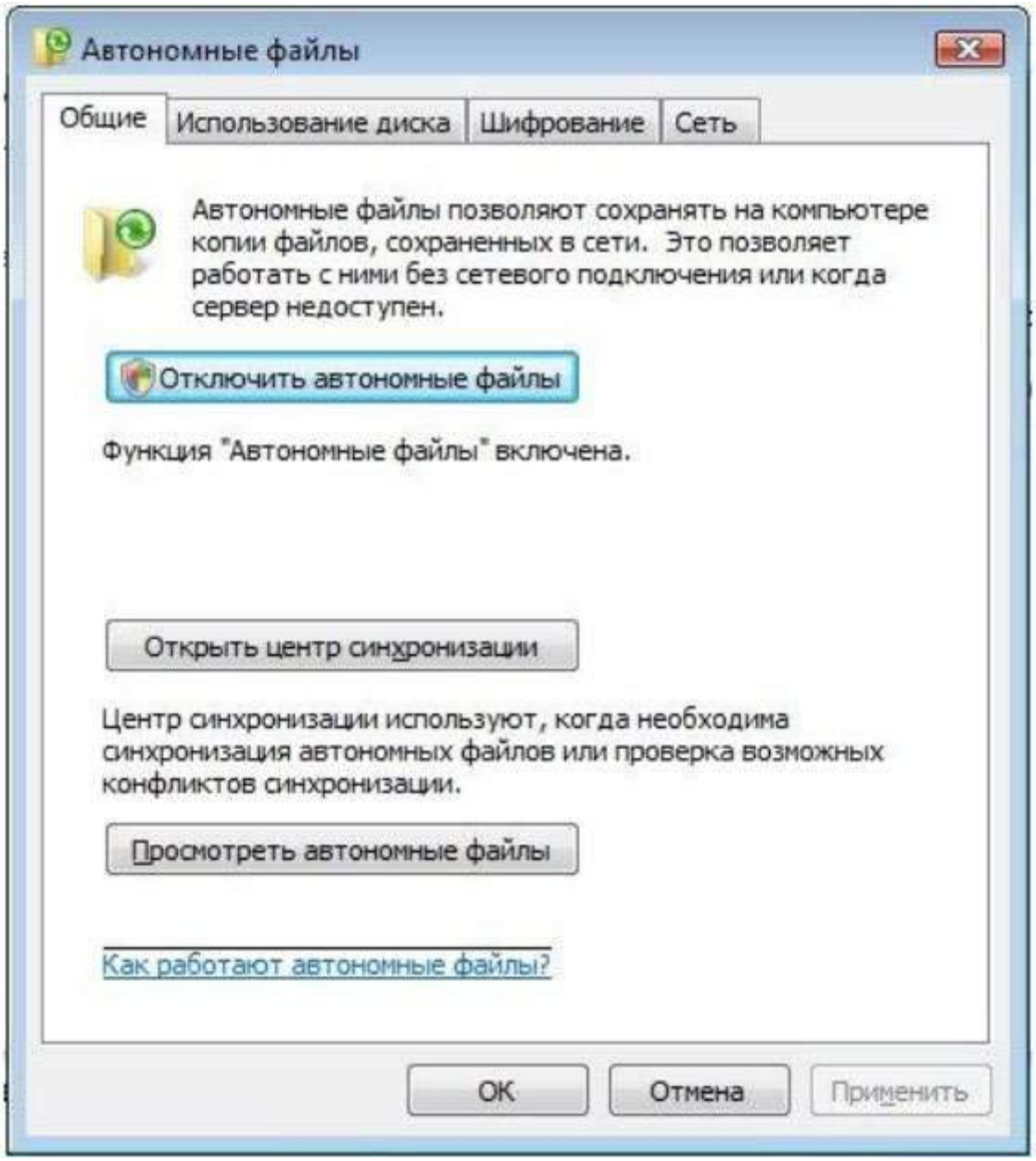


Рис.3. Настройка автономных файлов.

На виртуальной машине с Windows Vista откройте Панель управления и там Автономные файлы (рис.3). По умолчанию в Windows Vista поддержка автономных файлов включена (а в Windows Server 2008 – выключена, что логично, т.к. сервер – это не ноутбук, и его нечасто отключают от сети, чтобы работать на нем дома).

Задание. *На виртуальной машине с Windows Vista откройте подключенный сетевой диск. На нем создайте папку. Сделайте ее автономно доступной (по щелчку правой клавишей мыши выберите из контекстного меню «Всегда доступны в автономном режиме»). Поместите туда файлы. Как и в предыдущем случае, отключите виртуальную машину от сети. Убедитесь, что файлы из автономной папки доступны.Внесите в автономные файлы какие-нибудь изменения. Подключите сеть. В Панели управления откройте Центр синхронизации. Запустите вручную синхронизацию автономных фалов. Проверьте, что измененные файлы появились и на сервере. Посмотрите*

вариант настройки синхронизации автономных файлов по расписанию (в частности – по событиям, таким как вход в систему и т.п.) **DFS** Служба DFS позволяет создать общую иерархию файловых ресурсов, предоставляемых в общий доступ несколькими серверами. При этом пользователь будет работать с логическим путем вида <имя сервера>\<корень DFS>\<папка> или <имя домена>\<корень DFS>\<папка> вне зависимости от того, на каком сервере физически находится данная папка. Более того, в целях повышения отказоустойчивости, синхронизируемые копии одной и той же папки (реплики) могут находиться на нескольких серверах. Для начала, проверим в Server Manager список служб роли File Services и при необходимости добавим в него Distributed File Services.

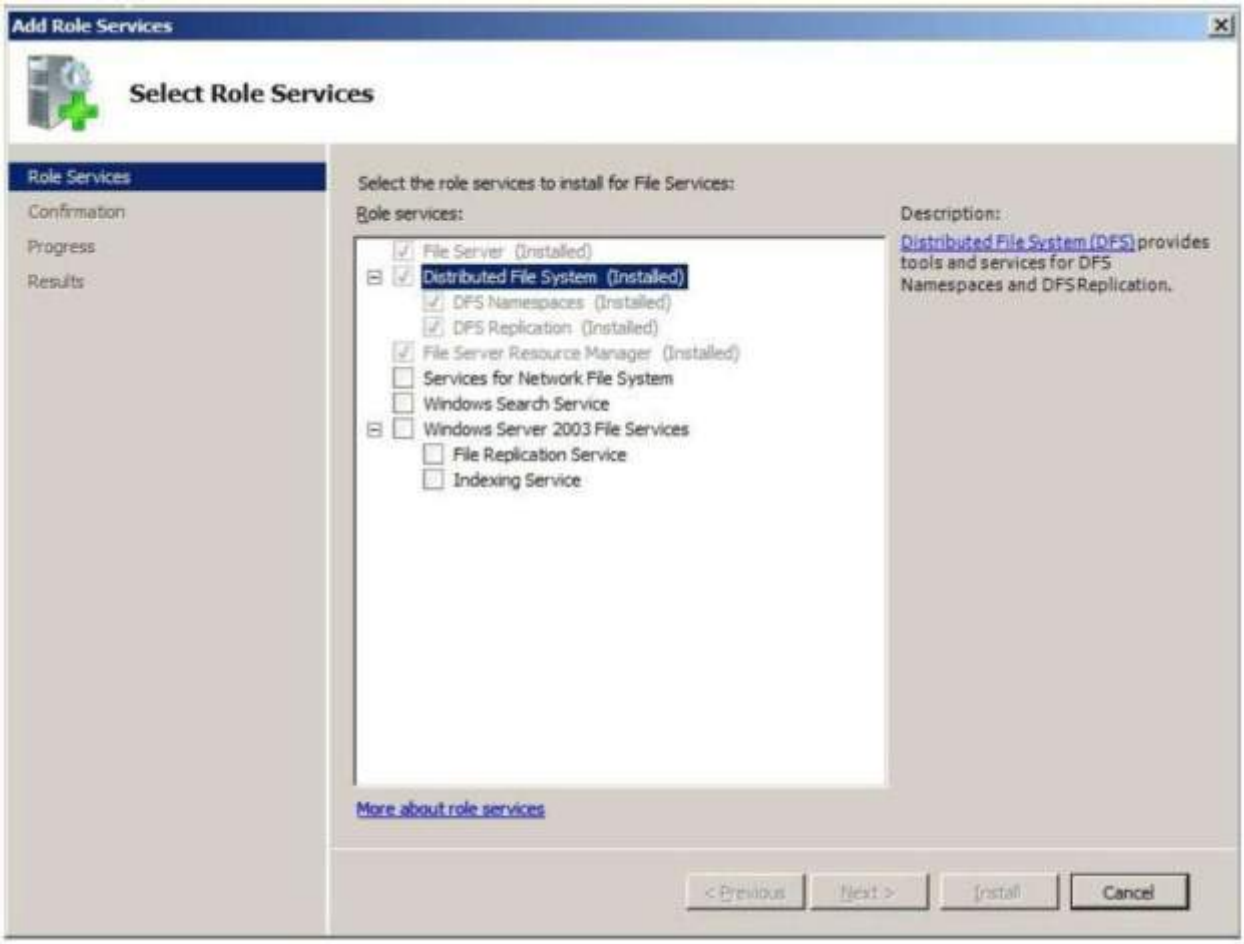


Рис.4. Роли служб File Services.

После этого надо создать новое пространство имен DFS (namespace) или как его еще называют, корень DFS. Это можно сделать в процессе установки службы (будет запущен соответствующий мастер), а если DFS уже была установлена, то можно воспользоваться оснасткой DFS Management (рис.5) из меню Administrative Tools. В ней надо открыть узел Namespaces и выбрать ссылку New namespace… Окна мастера создания нового корня DFS представлены на рисунках 6.-8. Нужно последовательно выбрать имя сервера, название для корня DFS (рис.7, при этом будет создана и предоставлена в общий доступ папка, расположение и разрешения для которой можно просмотреть, нажав кнопку Edit Settings), его тип – основанный на домене (domain-based) или

отдельно стоящий (stand-alone). Выберем второй тип, в этом случае, имена ресурсов будут иметь вид <имя сервера>\<корень DFS>\<папка>. Если выбрать тип Domain-based namespace, то пространство имен будет вида <имя домена>\<корень DFS>\<папка>. Когда пространство имен создано, в него можно добавлять папку (ссылка New Folder в окне администрирования корня DFS – рис.6.9). При этом надо указать, как будет называться папка в логическом пространстве имен DFS и какой предоставляемой в общий доступ физической папке это имя соответствует (рис.10).

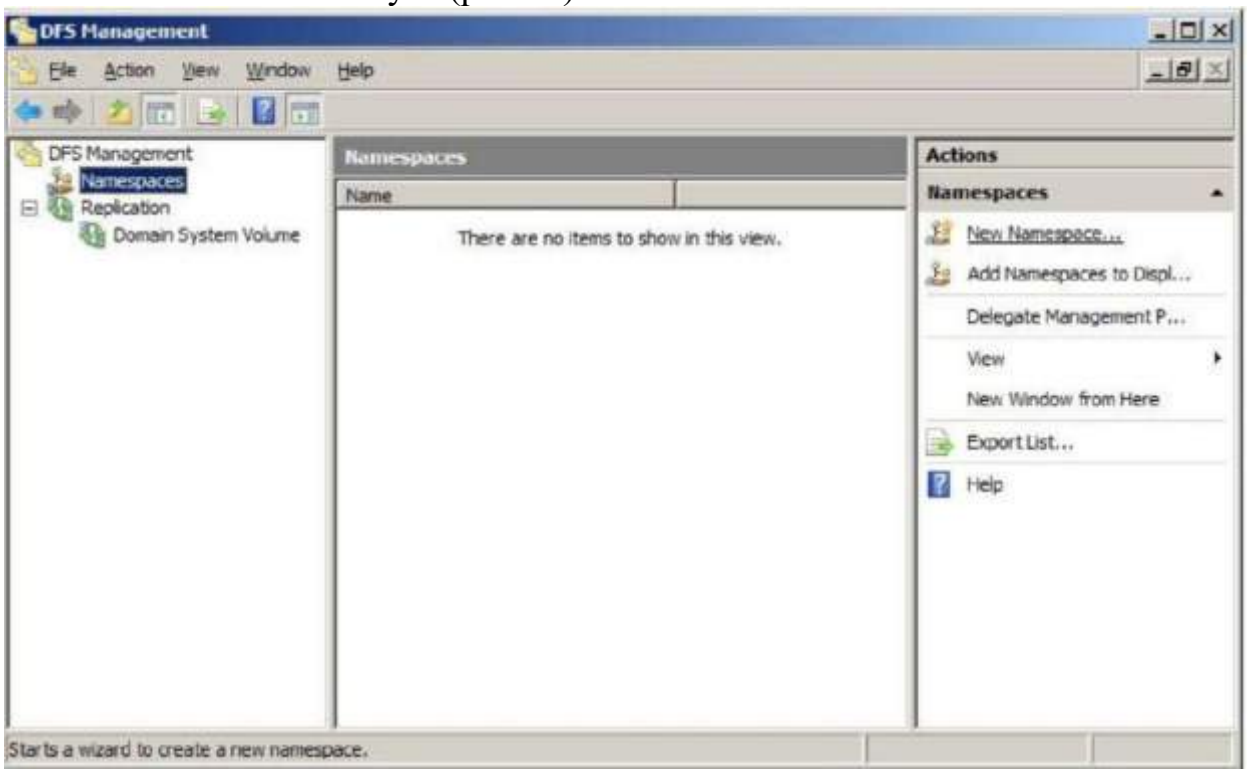


Рис.5. Окно оснастки DFS Management.

Задание. *На сервере создайте корень DFS. В нем создайте папку, указывающую на ранее созданную общую папку с файлами. Проверьте доступ к ней с рабочей станции по пути, использующему пространство имен DFS (например, Пуск, \\S08\Files\test1 для пространства имен Files на сервере S08). В оснастке DFS Management измените путь к папке в пространстве имен DFS (ссылка Move Folder). Например, чтобы новый путь был \\S08\Files\test2\test1. Проверьте ее доступность по новому пути. Этот пример показывает еще одну удобную возможность, предоставляемую DFS – можно группировать ресурсы, независимо от их физического размещения.*

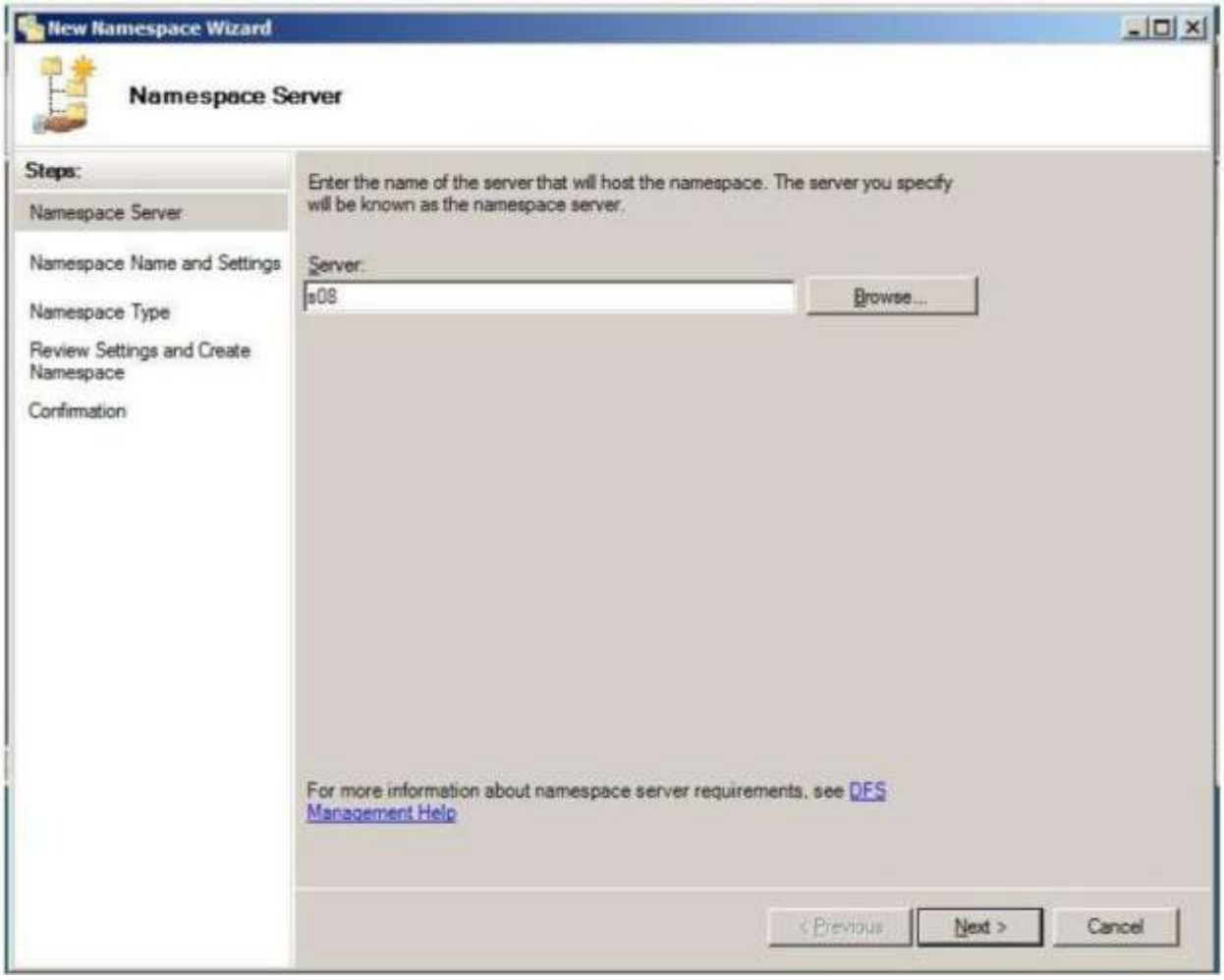


Рис.6. Создание нового корня (пространства имен) DFS. Выбор сервера.

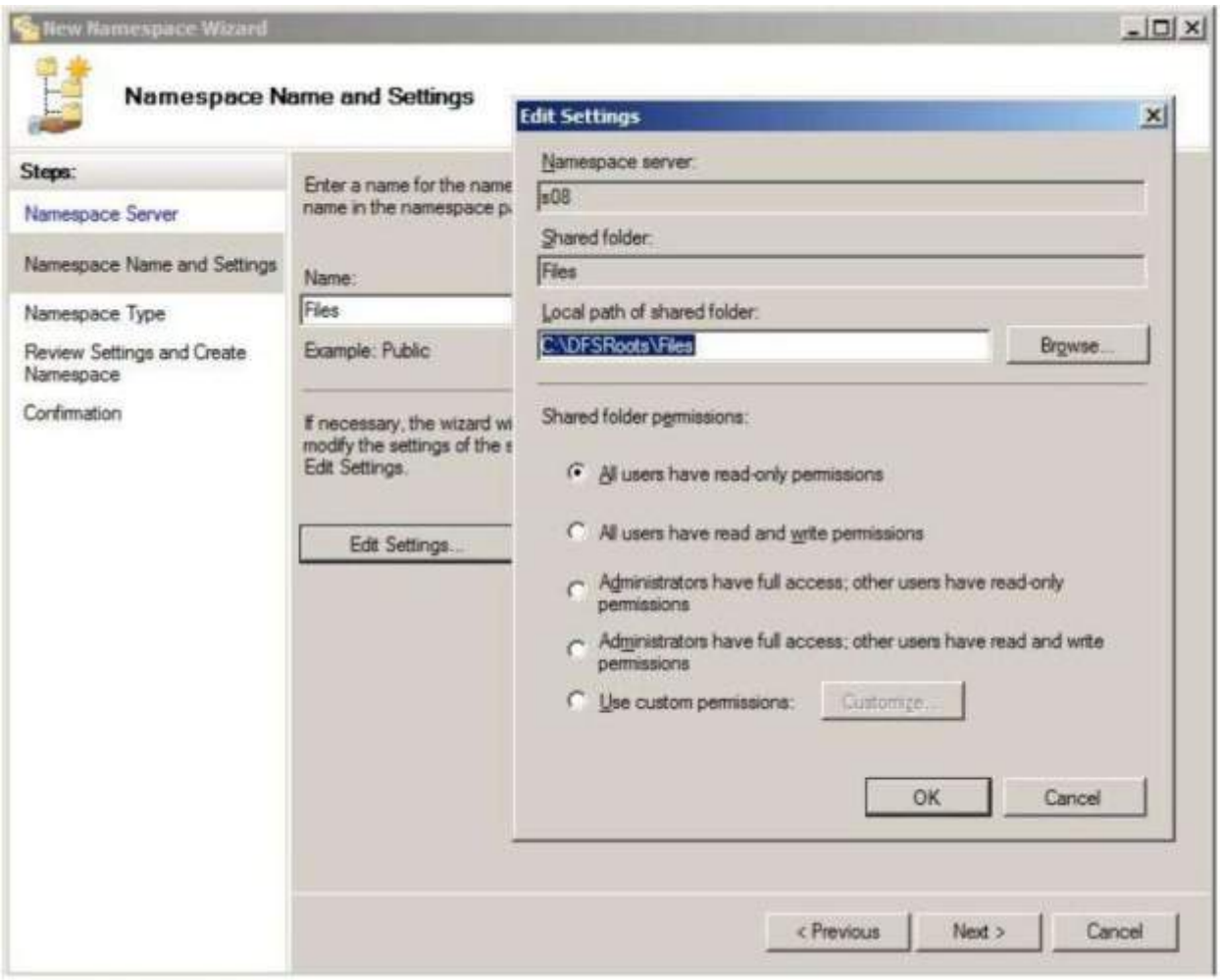


Рис.7. Создание нового корня DFS. Задание имени и разрешений.

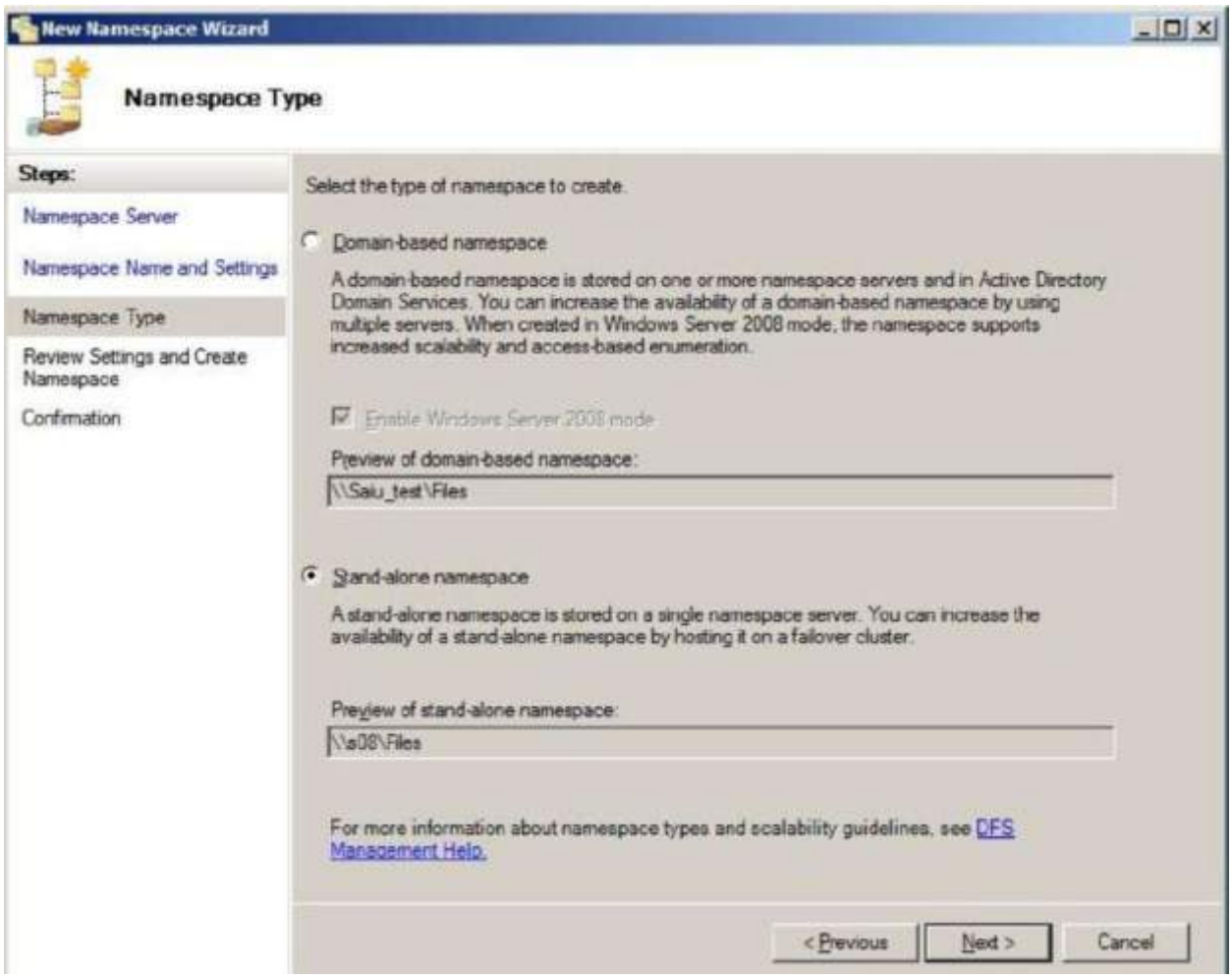


Рис.8. Создание нового корня DFS. Выбор типа

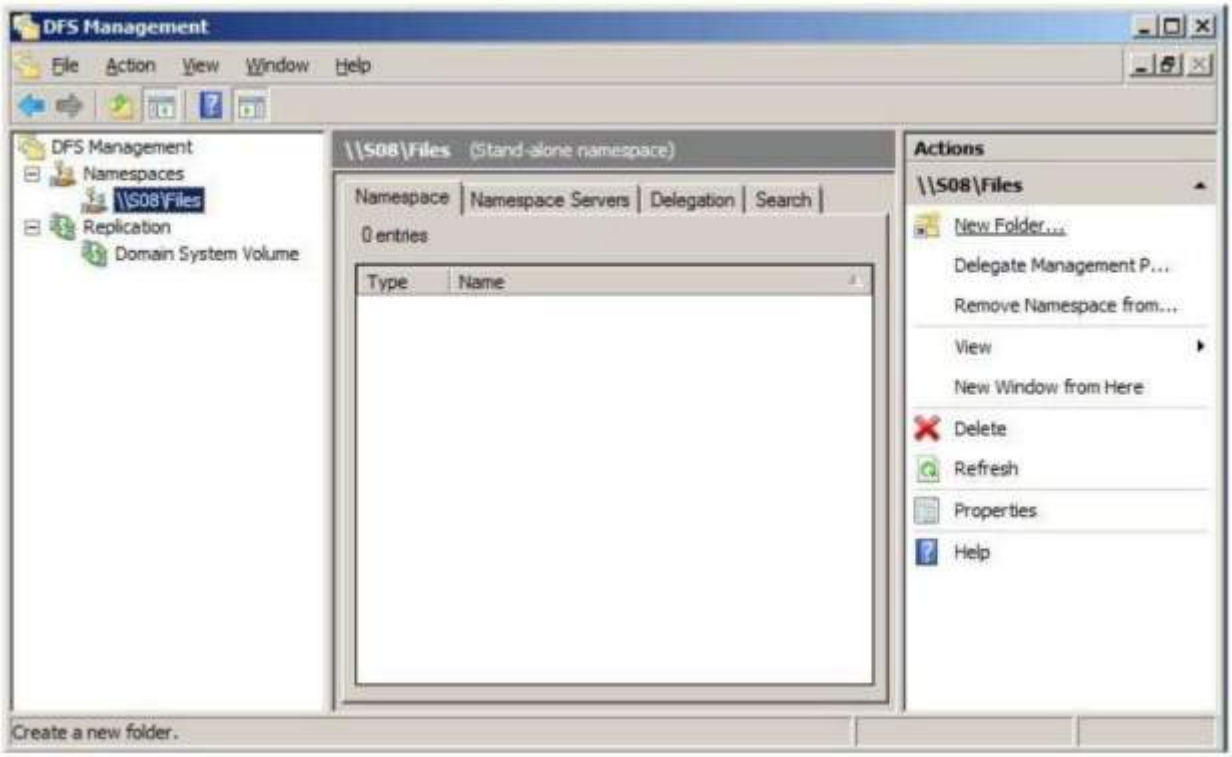


Рис. 9. Просмотр папок в данном корне.

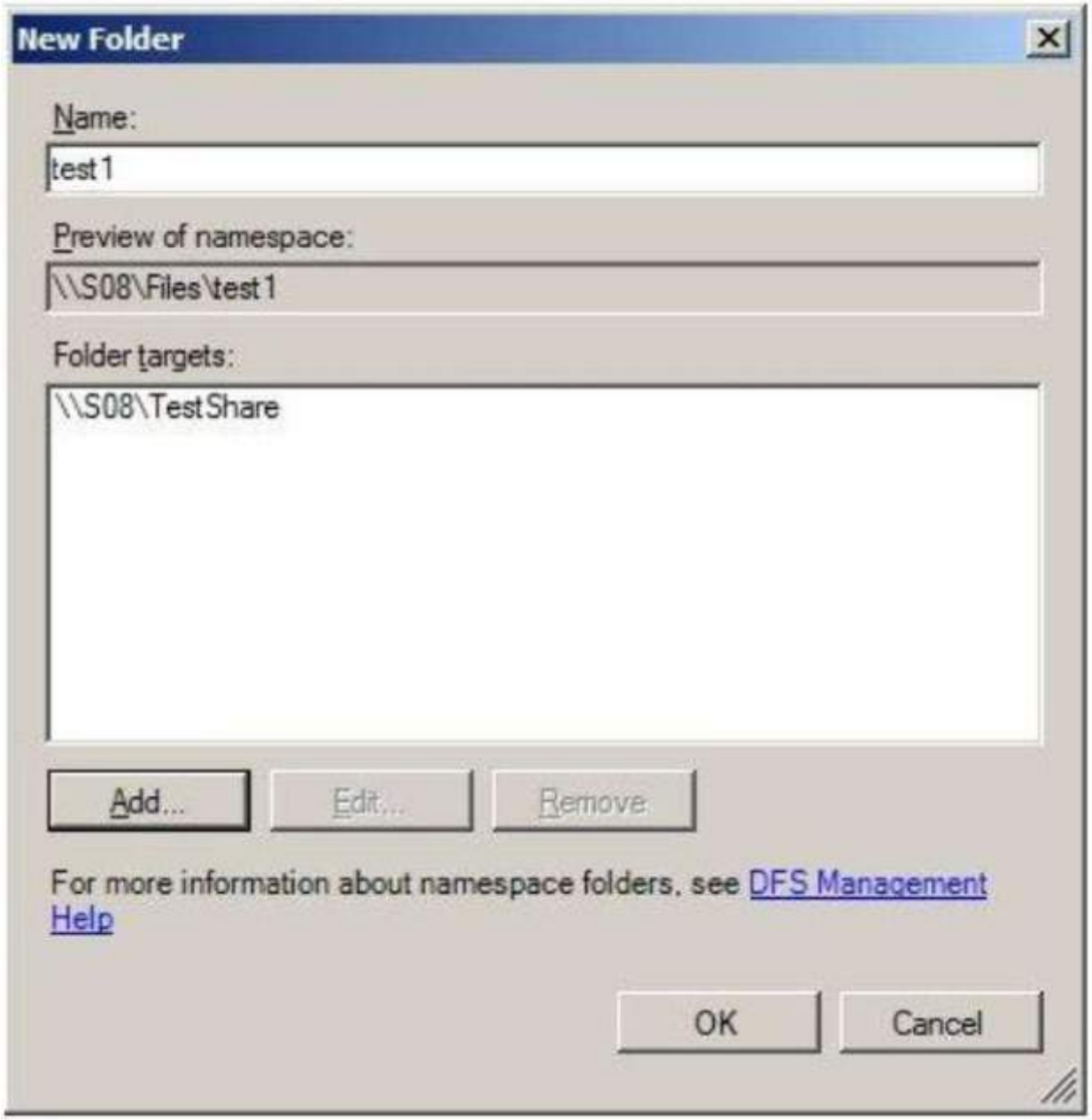


Рис. 10. Добавление новой папки.

ПРАКТИЧЕСКАЯ РАБОТА № 31.
НАСТРОЙКА DNS И DHCP.

Цель работы:
Научиться выполнять настройку DNS И DHCP.

Используемое программное обеспечение
Для выполнения данной лабораторной работы Вам понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или **Vista и** установленным программным обеспечением Microsoft Virtual PC 2007 SP1. А также 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista. **DNS сервер** Во второй лабораторной работе мы уже установили DNS сервер. **DNS** — это система именования (и поддерживающие ее службы)

компьютеров и сетевых служб, которая сопоставляет имена компьютеров и сетевые адреса, организуя их в доменную иерархическую структуру. Система именования DNS используется в сетях TCP/IP, например, в интернете и в большинстве корпоративных сетей, для поиска компьютеров и служб по понятным именам. Когда пользователь вводит DNS-имя компьютера в приложении, DNS находит имя компьютера и другую связанную с ним информацию, например его IP-адрес или службы, которые он предоставляет в сети. Этот процесс называется разрешением имен. DNS находит имена компьютеров и служб и сопоставляет их с числовым адресом, который требуется операционным системам и приложениям для идентификации компьютера в сети. Служба доменных имен — это главный метод разрешения имен в Windows Server. При использовании DNS необходимо развертывание роли сервера доменных служб ActiveDirectory.

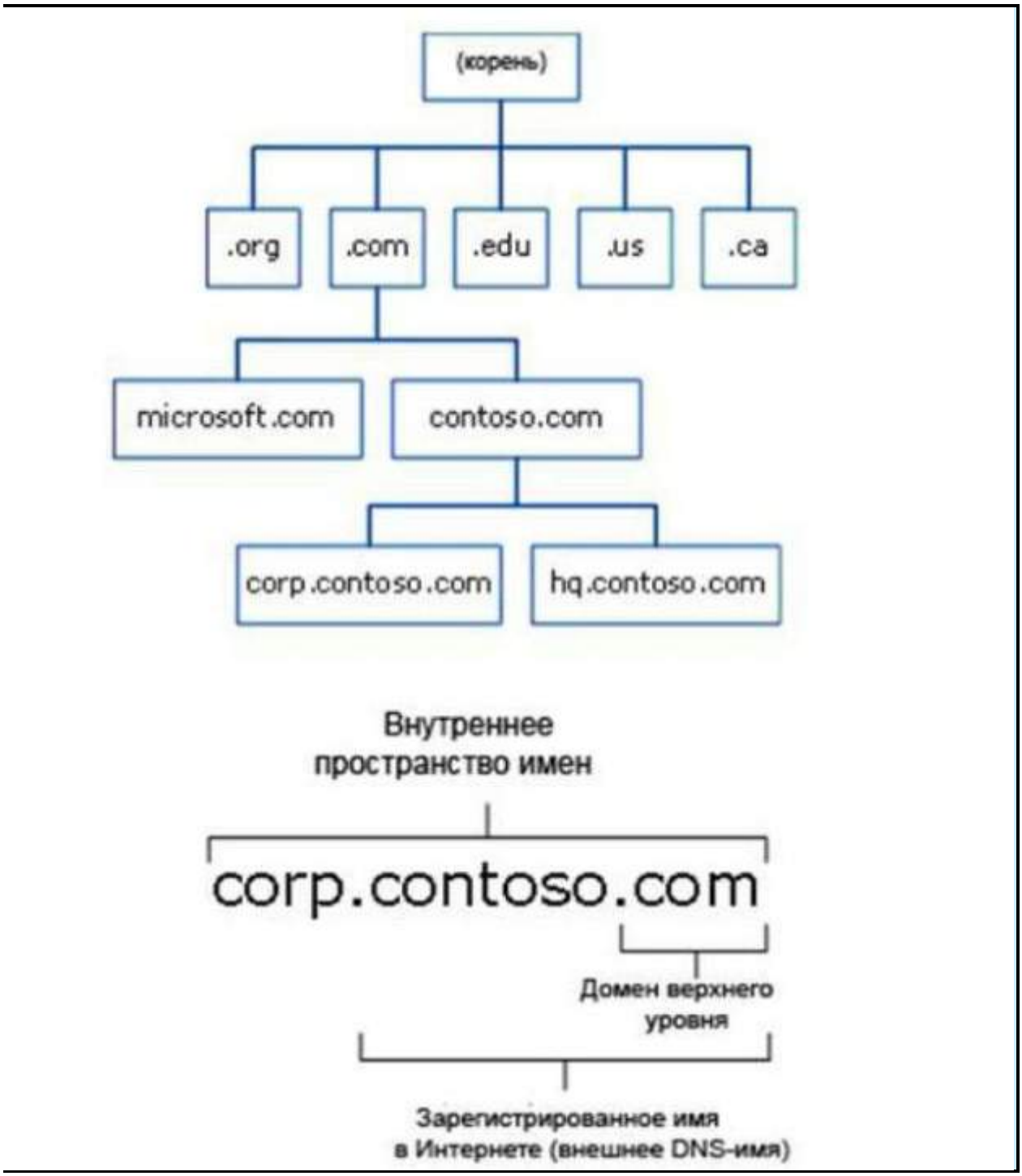


Рис.1. Организация пространства имен DNS.

Имя DNS состоит из двух или более частей, разделенных точками (.). Последняя часть имени (справа) называется доменом верхнего уровня (TLD – top-level domain). Другие части имени — это дочерние домены домена верхнего уровня или другого дочернего домена. Имена TLD бывают функциональными или географическими. Дочерние домены, как правило, указывают на организацию, владеющую доменным именем.

Обратный DNS-запрос

Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP адресу — IP адрес по таблице соответствия преобразуется в доменное имя, и посылается запрос на информацию типа PTR.

Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен in-addr.arpa, записи в котором используются для преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса 11.22.33.44 можно запросить у DNS-сервера запись 44.33.22.11.inaddr.arpa, и тот вернѐт соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие октеты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце. При запросе осуществляется считывание записи PTR, содержащей искомое доменное имя. Если запись отсутствует, то IP-адрес считается не имеющим обратного DNS. DNS-запись in-addr.arpa выглядит так:
78.56.34.12.in-addr.arpa. IN PTR domain.ltd.
Это будет означать, что имени хоста domain.ltd соответствует IP-адрес 12.34.56.78.

Понятие записей ресурсов

Объекты в иерархии DNS идентифицируются с помощью *записей ресурсов (Resource Record)*. Они используются для выполнения основных операций поиска пользователей и ресурсов внутри указанного домена и уникальны для содержащего их домена. Рассмотрим некоторые типы записей.

1. *Начальная запись зоны SOA (Start of Authority)*. Указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону, тайминги кеширования зонной информации и взаимодействия DNS-серверов.
2. *Записи хостов (записи A, Address Record).* Наиболее часто встречающийся тип записей ресурсов. Содержит имя хоста и соответствующий ему IP-адрес.
3. *Записи сервера имен (Name Server – NS).* Указывают, какие компьютеры в базе данных DNS являются серверами имен – то есть DNS-серверами для конкретной зоны. Для каждой зоны может существовать только одна запись типа SOA, но может быть несколько NS – записей.
4. *Запись AAAA (IPv6 address record)* связывает имя хоста с адресом протокола IPv6.
5. *Запись CNAME (canonical name record)* или *каноническая запись имени* позволяет присваивать хосту мнемонические имена. Мнемонические имена, или псевдонимы, широко применяются для связывания с хостом какой-либо функции, либо просто для сокращения имени.
6. *Запись MX (mail exchange)* определяет почтовый сервер - машину, которая обрабатывает почту для данного домена.
7. *Запись SRV (server selection)* используется для поиска серверов, обеспечивающих работу тех или иных служб в данном домене.
8. *Запись PTR (pointer)* или *запись указателя* связывает IP хоста с его каноническим именем.

Понятие зоны

Зона логический узел в дереве имѐн.

Рассмотрим различные типы зон в DNS.

Зона прямого просмотра (forward lookup zone) создается в DNS по умолчанию во время установки. Она необходима для преобразования доменного имени в IP-адрес и информацию о ресурсах. Большинство записей в прямой зоне типа A. В дополнение к зоне прямого просмотра мы в этой лабораторной работе создадим *зону обратного просмотра (reverse lookup zone)*, которая реализует обратный DNSзапрос. Развертывание зоны обратного просмотра обычно улучшает производительность DNS и существенно повышает успешность DNS-запросов. Зона обратного просмотра состоит почти целиком из записей типа PTR (Pointer).

Первичная зона (Primary zone). В DNS (без интегрированной Active Directory) один сервер служит первичным DNS – сервером зоны, и все изменения, выполняемые в данной зоне, выполняются на этом конкретном сервере. Один DNS – сервер может содержать несколько зон, будучи первичным для одной зоны и вторичным для другой. Однако если зона является первичной, все запрошенные изменения для данной зоны должны выполняться на сервере, содержащим основную копию зоны.

Вторичная зона (Secondary zone) создается для обеспечения резервирования и разгрузки первичной зоны. Однако каждая копия базы данных DNS доступна только для чтения, т.к. все модификации записей выполняются в первичной зоне. Один сервер DNS может содержать несколько первичных и вторичных зон.

Зона-заглушки (Stub zone) представляет собой зону, которая не содержит никакой информации о членах домена, а служит только для переадресации запросов к списку назначенных серверов имен для различных доменов. Поэтому она содержит только записи NS, SOA и связанные записи (glue records – записи A, которые используются в сочетании с конкретной записью NS для преобразования IP-адреса конкретного сервера имен). Сервер, содержащий зону-заглушку какого-либо пространства имен, не управляет зоной. Она используется для ускорения работы. Для выполнения данной лабораторной работы необходимо будет задействовать рабочую станцию и сервер. На рабочую станцию заходим под пользователем labos (пароль Lab0s123). На сервере с помощью оснастки DNS Manager (Start-> Administrative Tools-> DNS Manager) можно посмотреть, какие типы записей были созданы при установке DNS, а также убедиться в том, что по умолчанию была создана зона прямого просмотра. Для этого нужно щелкнуть по нашему серверу S08, далее выбрать папку Forward Lookup Zones (зоны прямого просмотра), а там выбрать домен Saiu_test

(рис. 2). Примечание: в примерах данной работы используется IP-адрес для сервера и рабочей станции, как и в предыдущих лабораторных работах: 192.168.1уу.1 и 192.168.1уу.2, где уу – номер компьютера. В данном случае, номер компьютера равен 14 и в последующих примерах везде будет использоваться именно он.

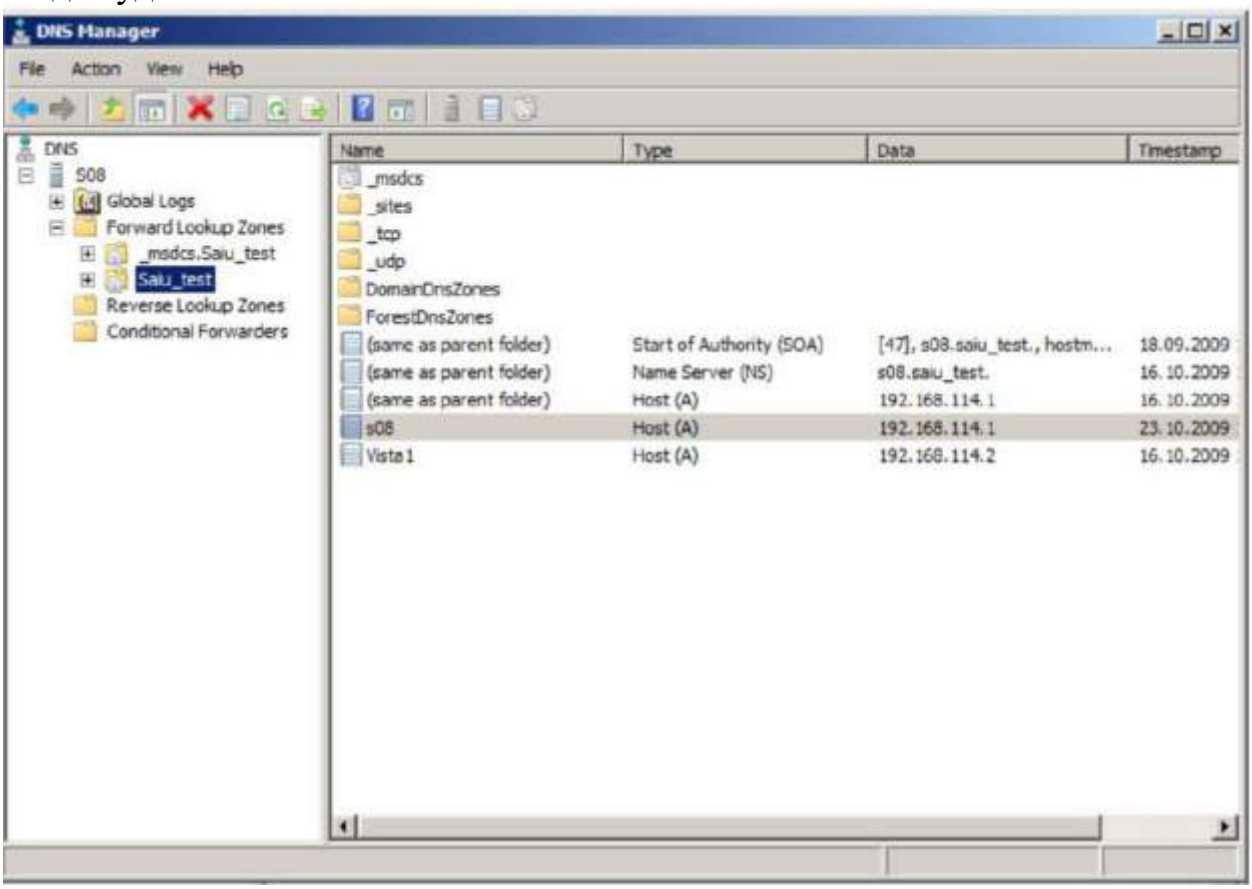


Рис.2. Просмотр записей и зон DNS.

Как видим, были созданы начальная запись зоны (SOA), записи хостов (A) и запись сервера имен (NS). На рабочей станции воспользуемся командой nslookup (name server lookup - поиск на сервере имѐн), которая предоставляет пользователю интерфейс командной строки для обращения к системе DNS, а также позволяет задавать различные типы запросов и запрашивать произвольно указываемые сервера (рис.3). В ответ на приглашение «>» можно ввести имя нашего виртуального сервера – s08.saiu_test и получить его ip-адрес – 192.168.114.1. Если ввести ip-адрес, то в имя он не разрешится.

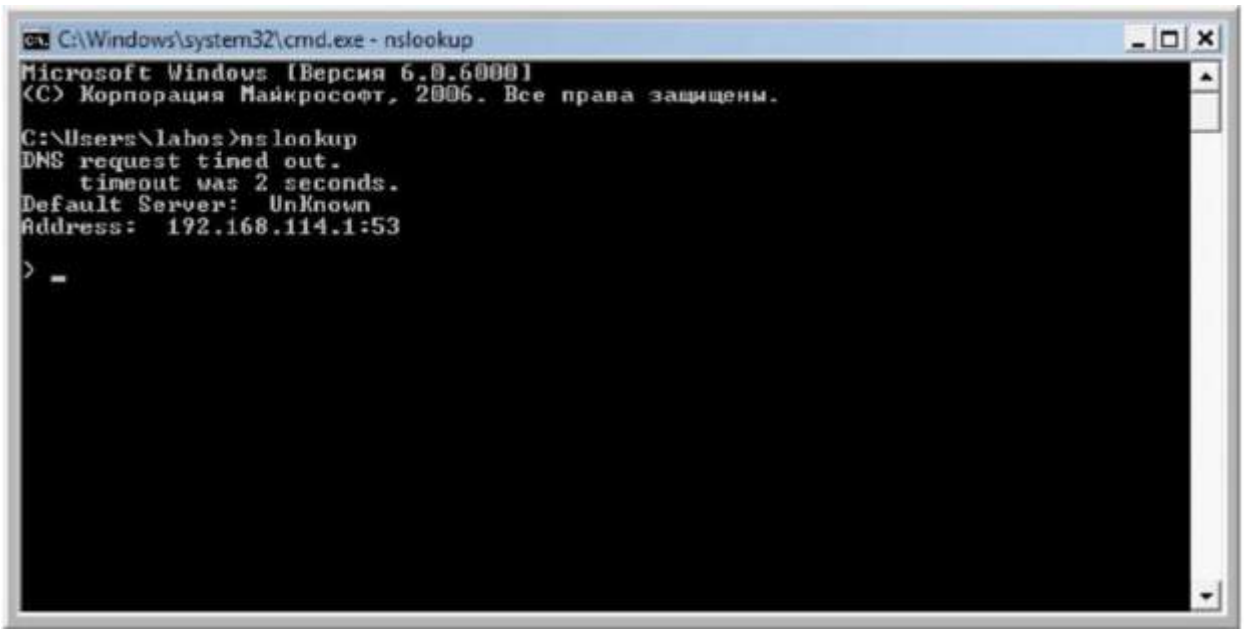


Рис. 3. Пример работы команды nslookup.

Данный пример подтверждает, что на сервере есть зона прямого просмотра (IP-адрес определяется правильно - Address: 192.168.114.1). Но на нет зоны обратного просмотра или в ней для искомого адреса, т.е. для него не создана запись (это можно также проверить на сервере, посмотрев в оснастке DNS папку Reverse Lookup Zones). Создадим псевдоним (запись CNAME), чтобы рабочая станция смогла обратиться к серверу и по альтернативному имени. Например, мы планируем на сервере s08 организовать web-сервер, и хотим, чтобы к нему можно было обратиться www.saiu_test. Для этого на оснастке DNS Manager правой кнопкой мыши щелкаем по домену Saiu_test и из списка выбираем New Alias (CNAME)… (рис. 4). Задаем имя псевдонима www и хост s08.Saiu_test.

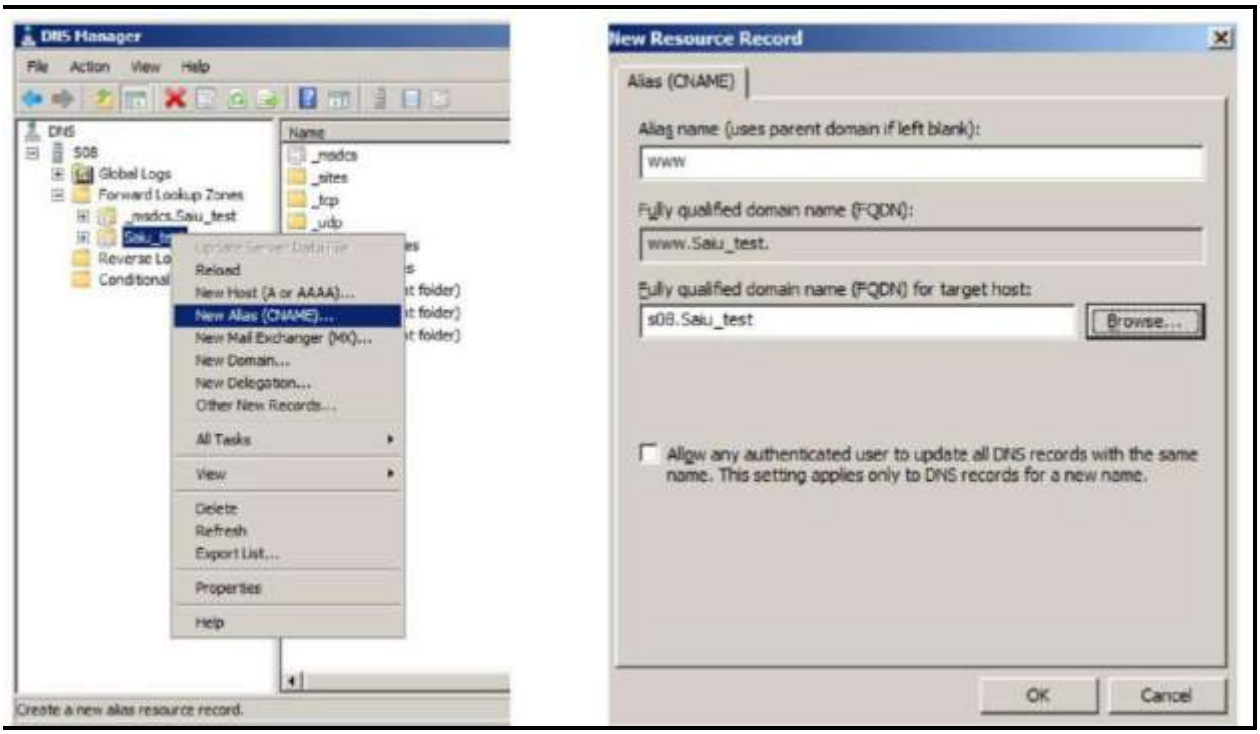
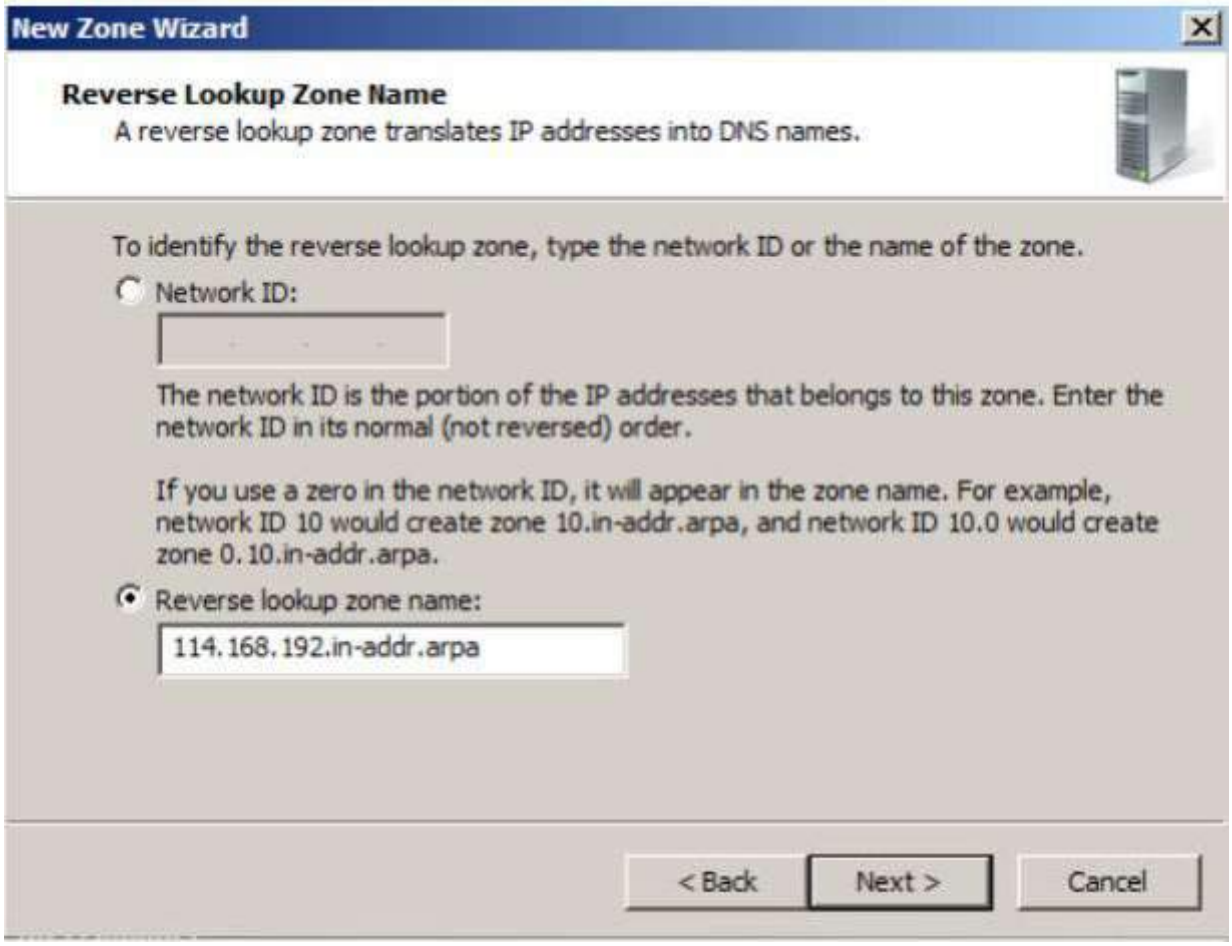


Рис.4. Создание псевдонима записи типа CNAME.

Теперь в списке записей прямой зоны появилась запись типа CNAME с именем www. На рабочей станции теперь можно проверить доступность псевдонима www.saiu_test с помощью команды nslookup www.saiu_test. Теперь настроим обратное разрешение имен. Для этого понадобится создать обратную зону. В DNS Manager на вкладке Action выбираем New Zone… Создаем Reverse Lookup Zone и изменяем только: имя во вкладке Reverse Lookup Zone Name на 114.168.192.inaddr.arpa (рис.7.5) для сети 192.168.114.0 (или другое имя при использовании другого адреса сети). И при вопросе о Dynamic Update выбираем Allow only secure dynamic updates (разрешить только безопасные динамические обновления). Теперь в папке обратных зон появилась новая обратная зона с заданным именем. Но рабочая станция все равно не может получить имя сервера, поскольку не создана запись указателя (PTR), связывающая IP хоста с его каноническим именем. Для этого на сервере выполняем команду ipconfig с ключом /registerdns (рис.6). Прим.В операционных системах Microsoft Windows ipconfig — это утилита командной строки для вывода деталей текущего соединения и управления клиентскими сервисами DHCP и DNS. Утилита ipconfig позволяет определять, какие значения конфигурации были получены с помощью DHCP, APIPA или другой службы IPконфигурирования либо заданы администратором вручную.


New Zone Wizard
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone.
Network ID:
The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.
If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.
Reverse lookup zone name:
114.168.192.in-addr.arpa
< Back
Next >
Cancel

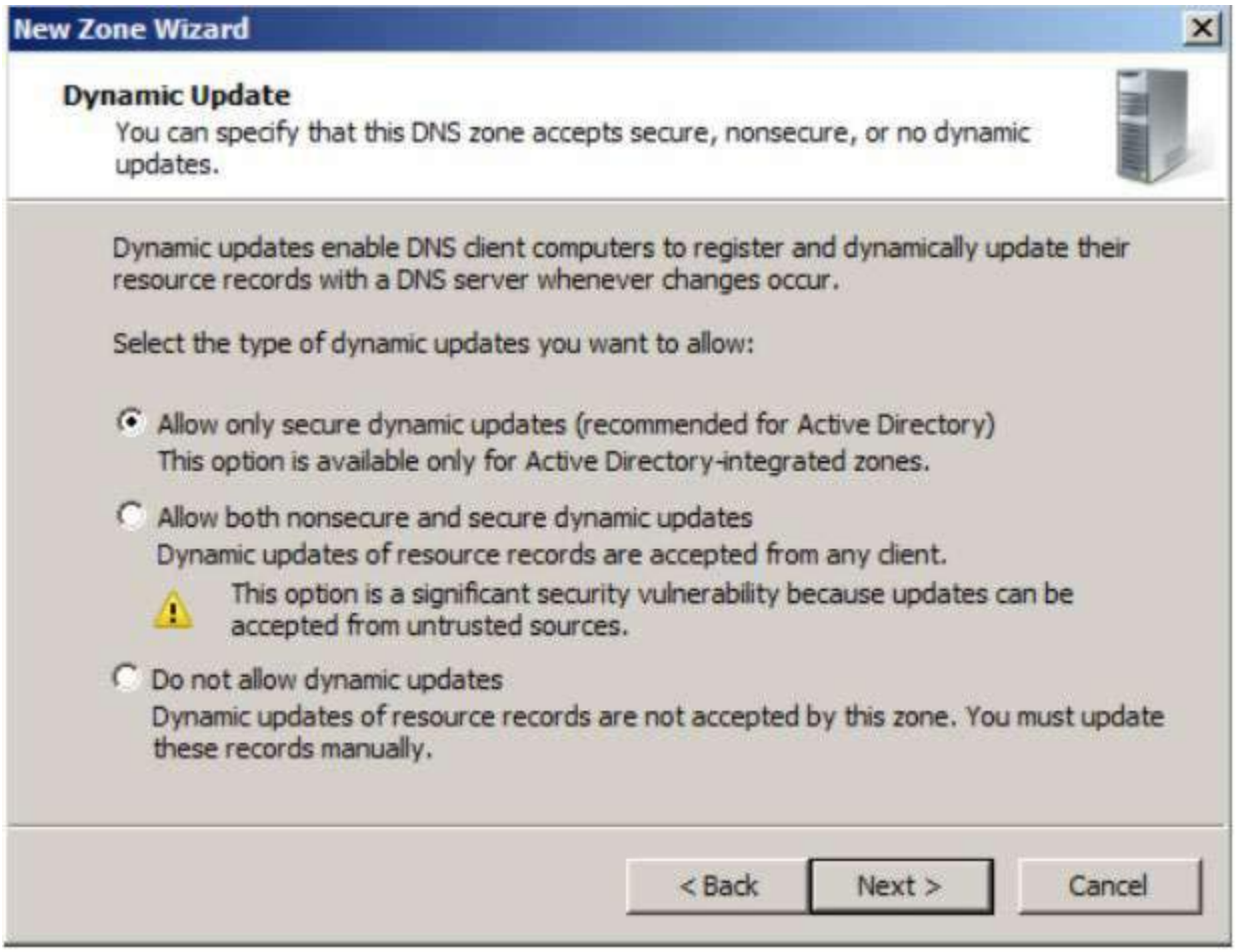


Рис.5. Создание обратной зоны

Ключи команды ipconfig.

Ключ	**Описание**
/all	Отображение полной информации по всем адаптерам.
/release адаптер]	Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан) или для заданного адаптера. Этот ключ отключает протокол

	TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.
/renew [адаптер]	Обновление IP-адреса для определѐнного адаптера или если адаптер не задан, то для всех. Доступно только при настроенном автоматическим получением IP-адресов.
/flushdns	Очищение DNS кэша.
/registerdns	Команда обновления регистрации DNS-клиента
/displaydns	Отображение содержимого кэша DNS.
/showclassid адаптер	Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическим получением

IP-адресов.	
/setclassid адаптер [код_класса]	Изменение кода класса DHCP. Доступно только при настроенном автоматическим получением IP-адресов.
/?	Справка.

Рис.6. Обновление регистрации DNS-клиента.

Выполнив эту команду на сервере и клиентской станции, можно проверить, что в обратной зоне появились две новые записи типа PTR (рис.7), которые позволяют по ip-адресу узнать имя. Их также можно было создать и в оснастке DNS. В частности, теперь команда nslookup, введенная на рабочей станции, показывает не только IP-адрес сервера DNS (как было на рис.7.3), но и его имя - s08.saiu_test.

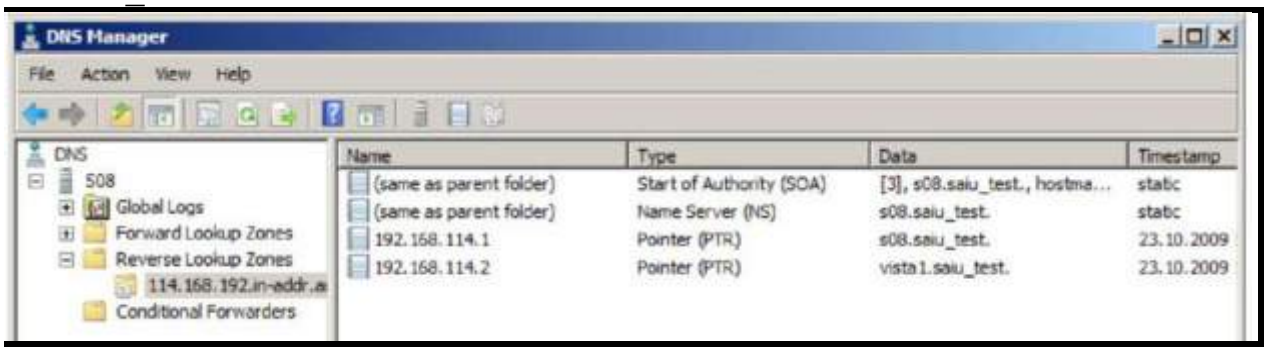


Рис.7. Записи типа PTR:192.168.114.1 – IP-адрес сервера, 192.168.114.2 – IP-адрес рабочей станции.

Добавление роли DHCP

DHCP (*Dynamic Host Configuration Protocol* — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IPадрес и другие параметры, необходимые для работы в сети TCP/IP. Для автоматической конфигурации компьютер-клиент на этапе конфигурации сетевого устройства обращается к *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. Для использования протокола TCP/IP в сети администратор должен задать для каждого из компьютеров по меньшей мере три параметра - IP-адрес, маску подсети и адрес используемого по умолчанию шлюза. При этом, каждый компьютер должен иметь уникальный IP-адрес. Кроме того, присвоенный адрес должен находиться в диапазоне подсети, к которой подключено устройство. В большой сети иногда бывает трудно определить, к какой же из подсетей подключен тот или иной компьютер. Однако DHCP-сервер "знает", из какой подсети приходит запрос на получение IP-адреса, и назначит клиенту правильный адрес. Если в сети используются Windows Internet Naming Service (WINS) и Domain Name Service (DNS), то IP-адреса WINS и DNSсерверов также

может указывать DHCP-сервер. Установим и сконфигурируем DHCP-сервер. На сервере S08 из оснастки Server Manager добавляем роль DHCP. На вкладке DHCP Scopes добавляем адреса, которые могут быть использованы. Пусть, например,распределяемые адреса будут начинаться с адреса 192.168.114.2 и заканчиваться адресом 192.168.114.100, а назовем мы эту группу адресов «192.168.114.1» (по адресу сервера). Задаем маску и шлюз соответственно: 255.255.255.0 и 192.168.114.1. Активируем этот набор адресов (рис.8).

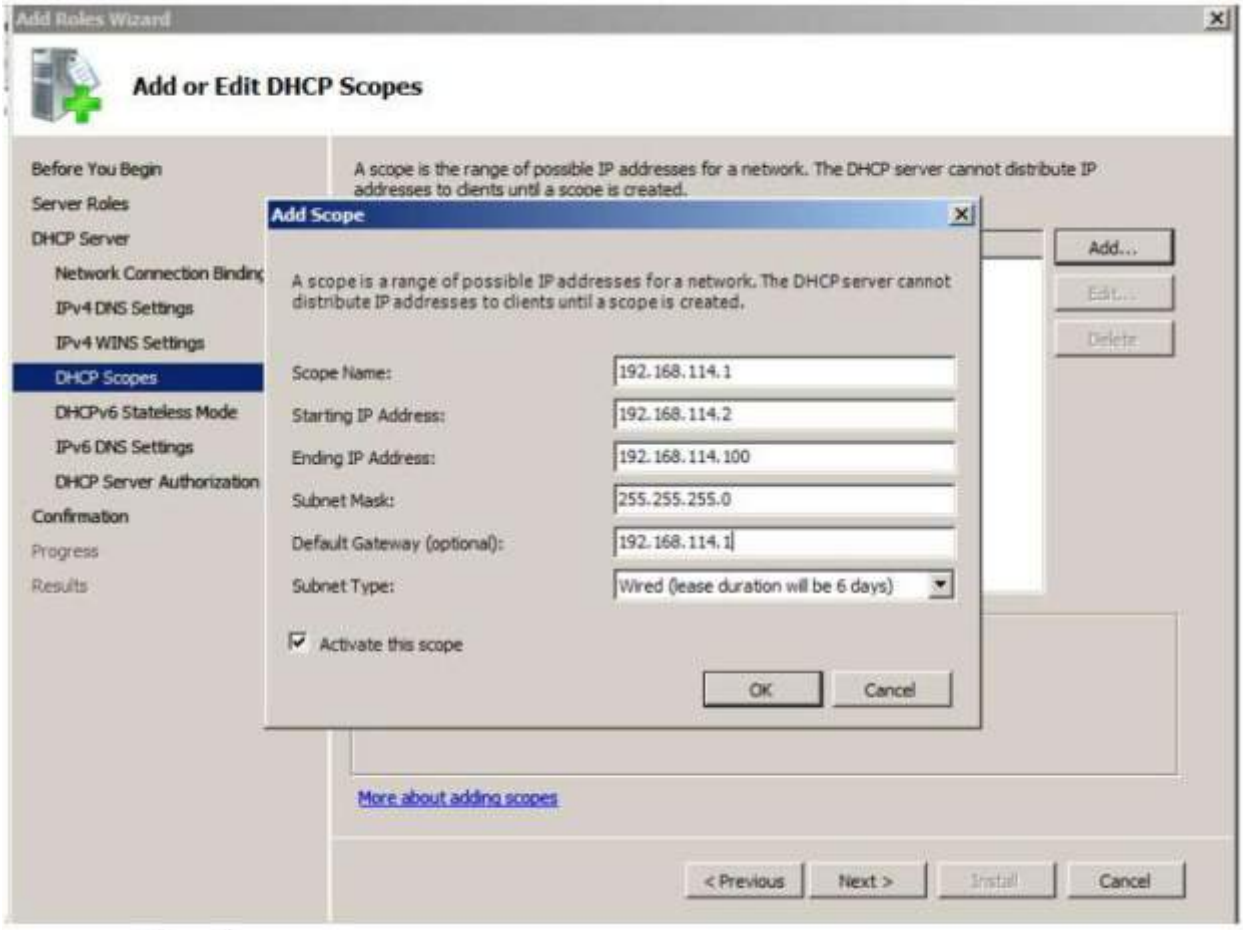


Рис.8. Конфигурирование DHCP-сервера в процессе установки.

Рис.9. Отчет об установке роли DHCP.

Далее продолжаем установку так, чтобы получились параметры, аналогичные представленным на рис.9. Когда роль DHCP на сервере установлена, на рабочей станции нужно сделать так, чтобы получать IP-адрес и DNS автоматически, а не прописывать их вручную. Это указывается в настройках протокола TCP/IP v.4 в свойствах сетевого интерфейса. Сделаем подобную настройку и протестируем ее работу. Можно поменять параметры пула раздаваемых адресов с помощью оснастки Server Manager, где выбираем роль DHCP, и, находя там вкладку Scopes, меняем, например, начальный IP-адрес, на 192.168.114.10. 53

ПРАКТИЧЕСКАЯ РАБОТА №32.
СЛУЖБЫ INTERNET INFORMATION SERVICES (IIS 7.0). УСТАНОВКА И ОСНОВЫ АДМИНИСТРИРОВАНИЯ WEB- И FTP-СЕРВЕРА

Цель работы:

Научиться выполнять установку и администрирование WEB и FTP сервера.

Используемое программное обеспечение

Для выполнения данной лабораторной работы Вам понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1 и 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista. В ходе работы на виртуальной машине с Windows Server 2008 будет организован web- и ftp-сервер.

Настройка параметров сети для виртуальных машин

В ходе предыдущей лабораторной работы мы изменяли настройки сетевых параметров на виртуальной машине с Windows Vista для использования DHCP сервера. Поэтому после загрузки виртуальной машины проверьте, получила ли она настройки вообще и правильные ли они. Это можно сделать, например, выполнив команду ipconfig /all.

Если при работе в классе виртуальная машина получила адрес от другого DHCP сервера, завершите сеанс текущего пользователя, зайдите под учетной записью локального администратора Vista1\adm пароль 123qwe и пропишите вручную нужные настройки для протоколов TCP/IP v.4.

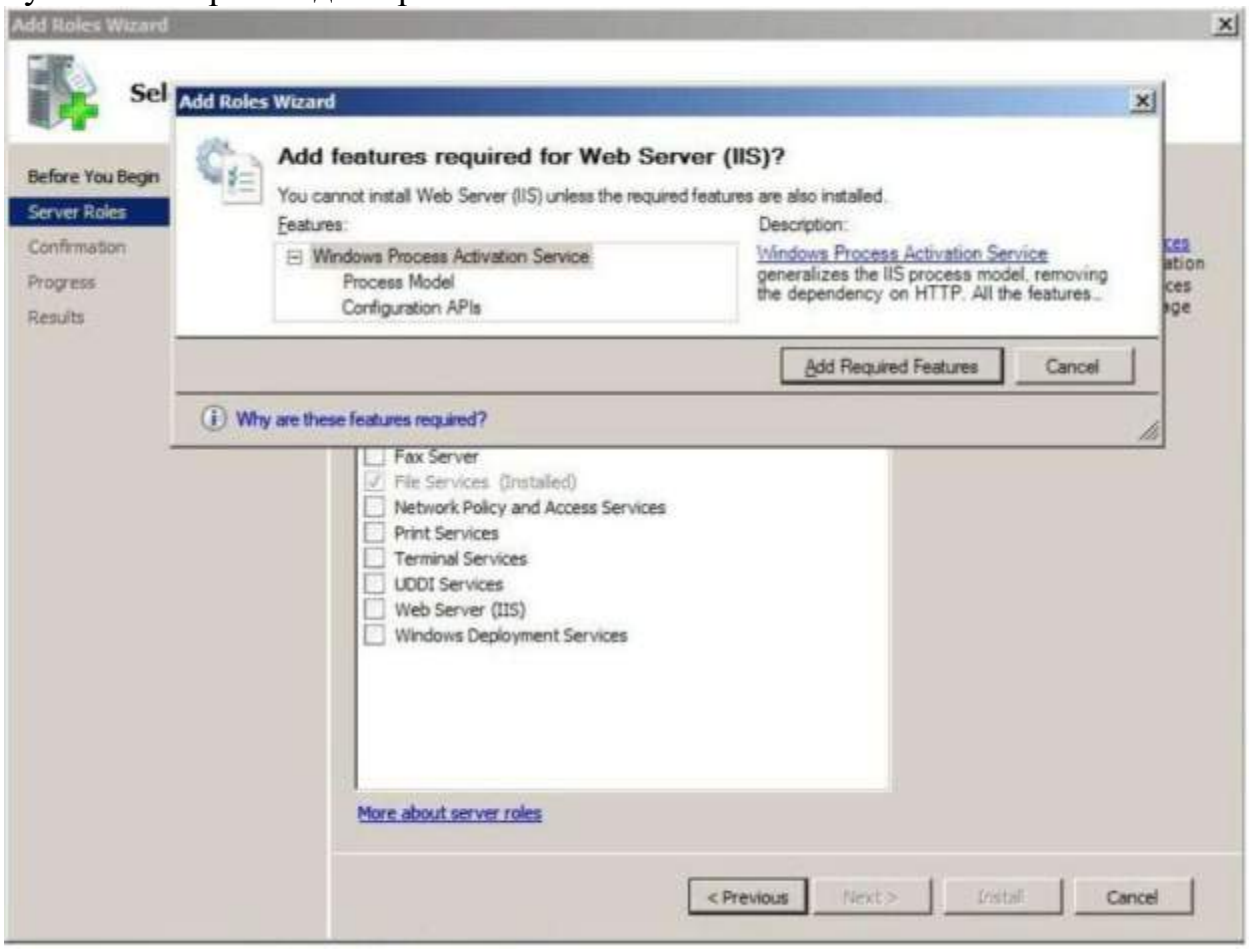


Рис.1. Установка роли Web server требует установки компоненты Windows Process Activation Service.

Установка IIS 7.0

В состав серверных операционных систем Microsoft входят службы Internet Information Services, которые и обеспечивают функциональность web- и ftp-сервера. IIS 7.0 имеет модульную архитектуру и рекомендуется устанавливать только нужные вам компоненты. Для установки IIS запустим Server Manger и добавим роль Web Sever. Вместе с ней будет предложено установить Windows Process Activation Service (рис.1). Обратите внимание на перечень устанавливаемых по умолчанию модулей. Они обеспечивают работу web-сервера со статическим содержимым. Если требуется использовать технологии

ASP, ASP.Net, CGI и т.п. потребуется дополнительно отметить соответствующий модуль. Для лабораторной нам понадобится ftp-сервер, поэтому при установке отмечаем службу FTP Publishing Service (рис.2).

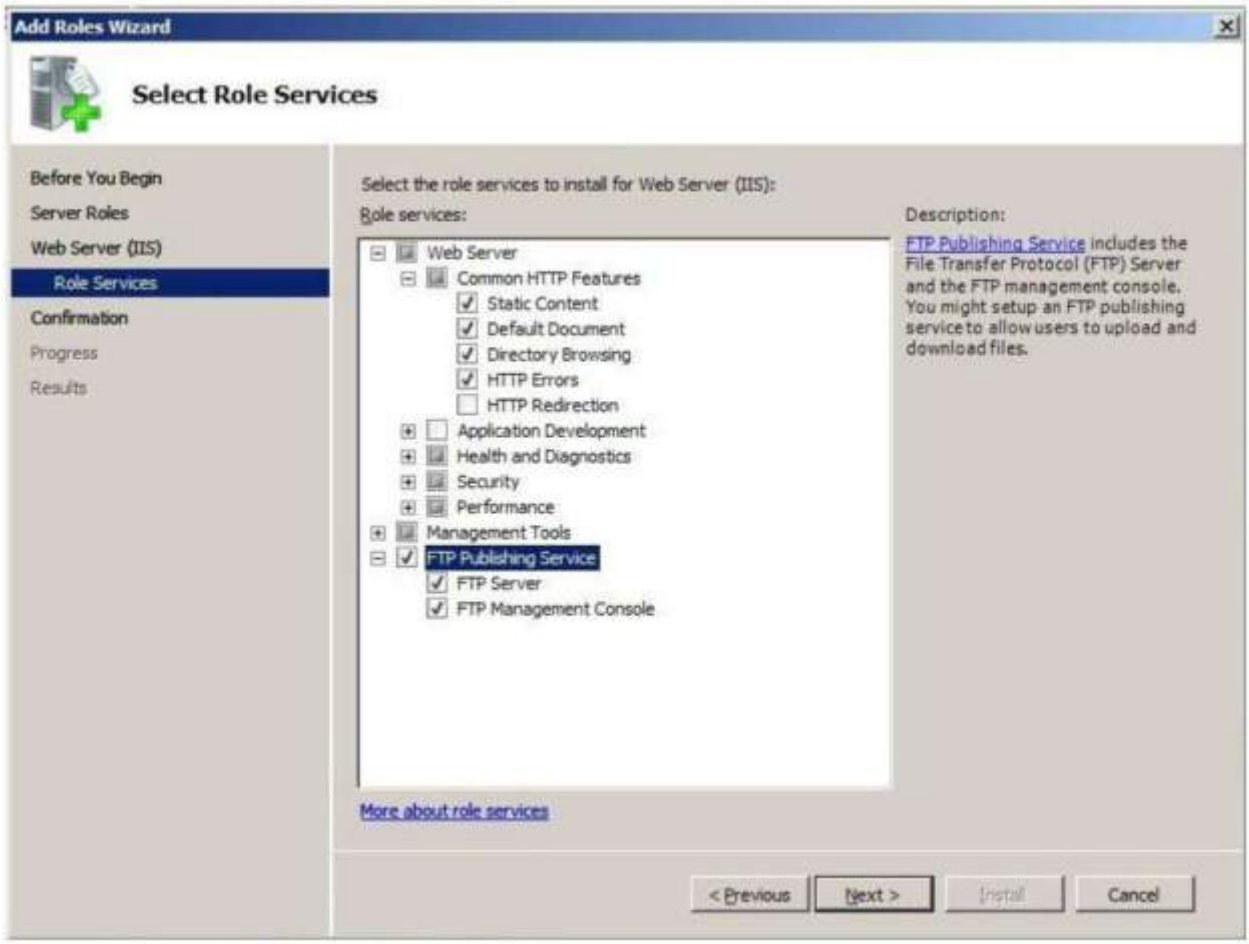


Рис.2. Устанавливаемые модули.

При выборе FTP Publishing Service мастер установки также предложит включить в установку компоненты управления от предыдущей версии - IIS 6.0. Они потребуются для администрирования FTP сервера.

WEB-сервер

После успешной установки проверим, работает ли web-сервер. Запустите браузер на сервере и в строке адреса наберите http://<имя web-сервера>. Вы должны увидеть стандартную первую страницу web-сервера IIS с надписью «Добро пожаловать» на разных языках (рис.3). Проделайте то же самое с рабочей станции. Если начальная страница видна с сервера, но недоступна с рабочей станции, проверьте настройки сетевого подключения. Кроме того, в некоторых случаях проблема может быть вызвана работой встроенного межсетевого экрана Windows Server 2008. Настройки можно проверить в Панели управления (Control Panel -> Windows Firewall). Для используемого сетевого интерфейса должны быть разрешены исключения и в списке исключений должно быть отмечено World Wide Web Services (HTTP) – рис.4. Эту настройку делает мастер установки при добавлении роли, но возможно по каким-то причинам она не появилась.

Рис.3. Страница приветствия.

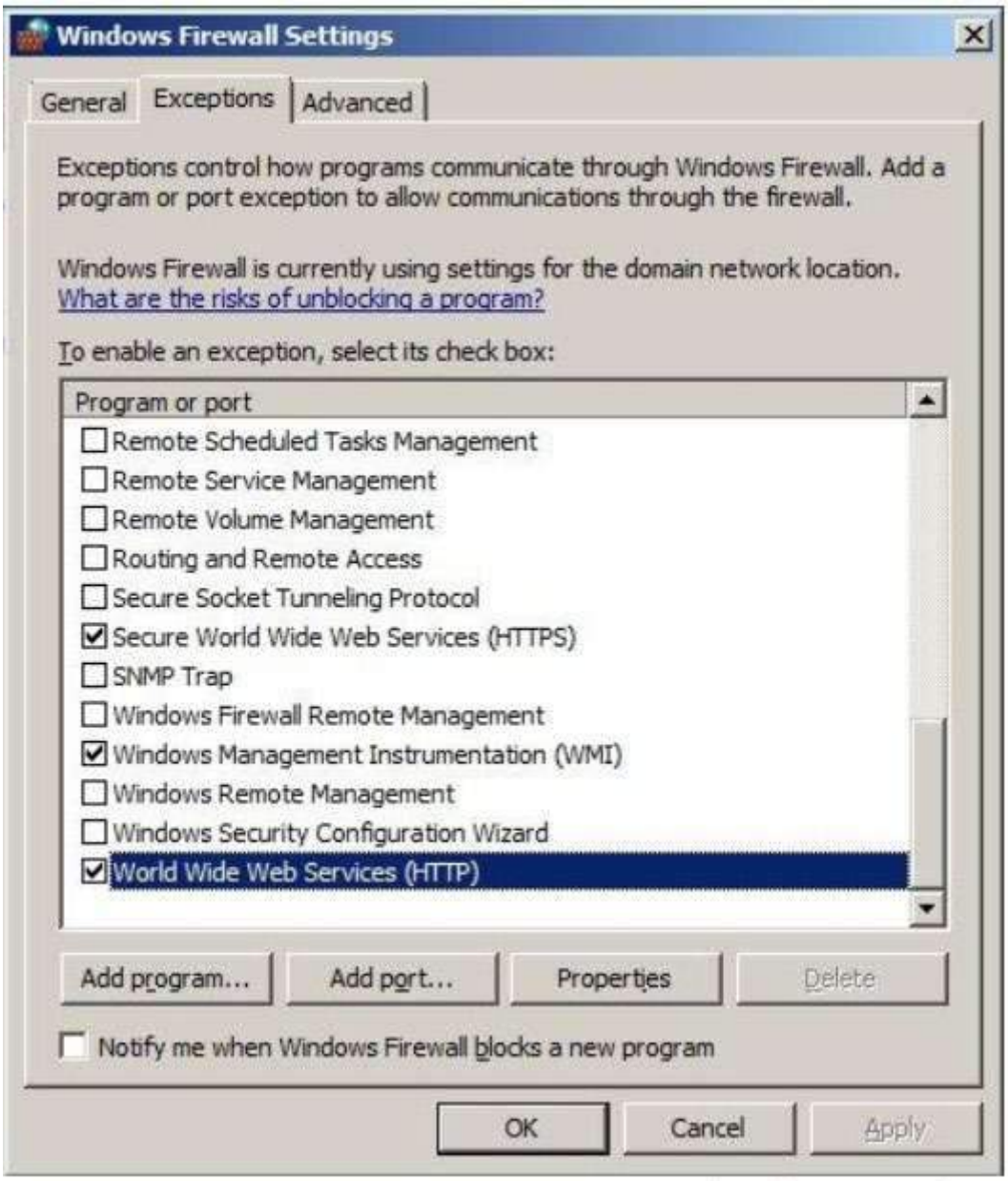


Рис.4. Проверка настройки Windows Firewall.

Теперь, когда мы добились того, что сервер доступен не только локально, но и извне, познакомимся с инструментами администрирования. В меню Administrative Tools найдите оснастку Internet Information Services (IIS) Manager. В оснастке раскройте узел со списком сайтов и, выделив сайт Default Web Site, в правой части окна в группе Actions нажмите ссылку Basic Settings. В появившемся окне вы увидите путь к домашнему каталогу сайта (рис.5), в нашем случае это C:\inetpub\wwwroot. Если открыть этот каталог, в нем найдете файл iisstart.htm, который и выводится при запросе заглавной страницы сайта. Посмотрим, где эту настройку можно поменять.

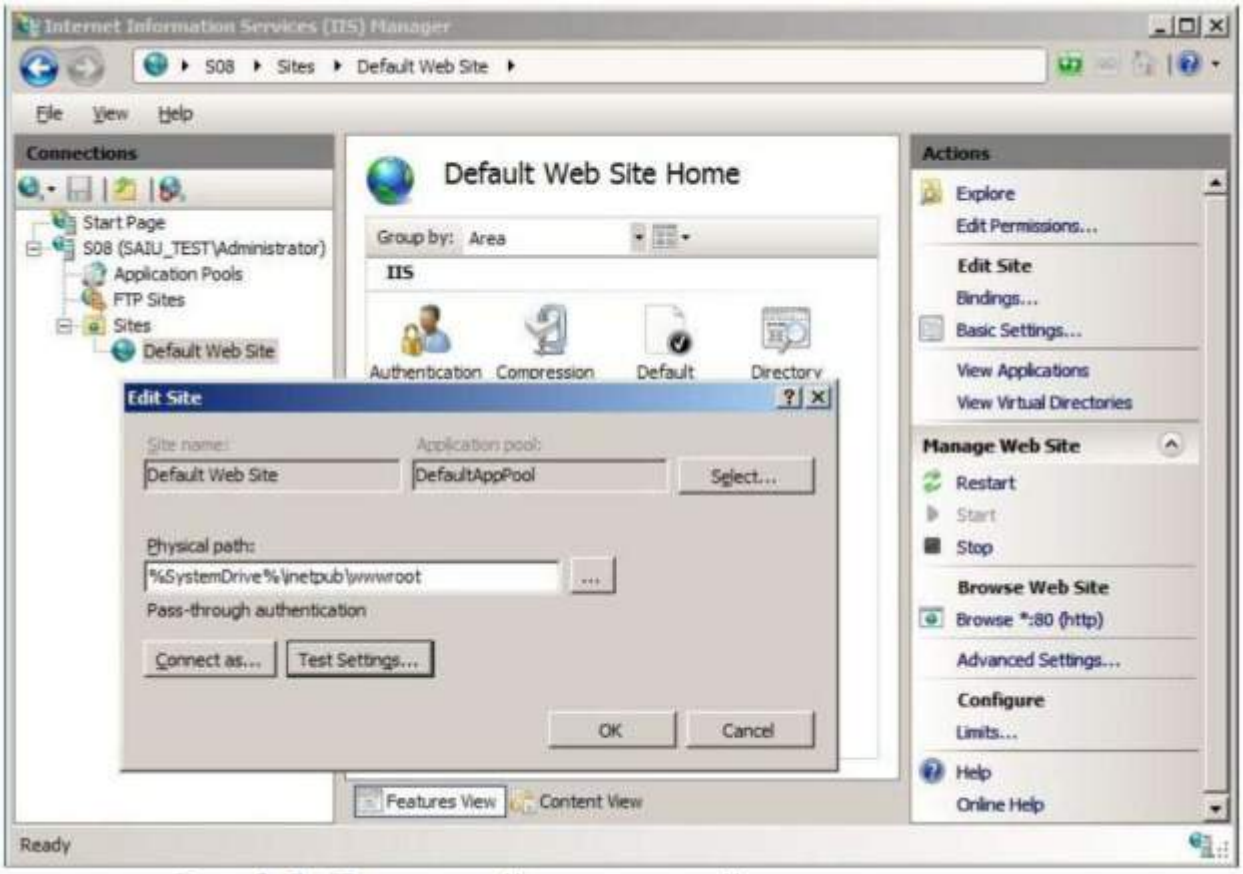


Рис.5. Домашний каталог сайта по умолчанию.

Закройте окно Edit Site и в центральной части окна оснастки Internet Information Services (IIS) Manager откройте ссылку Default. Вы перейдете в раздел настройки страницы по умолчанию, возвращаемой сервером, если в запросе клиента явно не указан полный пусть и название файла (рис.6). Названия страниц расположены в порядке убывания приоритета. Список можно редактировать.

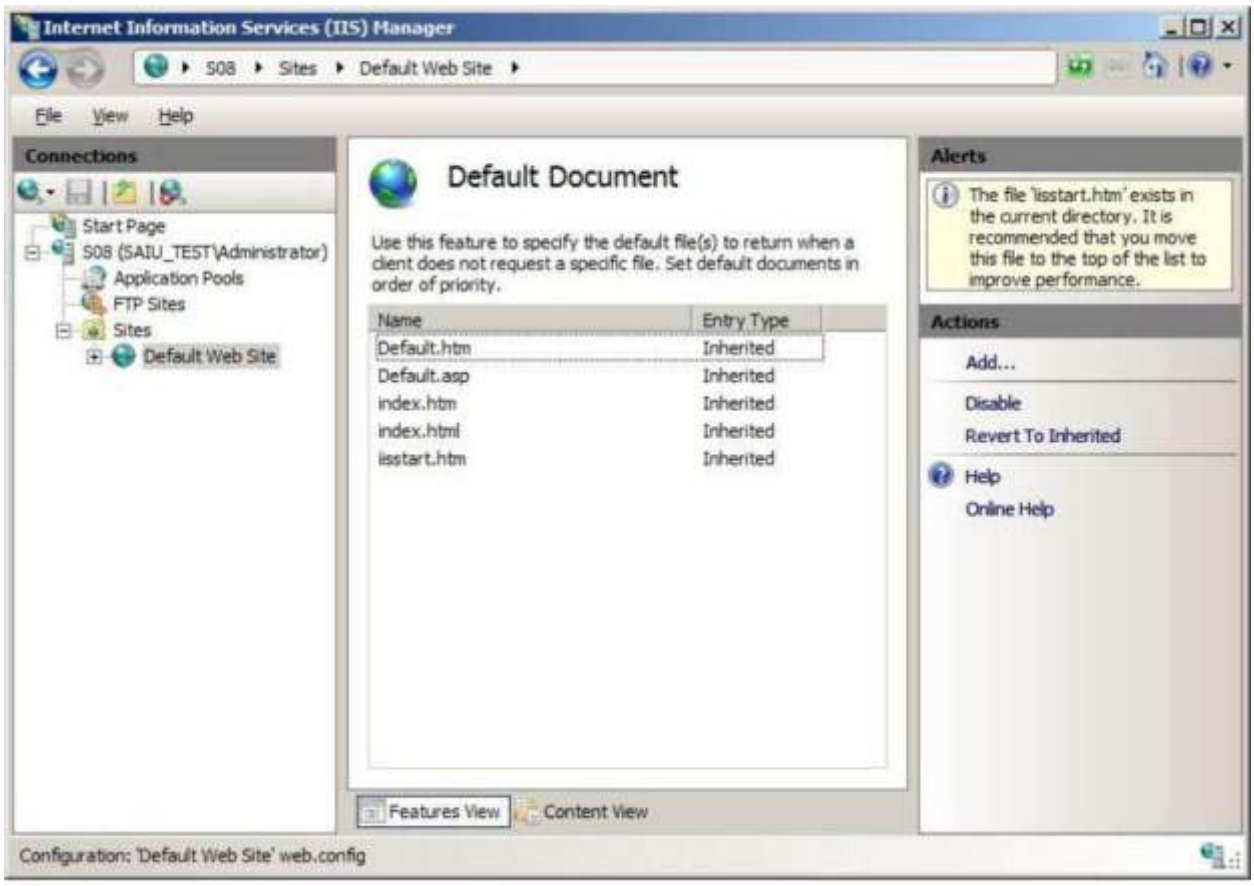


Рис.6. Настройка страницы по умолчанию.

Задание. *Создайте свою web-страницу (например в редакторе Word) сохраните ее в корневом каталоге сайта с названием default.htm. В браузере снова наберите http://<имя web-сервера>, убедитесь, что теперь при обращении к серверу отображается новая заглавная страница.* Теперь посмотрим, как организовать иерархию каталогов. Вариант первый – создание подкаталогов в каталоге сайта.

Задание. *Создайте в каталоге C:\inetpub\wwwroot подкаталог cat1, поместите туда начальную страницу и проверьте работу ссылки http://<имя webсервера>/cat1*

Возможности по более гибкой настройке предоставляют виртуальные каталоги. Пусть, например, нужные нам файлы лежат в папке E:\test и мы хотим подключить ее к дереву каталогов нашего сайта под именем cat2. Для этого в правой части окна оснастки Internet Information Services (IIS) Manager найдите ссылку View Virtual Directories и в открывшемся окне нажмите ссылку Add Virtual Directory. После этого укажите физическое расположение каталога и псевдоним (Alias), под которым он будет подключен к дереву каталогов сайта (рис.7).

Рис.7. Создание виртуального каталога.

Задание. *Создайте виртуальный каталог и пометите в него какой-нибудь HTMLдокумент. Протестируйте правильность сделанных настроек.* **FTP-сервер** Перейдем теперь к администрированию установленного нами FTP-сервера. В отличие от web-сервера, ftp-сервер по умолчанию не запускается (даже если он установлен на компьютер). Видимо считается, что эта служба потенциально более опасна с точки зрения подверженности сетевым атакам. Поэтому первое, что мы делаем – запускаем службу FTP Publishing Service с помощью оснастки Services из меню Administrative Tools (рис.8). Здесь же можно изменить тип запуска с ручного (Manual) на автоматический (Automatic). Теперь откройте каталог C:\inetpub\ftproot и запишите в него какой-нибудь файл. На сервере, набрав в браузере ftp://<имя web-сервера>, проверьте работу ftpсервера. Теперь выполните ту же проверку на виртуальной машине с Windows Vista. Она может не пройти по следующей причине. Протокол FTP при работе создает два соединения. Первое устанавливает клиент на 21-й TCP-порт сервера. Второе в зависимости от режима протокола устанавливает или клиент (пассивный режим), или сервер (активный режим). При настройках по умолчанию браузер Internet Explorer использует пассивный режим протокола и второе соединение, устанавливаемое клиентом с сервером, блокируется его межсетевым экраном. Чтобы все заработало правильно, можно или внести изменения в настройки межсетевого экрана на сервере, или в настройках браузера сбросить переключатель «Использовать пассивный FPT-протокол …» (рис.9: Сервис->Свойства обозревателя вкладка «Дополнительно»).

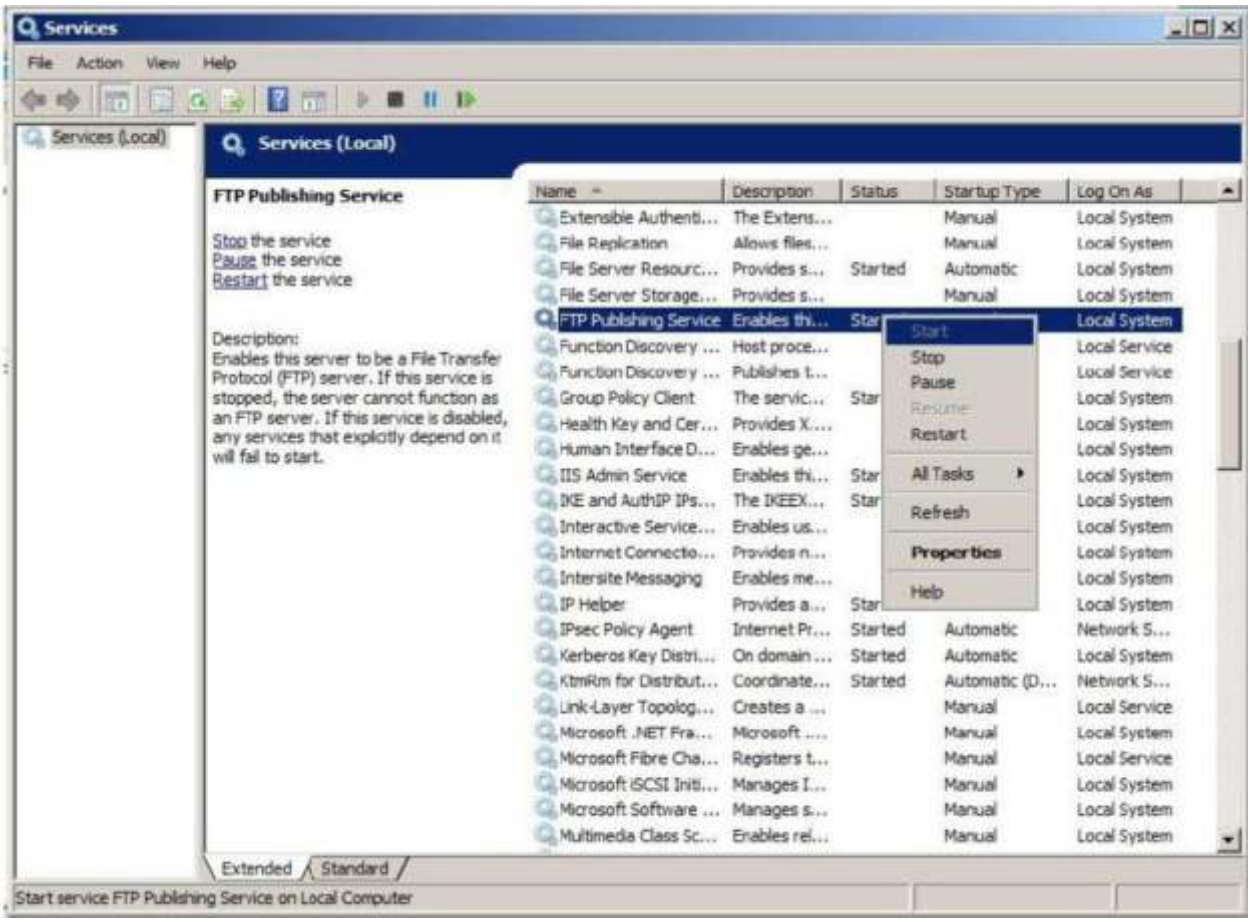


Рис. 9. Запуск службы FTP Publishing Service.

После того, как мы проверили доступность FTP-сервера с другого компьютера, рассмотрим некоторые вопросы, связанные с его администрированием. Если в оснастке Internet Information Services (IIS) Manager перейти на узел FTP Sites, мы увидим надпись, что управление FTP-сайтами осуществляется с помощью оснастки Internet Information Services (IIS) 6.0 Manager и ссылку для ее запуска (также эту оснастку можно запустить из меню Administrative Tools). Открыв свойства FTP-сайта Default FTP Site (рис.10) на вкладке Home Directory, можно узнать расположение домашнего каталога FTP-сайта и настройки для него (разрешено чтение, не разрешена запись).

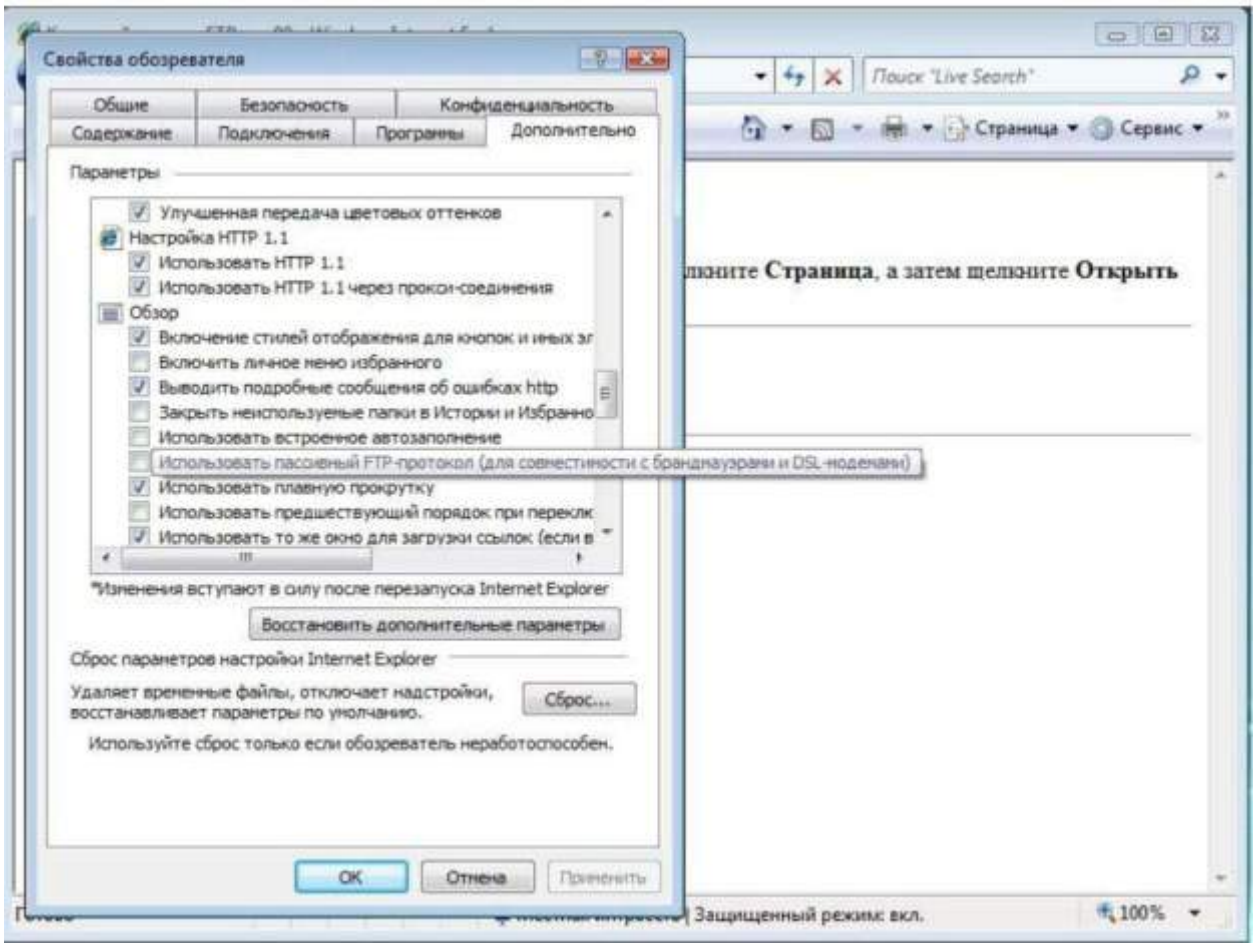


Рис.9. Настройка Internet Explorer для использования FTP в активном режиме.

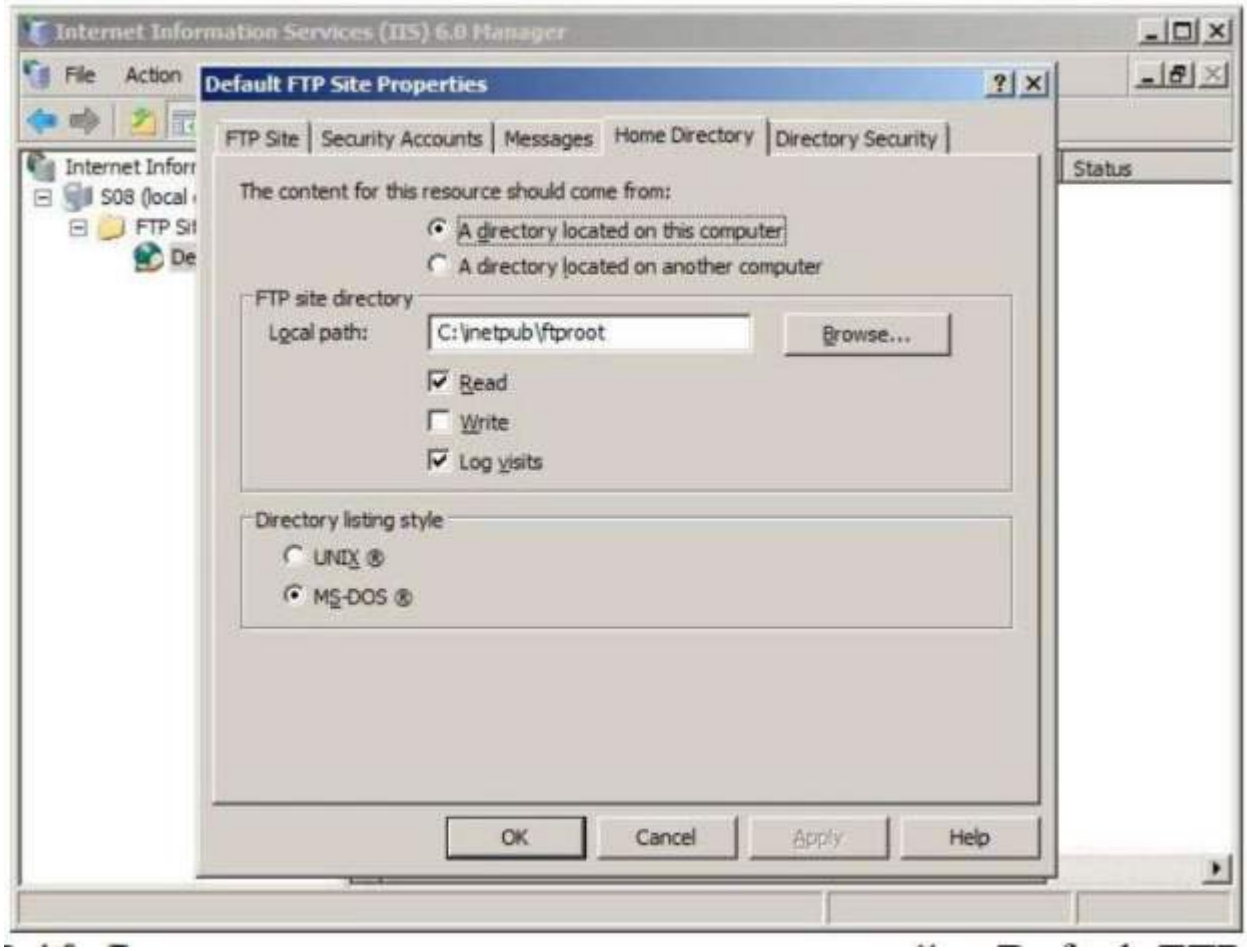


Рис.10. Расположение домашнего каталога сайта Default FTP Site.

На вкладке Security Accounts (рис.11) указано, что к FTP-серверу разрешен анонимный доступ и для него используется учетная запись IUSR_<имя сервера> (в нашем случае IUSR_S08). Эта учетная запись при настройках по умолчанию используется также и Web-сервером. Это надо учитывать при работе с разрешениями на файловой системе.

Задание. *В каталоге C:\inetpub\ftproot создайте две папки public и private и запишите туда какие-нибудь файлы. В свойствах папки private запретите полный доступ к ней для учетной записи IUSR_S08. Из виртуальной машины с Windows Vista попробуйте открыть через FTP ту и другую папку. Опишите результат. Задание. Отключите анонимный доступ для FTP-сайта. Попробуйте снова подключиться с удаленного компьютера. На запрос имени пользователя и пароля введите данные действующей учетной записи (например, test_saiu\labos с паролем Lab0s123). Опишите результат.*

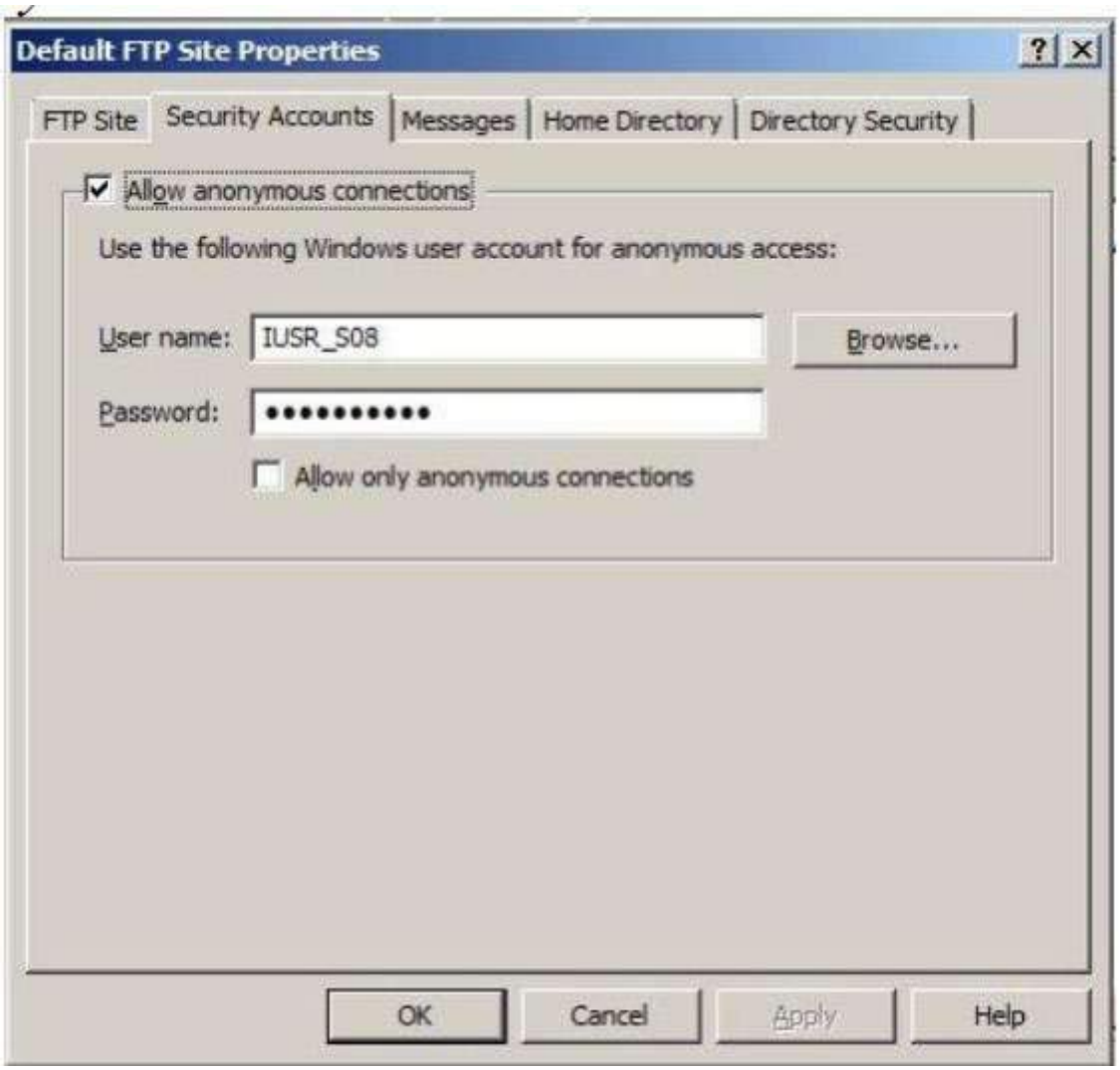


Рис.11. Настройка параметров анонимного доступа к FTP-серверу.

Прим. При работе через Internet Explorer с доступом к папке Private в последнем задании тоже возникают проблемы (но к папке Public получить доступ можно). Можно попробовать проверить с другими FTP-клиентами и постараться разобраться. Прим2. Протокол FTP передает имя пользователя и пароль открытым текстом. Это надо учитывать и стараться использовать дополнительные средства для защиты FTPсоединения или использовать для доступа по FTP специально для этого созданные учетные записи с ограниченными привилегиями в сети.

ПРАКТИЧЕСКАЯ РАБОТА № 33.
УДАЛЕННОЕ УПРАВЛЕНИЕ WINDOWS SERVER 2008
Цель работы:
Научиться выполнять удаленное управление Windows Server 2008,
Используемое программное обеспечение
Для выполнения данной лабораторной работы Вам понадобится компьютер с операционной системой Microsoft Windows XP, Windows Server 2003 или Vista и установленным программным обеспечением Microsoft Virtual PC 2007 SP1 (с

ОС Windows 7 и Windows Virtual PC) и 2 подготовленные виртуальные машины с Windows Server 2008 и Windows Vista.

Remote Server Administration Tools

Для удаленного администрирования предыдущих серверных операционных систем семейства Windows (т.е. Windows 2000 Server и Windows Server 2003) на рабочую станцию администратора нужно было установить пакет инструментов из файла Adminpak.msi с дистрибутива соответствующего сервера. С выходом Windows Server 2008 все несколько изменилось и теперь для этого используется пакет RSAT, который можно свободно загрузить с сервера Microsoft. Он существует в версиях для Windows Vista SP1 и Windows 7.

Задание. Из файла, прикладываемого к описанию работы, установите на рабочую станцию с Windows Vista утилиты удаленного администрирования (для этого вам понадобится зайти под учетной записью с административными привилегиями). Прим. Если на виртуальной машине установлена ОС Windows Vista без SP1, то предварительно нужно поставить этот пакет обновлений. При этом надо читывать, что для его установки потребуется не менее 6Гб свободного пространства на диске, где установлена ОС.

После установки, средства администрирования из состава RSAT необходимо активировать из "Панели управления" (Control Panel). Активированные приложений появятся в папке «Администрирование» (Administrative Tools) на локальном компьютере.

Служба удаленного терминала

Также удаленное управление сервером можно осуществлять через удаленный терминал. В этом случае, управляющие утилиты (и другие приложения, запускаемые из терминала), выполняются на сервере, а на клиентский компьютер передается только картинка рабочего стола пользователя. Служба терминалов использует протокол RDP (Remote Desktop Protocol), кроме того, в Windows Server 2008 появилась возможность использования удаленного терминала через web-интерфейс. Начнем с того, что в Server Manager добавляем серверу роль Terminal Services. На рисунке 1 представлены службы, относящиеся к данной роли. Для выполнения первой части лабораторной работы нам понадобится только служба Terminal Server. Если ее отметить, то появится предупреждение о том, что установка служб удаленного терминала на контроллер домена нежелательна по соображениям безопасности (рис.2): удаленные пользователи получат доступ к консоли контроллера домена. Но так как наша виртуальная сеть включает только один сервер, это предупреждение сейчас игнорируем.

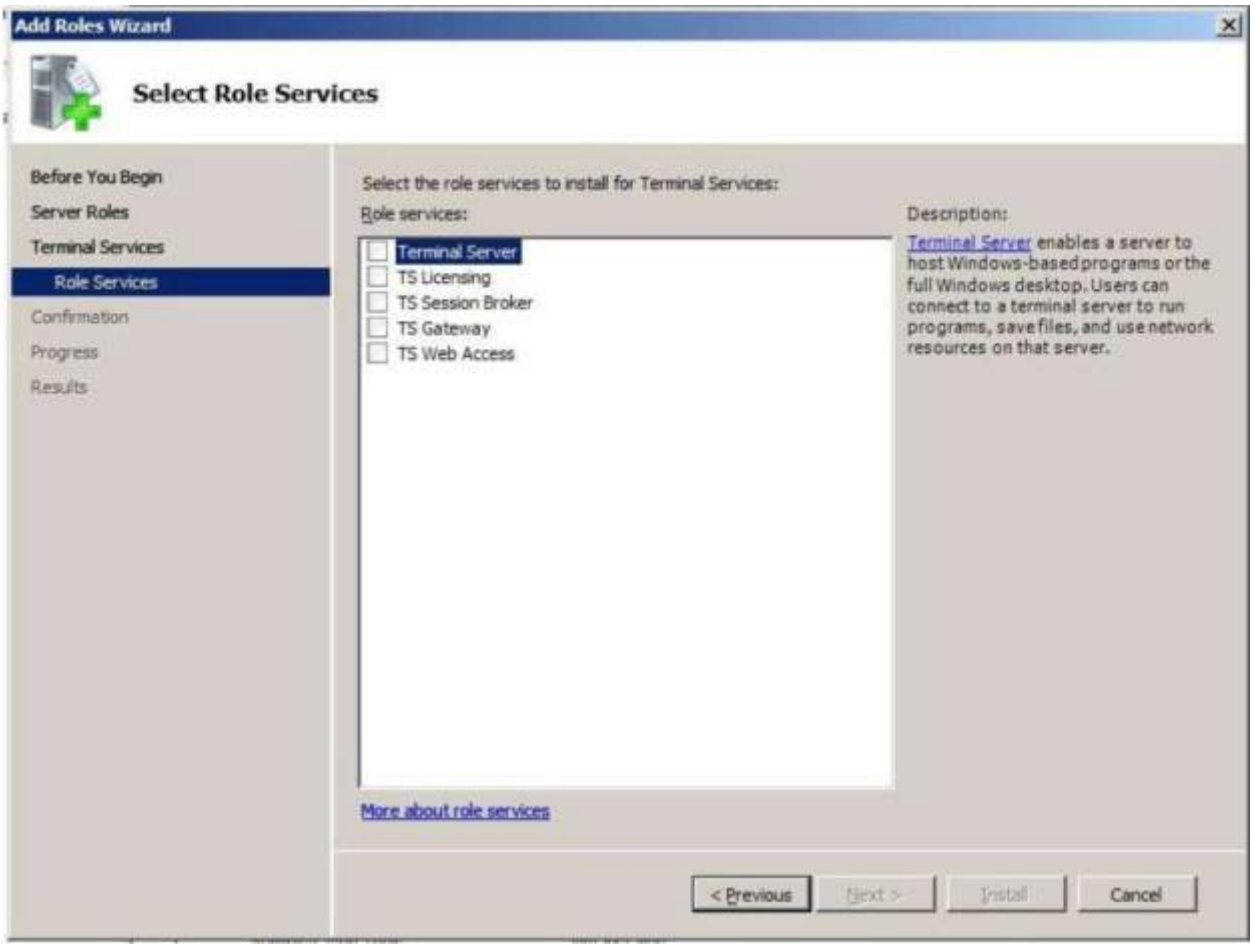


Рис. 1. Службы, относящиеся к роли Terminal Sevices

Рис. 2. Предупреждение о том, что установка служб удаленного терминала на контроллер домена нежелательна

Следующее окно мастера установки роли (рис.3) позволяет указать способ выполнения аутентификации при подключении. Более безопасный тип – Network Level Authentication, но он поддерживается не во всех случаях. Выберем его, т.к. у нас новая версия клиентской ОС (Windows Vista) и подключаемся мы фактически из локальной сети, поэтому проблем с совместимостью быть не должно. После этого будет запрошен тип лицензирования устанавливаемого сервера терминалов (рис.4). В нашем случае отметим первый вариант и получим пробную 120-дневную лицензию на использование сервера терминалов (для целей обучения этого будет вполне достаточно). Последнее окно мастера позволяет указать пользователей и группы, которым разрешен терминальный доступ. Здесь для выполнения лабораторной работы также достаточно оставить предлагаемый вариант – только группу Administrators.

После этого начнется установка выбранной службы. Для ее окончания нужно будет перезагрузить виртуальную машину, после чего снова войти под администратором и закончить процедуру установки.

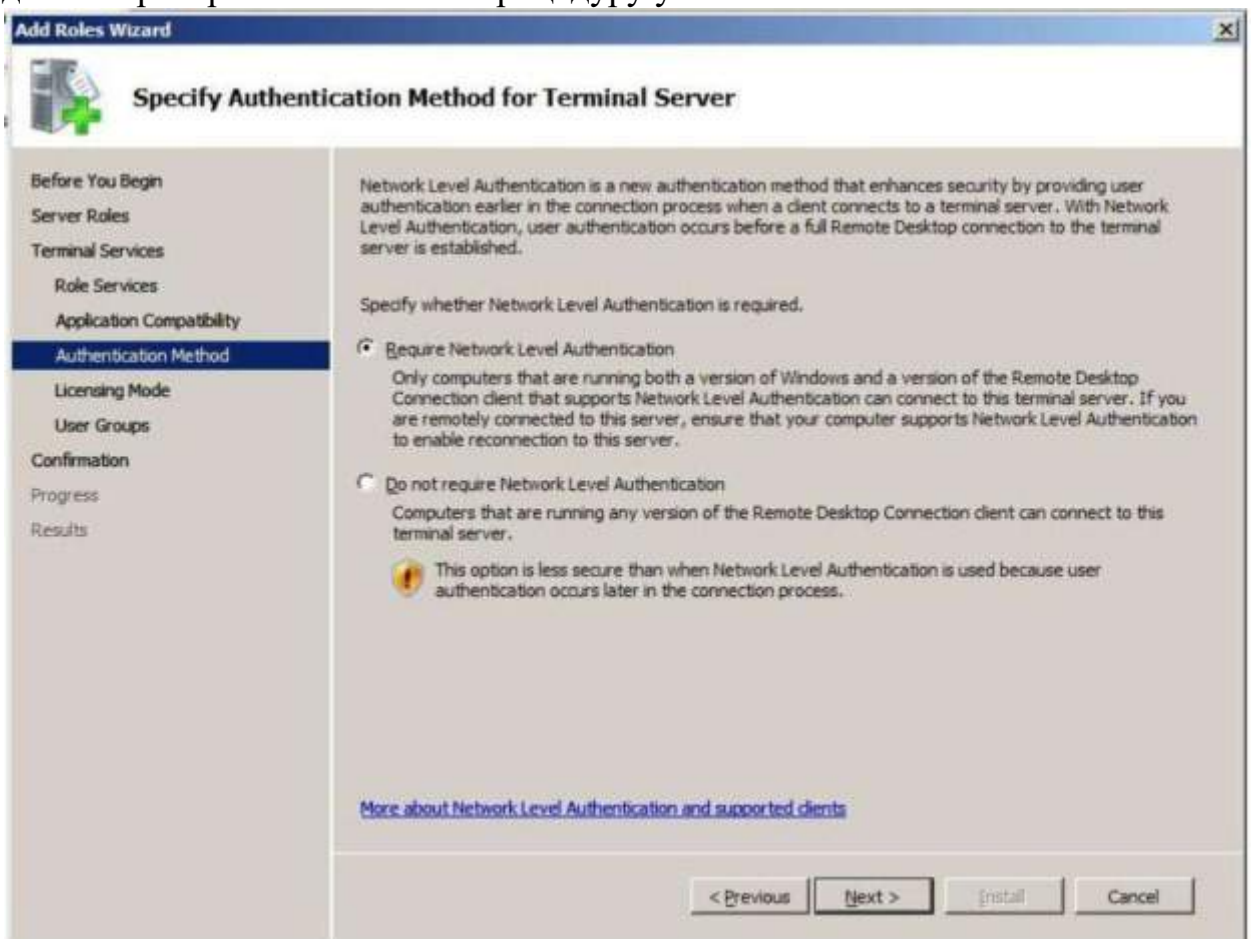


Рис.3. Выбор типа аутентификации.

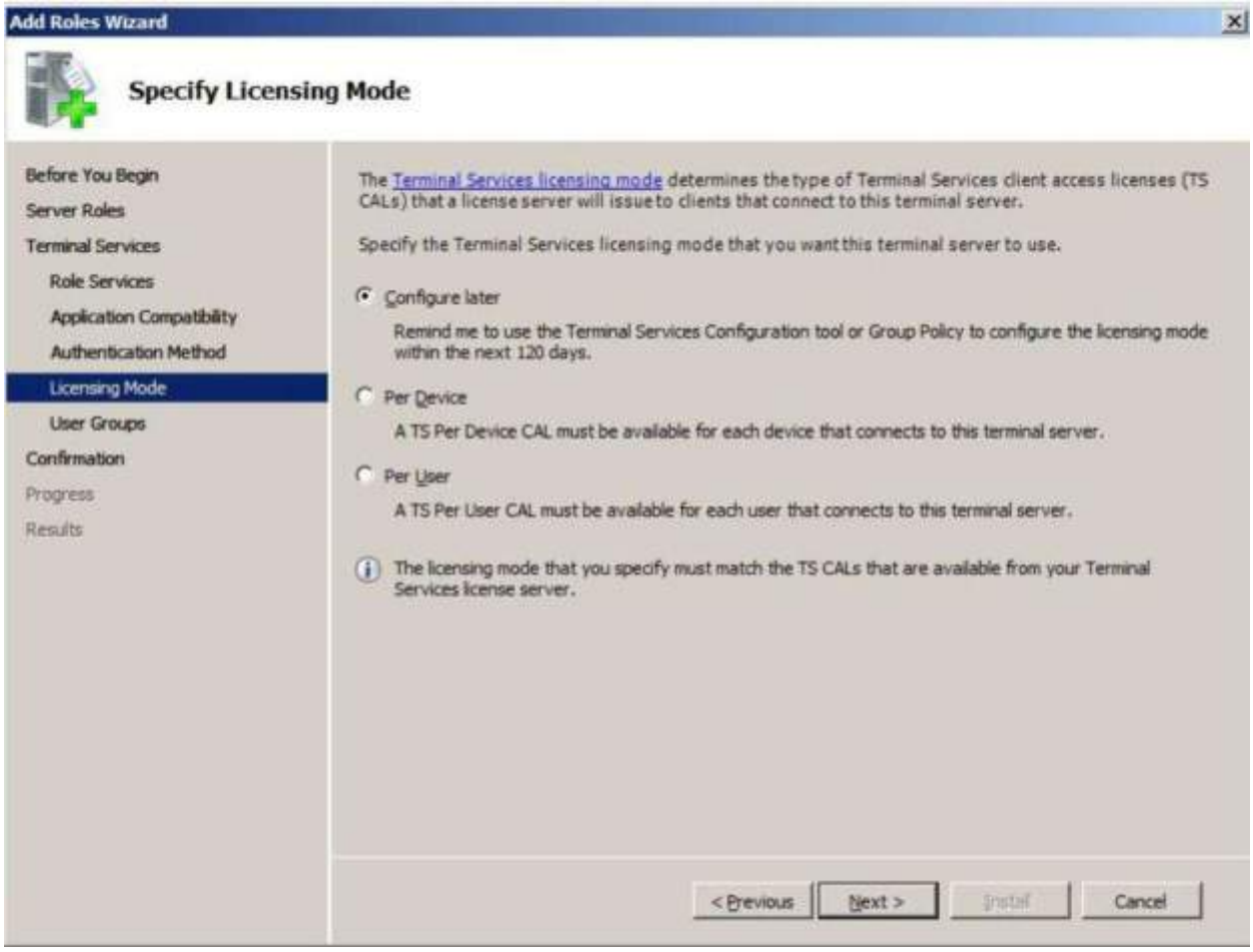


Рис.4. Выбор типа лицензирования.

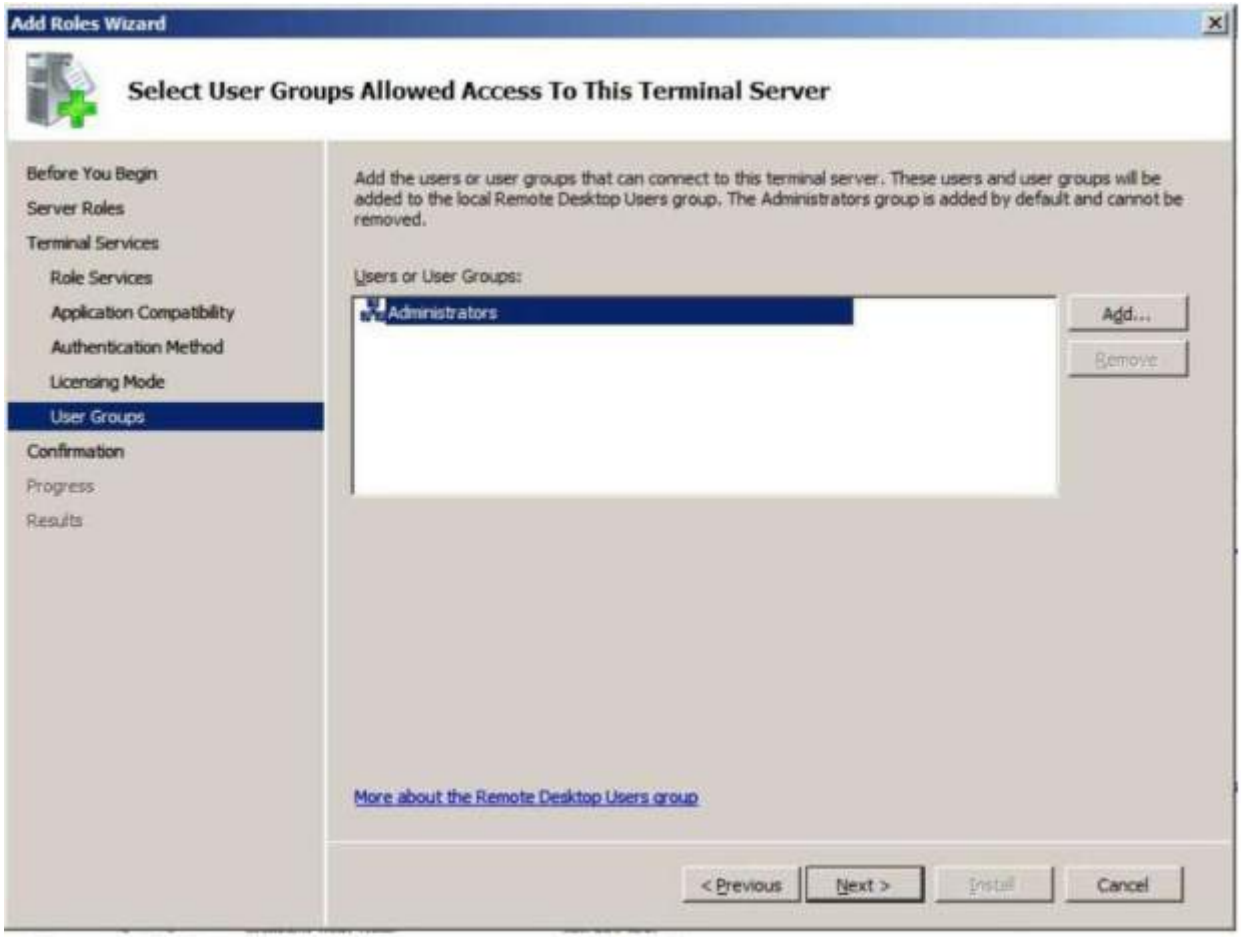


Рис.5. Выбор групп пользователей для терминального доступа.

Теперь, чтобы работать на сервере и на рабочей станции под разными учетными записями, создайте нового доменного пользователя adms с паролем 123qweQWE и включите его в группу Administrators (делается это с помощью оснастки Active Directory Users and Computers). С рабочей станции подключитесь к серверу терминалов (Пуск->Все программы->Стандартные->Подключение к удаленному рабочему столу). Для этого в окне терминального клиента сначала кажите имя или ip-адрес сервера (рис.6), а потом учетную запись, от имени которой будет производиться подключение. Обратите внимание, что по умолчанию считается, что вводимая учетная запись – локальная. Поэтому при использовании доменных записей надо полностью вводить имя домена и имя пользователя, например, SAIU_Test\adms.

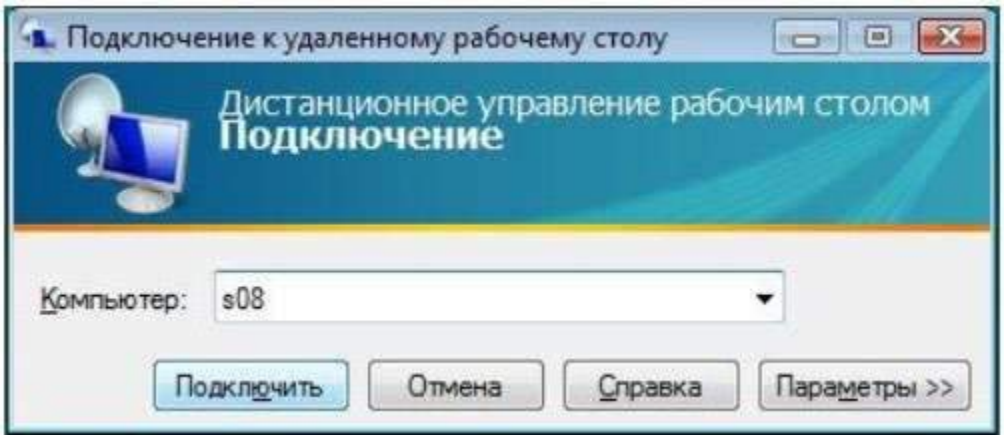


Рис.6. Выбор компьютера для подключения.

Административная оснастка Terminal Services Manager (Start->Administrative Tools-> Terminal Services) позволяет отслеживать текущие сессии, пользователей работающих в данных сессиях и запускаемые ими процессы (вкладка Processes). Пользователю можно отправить сообщение, при наличии соответствующих прав завершить выполнение отдельного процесса или сессии пользователя вообще, выполнить другие действия. В терминальной сессии доступен буфер обмена, через который можно передавать данные на удаленный (локальный) компьютер. Аналогичным образом можно копировать и файлы.

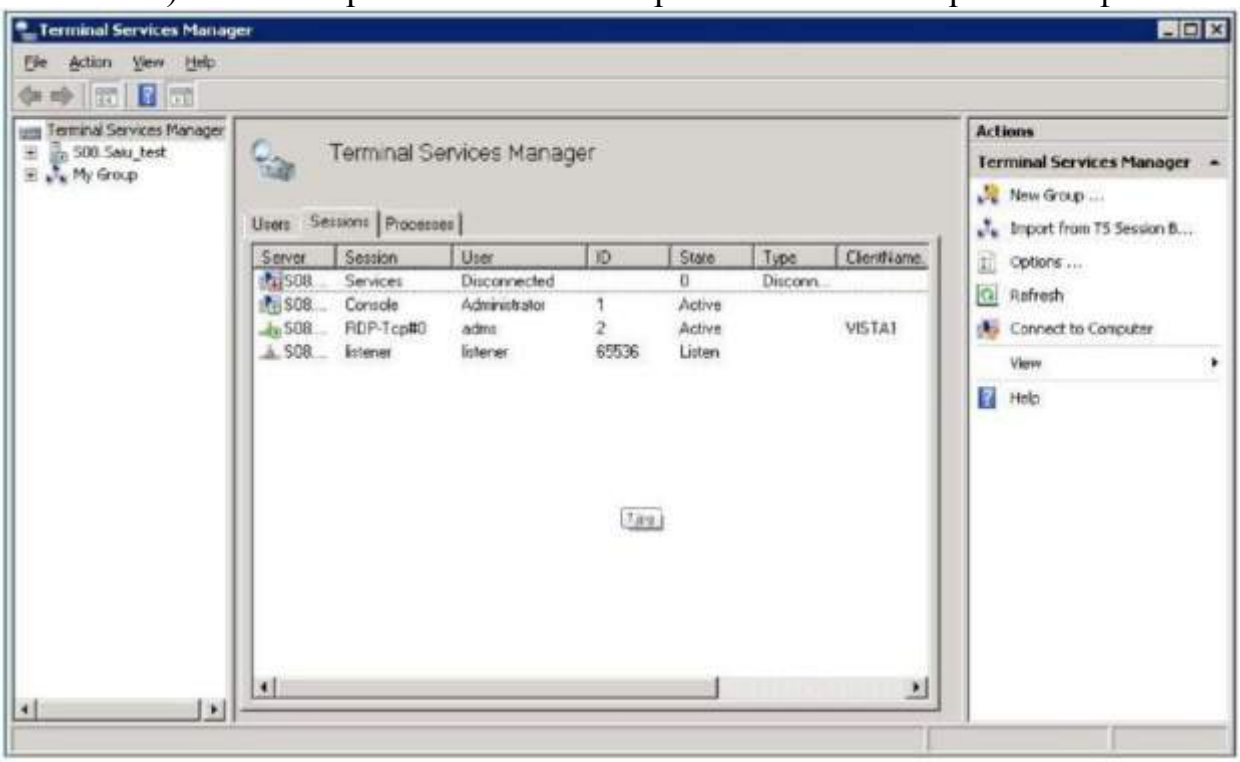


Рис.7. Окно оснастки Terminal Services Manager.

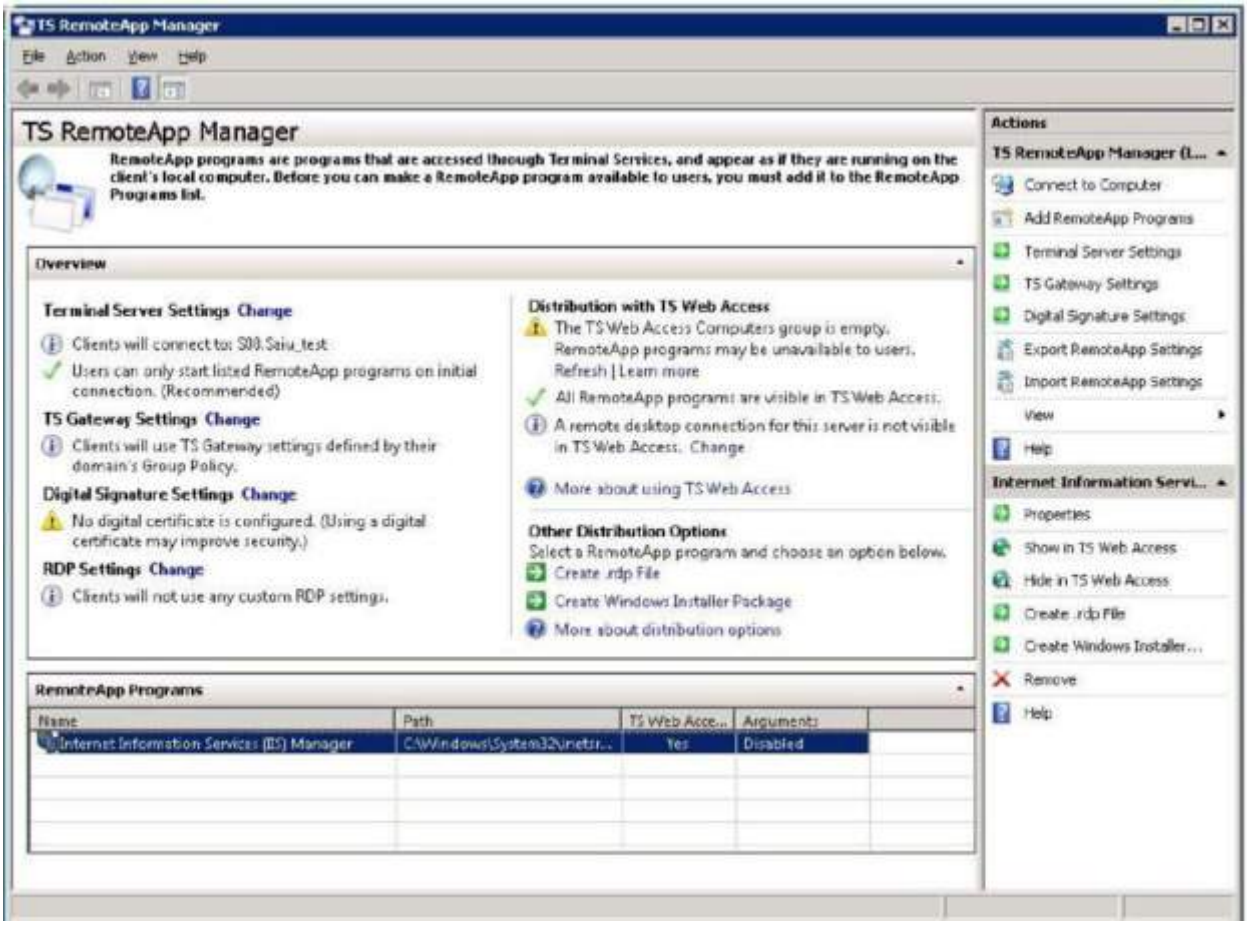


Рис.8. Окно оснастки TS RemoteApp Manager.

Зачастую администратору надо сделать так, чтобы пользователь, не выбирая компьютер и параметры подключения, мог быстро подключиться к нужному серверу и получить нужное ему приложение. Такую настройку можно сделать с помощью оснастки TS RemoteApp Manager (рис.9.8). Выбрав ссылку Add RemoteApp Programs, можно добавить приложение, «публикуемое» на терминальном сервере. Когда приложение добавлено (на рис.8 это оснастка IIS Manager), можно создать для него .rdp файл (ссылка Create .rdp file). Теперь клиент, получивший этот файл, может его запустить, ввести имя пользователя и пароль (если это предполагают настройки) и получить доступ к нужному приложению, как будто оно запущено локально.

***Задание**. «Опубликуйте» приложение. Проверьте работу сделанных настроек. Что будет отображаться на сервере в оснастке Terminal Services Manager, когда пользователь запустил удаленное приложение? А когда закрыл его? Посмотрите описания опубликованного приложения в TS RemoteApp Manager и свойства .rdp файла.*

Как Вы убедились в ходе выполнения задания, если пользователь закрывает окно опубликованного приложения или окно терминального клиента, его сессия не заканчивается. Таким образом, удаленный пользователь может запустить какую-то программу на выполнение, а спустя некоторое время (часы, дни …) – подключиться, чтобы проверить результаты. В одних случаях, это может быть полезно. Но в других – может понадобиться автоматически закрывать неактивные в течение определенного времени сессии (для экономии

ресурсов сервера, из-за ограниченного числа терминальных лицензий). Такую настройку можно сделать в оснастке Active Directory Users and Computers в свойствах учетной записи пользователя (рис.9).

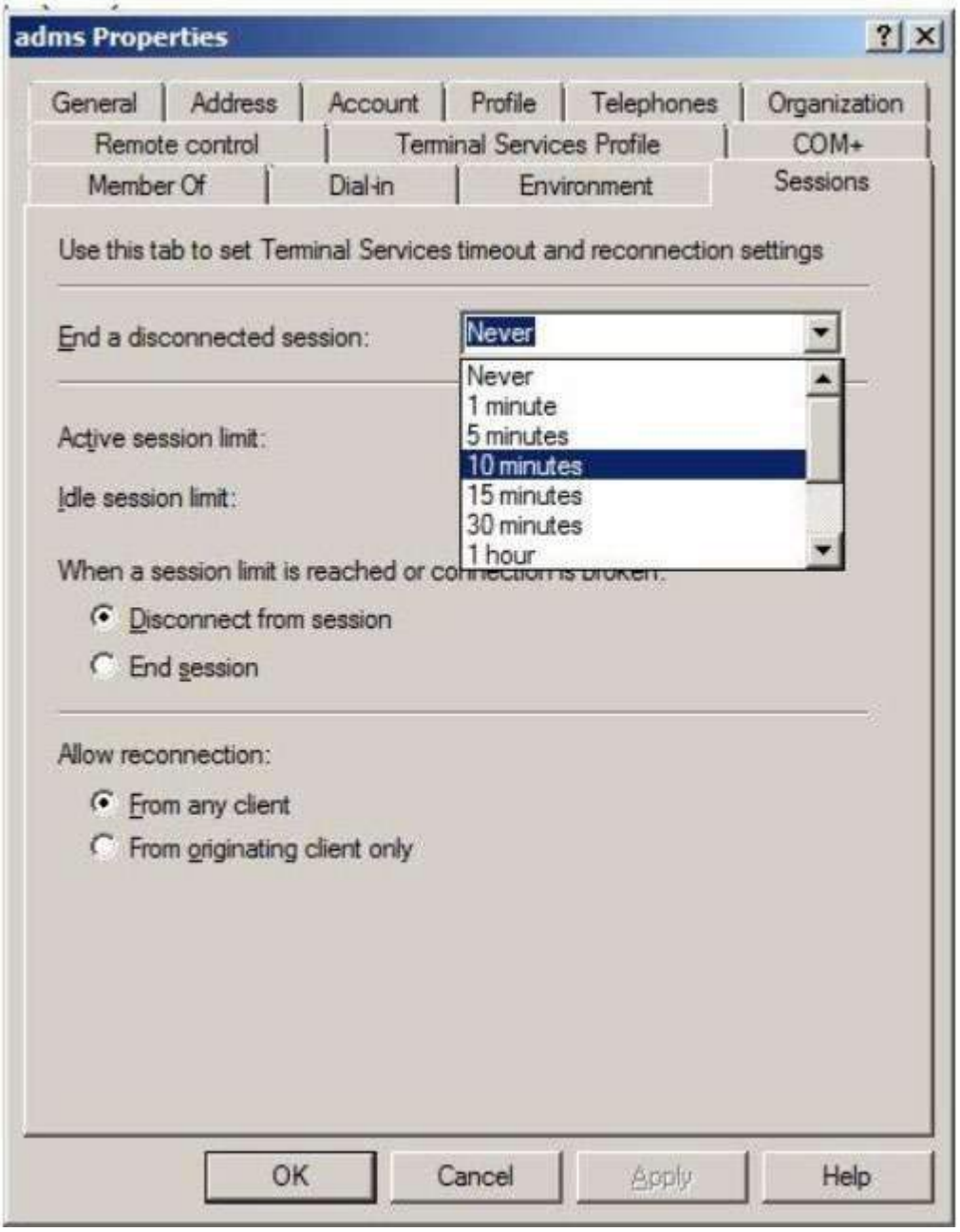


Рис.9. Настройка автоматического завершения неактивных сессий в свойствах учетной записи пользователя

Доступ к службе удаленного терминала через web-интерфейс

Теперь рассмотрим, как настроить работу с удаленным терминалом через webинтерфейс. Это может понадобиться в случаях, когда пользователи по каким-то причинам не могут использовать обычный терминальный клиент (фильтрация трафика провайдером и т.д.). Для начала, нужно установить дополнительную службу. В оснастке Server Manager запустите добавление служб для роли Terminal Services. В окне аналогичном, представленному на рис.1, отметьте службу TS Web Access. Появится запрос на добавление связанных компонент – модулей IIS, обеспечивающих работу с динамически

формируемым содержимым (ASP.Net, ISAPI и т.д.). После успешной установки, в оснастке Internet Information Services (IIS) Manager проверьте, что у web-сайта Default Web Site появился раздел TS. На рабочей станции запустите Internet Explorer и в строке адреса наберите http://<имя сервера>/ts В открывшемся окне перейдите на вкладку Remote Desktop (рис.10). При необходимости добавьте сайт в список доверенных, чтобы с него можно было запускать активное содержимое. Для этого в меню **Сервис** выберите **Свойства обозревателя**, на вкладке **Безопасность** откройте список надежных узлов и добавьте в него наш узел (рис.11). После этого попробуйте подключиться к серверу. В остальном работа через web-интерфейс ничем особо не отличается от работы с использованием терминального клиента.

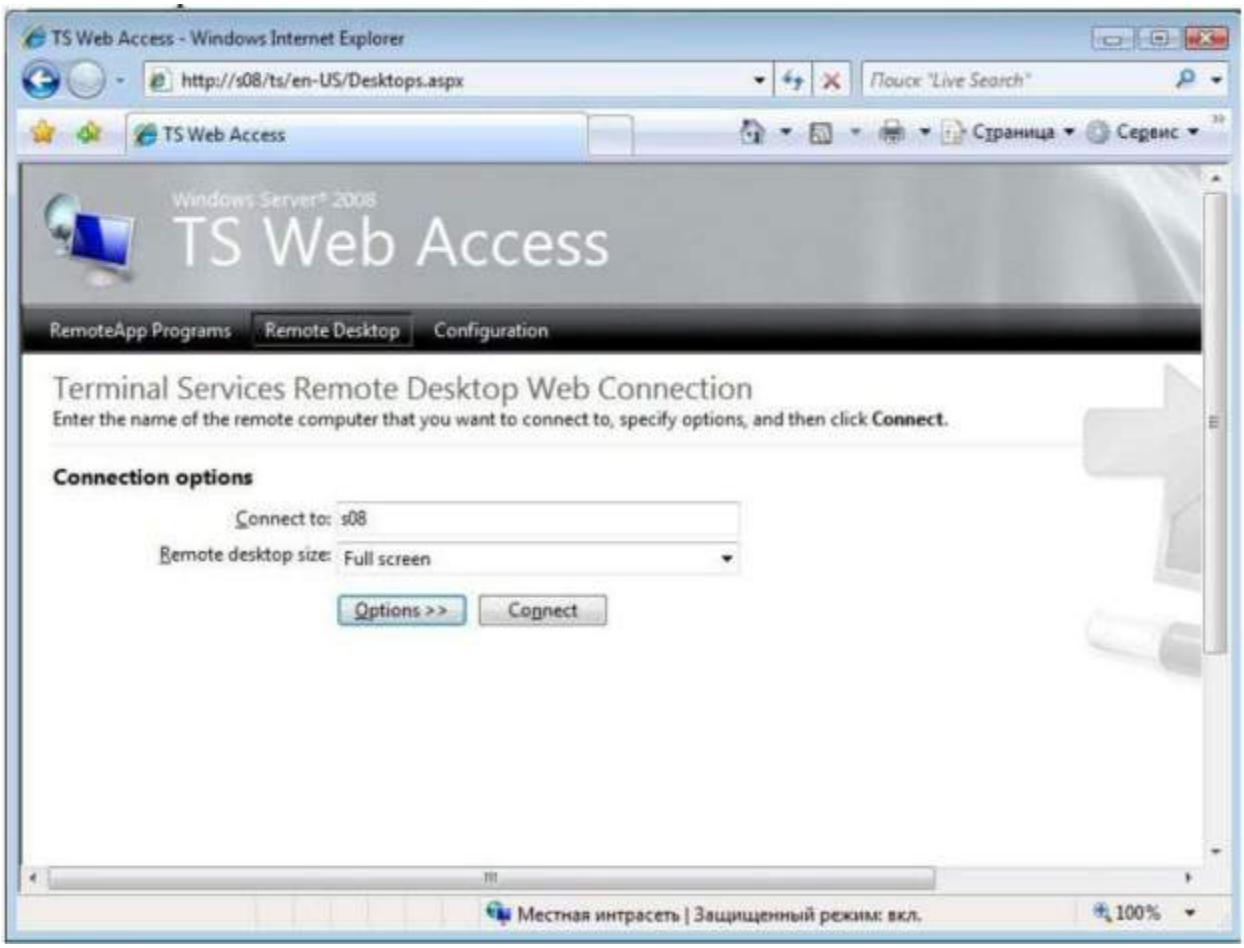


Рис.10. Подключение к терминальному серверу через web-интерфейс.

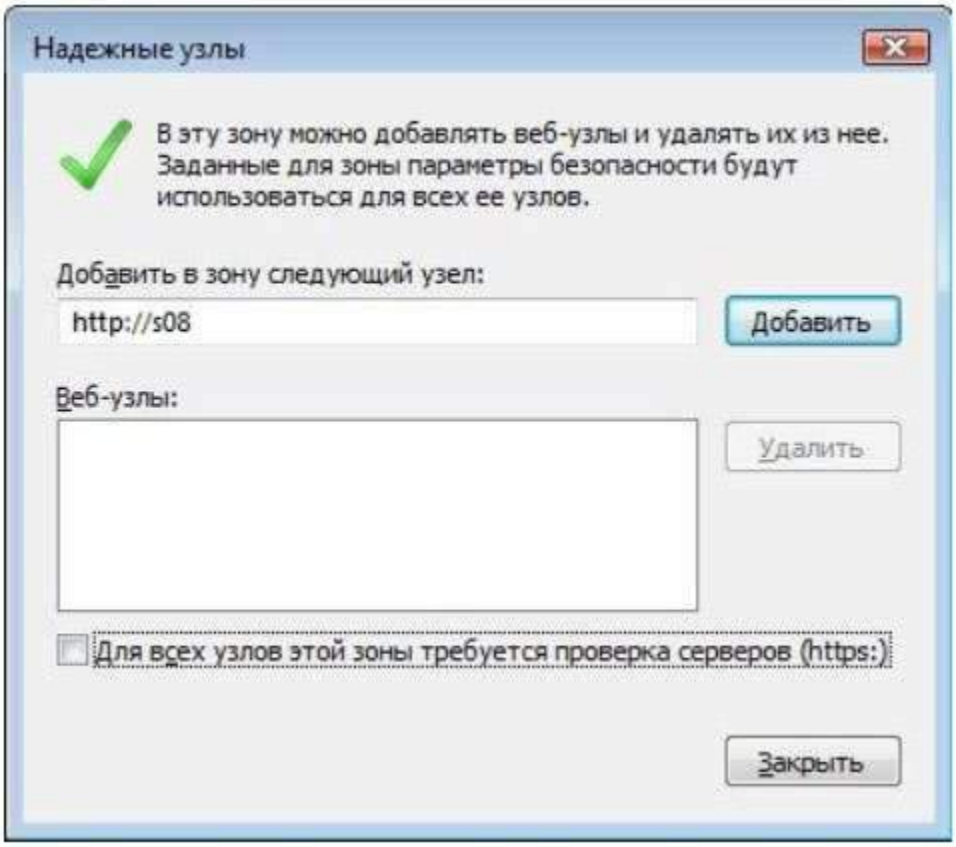


Рис.11. Добавление узла в список надежных.

ПРАКТИЧЕСКАЯ РАБОТА №34.
АВТОМАТИЧЕСКОЕ ОБНОВЛЕНИЕ ОПЕРАЦИОННОЙ СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ СЛУЖБЫ WSUS

Цель работы:

Научиться выполнять автоматическое обновление операционной системы с использованием службы WSUS.

В данной практической работе мы рассмотрим пример организации автоматического обновления программного обеспечения в сети предприятия. Речь будет идти об обновлении ПО разработки Microsoft и использовании программного средства Window Server Update Services (WSUS). Этот продукт доступен для бесплатного получения с сайта Microsoft (дополнительную информацию можно получить на странице WSUS, http://technet.microsoft.com/ru-ru/wsus/default(en-us).aspx).

Часть 1. Установка сервера обновлений.

Задача организации своевременной установки обновлений и исправлений является очень важной как с точки зрения обеспечения информационной безопасности, так и для обеспечения стабильности работы системы. Для отдельно стоящего компьютера с операционной системой Windows XP она может быть решена путем настройки службы автоматического обновления – Пуск->Панель управления -> Автоматическое обновление (рис.1). Аналогичные настройки можно сделать и в более поздних версиях ОС.

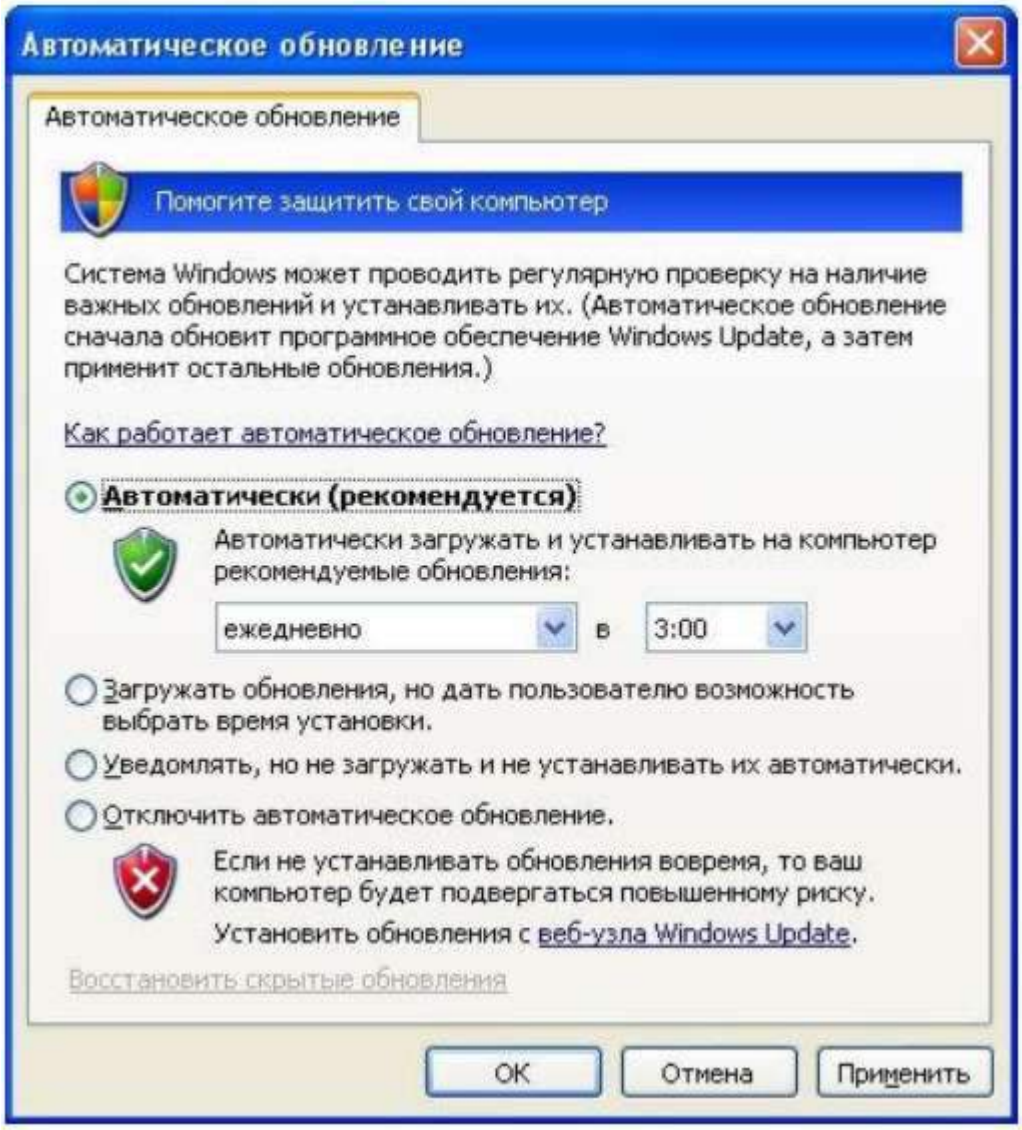


Рис.1. Настройка службы автоматического обновления

В сети предприятия (начиная уже с сетей в несколько десятков компьютеров), использование такого подхода имеет ряд недостатков: - неэффективное использование трафика, т.к. каждый компьютер будет скачивать одни и те же обновления; - сложно контролировать распространение обновлений; - нет возможности определить для отдельных узлов специальный порядок установки обновлений (это может потребоваться, если используются приложения, несовместимые с отдельными обновлениями). Перечисленные задачи можно решить внедрением WSUS. В этом случае, служба автоматического обновления рабочей станции будет получать обновления с корпоративного сервера WSUS в соответствии с определенной администратором политикой (предполагается, что компьютеры организованы в домен Windows). Текущая версия программы - WSUS 3.0 SP2. Для ее успешного развертывания нужно учитывать следующие требования и ограничения: продукт устанавливается на ОС Windows Server 2008 или Windows Server 2003 Service Pack 1 и выше; WSUS не будет работать на серверах, где запущена служба Terminal Services; для работы продукта потребуется web-сервер Internet Information Services (IIS); при этом, если на том же сервере размещаются еще какие-то web-сайты, то кроме сайта WSUS

допускается не более 1 сайта, использующего TCP-порт 80; WSUS не может быть установлен на сжатые диски (т.е. туда, где для экономии места используется компрессия средствами NTFS); для установки WSUS потребуется минимум 1 Гб дискового пространства на системном разделе, 2 Гб – на разделе, где будет храниться база данных и не менее 20 Гб для хранения самих обновлений (конкретный объем зависит от списка обновляемых продуктов и может превышать 40 Гб). Прим.: в ходе установки WSUS для учебных целей выполнение последнего требования необязательно – см. ниже; для обслуживания базы данных WSUS может использоваться уже установленный в сети Microsoft SQL Server 2005, а при его отсутствии – будет установлена урезанная версия, называемая Windows Internal Database. Рассмотрим теперь установку продукта на Windows Server 2008. Предположим, что ранее служба IIS не была установлена. Поэтому с помощью оснастки Server Manager надо добавить эту роль (рис.2). При этом, надо учитывать, что входящий в состав Windows Server 2008 IIS 7.0 имеет модульную структуру и по умолчанию не все требуемые для WSUS модули будут установлены. Стоит проверить, чтобы были отмечены для установки следующие модули (рис.3): Common HTTP Features (включая Static Content); ASP.NET, ISAPI Extensions и ISAPI Features (в разделе Application Development); Windows Authentication (в разделе Security); IIS Metabase Compatibility (в разделе Management Tools, подраздел IIS 6 Management Compatibility). Для просмотра отчетов понадобится установить компонент Microsoft Report Viewer Redistributable, который доступен на сайте Microsoft по ссылке
http://www.microsoft.com/downloads/en/confirmation.aspx?familyId=bb196d5d-76c2-4a0e- 9458-267d22b6aac6&displayLang=en.

Когда все подготовительные действия выполнены, перейдем к рассмотрению самого процесса установки WSUS. После запуска мастер установки уточнит, что будет устанавливаться – полностью сервер или только консоль управления. Нам нужна полная установка.

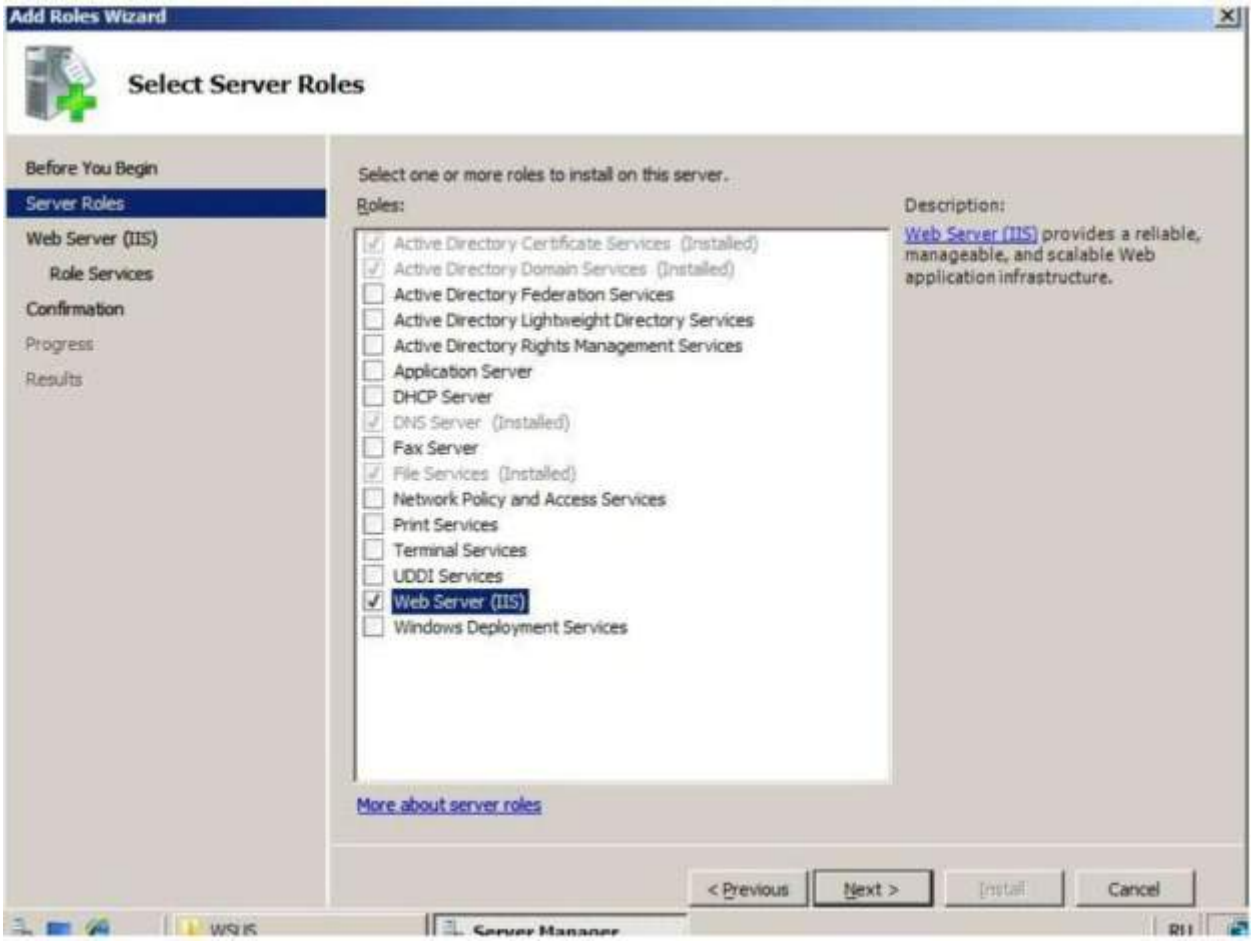


Рис.2. Добавление роли IIS.

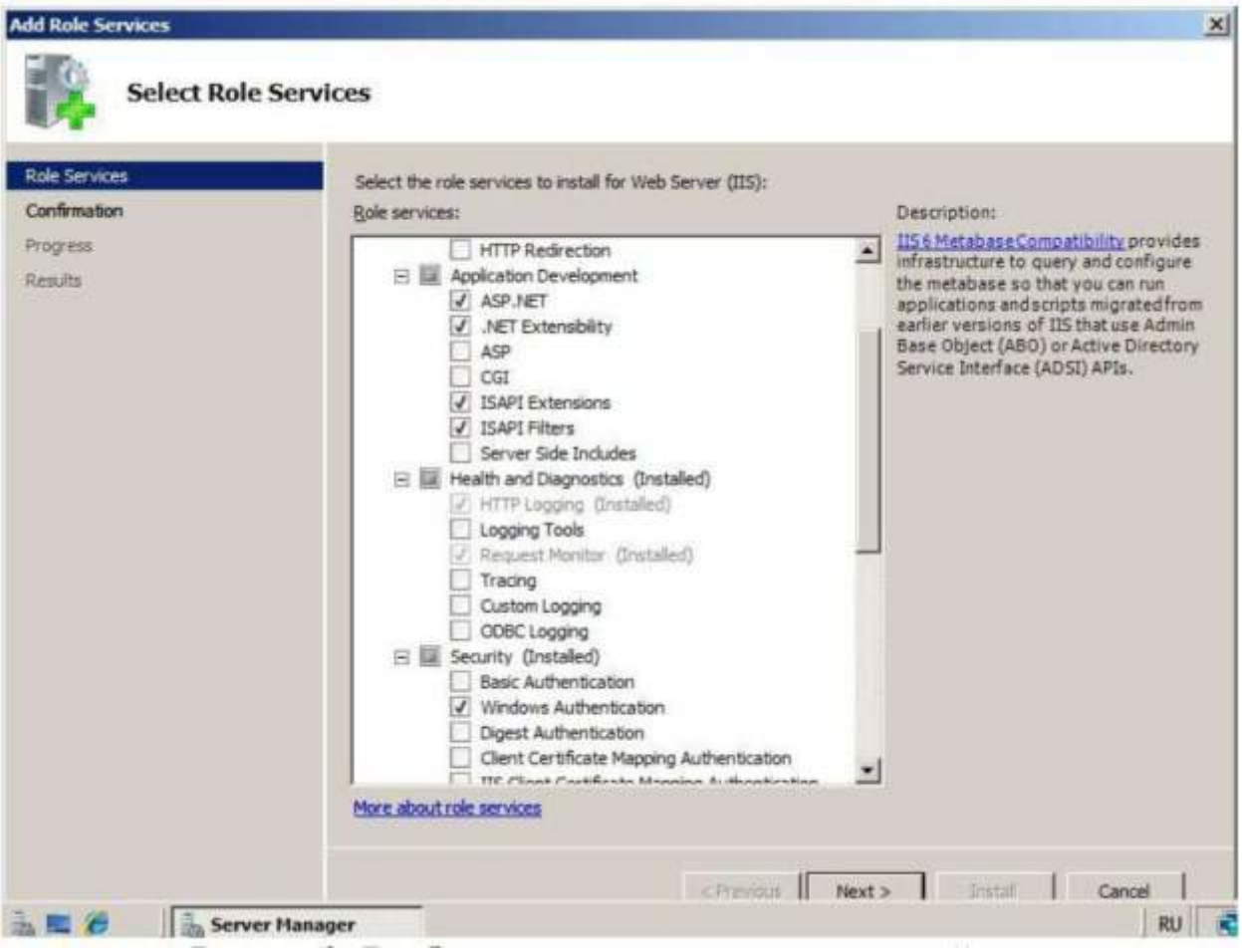


Рис.3. Выбор устанавливаемых модулей IIS.

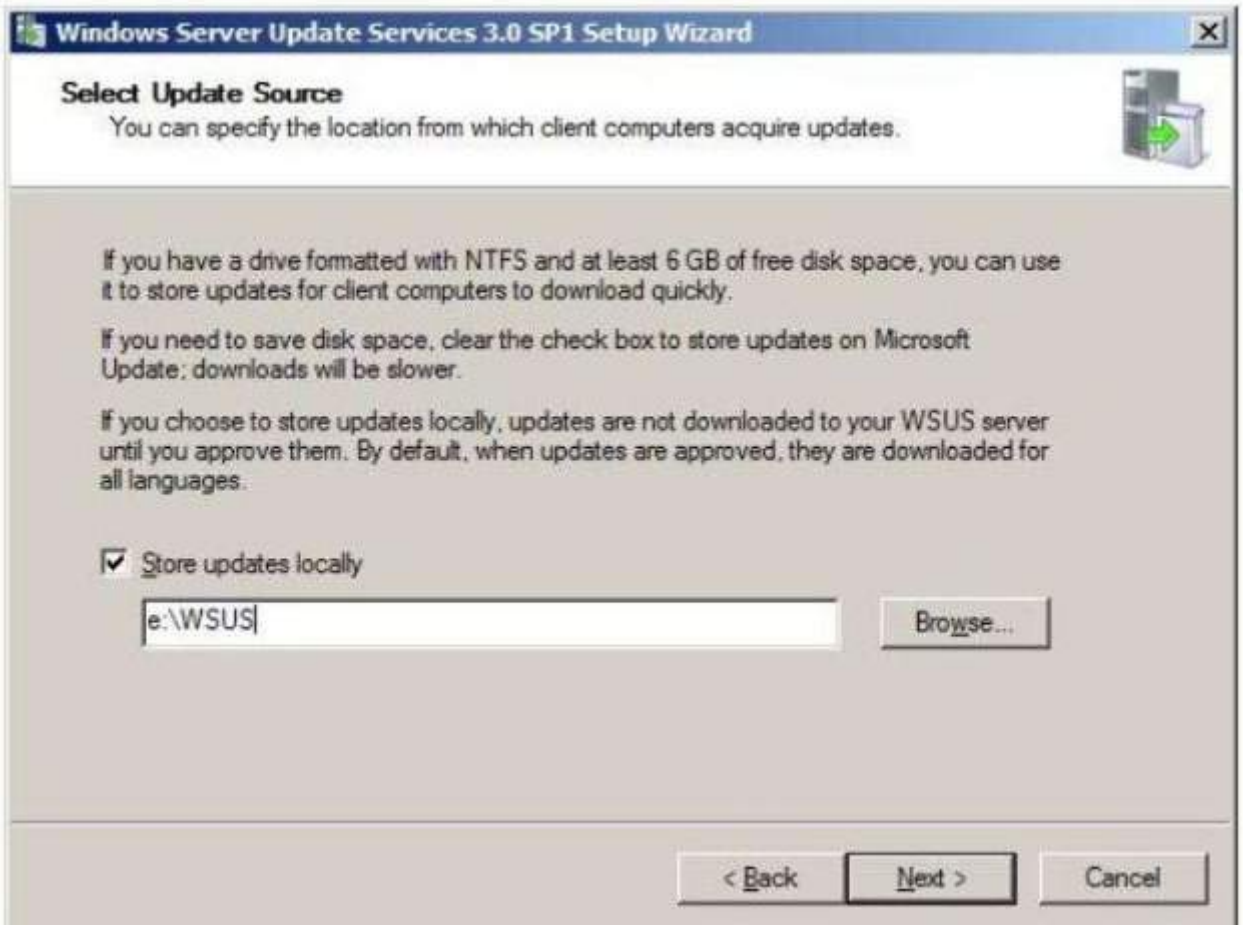


Рис.4. Выбор каталога для установки.

Далее, после подтверждения, что мы принимаем лицензионное соглашение, появится окно выбора каталога для установки (рис.10.4). Если установка выполняется исключительно в учебных целях, лучше сбросить флажок «Store updates locally», тогда сами обновления не будут скачиваться с сайта Microsoft на ваш сервер (синхронизироваться будет только информация о вышедших обновлениях). Как уже отмечалось выше, информацию об обновлениях WSUS хранит в базе данных СУБД Microsoft SQL Server. На рис.10.5 представлено окно, позволяющее определить, будет ли устанавливаться Windows Internal Database или для хранения данных будет использоваться уже установленный Microsoft SQL Server.

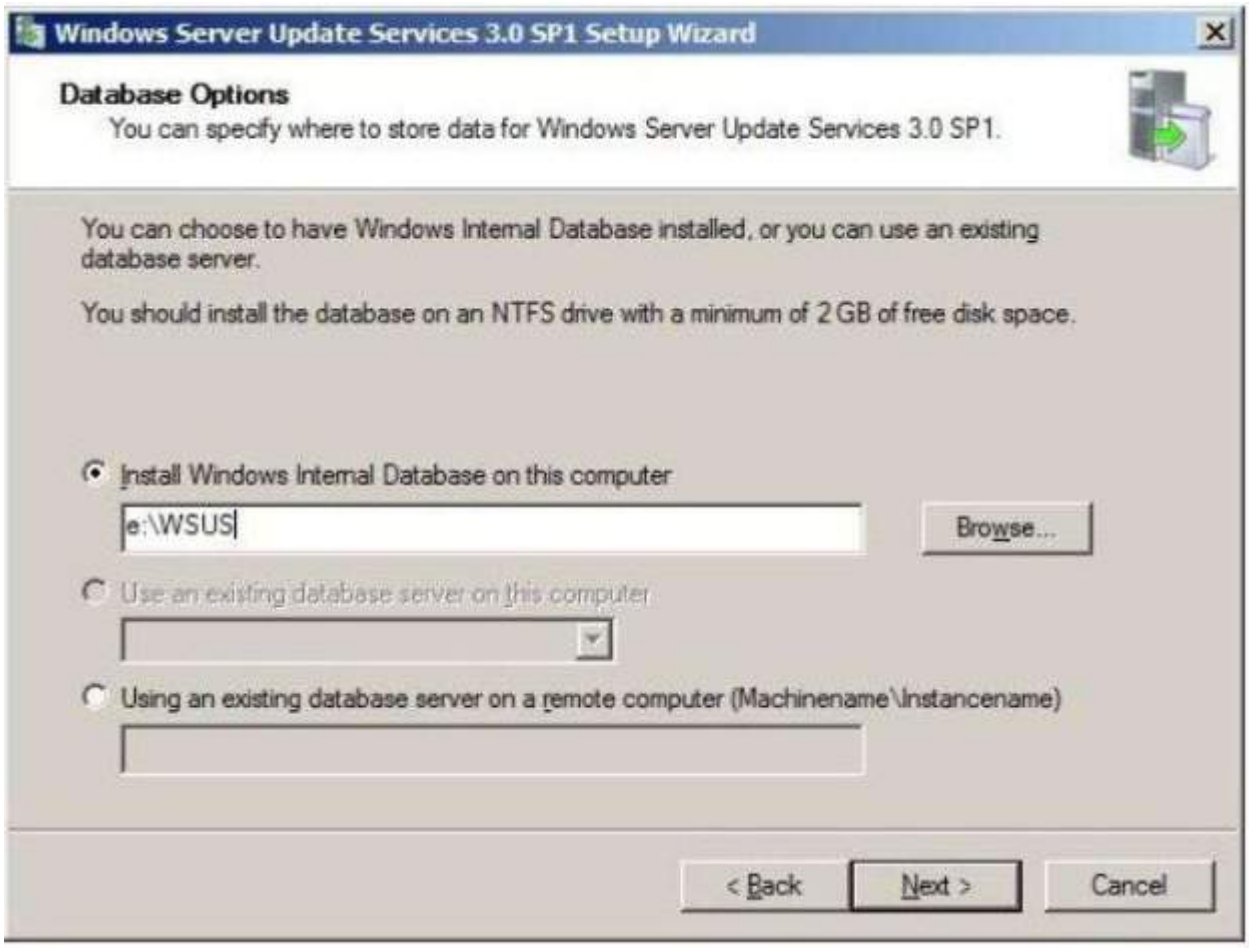


Рис.5 Настройки базы данных.

Следующее окно мастера позволяет сделать выбор между использованием для нужд службы WSUS сайта IIS по умолчанию и созданием нового сайта. Если оставить настройки по умолчанию, сайт WSUS будет доступен по ссылке вида http://<имя сервера> (т.к. используется 80-й TCP-порт его в ссылке указывать не надо).

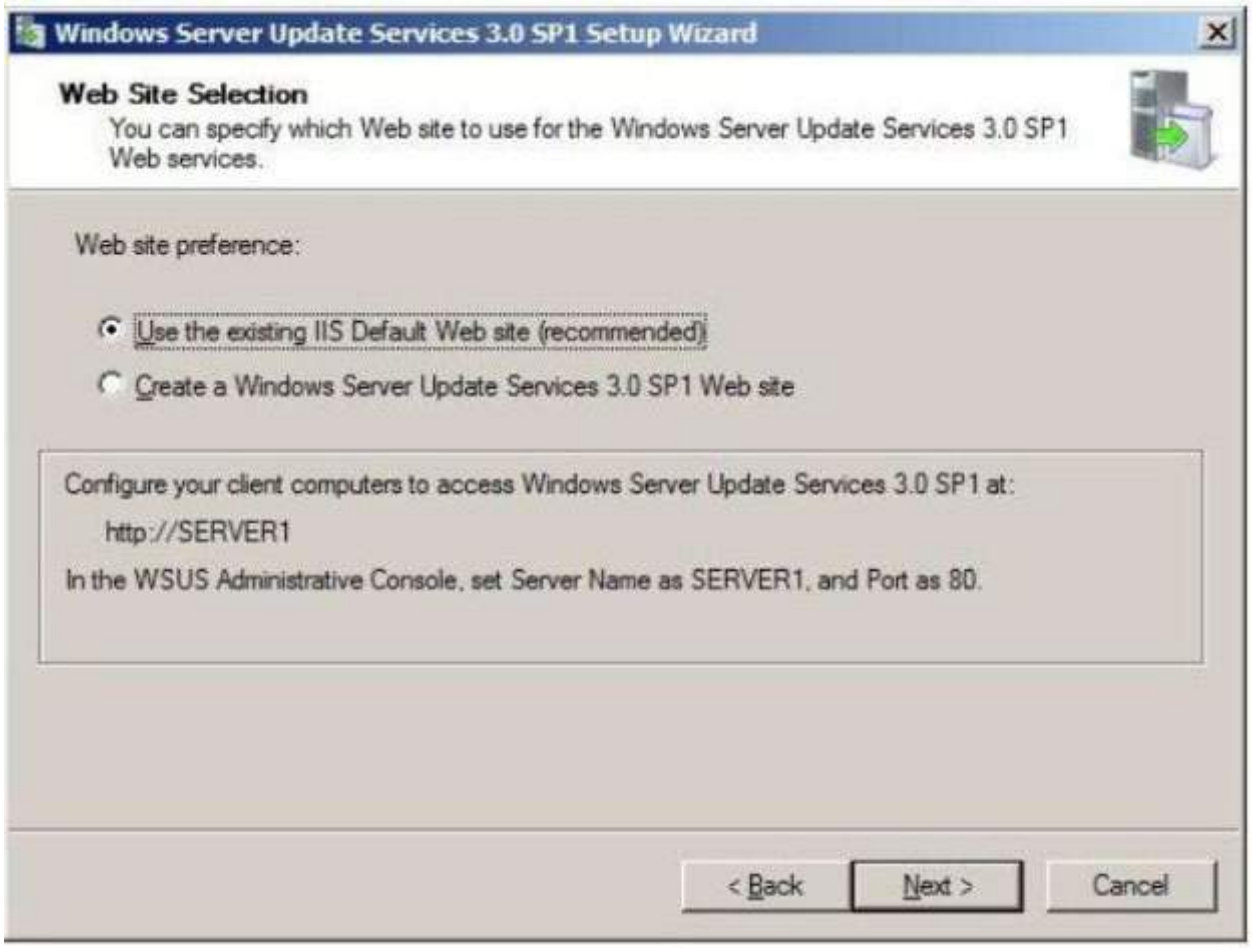


Рис.6. Выбор сайта.

После окончания работы мастера установки (Windows Server Update Services 3.0 SP1 Setup Wizard) запустится мастер конфигурирования. Главное, что здесь надо решить – организуем мы отдельно стоящий сервер обновлений или сервер, включенный в иерархию. В первом случае, обновления берутся напрямую с сайта Microsoft, во втором - вышестоящие по иерархии серверы раздают обновления подчиненным (рис.7). Дальнейшие окна мастера позволяют сделать настройки для работы через проксисервер (если такая схема используется); провести первую синхронизацию с сервером Microsoft (для этого должно быть установлено подключение к Интернет); выбрать языковые версии, для которых будут получаться обновления (рис. 8). Следующие окна позволяют указать обновляемые продукты и типы обновлений (рис. 9 -10). Список достаточно обширен и лучше выбрать только то ПО, которое используется в сети, и те типы обновлений, в которых есть потребность (тогда не придется хранить гигабайты ненужных обновлений и упростится задача администрирования).

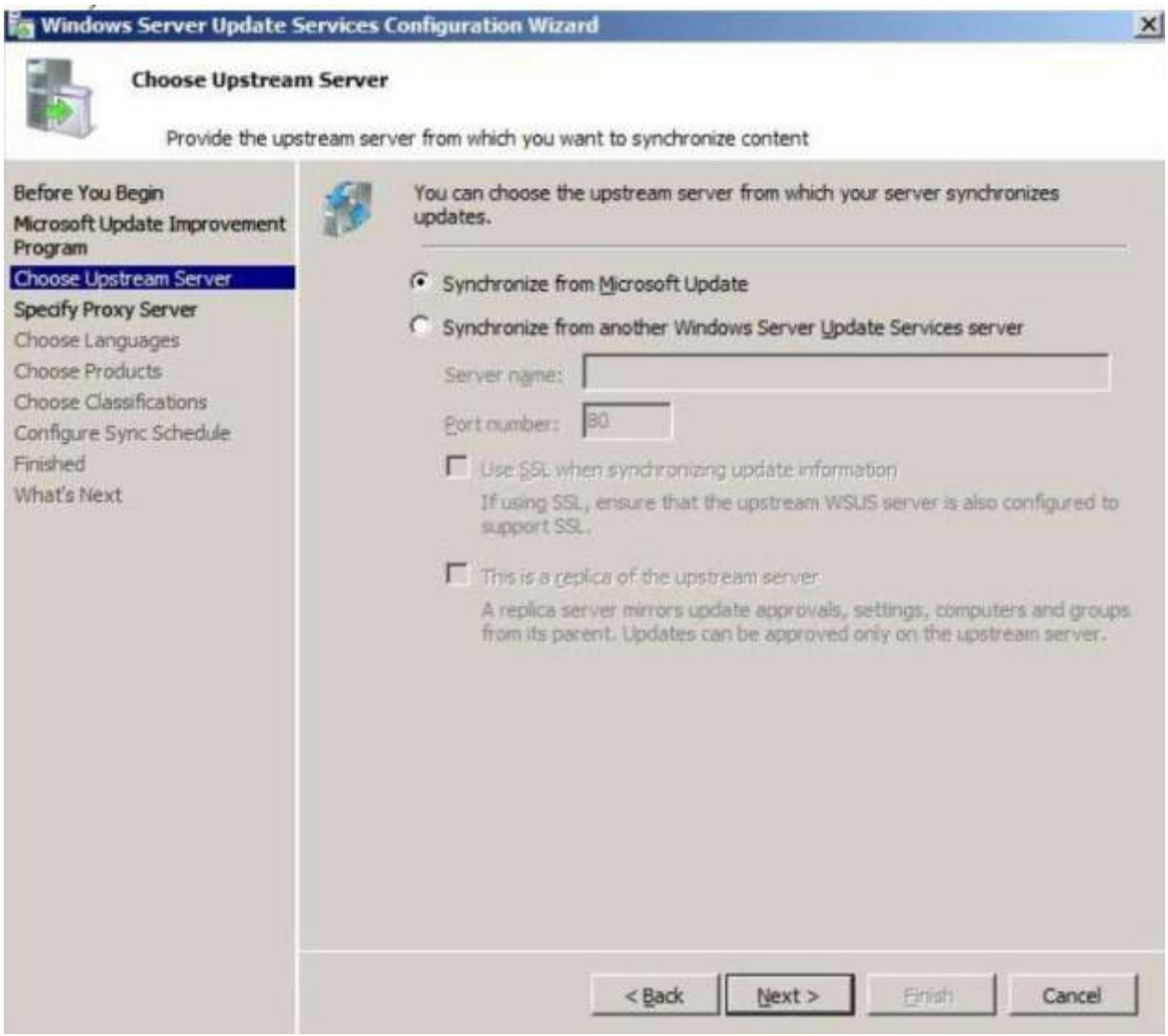


Рис.7. Выбор типа конфигурации – простая или иерархическая.

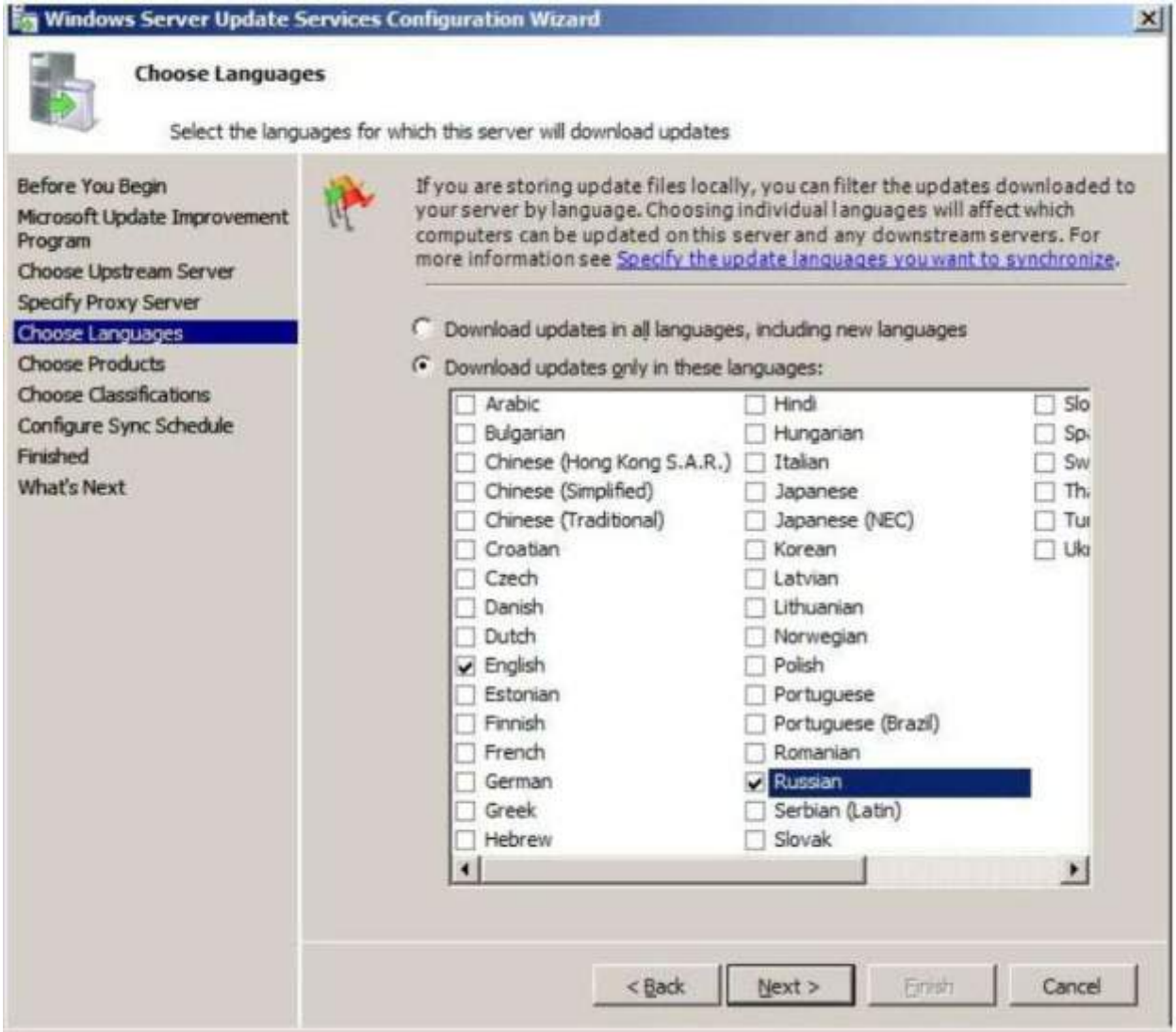


Рис.8. Выбор языковых версий.

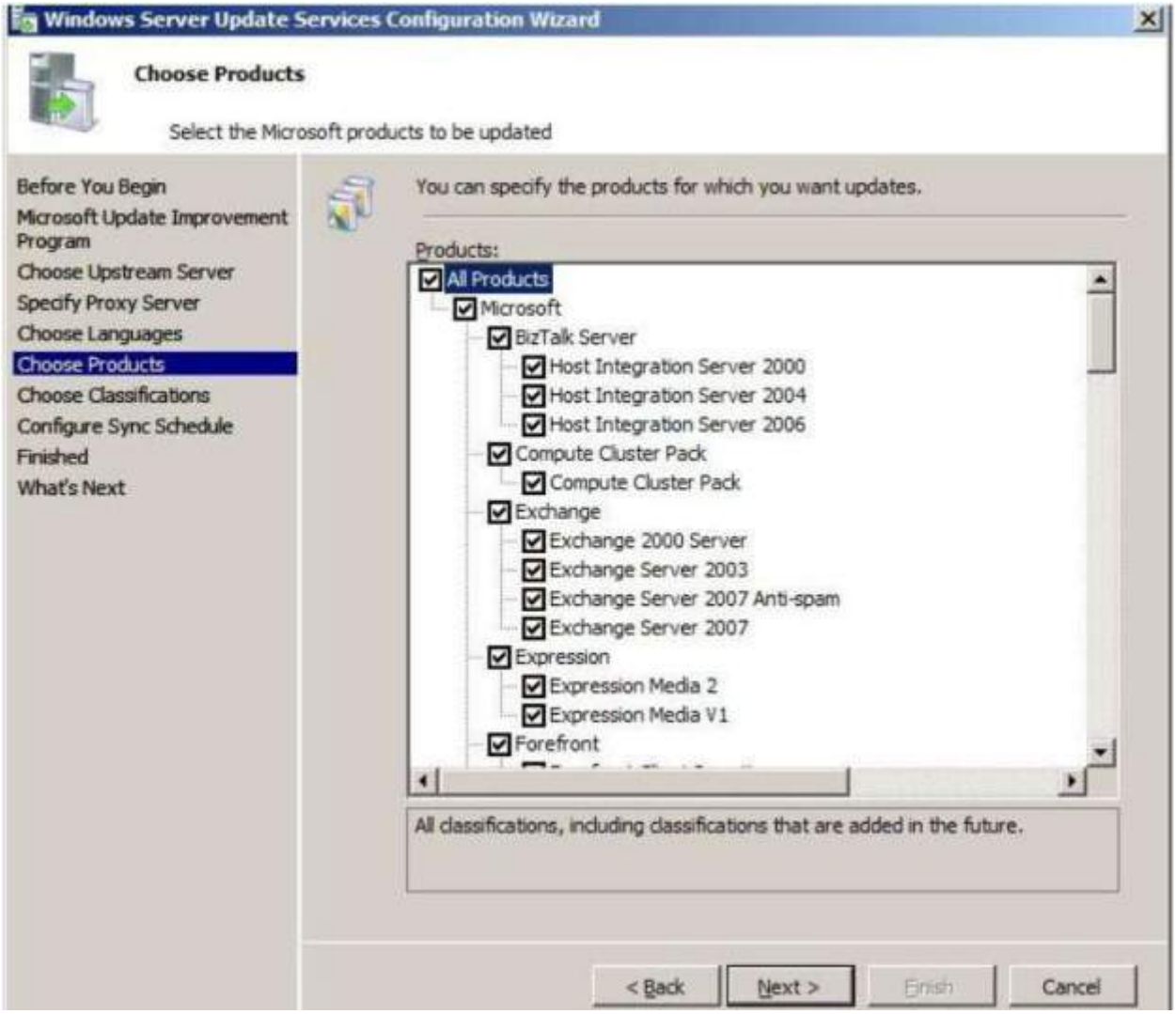


Рис.9. Выбор обновляемых продуктов.

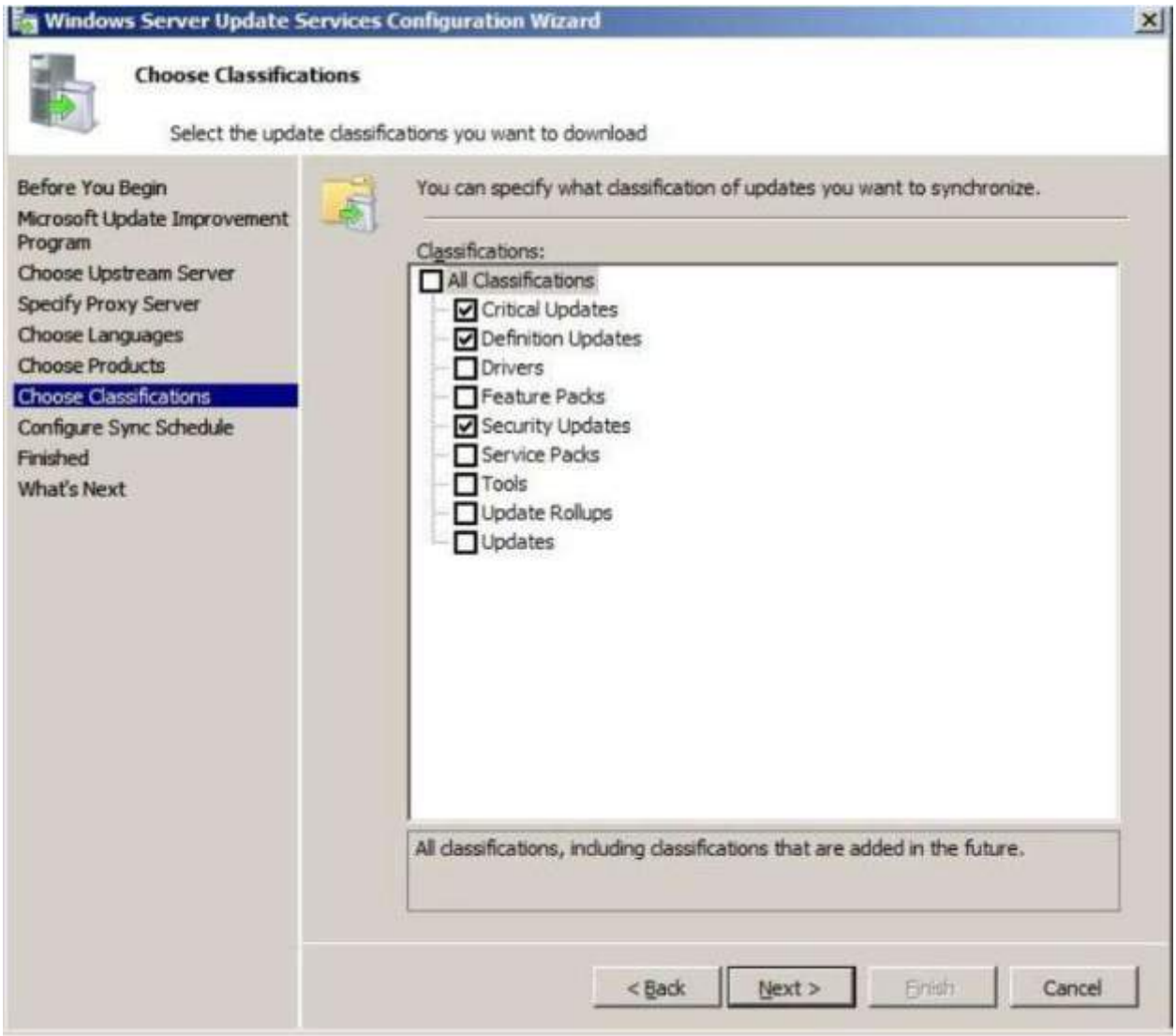


Рис.10. Выбор «классов» обновлений.

Дальше можно указать расписание синхронизации с сервером Microsoft и нужно ли проводить начальную синхронизацию сразу после настройки (этот флажок можно снять).

Задание. *Перед запуском виртуальной машины с Windows Server 2008, добавьте ей дополнительный виртуальный жесткий диск объемом 10 Гб (для экономии места, можно выбрать тип Dynamically expanding (динамически увеличивающийся)) Дистрибутив WSUS поместите в одну из папок на жестком диске. Подключите ее к виртуальной машине. Подготовьте сервер с Windows Server 2008 к установке сервера обновлений.Выполните установку и начальное конфигурирование WSUS.*

Часть 2. Управление обновлениями

Теперь рассмотрим порядок действий по настройке сервера обновлений для эффективного использования в конкретной информационной системе. Настройки делаются через оснастку Microsoft Windows Server Update Services 3.0 SP1, которая после установки должна появиться в разделе Administrative Tools меню Start (рис.11). Начнем с управления группами компьютеров. По умолчанию создается группа Unassigned Computers, в которую будут помещаться все компьютеры. С помощью контекстного меню узла All

Computers можно создать новую группу, как это показано на рисунке. Если заранее создать группы, можно будет сразу определить, какие обновления устанавливать на компьютеры, относящиеся к той или иной группе. Можно сделать правило для автоматического одобрения (approval) установки обновлений для определенных групп или всех компьютеров. Делается это из раздела Options, пункт Automatic Approvals (рис.12). Там можно создать собственное правило или отредактировать правило по умолчанию (Default Automatic Approval Rule).

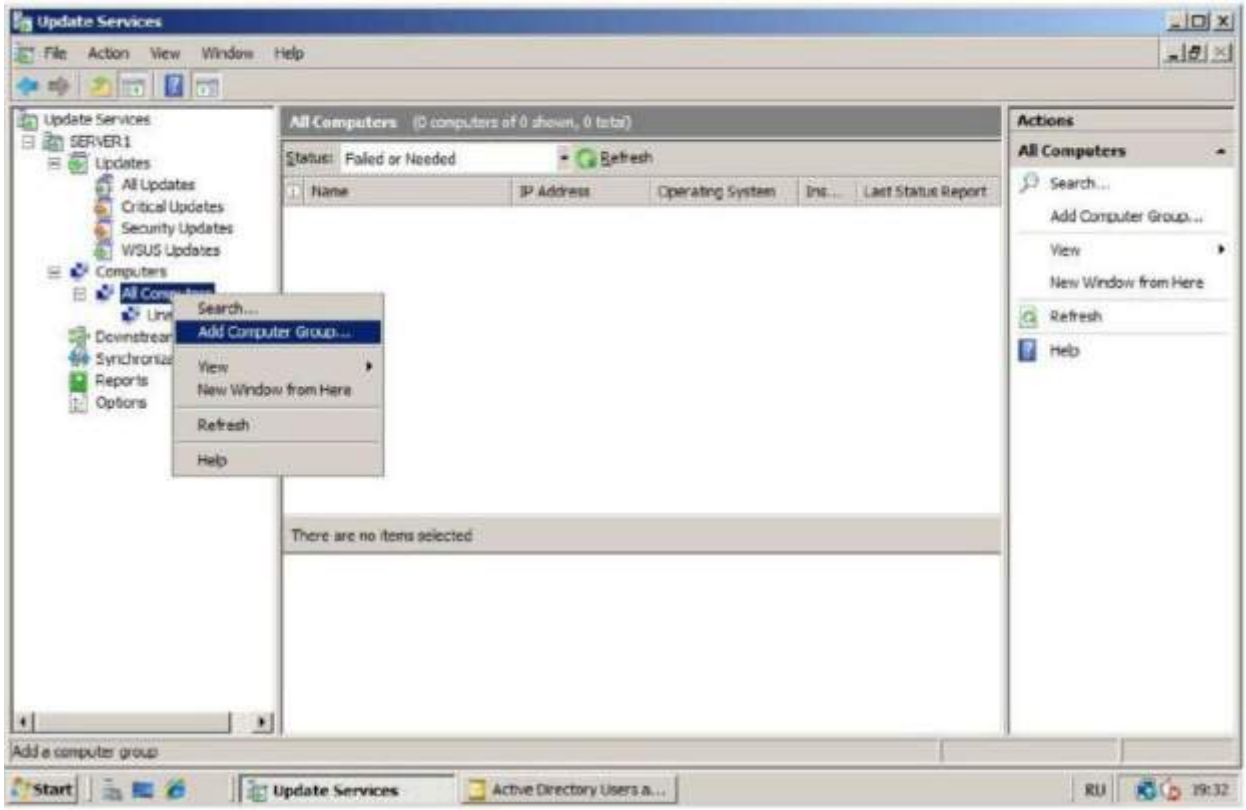


Рис.11. Создание новой группы компьютеров.

Рис.12. Настройка правил обновления.

Когда правила определены, можно провести синхронизацию с сервером Microsoft для получения перечня обновлений (рис.13). Синхронизация может быть запущена вручную из раздела Synchronizations или проводиться по расписанию (для успешной синхронизации должно быть установлено подключение к Интернет).

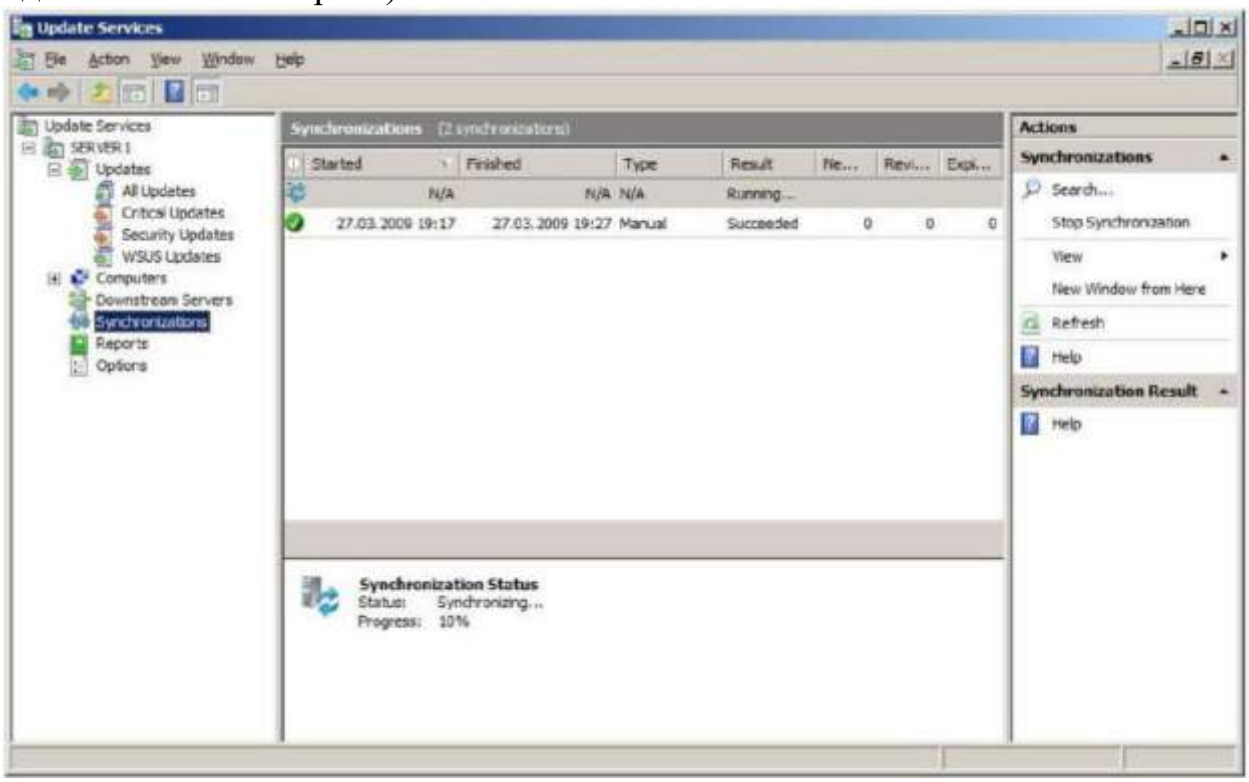


Рис.13. Настройка синхронизации.

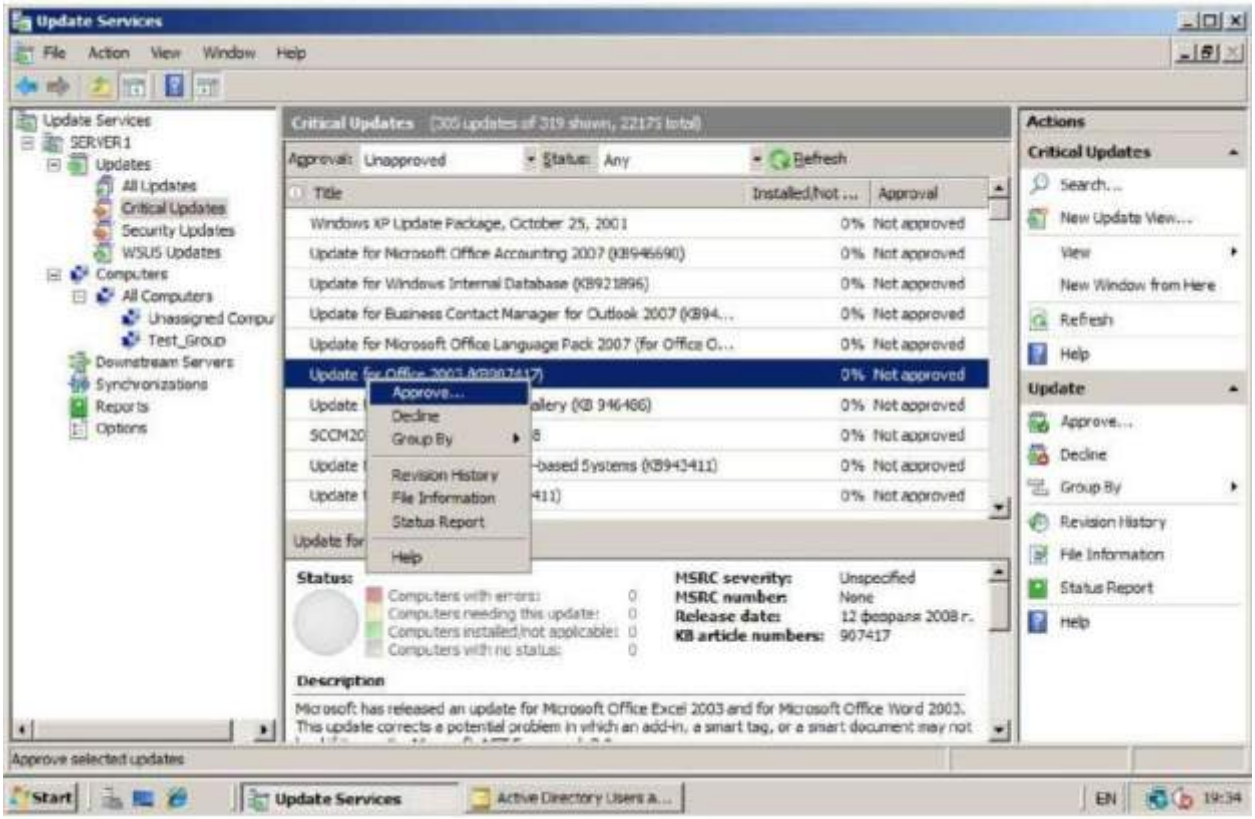


Рис.14. Одобрение обновлений вручную.

После того как проведена синхронизация и сработало правило «автоматического одобрения», отдельные обновления могут оказаться не одобренными к распространению. Администратор может их одобрить вручную, выбрав в разделе Updates с помощью фильтра и воспользовавшись контекстным меню (рис.14).

***Задание**. Создайте группы компьютеров. Подготовьте правило автоматического одобрения обновлений с учетом созданной структуры групп. Проведите синхронизацию с сервером Microsoft. Если какие-то из критических обновлений не одобрены автоматически, сделайте нужные настройки вручную.*

Часть 3. Распространение обновлений

Как уже отмечалось выше, для эффективного использования WSUS нужно, чтобы компьютеры были организованы в домен Windows. Тогда с помощью доменной политики можно настроить службу обновлений компьютеров-членов домена на получение обновлений с сервера WSUS. Для редактирования политики в меню Administrative Tools выберем оснастку Group Policy Management, в ней найдем доменную политику по умолчанию – Default Domain Policy, и в контекстном меню выберем пункт Edit. В открывшемся окне редактора политик раскроем узел Computer Configuration ->Policies-> Administrative Templates. В контекстном меню узла Administrative Templates выберем добавление шаблона Add/Remove Templates (рис. 15).

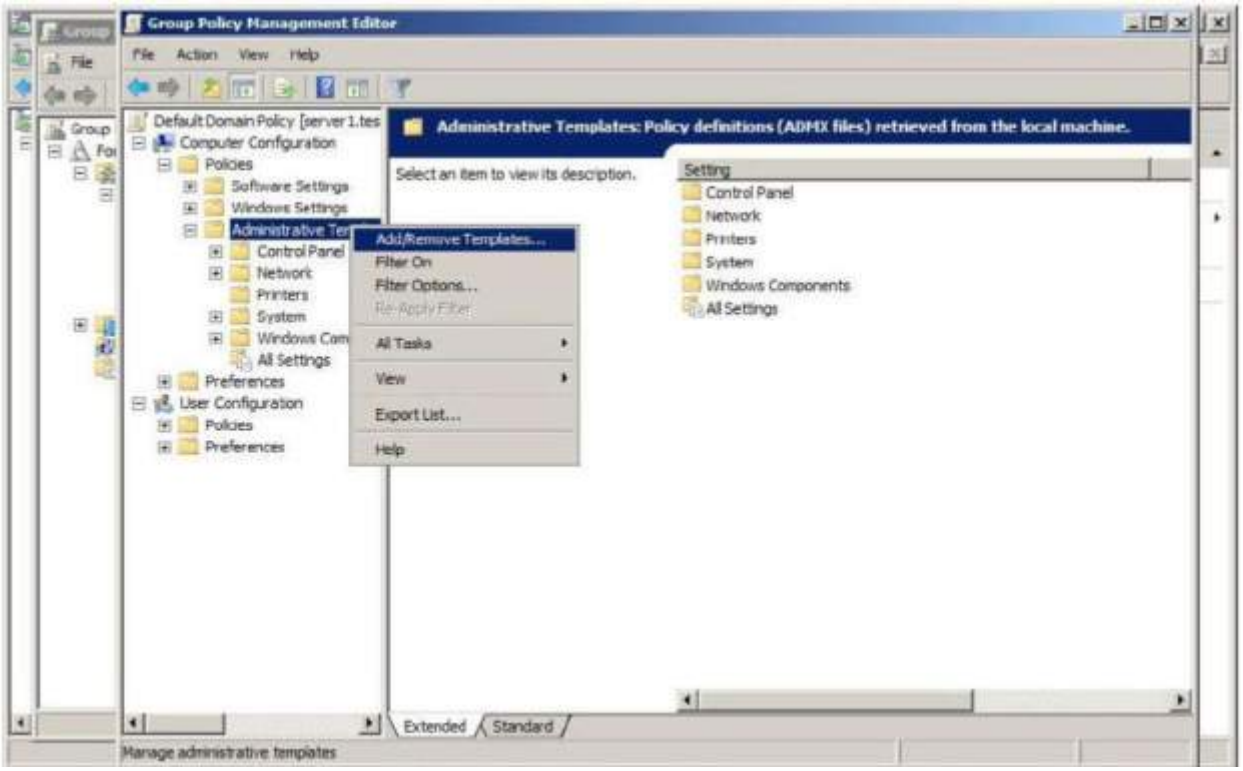


Рис.15. Добавление административного шаблона.

В папке для шаблонов (например, C:\Windows\inf) найдем шаблон **wuau**, записанный туда при установке WSUS (рис.16). После того как шаблон добавлен, понадобится настроить компьютеры на получение обновлений. Поочередно раскроем узлы политики Computer Configuration -> Administrative Templates -> Windows Components -> Windows Update. Двойным щелчком откроем Specify intranet Microsoft update service location, активируем политику (переключатель - в Enabled) и пропишем URL сервера обновлений в строках Set the intranet update service for detecting updates и Set the intranet statistics server (рис.16). На рисунке представлена настройка для сервера обновлений Server1.

Среди прочих политик для службы Windows Update хотелось бы также отметить Automatic Updates detection frequency, позволяющую определить частоту проверки рабочей станцией наличия новых обновлений, и Configure Automatic Updates Properties, которая дает возможность указать правила работы с обновлениями – устанавливать, только уведомлять пользователя и т.д.

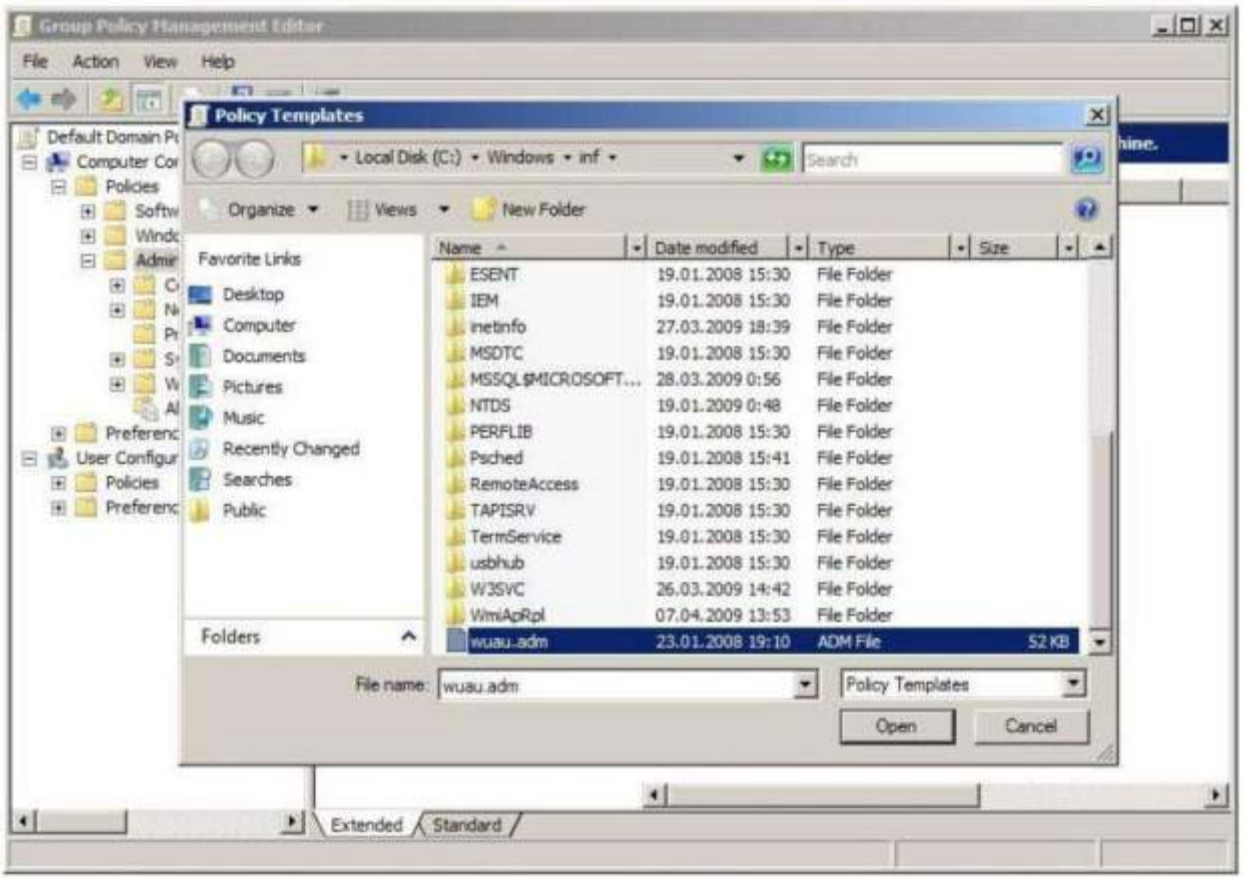


Рис.15. Добавление административного шаблона (продолжение).

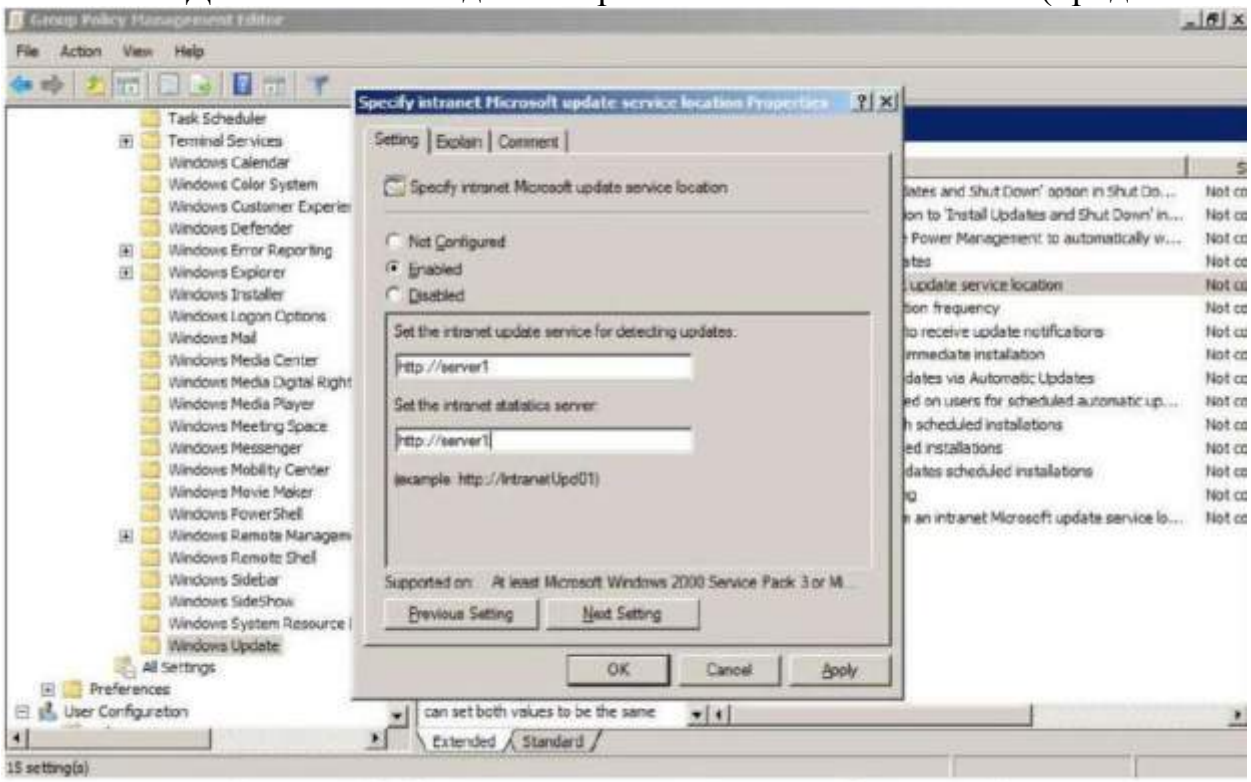


Рис.16. Описываем путь к серверу обновлений.

Когда настройки сделаны и сохранены, можно дождаться момента, когда они применятся, или ускорить это процесс, выполнив на компьютерах команду gpupdate /force. После того, как компьютер обратится за обновлениями,

администратор сможет увидеть его в консоли управления и при необходимости переместить его из группы Unassigned Computers в какую-либо другую (рис. 17). Также администратору доступна информация о числе обновлений, требующихся для данного компьютера, ошибках при установке обновлений и т.д. Чтобы увидеть общую картину, можно сформировать отчеты (узел Reports).

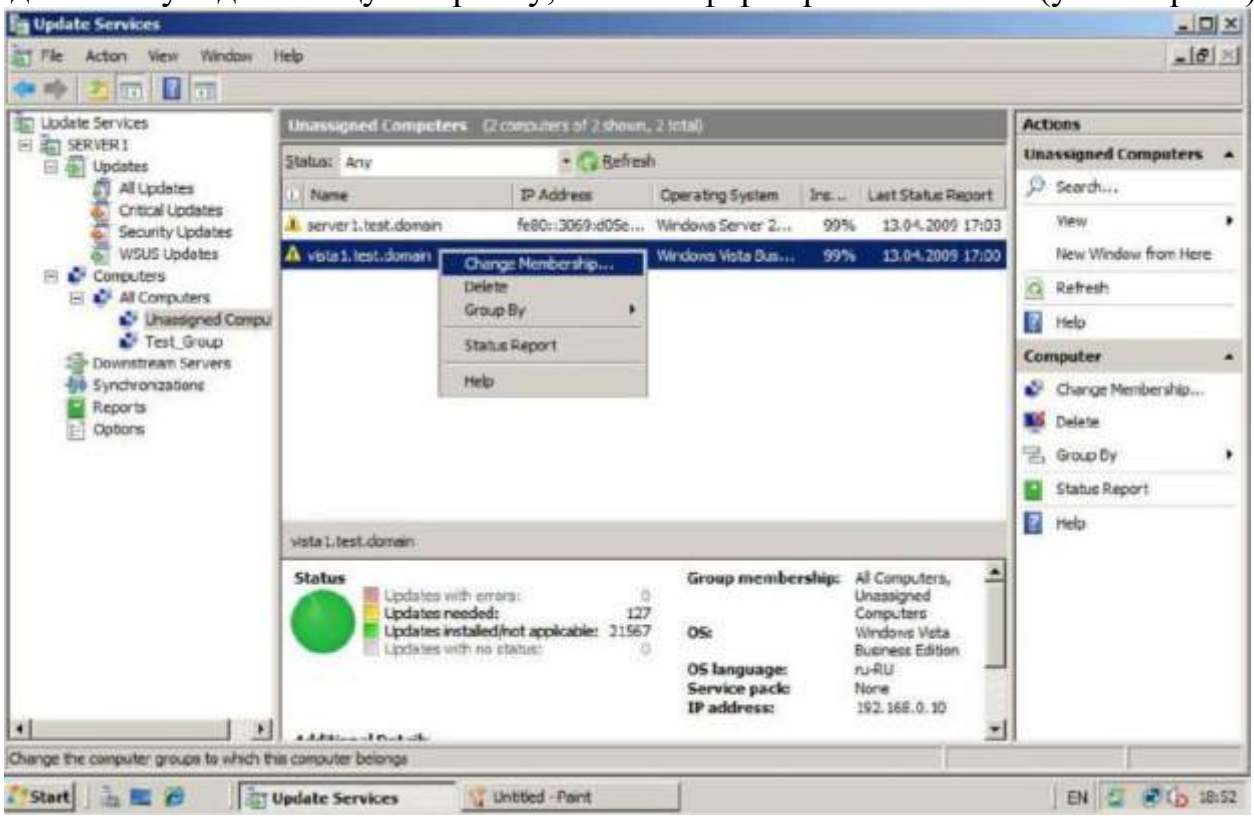


Рис. 17. Перемещение компьютера в другую группу.

***Задание**. Настройте политику распространения обновлений. Проверьте ее работу. Сформируйте отчет о распространении обновлений.*

ПРАКТИЧЕСКАЯ РАБОТА № 35.
РЕЗЕРВНОЕ КОПИРОВАНИЕ В WINDOWS SERVER 2008

Цель работы:
Научиться выполнять резервное копирование в Windows Server 2008.

Цель данной практической работы – познакомиться со средствами организации резервного копирования в операционной системе Microsoft Windows Server 2008. Важность процедуры резервного копирования очень высока. В тех случаях, когда сбои или действия пользователей (случайные или преднамеренные) приводят к изменению или удалению данных, повреждению программных компонент системы, резервное копирование позволяет снизить причиненный ущерб и значительно ускорить восстановление системы. При разработке политики резервного копирования нужно определить, как минимум, следующие параметры:
- частоту выполнения резервных копий;
- порядок восстановления данных из резервных копий;

- объем носителей информации, выделяемых для хранения резервных копий;- количество хранимых копий;
- вопросы обеспечения безопасности носителей резервных копий.

Для выполнения лабораторной работы сконфигурируйте виртуальную машину с Windows Server 2008 так, чтобы кроме диска, куда установлена операционная система, у нее были еще два локальных диска одинакового размера (например, диск C: с ОС и диски E: и F: для экспериментов). Также для выполнения резервного копирования по расписанию понадобится один неформатированный раздел большого размера.

Рис.1. Оснастка Server Manager позволяет добавить компоненты.

Утилиты резервного копирования Windows Server 2008 существенно отличаются от того, что было в Windows Server 2003, где эти задачи решались с помощью утилиты ntbackup. Чтобы их использовать, для начала требуется их установить. Делается это с помощью оснастки Server Manager, где надо выбрать пункт Add Feature в разделе Features (рис.1) и в появившемся списке выбрать пункт Windows Server Backup Features (рис.2.).

Как видно на рис. 2, предлагается выбрать следующие опции:
- Windows Server Backup;
- Command-line tools (утилиты командной строки).

Установка последних, позволяет управлять резервным копированием с помощью сценариев и требует установки Windows PowerShell.

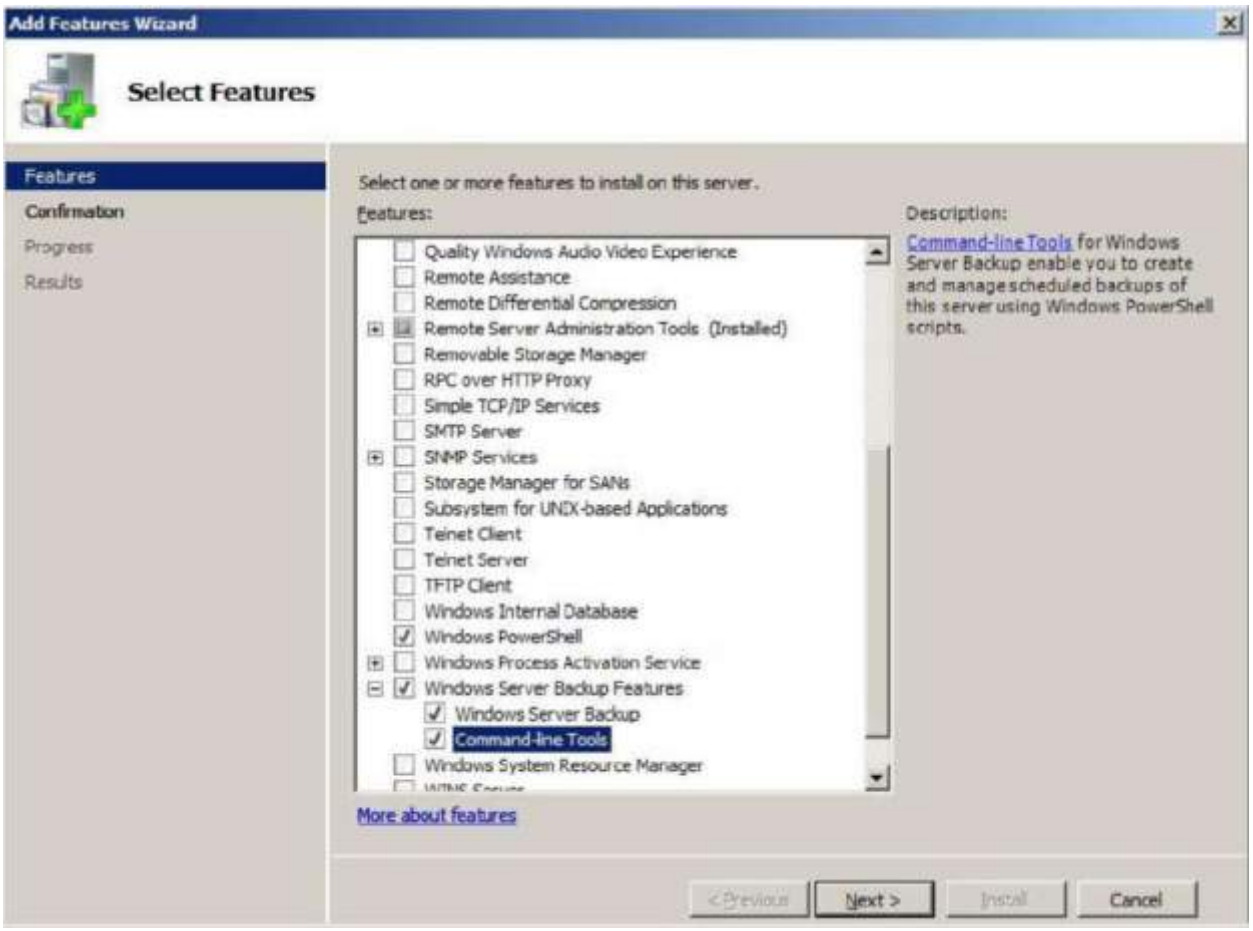


Рис.2. Добавляем утилиты администрирования.

После установки, в меню Administrative Tools становится доступной оснастка Windows Server Backup. С ее помощью можно проводить резервное копирование данных на локальном или удаленном компьютере (если это разрешено настройками). Рассмотрим, как это происходит. Запустим утилиту. Резервное копирование может проводить пользователь, состоящий в группе Administrators (Администраторы) или Backup Operators (Операторы архива). При этом, у членов группы Backup Operators при запуске оснастки Windows Server Backup будет дополнительно запрашиваться пароль (в окне User Account Control), т.к. эти операции относятся к разряду потенциально опасных. В окне оснастки в списке доступных действий (Actions), расположенном в правой части экрана, выберем опцию Backup Once … (т.е. однократная архивация). Запустившийся мастер резервного копирования предложит выбор между настройками для уже запланированного копирования (The same options that you used in the Backup Schedule Wizard for scheduled backups) и новыми (Different options). Нужно выбрать второй вариант (если, как в нашем примере, утилита ранее не использовалась, то первый пункт списка будет неактивен). Следующее окно мастера позволяет выбрать, производить ли полное резервное копирование или копирование отдельных разделов (рис.3). Здесь проявляется первое отличие новых инструментов – резервное копирование отдельных папок и файлов производить нельзя, только логический диск целиком. Хотелось бы также обратить внимание на надпись в нижней части экрана, там дается ссылка

на раздел справки, описывающий выполнение с помощью утилиты командной строки резервного копирования только состояния системы (System State). Выберем вариант Custom. Тогда на следующем экране появится список дисков (рис.4). Устанавливая или снимая отметки, можно указать, данные с каких дисков помещаются в резервную копию. Опция Enable System Recovery включает в архив разделы, где находятся компоненты операционной системы и файлы необходимые для загрузки (т.е. отметку напротив этих разделов будет не снять). Предположим, нам нужно сделать резервную копию диска E:, на котором находятся пользовательские данные. Тогда отметки устанавливаем так, как это сделано на рис.4 и переходим к следующей стадии, на которой нужно определить, куда будет производиться копирование. Это может быть локальный диск (жесткий диск, пишущий DVD-привод и т.д.) или сетевая папка. Надо учитывать, что архивная копия не может сохраняться на диск, входящий в перечень архивируемых. Также нельзя сохранить архив на диск, где хранятся файлы операционной системы

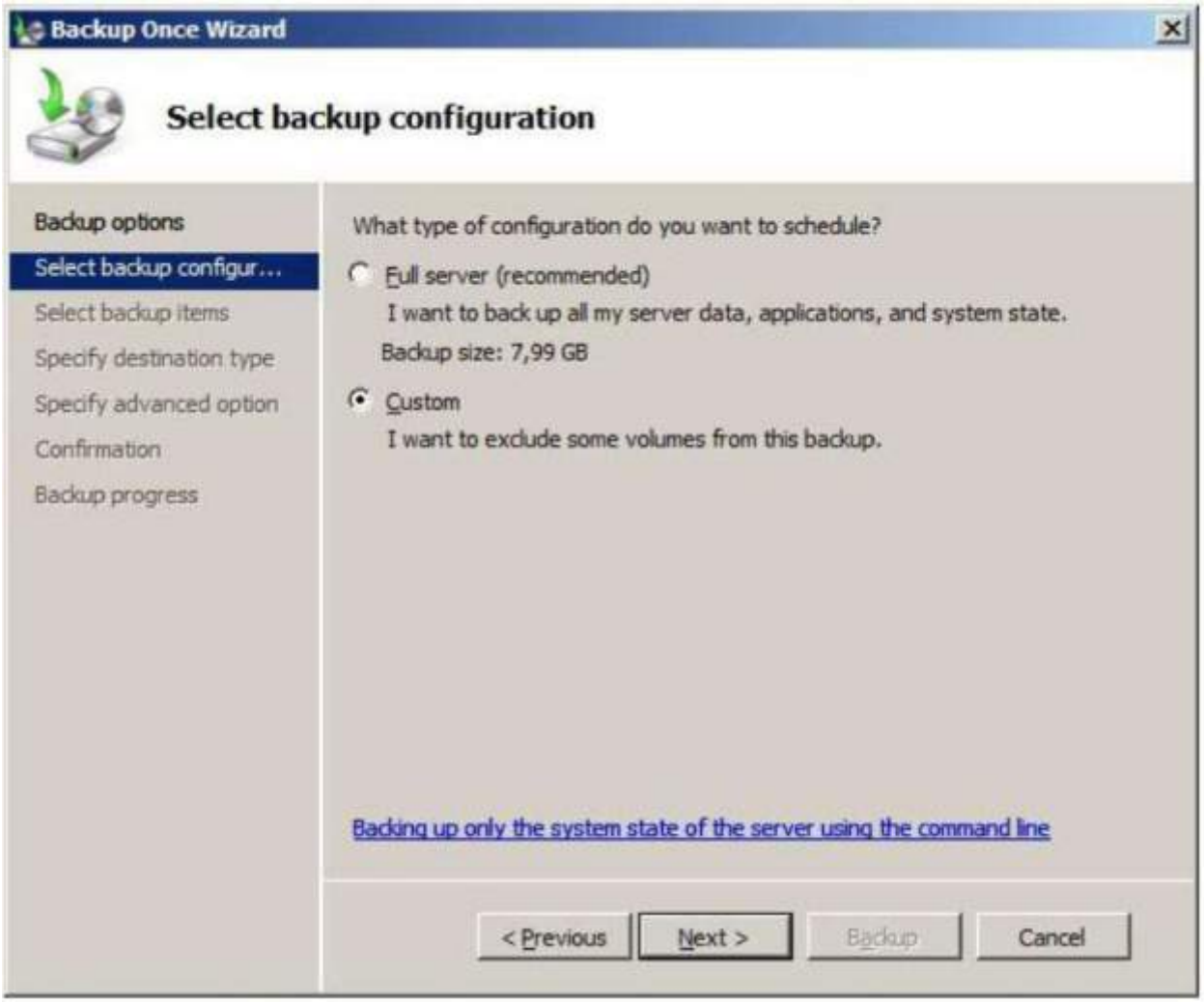


Рис.3. Выбор между полным резервным копированием и копированием отдельных дисков.

Учитывая все вышеизложенное, в рассматриваемом примере можно сделать резервную копию диска E: на диск F:, в сетевую папку или на DVD-диск.

Выберем первый вариант, что и укажем в следующем окне мастера. После чего будет предложено выбрать тип резервного копирования (рис.5).

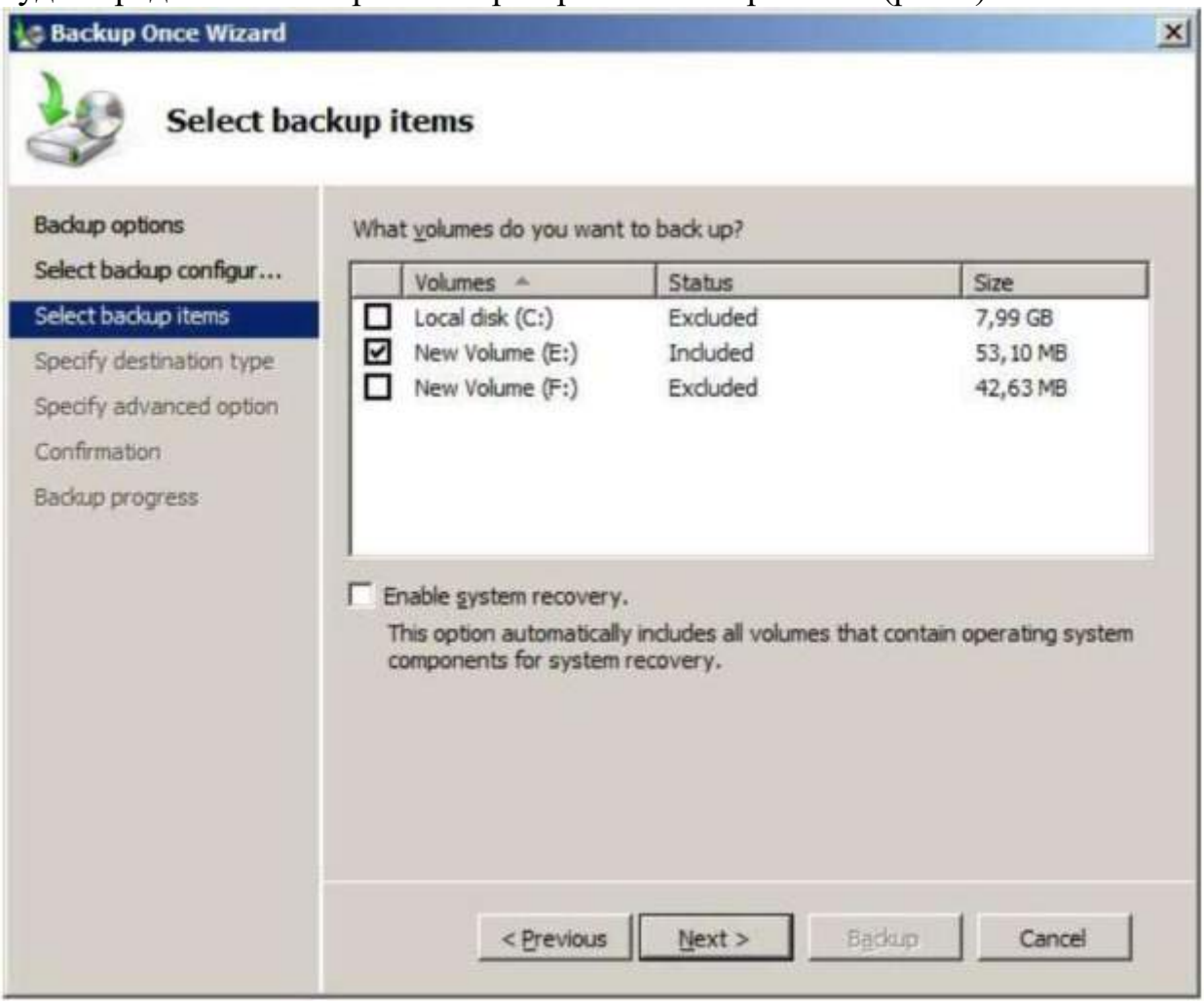


Рис.4 Выбор дисков для резервного копирования.

Рис.5 Выбор типа копирования.

Служба Volume Shadow Copy Service (VSS) может при резервном копировании отмечать файлы, как помещенные в архив, или не делать это. Если кроме средств Windows Server 2008 используются и другие продукты для резервного копирования, рекомендуется выбрать вариант VSS copy backup. Если такого нет, можно смело выбирать вариант VSS full backup. В следующем окне мастера будет запрошено подтверждение и, если оно получено, запустится резервное копирование. В результате, в нашем примере на диске F: появится каталог WindowsImageBackup, в нем будет создан подкаталог, названный по имени архивируемого сервера, куда и попадет копия.

Задание. 1.*На учебном сервере (или виртуальной машине) выберите раздел для резервного копирования.*

2.С учетом рассмотренных ограничений и объема копируемого раздела, выберите место для размещения копии. Определите, от имени какой учетной записи будет проводиться эта операция.

3.Выполните однократное резервное копирование выбранного раздела.

4.Найдите каталог WindowsImageBackup. Разберитесь, как организовано хранение резервных копий и опишите это в отчете. В файл с какого типа (и с каким расширением) помещаются данные?

Теперь рассмотрим порядок восстановления данных из резервной копии. В первой части лабораторной работы была сделана резервная копия раздела E:. Пусть понадобилось восстановить содержимое одной из папок из этого раздела. При этом требуется сравнить текущее содержимое папки с архивной копией, т.е. восстанавливать нужно в другую папку. Запускаем оснастку Windows Server Backup и в списке Actions выбираем Recover (восстановление). Мастер восстановления уточняет, какой сервер будет восстанавливаться, после чего представит перечень имеющихся резервных копий (рис.6).

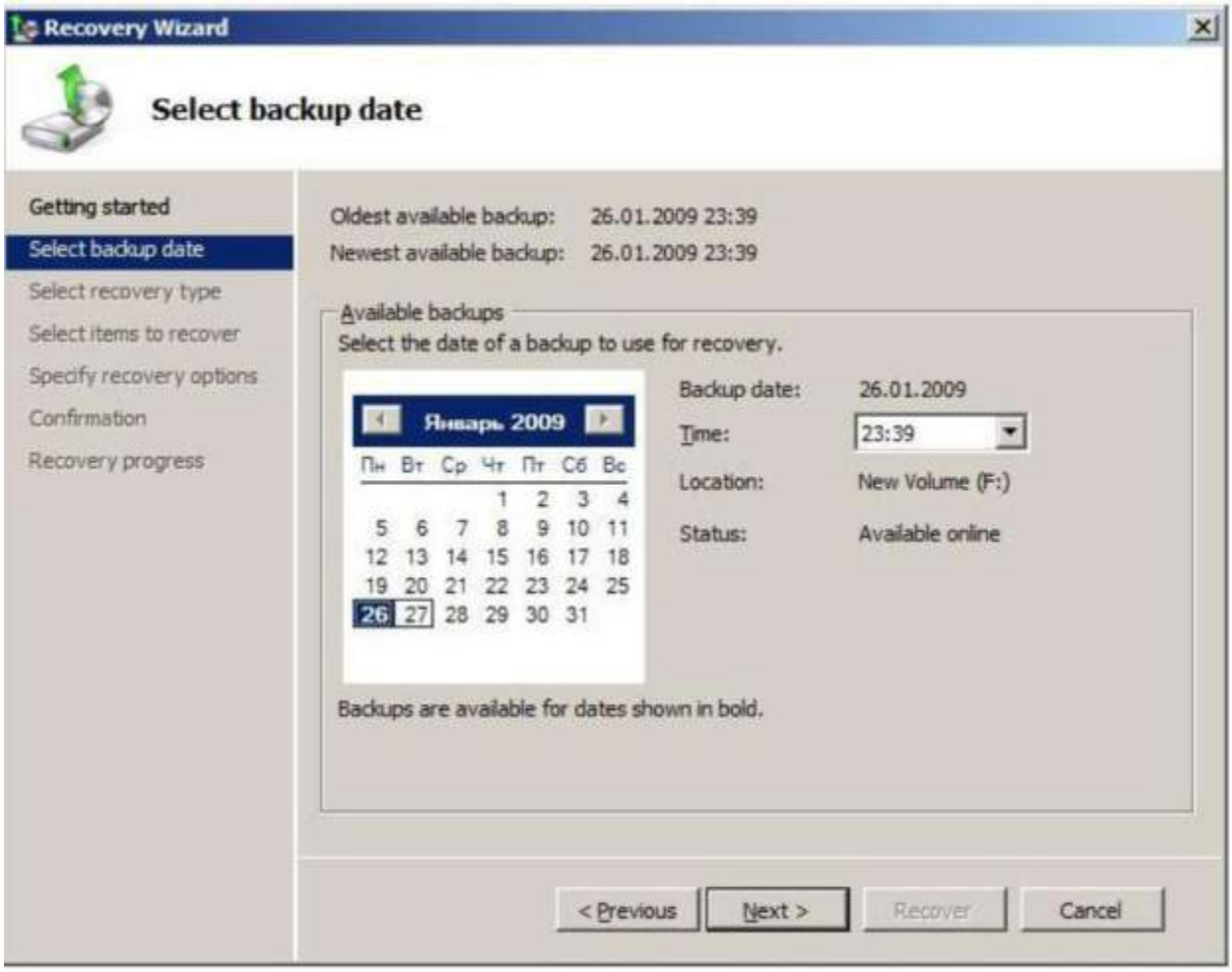


Рис.6. Перечень доступных резервных копий для выбранного сервера.

В следующем окне запрашивается, что именно восстанавливается. Нас интересует отдельная папка, потому выбираем вариант Files and folders (рис.7). Другие варианты – восстановление зарегистрированных приложений и восстановление раздела диска целиком.

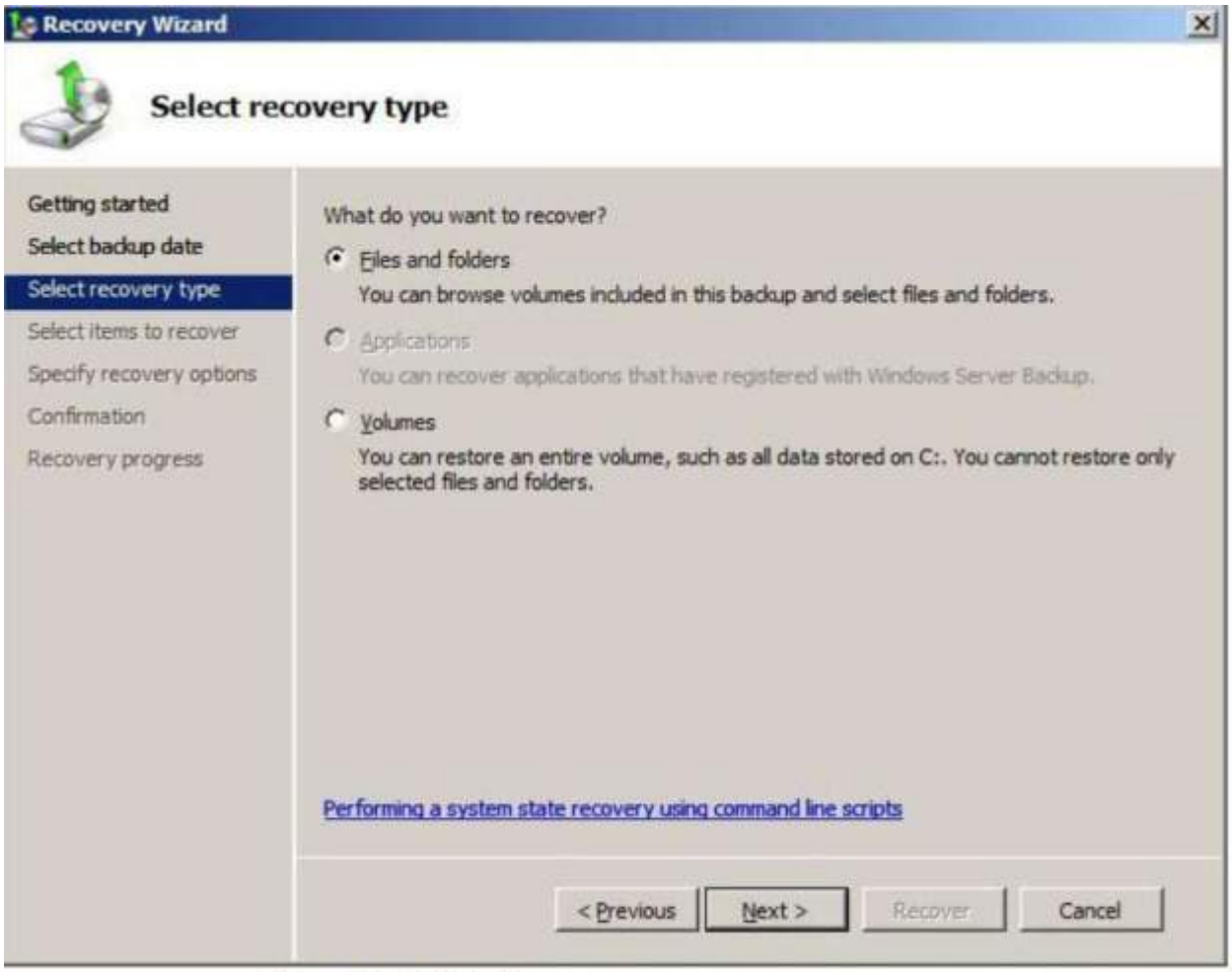


Рис..7. Выбор типа восстановления.

Рис..8. Параметры восстановления.

В следующем окне мастера в выпадающем списке нужно найти и выделить выбранную для восстановления папку. Если восстановить нужно несколько объектов, их выделяют совместно, удерживая клавишу Ctrl (или Shift для выделения диапазона). После этого выбирается путь для восстановления и задаются параметры. В нашем примере, мы хотим восстановить выбранную папку с файлами во вновь созданную папку restored (рис.8). Кроме пути (исходный или альтернативный), выбирается вариант действий при совпадении имен файлов и папок. Это особенно актуально, если восстанавливать файлы в исходную папку. Вариантов три – создавать копии, перезаписывать имеющиеся объекты восстанавливаемыми, оставить имеющиеся объекты. Последний из выбираемых в этом окне параметров указывает на то, восстанавливать ли настройки безопасности (т.е. списки контроля доступа к файлам). После выбора всех параметров будет запрошено подтверждение и начнется восстановление. ***Задание***. *Выберите из архива, созданного в предыдущей части работы, группу файлов для восстановления. Восстановите их в первый раз по исходному пути с сохранением копий, во второй раз - по альтернативному пути. Опишите, в чем разница в полученных результатах.* Теперь рассмотрим организацию резервного копирования по расписанию. Для этого в Windows Server Backup выберем опцию Backup Schedule. Первое окно запустившегося мастера информирует, что прежде чем устанавливать резервное копирование по

расписанию, нужно определить: - что будет копироваться (полное резервное копирование сервера или отдельные диски); - как часто надо проводить копирование;

- где размещать копии. При этом надо учитывать:

1) даже при выборе резервного копирования отдельных разделов, в их список обязательно должен быть внесен раздел (-ы) с операционной системой;

2) копирование может выполняться один или несколько раз в день;

3) для хранения результатов резервного копирования должен выделяться отдельный диск, внутренний или внешний (например, подключаемый по USB). Перед началом использования, он будет отформатирован мастером архивации. Рекомендуется, чтобы он был не менее чем в 1,5 раза больше по объему, чем архивируемые диски. Пусть требуется ежедневно делать резервное копирование диска раздела с операционной системой. В окне мастера аналогичном рис.3, выбираем вариант Custom, в окне аналогичном рис.4 – диск С (на котором расположена операционная система). Указываем расписание (рис.9). Дальше определяется диск (рис.10), он может быть не отформатирован. Диску будет назначена метка с названием сервера и датой определения резервного копирования, после чего будет проведено форматирование. Диску не назначается буква и он не будет доступен пользователям как обычный диск.

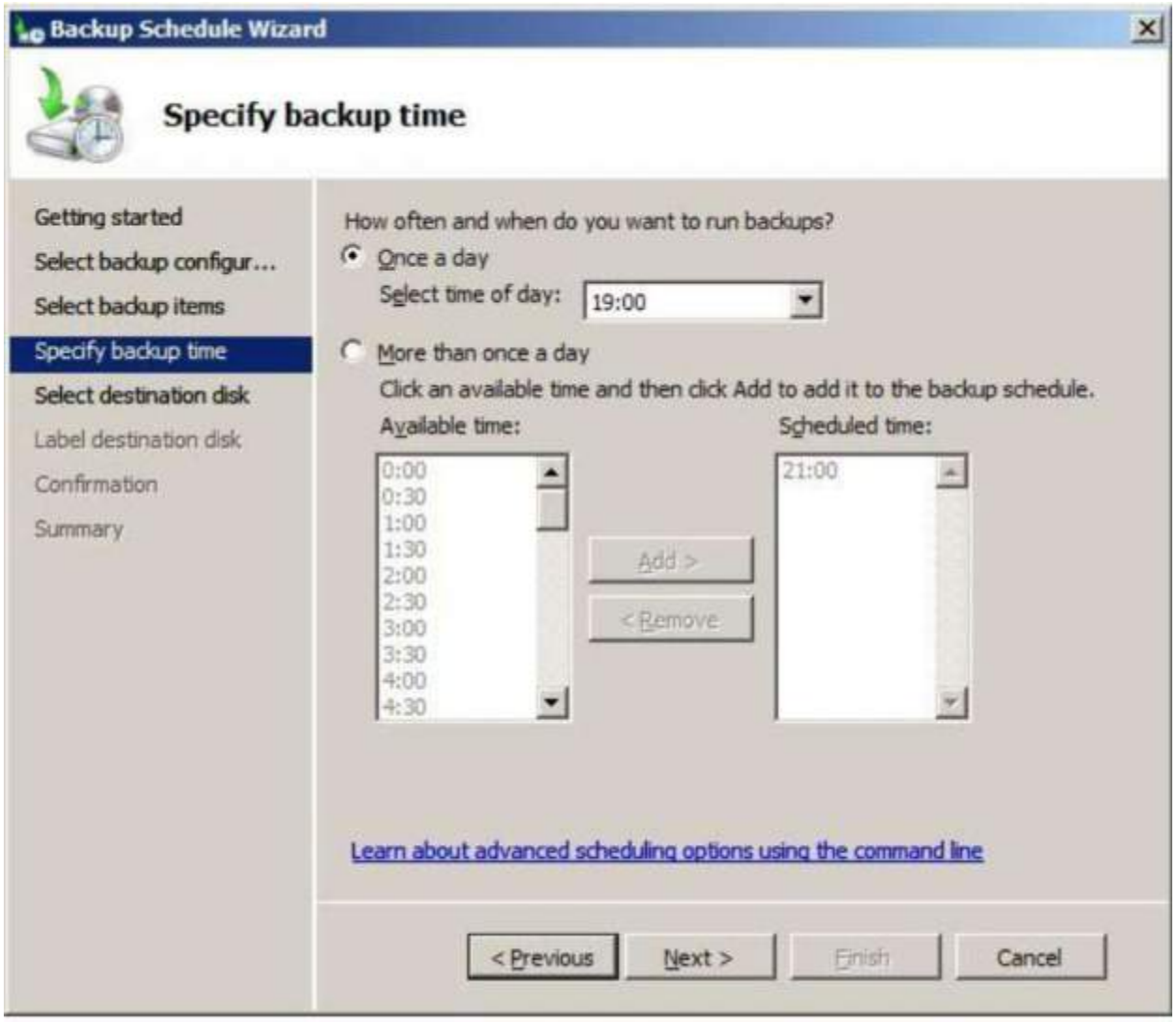


Рис.9. Расписание резервного копирования.

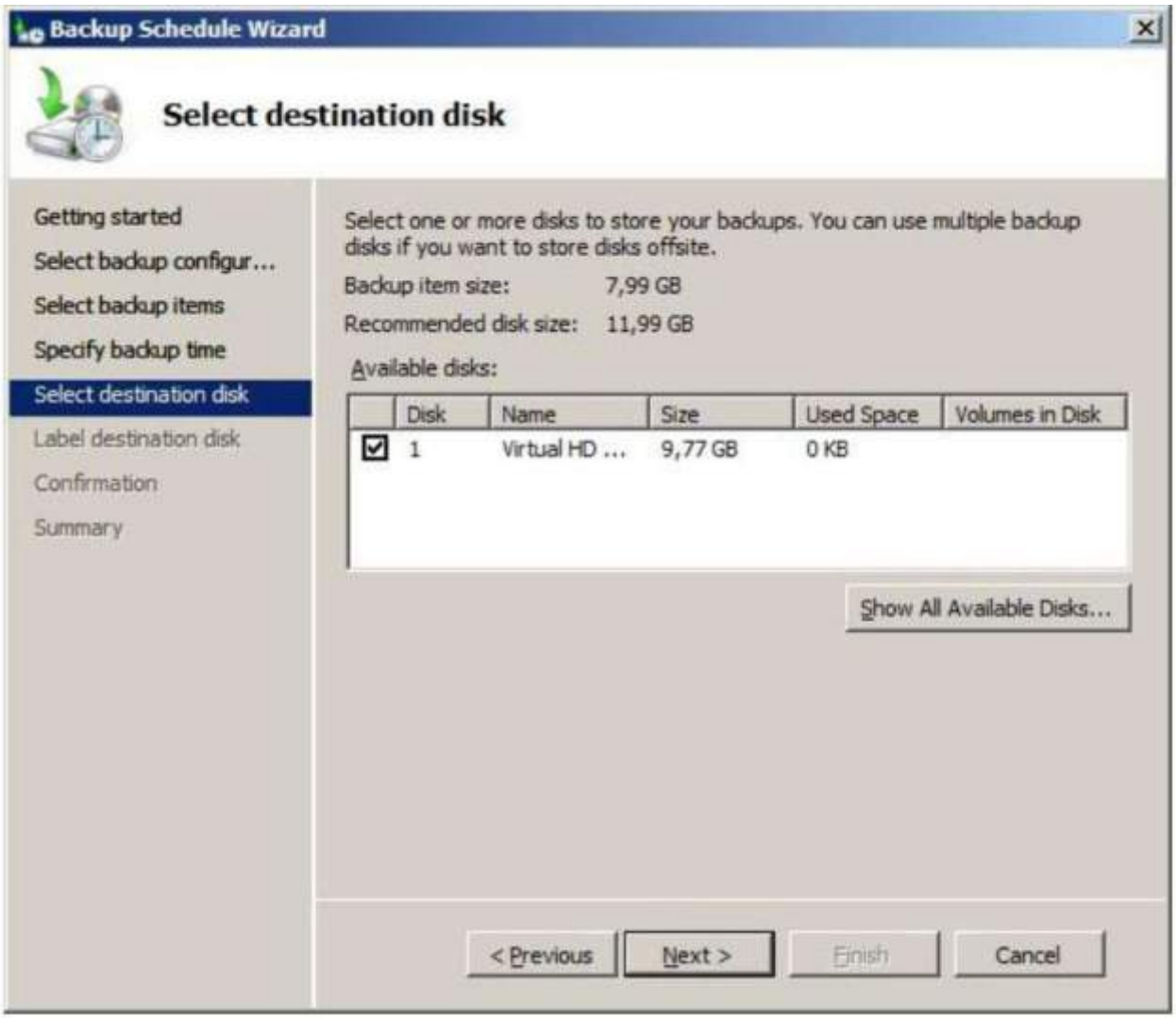


Рис.10. Диск для хранения резервных копий.

Когда работа по настройке автоматической архивации завершена, можно сделать дополнительные настройки, повышающие быстродействие для отдельных дисков. Для этого в списке Actions в оснастке Windows Server Backup выберите пункт Configure Performance Settings. В открывшемся окне (рис.11) можно установить, какой тип резервного копирования производить для диска – полное (full) или добавочное (Incremental). По умолчанию используется полное. Добавочное помещает в архив только измененные с момента последнего архивирования файлы, это позволяет провести резервное копирование быстрее, но более существенно снижает производительность сервера в период копирования (т.к. надо проводить проверку).

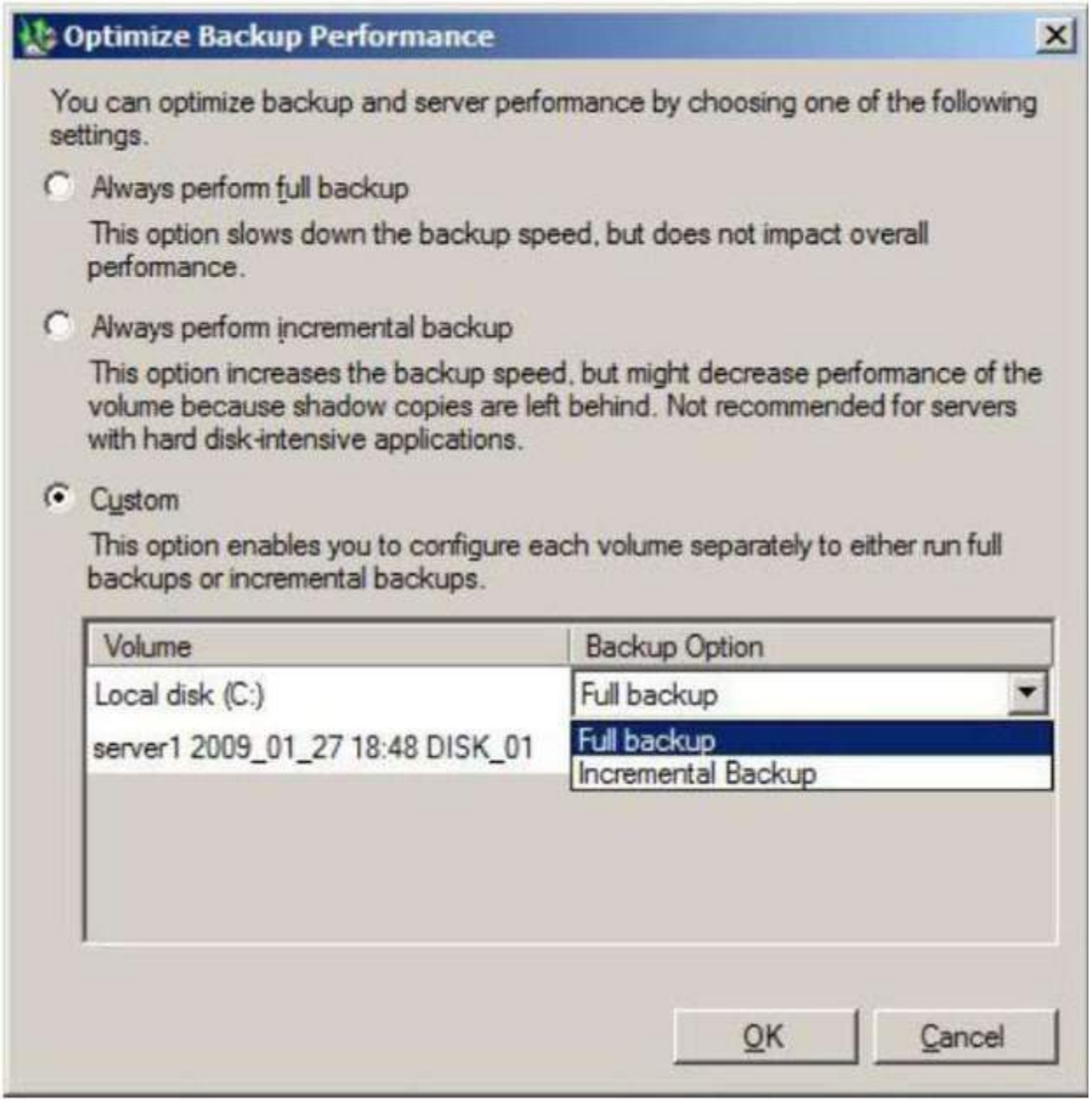


Рис.11. Выбор типа резервного копирования для диска.

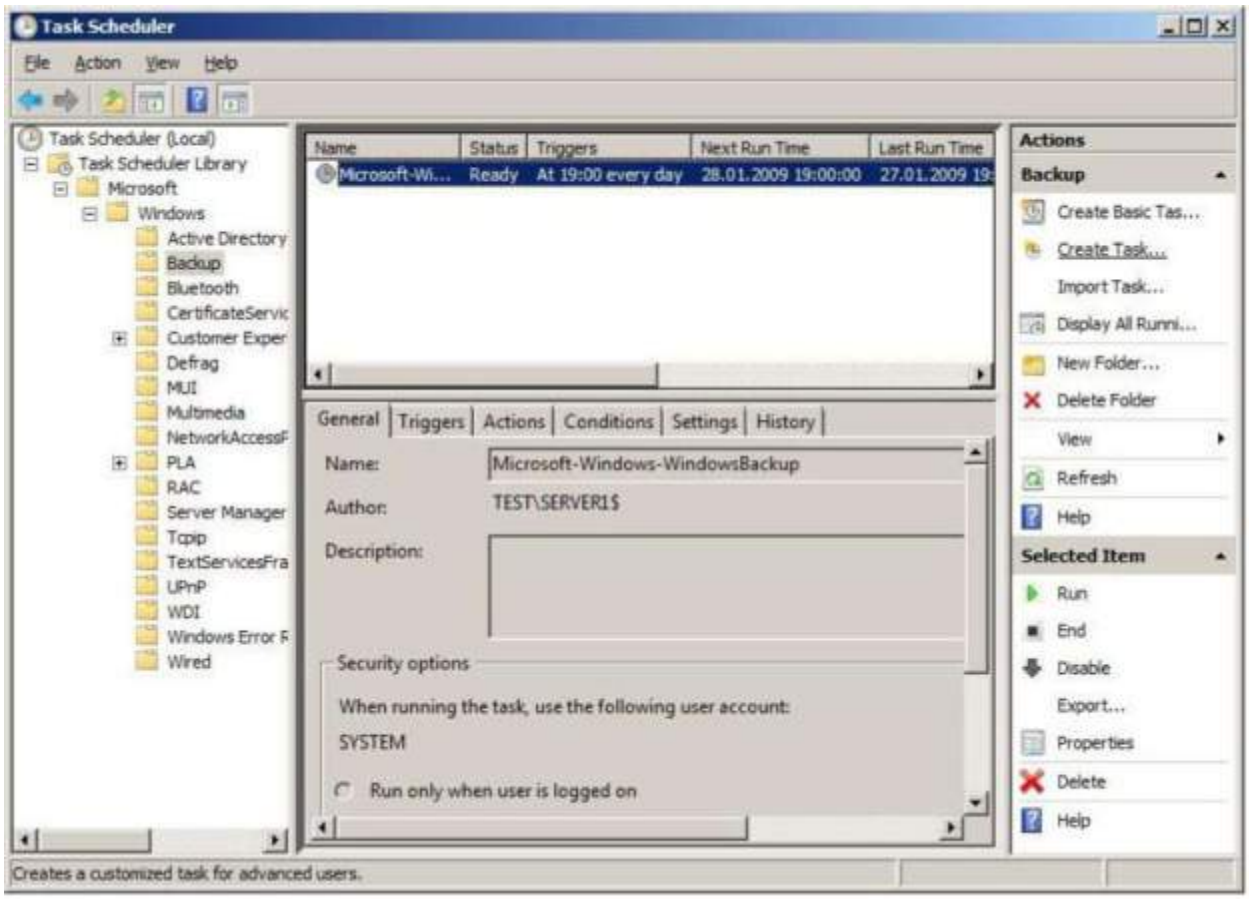


Рис.12. Параметры созданного задания.

Порядок восстановления такой же, как и при однократном копировании. Кстати, посмотреть параметры запланированного резервного копирования можно с помощью оснастки Task Scheduler (рис.12).

Задание. *Разработайте и реализуйте план ежедневного резервного копирования раздела с операционной системой. При выполнении лабораторной работы на виртуальной машине для хранения резервных копий можно подключить дополнительный виртуальный диск (настройка делается в свойствах виртуальной машины, когда она не запущена). Выберите такое время создания копии, чтобы результат можно было увидеть в ходе выполнения лабораторной. После создания копии, восстановите какой-либо из файлов. Используя опцию Backup Schedule оснастки Windows Server Backup, удалите запланированное задание на резервное копирование.* Резервное копирование из командной строки выполняется с помощью утилиты wbadmin.

Задание *Запустите wbadmin без ключей. По выведенной подсказке разберитесь в работе утилиты. Выполните из командной строки восстановление файлов, аналогичное тому, как делалось, при использовании графического интерфейса.*

ПРАКТИЧЕСКАЯ РАБОТА №36.
УСТАНОВКА И КОНФИГУРИРОВАНИЕ WINDOWS SERVER 2012 R2 ESSENTIALS.

Цель работы:

Получение практических навыков по установке и конфигурированию

Windows Server 2012 R2 Essentials

Общие сведения о Windows Server 2012 R2 Essentials

Windows Server 2012 R2 Essentials – это одна из редакций серверной операционной системы от компании Microsoft. Однако имеет множество отличий от редакций Standard и Datacenter. Что же умеет Essentials:

- Авторизация и аутентификация пользователей вашей сети (домен контроллер службы каталогов Active Directory)
- Файловое хранилище (роль файлового сервера)
- Удаленный доступ к корпоративной сети (VPN и DirectAccess сервер)
- Удаленный доступ к файловому хранилищу через Web-интерфейс (настроенный для этого IIS)
- Удаленный доступ к рабочем столам клиентских машин (шлюз удаленных рабочих столов)
- Резервное копирование клиентских машин (windows backup)
- Резервное копирование самого сервера (windows backup)
- Интеграция с облачными технологиями Microsoft (Office 365, Azure backup и т.д.)
- Консоль единой настройки Essentials, которая позволит настроить возможности описанные выше даже не подготовленному системному администратору.

Редакция Essentials имеет большинство ролей Windows Server. Некоторые из этих ролей настроены, некоторые доступны в полном объеме, некоторые как например Hyper-V с серьезными ограничениями. Компенсацией за эти все ограничения является более низкая цена, включенных 25 клиентских лицензий, централизованная и простая настройка. Вы можете использовать эту редакцию только для организаций, где число пользователей не превышает 25.

Таким образом Essentials очень хорошо подходит для малых организаций, которые бы хотели пользоваться большинством современных решений для обеспечения безопасности корпоративной сети, хранения документов, удаленного доступа, возможно, почтовые системы. Для тех организаций, которые не хотели бы тратить много денег как на саму ИТ инфраструктуру, так и на работу высококвалифицированных системных администраторов.

Установка и первоначальная настройка

Установка данной ОС стандартная процедура. В момент установки, если у вас один жёсткий диск, то необходимо разбить его на два раздела. Т.е. сделать так чтобы после установки в системе был второй уже отформатированный жесткий диск.

После первого входа в свежеустановленную ОС запустится мастер «Настройка Windows Server Essentials», который поможет произвести первоначальную настройку.

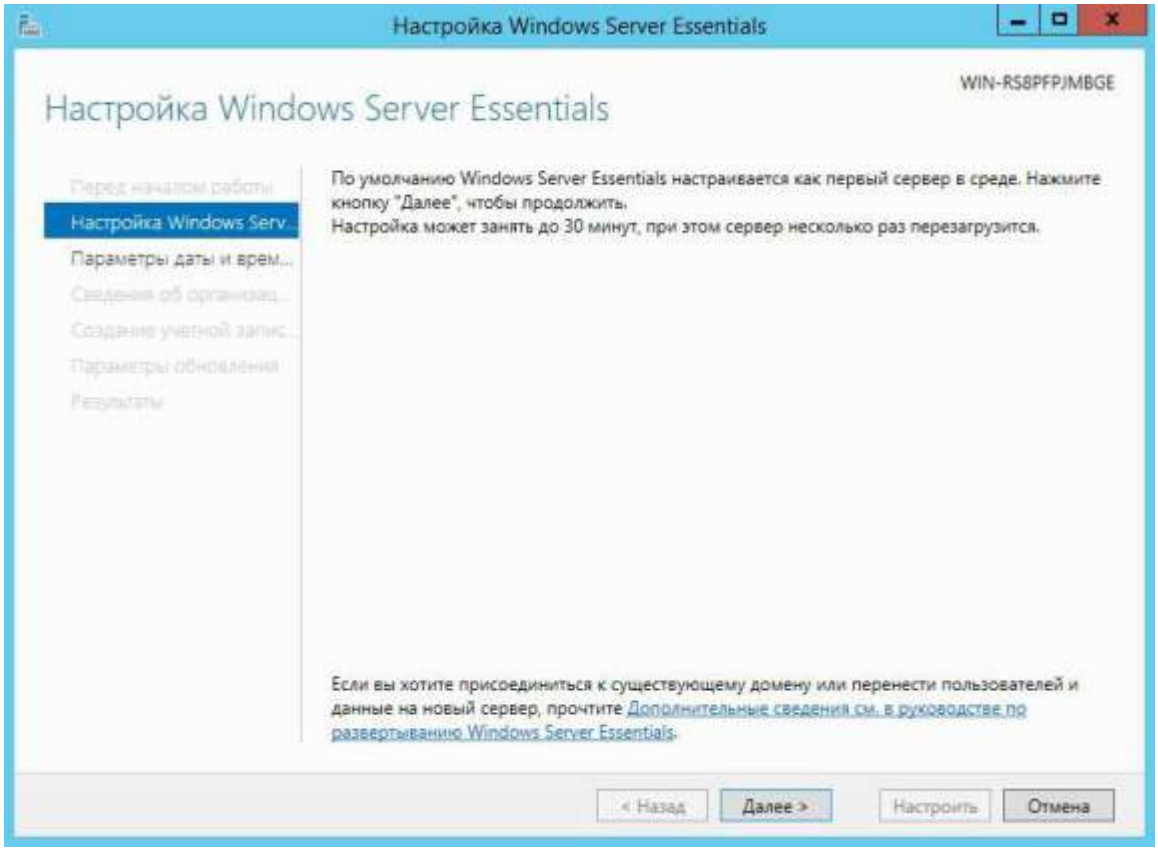


Рис.1 Мастер «Настройка Windows Server Essentials»

На первом шаге необходимо задать настройки даты и времени.

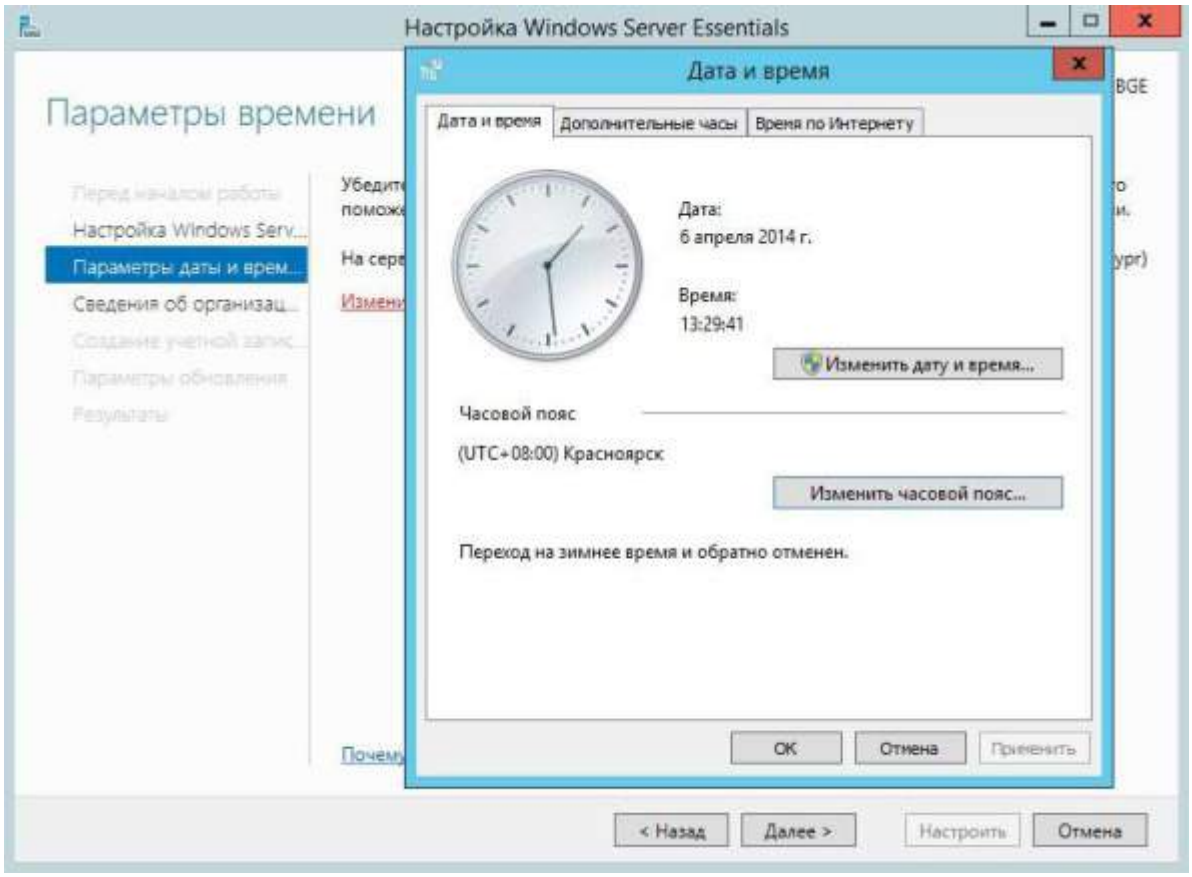


Рис.2 Окно настройки даты и времени

На втором шаге необходимо заполнить на английском языке название компании. Имя домена и имя сервера будут в таком случая сгенерированы автоматически, хотя конечно можно поменять их.

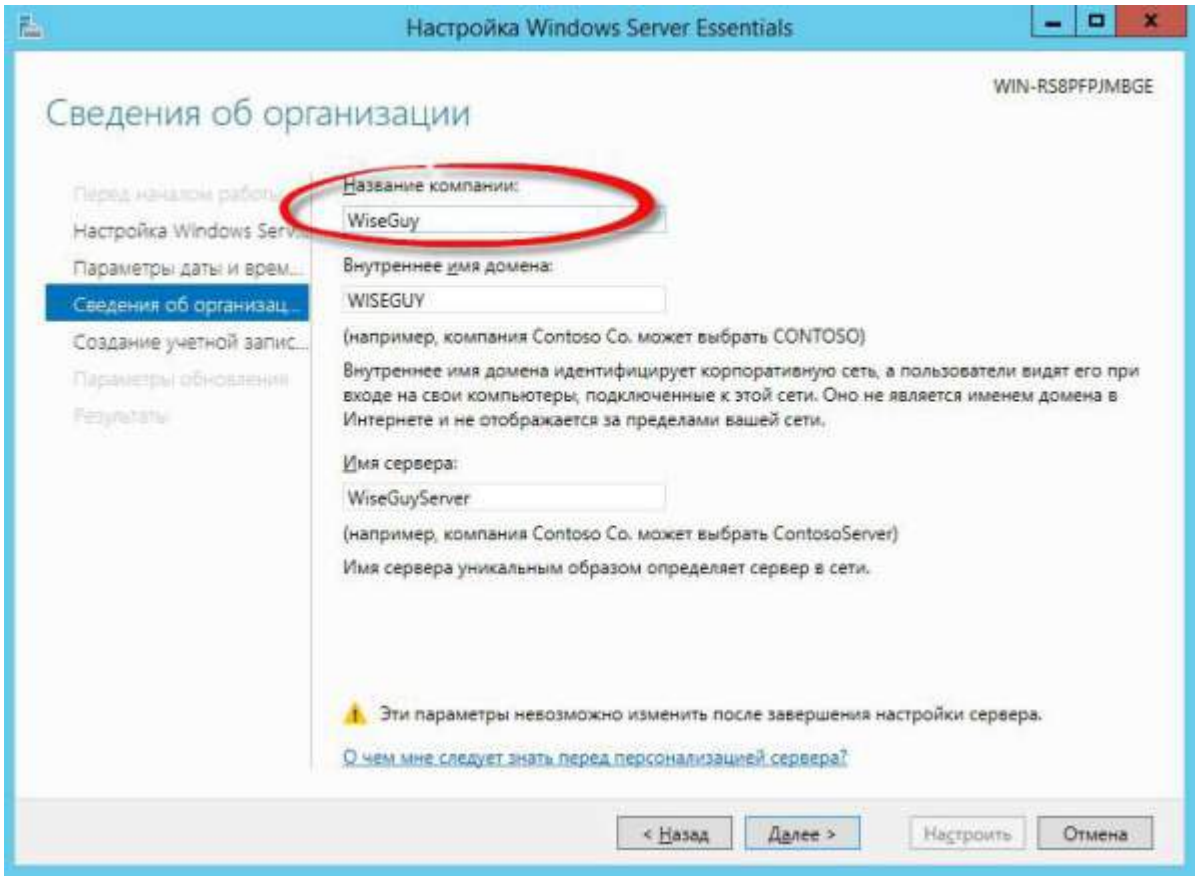


Рис.3 Окно заполнения на английском языке название компании

На следующем шаге необходимо

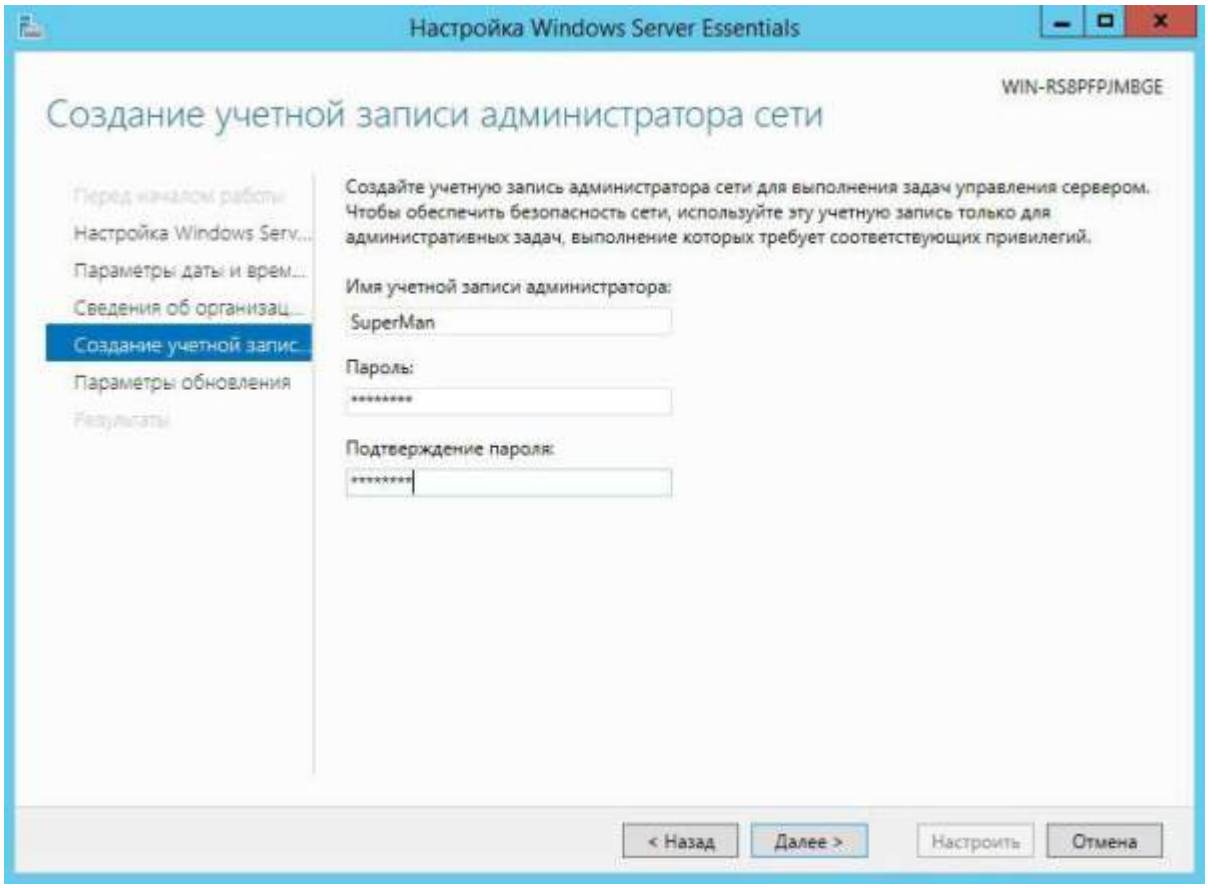


Рис.4 Окно заполнения имени администратора и задания его пароля.

На последнем шаге необходимо указать и нажать настроить

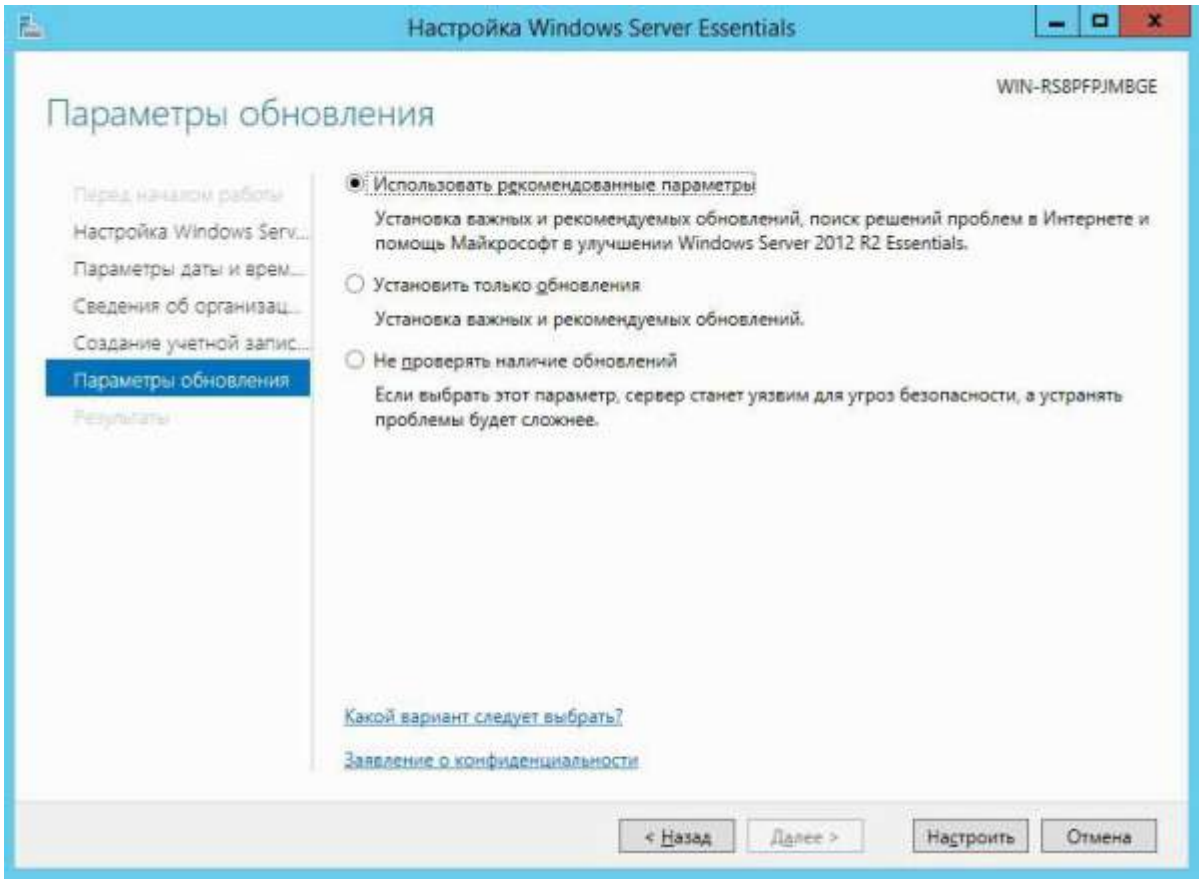


Рис.5 Окно выбора способа обновления системы

После этого запустится процесс, который произведет все необходимые первоначальные настройки. Это займет около 30 минут и потребует несколько перезагрузок. За это время ОС успеет в частности установить необходимые роли и настроить сервер в качестве домен контроллера для нового домена.

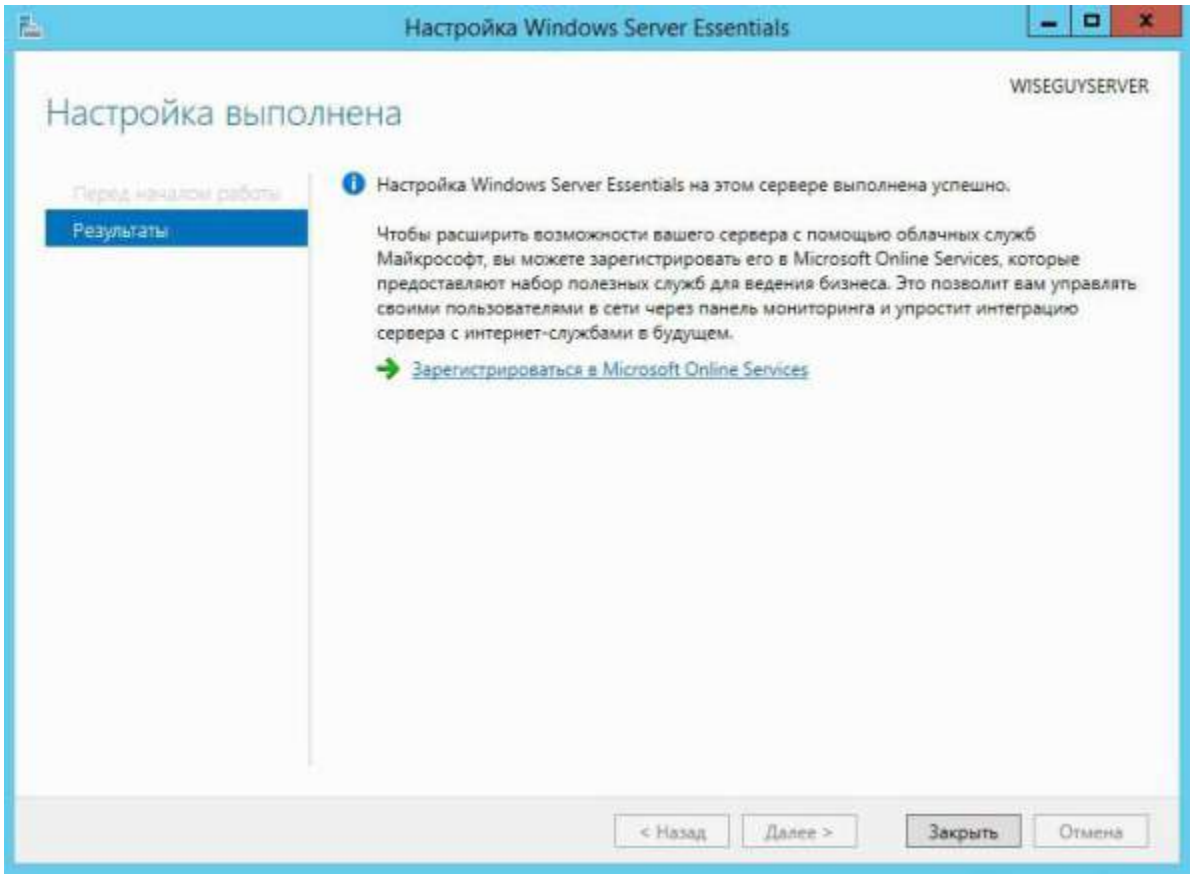


Рис.6 Окно завершения установки и начальной настройки

Настройка

Продукт очень большой и обширный, здесь будет рассмотрено о самых базовых возможностях настройки, такие как создание пользователей, настройка удаленного доступа, создание папок, подключение клиентов.

Вся настройка происходит в панели мониторинга, доступ к ней есть с рабочего стола, панели быстрого запуска и стартового экрана.

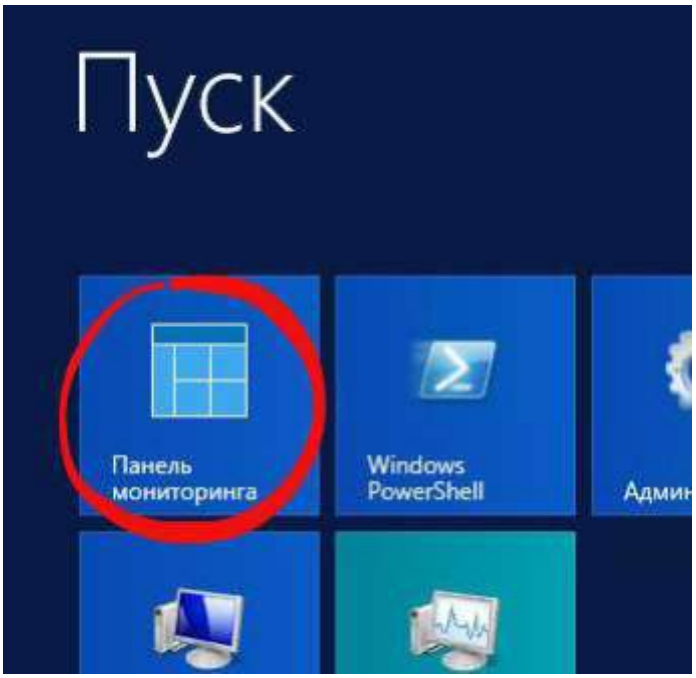


Рис.7 Вся настройка происходит в панели мониторинга

Создание пользователей

При первом запуске данной панели откроется вкладка установка, на которой можно выполнить ряд задач по настройке сервера.

Начнем с добавления пользователей. Щелкаем ссылку для добавления учетных записей.

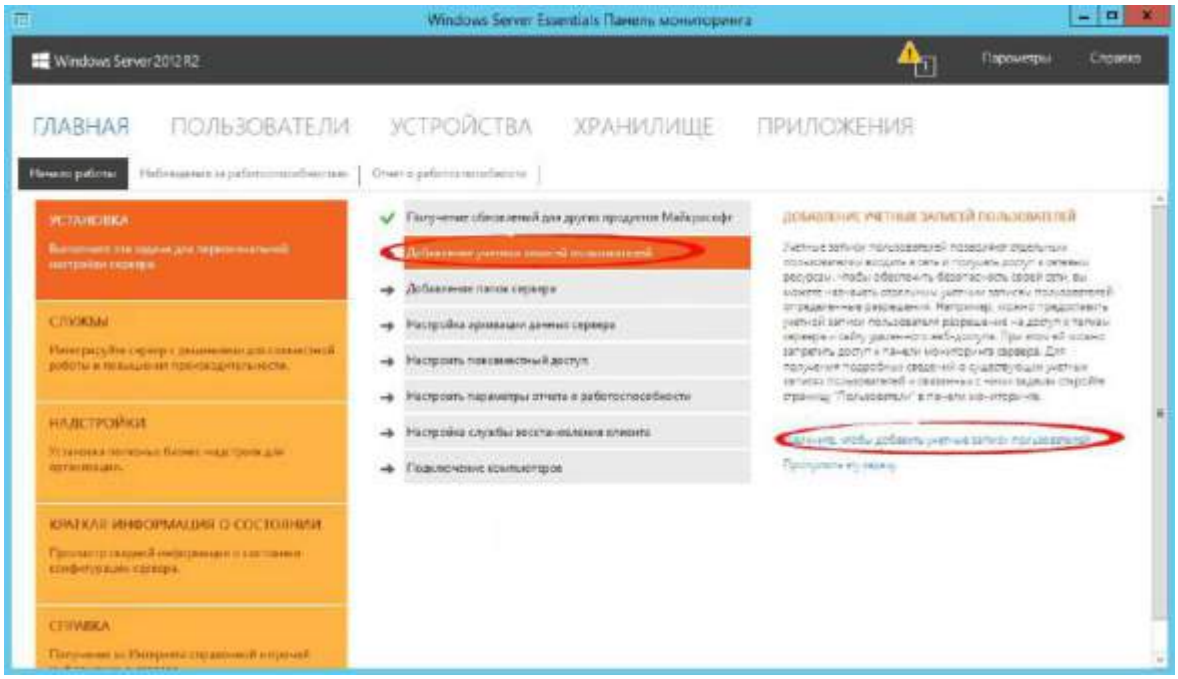


Рис.8 Окно добавления пользователей

Заполняем поля формы и нажимаем далее

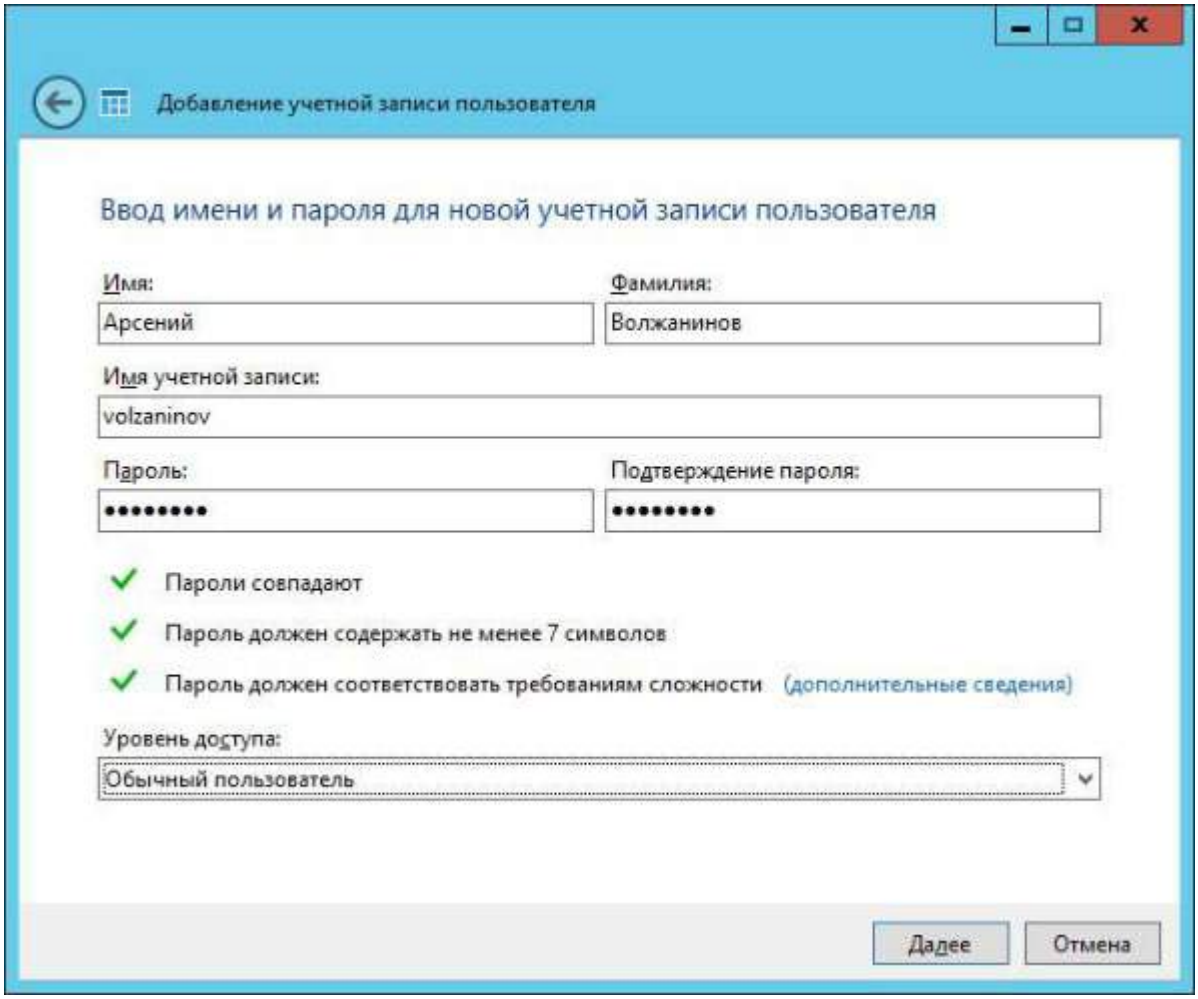


Рис.9 Окно добавления учетной записи

Выбираем уровень доступа к общим папкам, которые были созданы. На начальном этапе существует лишь одна – Организация. В дальнейшем вы можете менять разрешения на доступ как из свойств пользователя, так и из свойств папки.

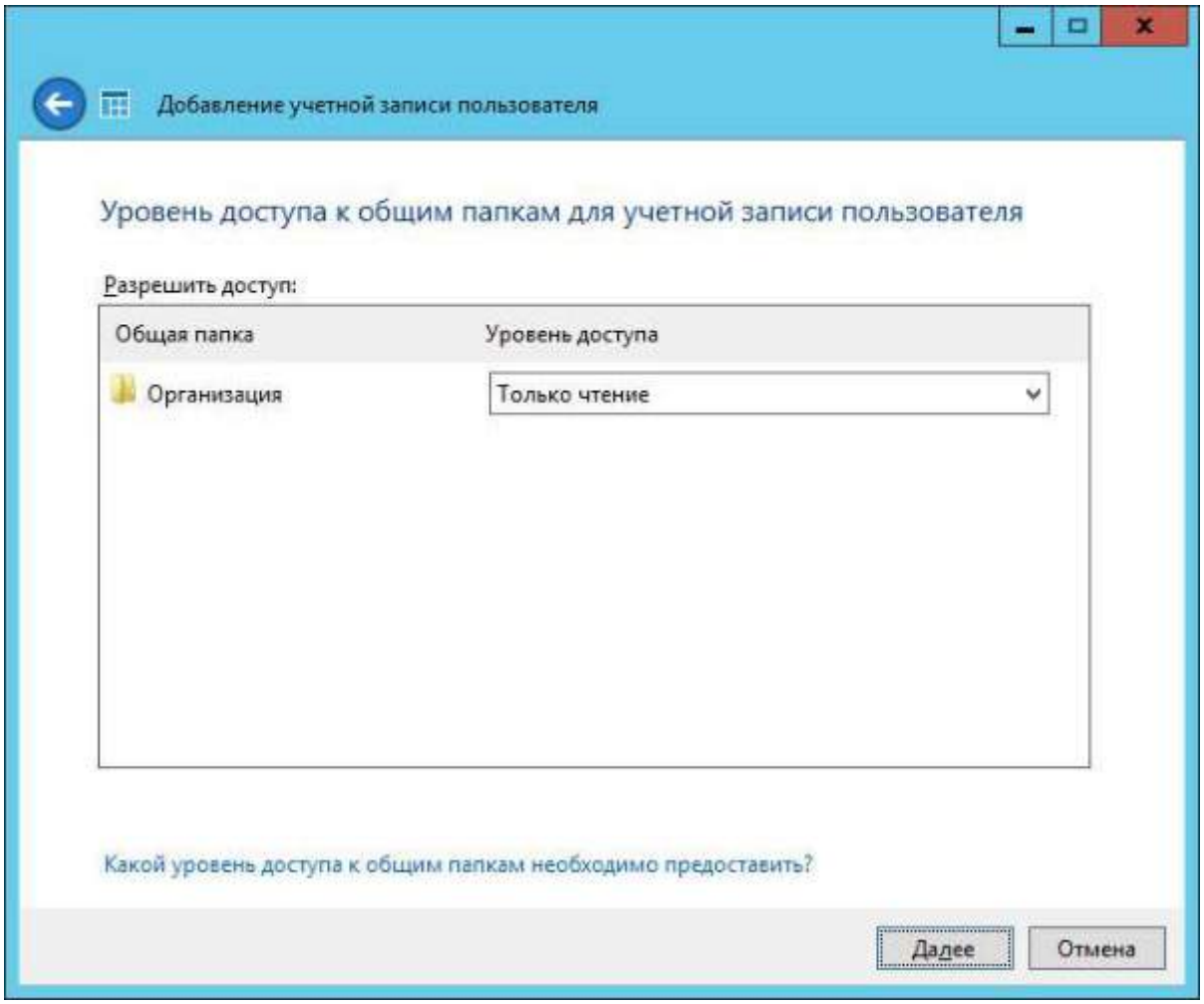


Рис.10 Уровень доступа к общим папкам

Далее устанавливаем, что будет доступно для пользователя удаленно.

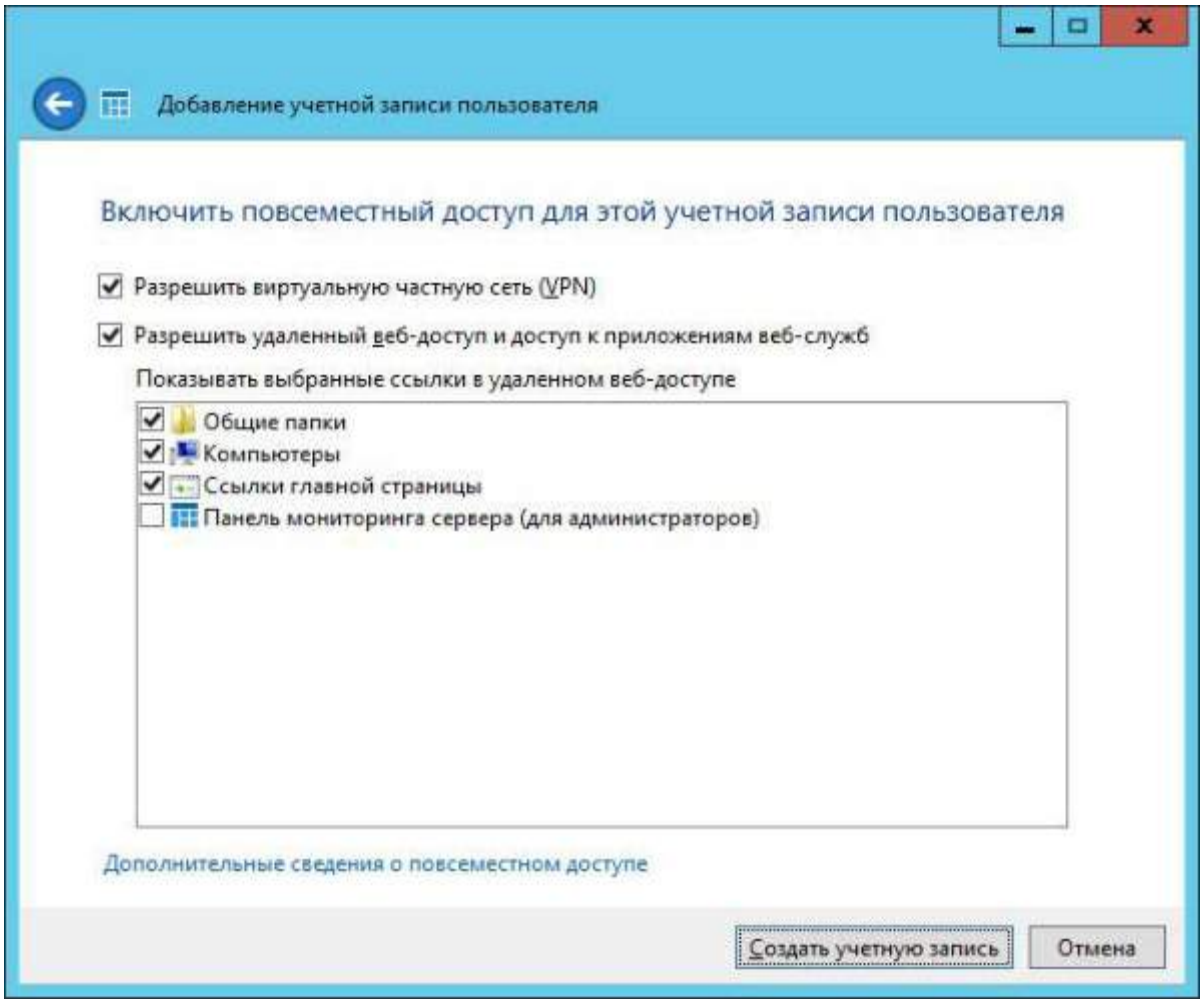


Рис.11 Пункты удаленного доступа

Учетная запись создана. Нажимаем закрыть.

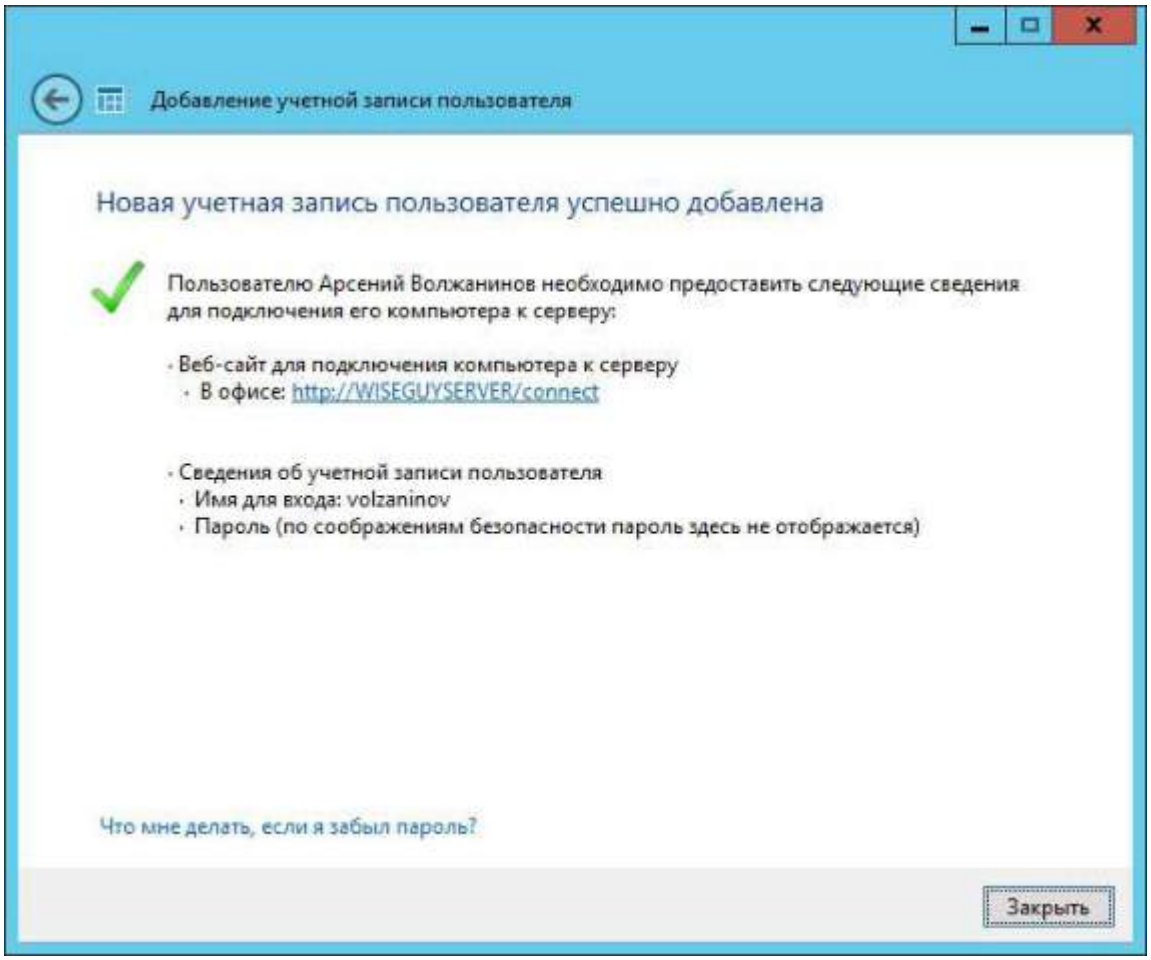


Рис.12 Окно завершения создания учетной записи

Подобным образом можно создать множество учетных записей. Безусловно, можно пользоваться и привычным и знакомым интерфейсом Active Directory Users and Computers, но в таком случае выдавать разрешения на доступ придется ручками.

Добавление папок сервера

Для добавление папок существует другой мастер, который поможет и создать папку на диске, и общий доступ для нее настроить, и разрешения выдать. Для его запуска необходимо щелкнуть соответствующую ссылку в панели мониторинга.

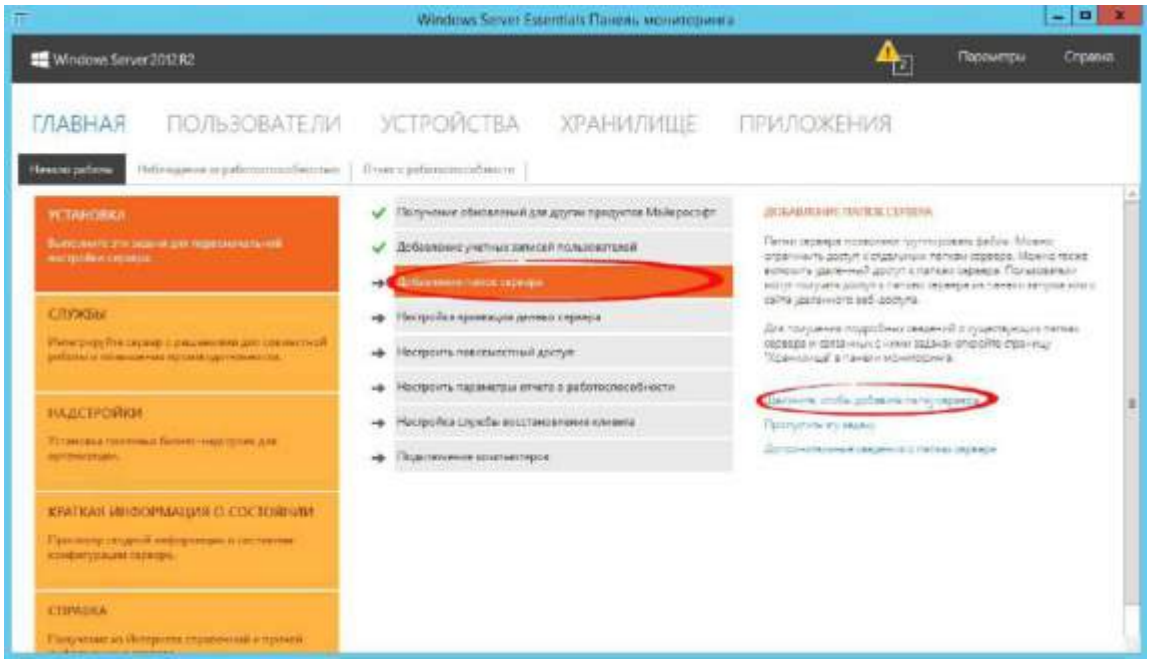


Рис.13 Панель мониторинга – добавление папок

В открывшемся окне мастера вводим название. Можно изменить расположение и добавить описание. Нажимаем далее.

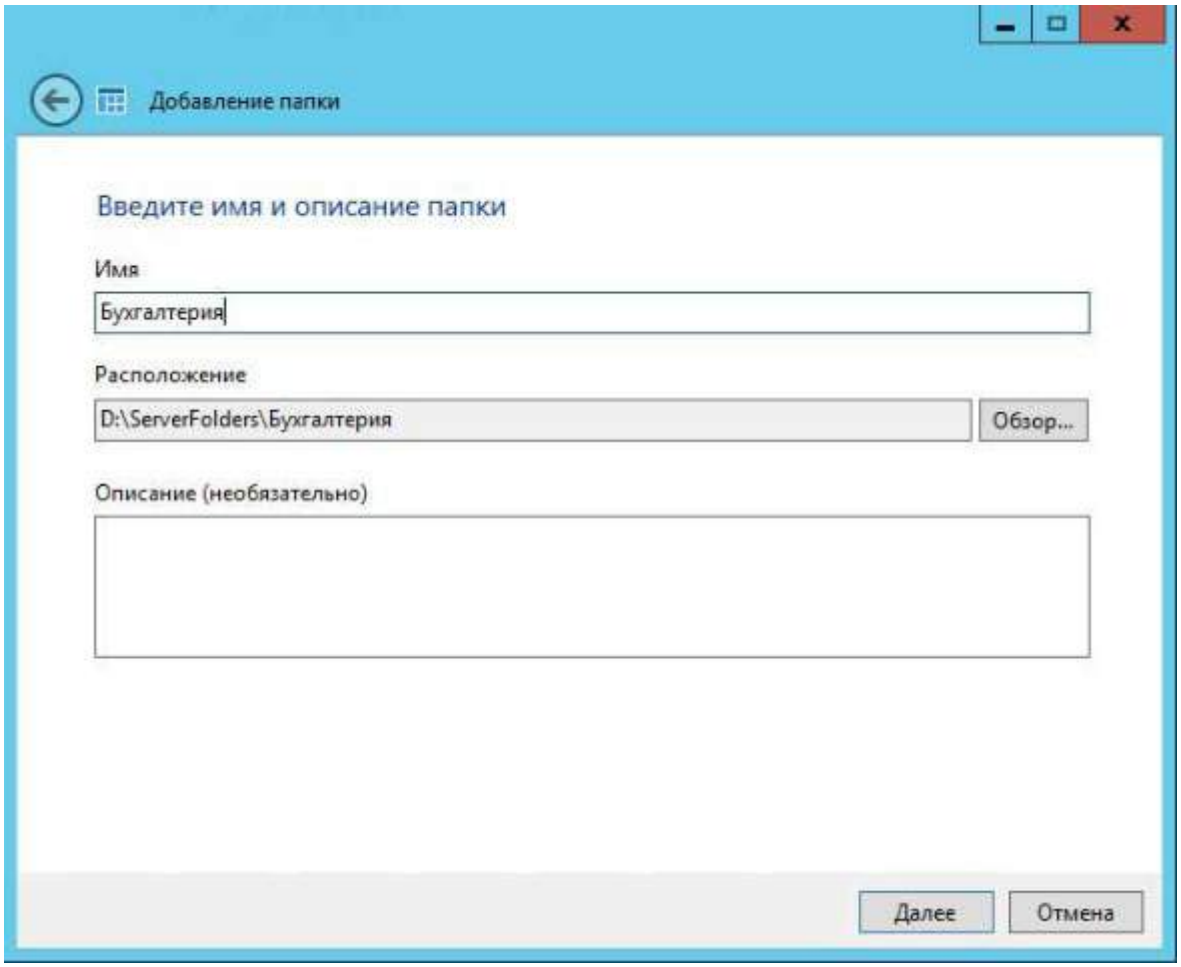


Рис.14 Окно ввода имени и описания папки

На следующей странице указываем необходимые разрешения. При необходимости делаем ее недоступной при удаленном доступе.

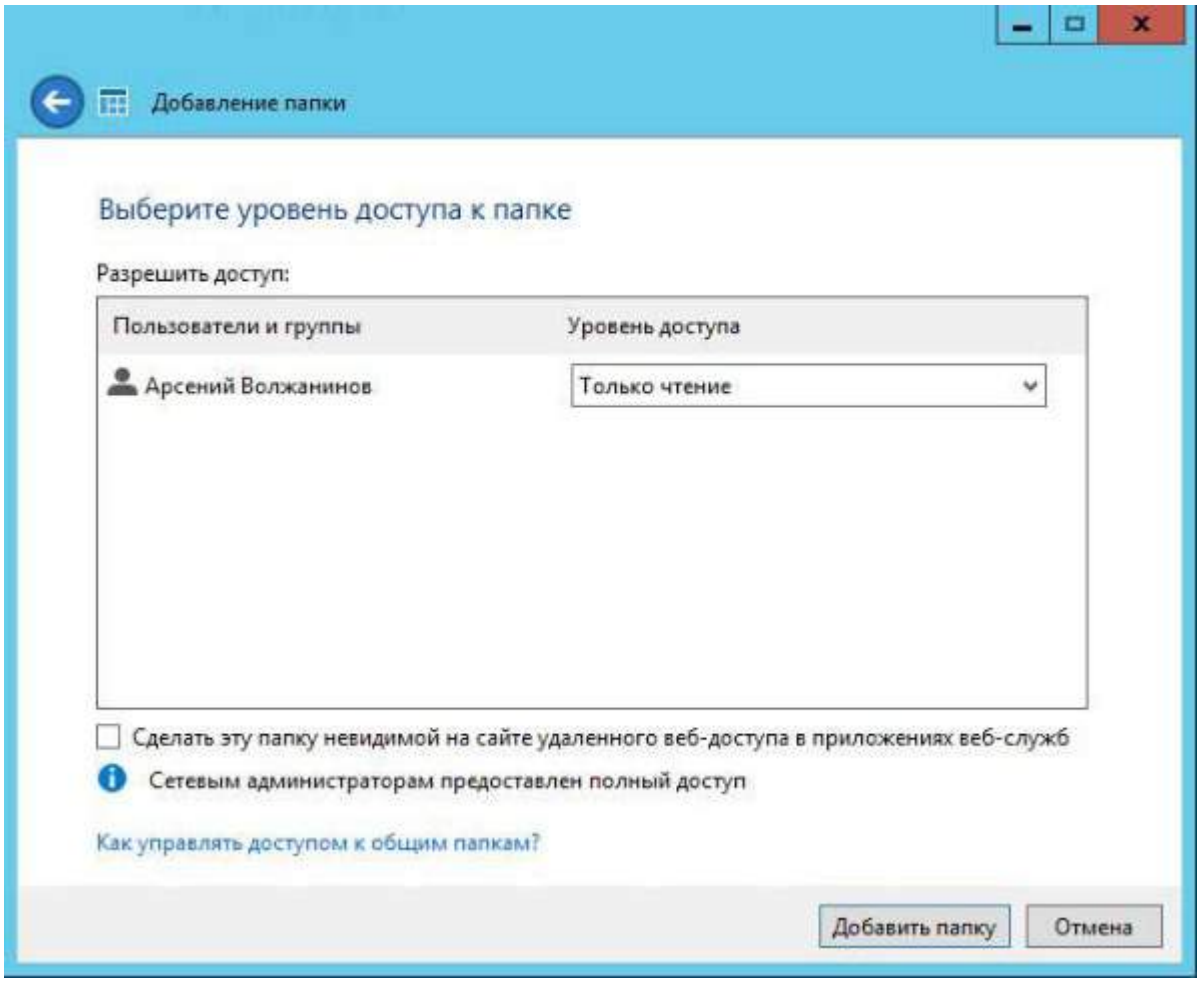


Рис. 15 Задание разрешения на папку

С последнего шага данного мастера можно запустить мастер настройки архивации. Нажимаем закрыть.

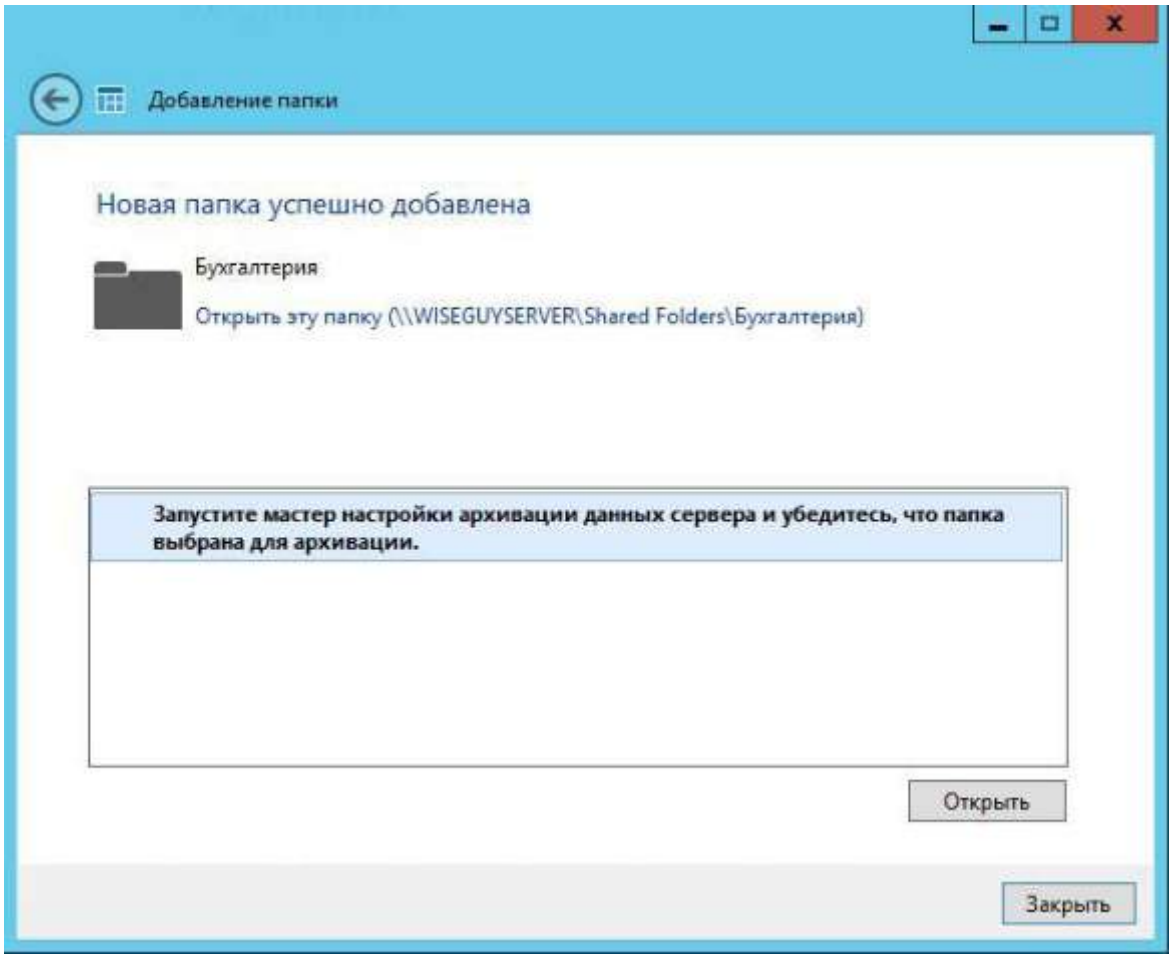


Рис.16 Окно завершения создания папки

Настройка удаленного доступа

Один, наверное, из самых сложных этапов настройки Windows Server 2012R2 Essentials. Настройка так же происходит с помощью мастера. Мастер традиционно запускается из панели мониторинга.

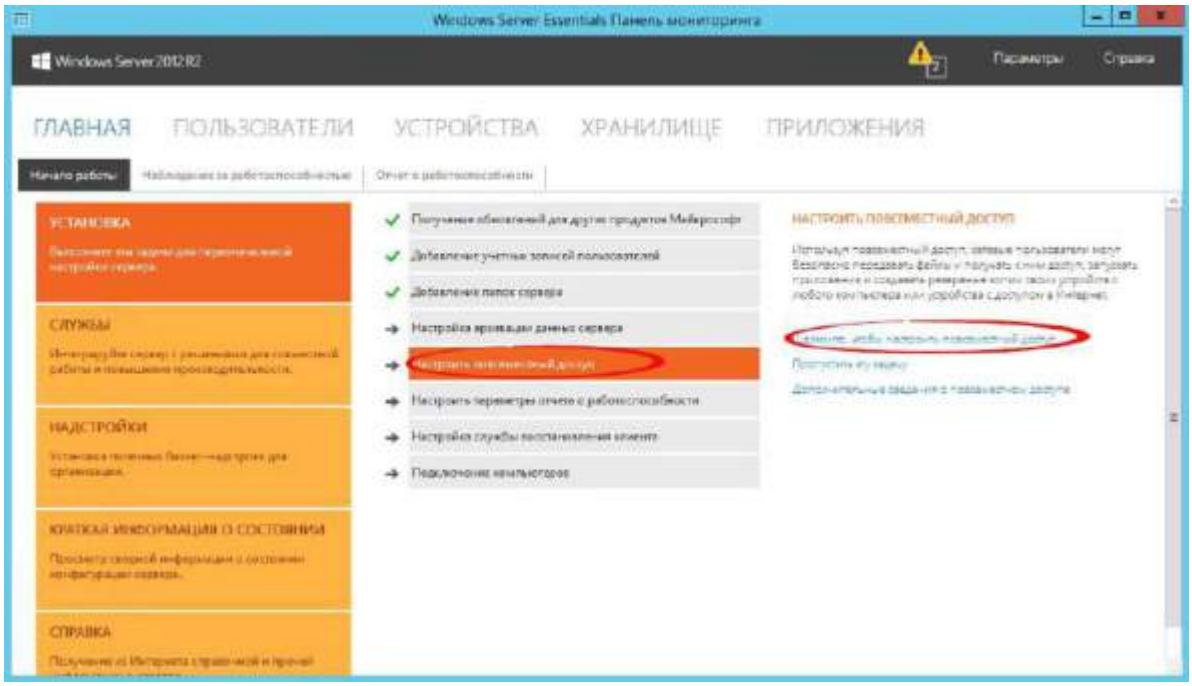


Рис.17 Панель мониторинга – настройка удаленного доступа

Первое что необходимо настроить это маршрутизатор – об этом сообщает мастер. На самом деле необходимо настроить перенаправление портов на маршрутизаторе. Для этого у маршрутизатора должен быть «белый» IP адрес. А на самом сервере лучше настроить статический IP адрес. Перенаправить нужно следующие порты 80, 443, 1723, 987 на IP адрес вашего сервера. В общем то процедуру настройки может выполнить и сам мастер, если ваш маршрутизатор поддерживает UPnP.

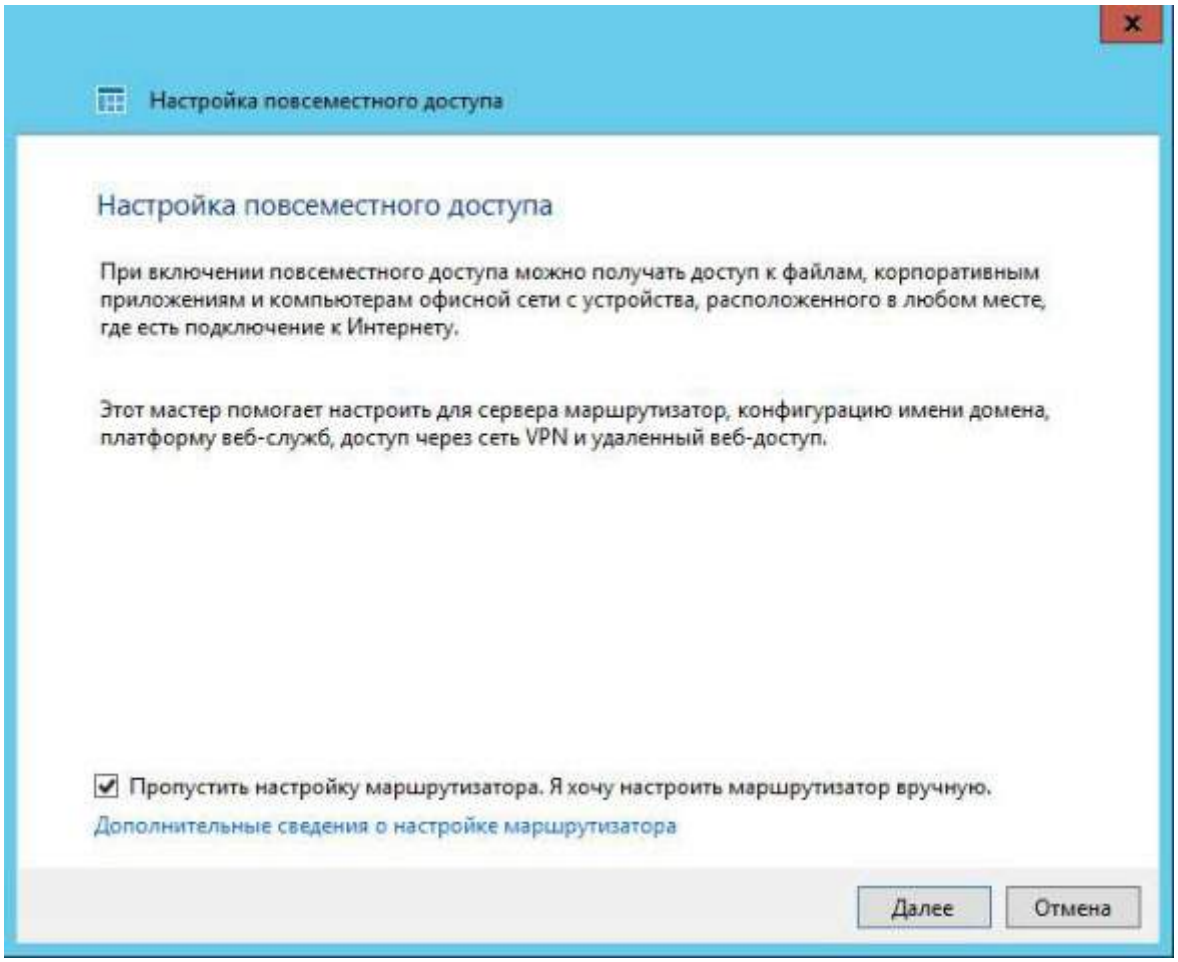


Рис.18 Настройка повсеместного доступа

После этого открывается новый мастер настройки доменного имени. Нажимаем далее.

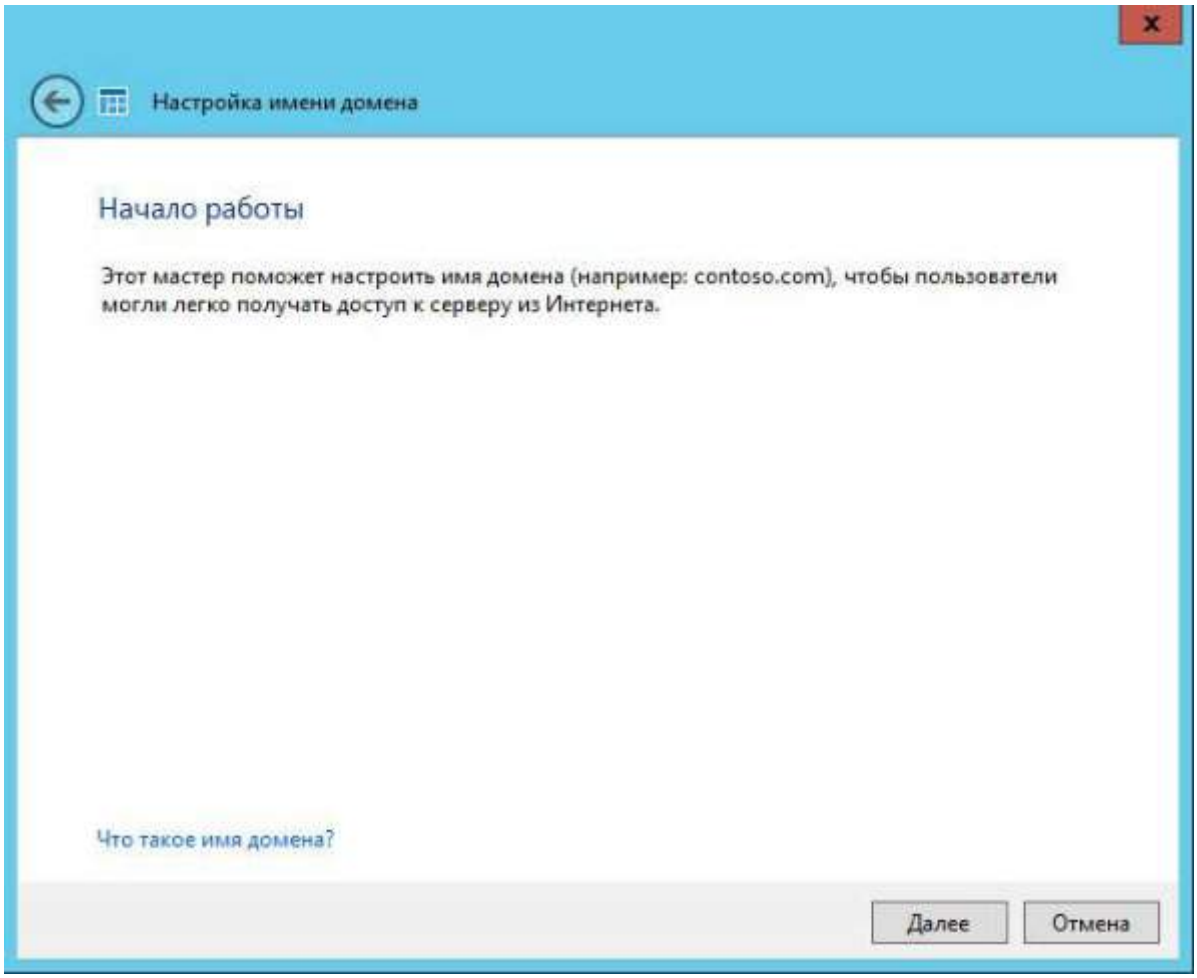


Рис. 19 Настройка имени домена

Мастер предложит ввести имя внешнего домена или создать новый. Для собственного домена понадобится сертификат, поэтому рассмотрим тут вариант настройки с использованием домена Microsoft. Выбираем другое имя домена и щелкаем далее.

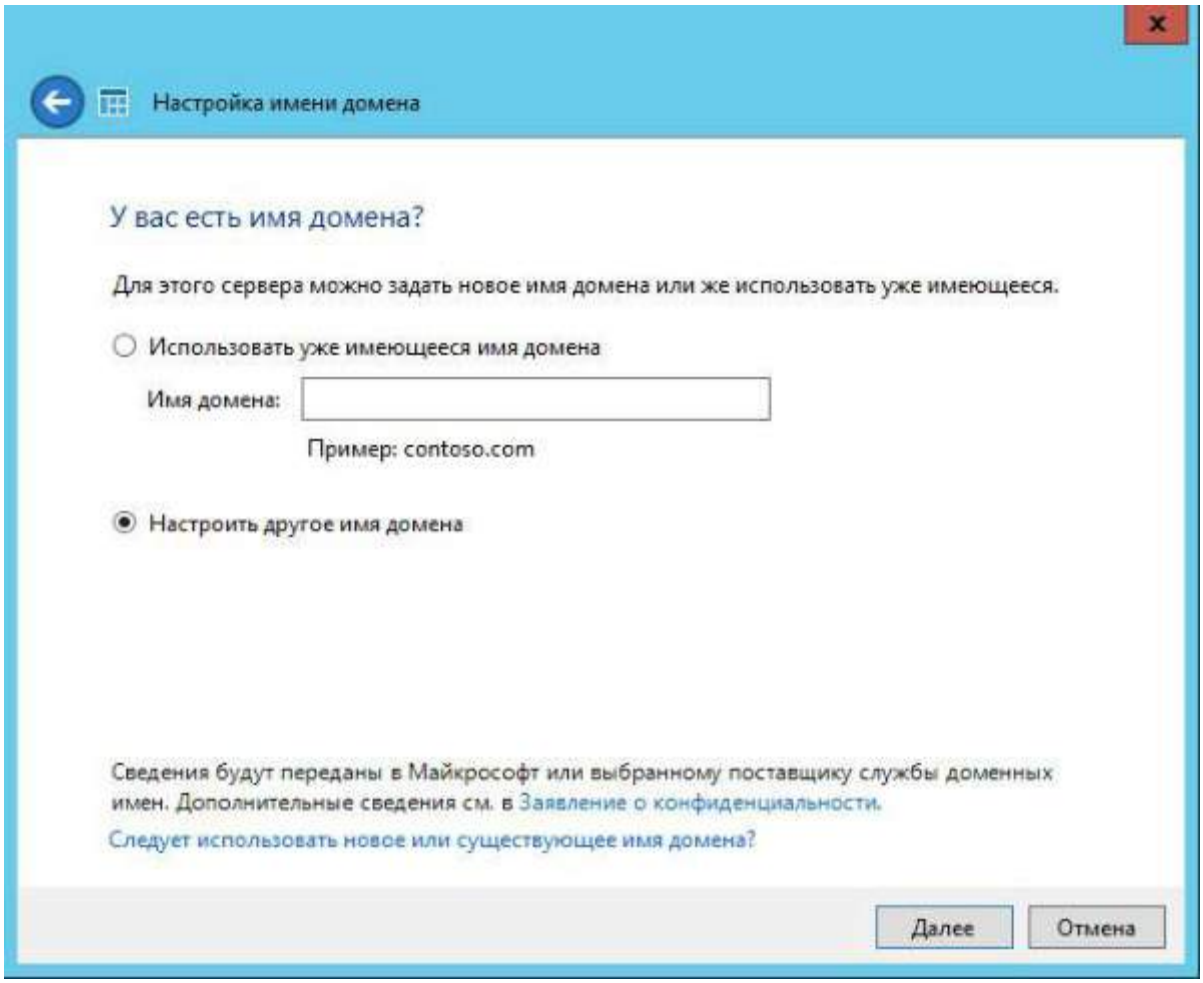


Рис.20 Настройка имени домена с использованием домена Microsoft

Рассмотрим вариант с доменом компании Microsoft.

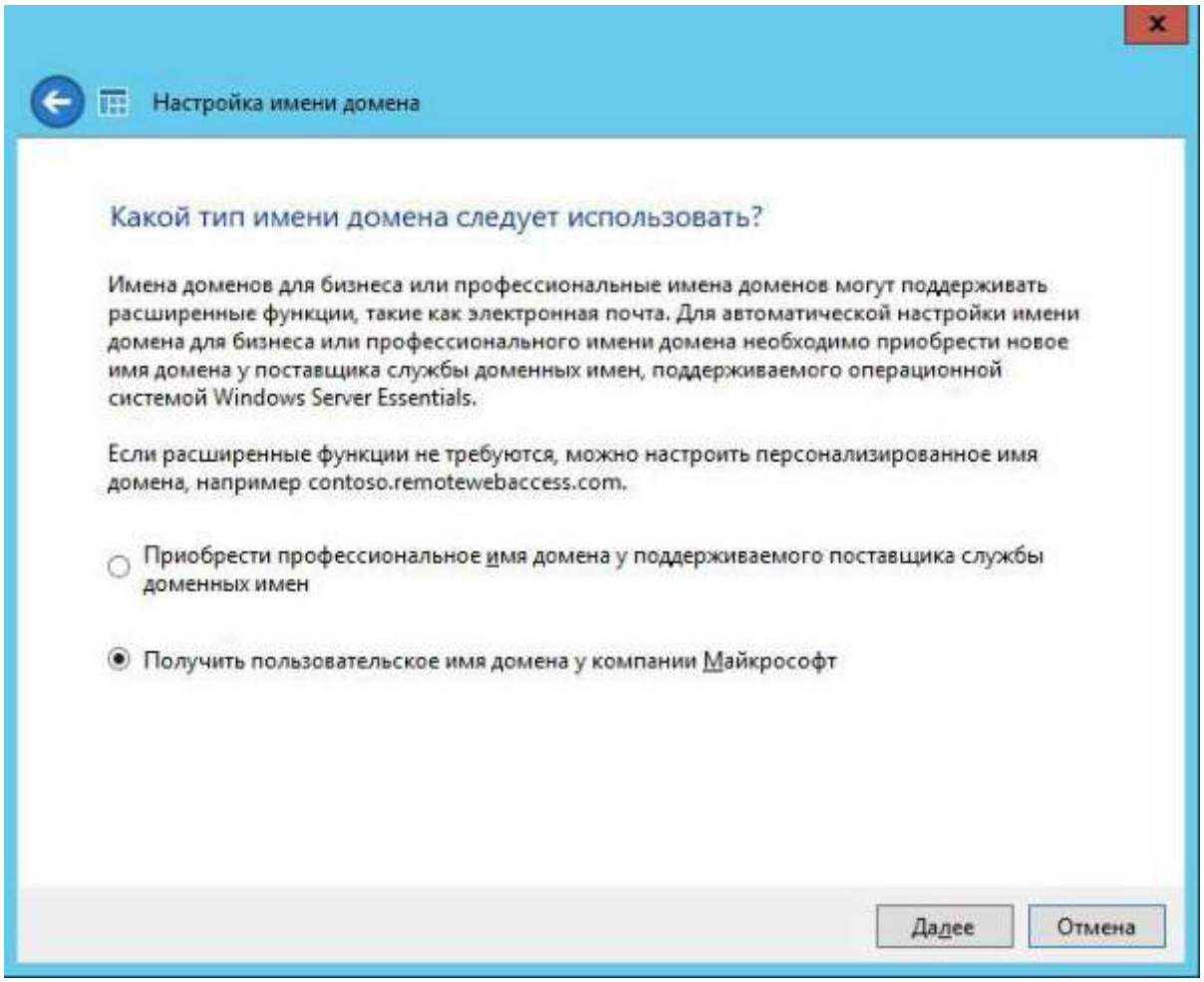


Рис.21 Настройка имени домена от Microsoft

Необходимо авторизоваться в Microsoft Account.

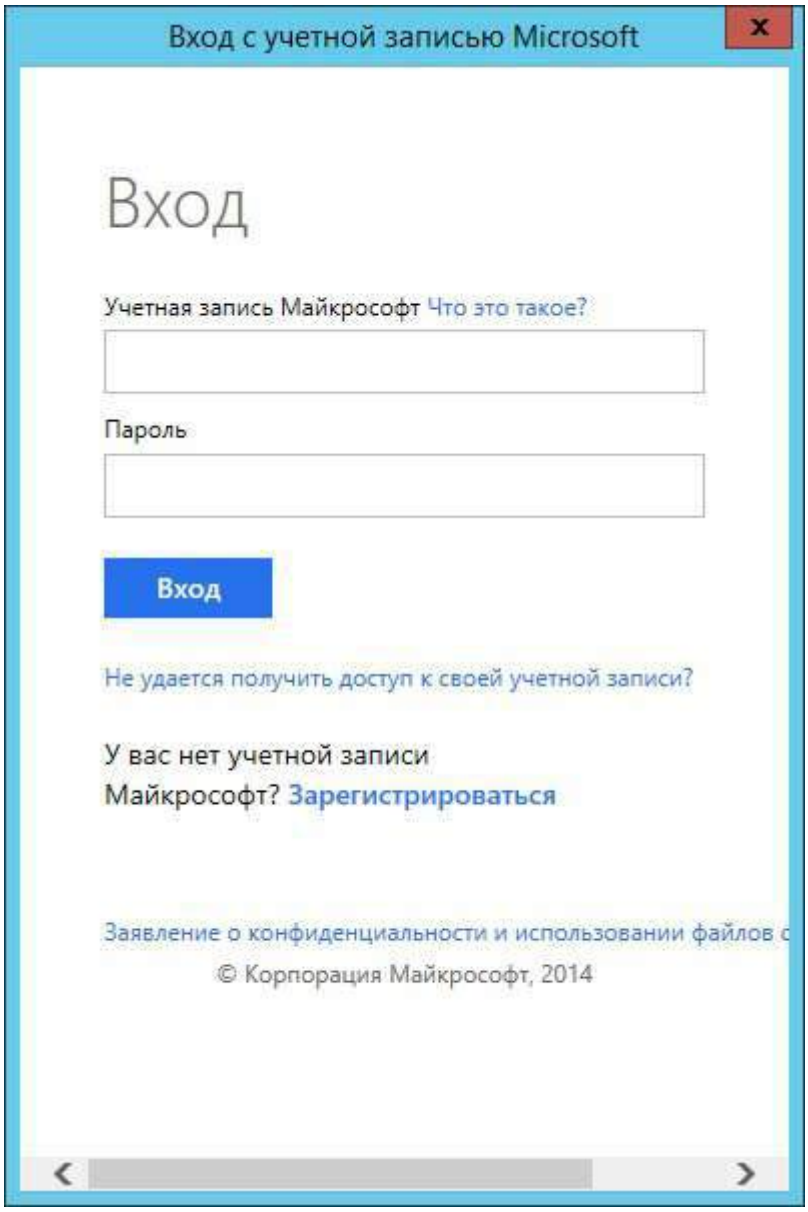


Рис.22 Авторизация в Microsoft Account

После авторизации принимаем заявление о конфиденциальности.

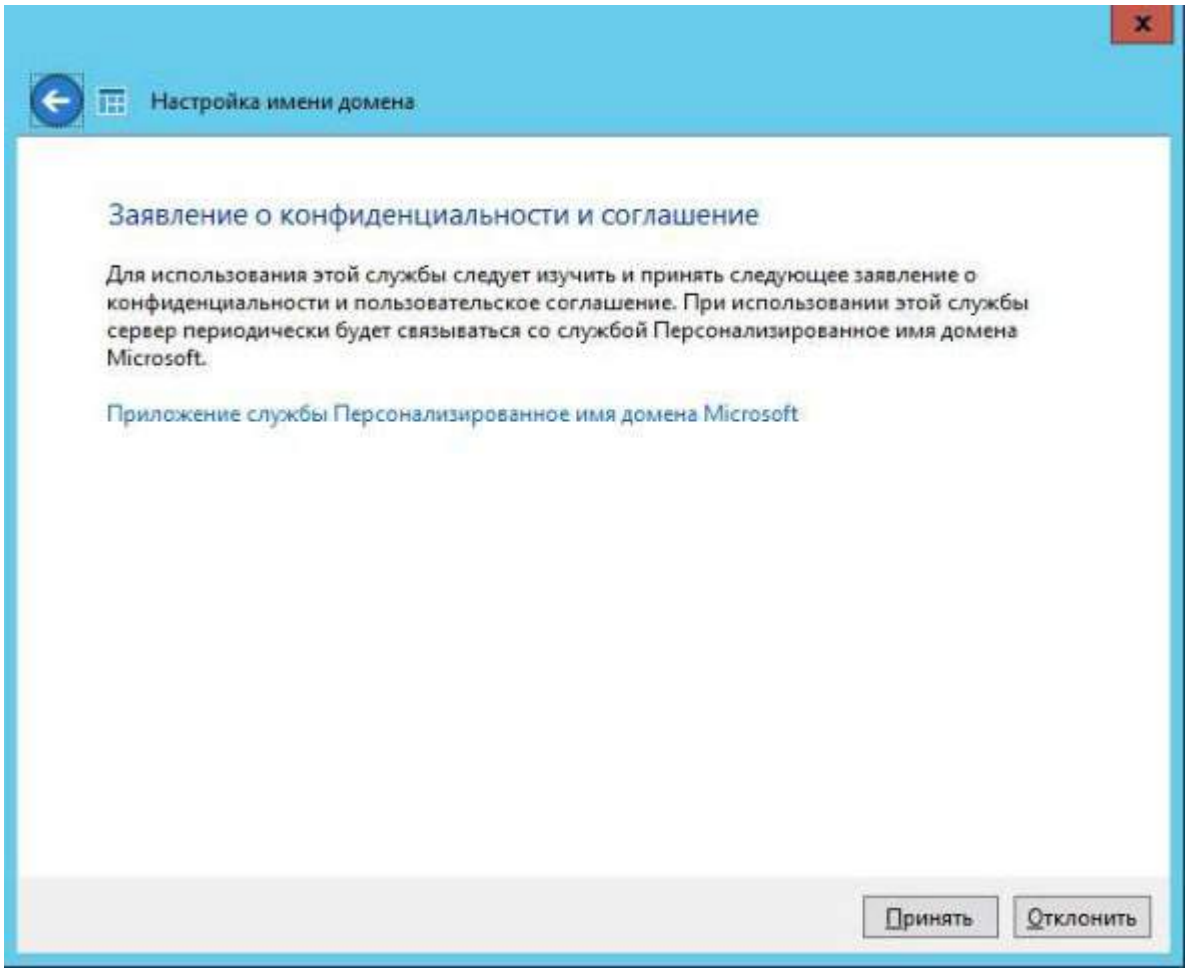


Рис.23 Заявление о конфиденциальности

Вводим имя домена и проверяем доступность, нажимаем настроить.

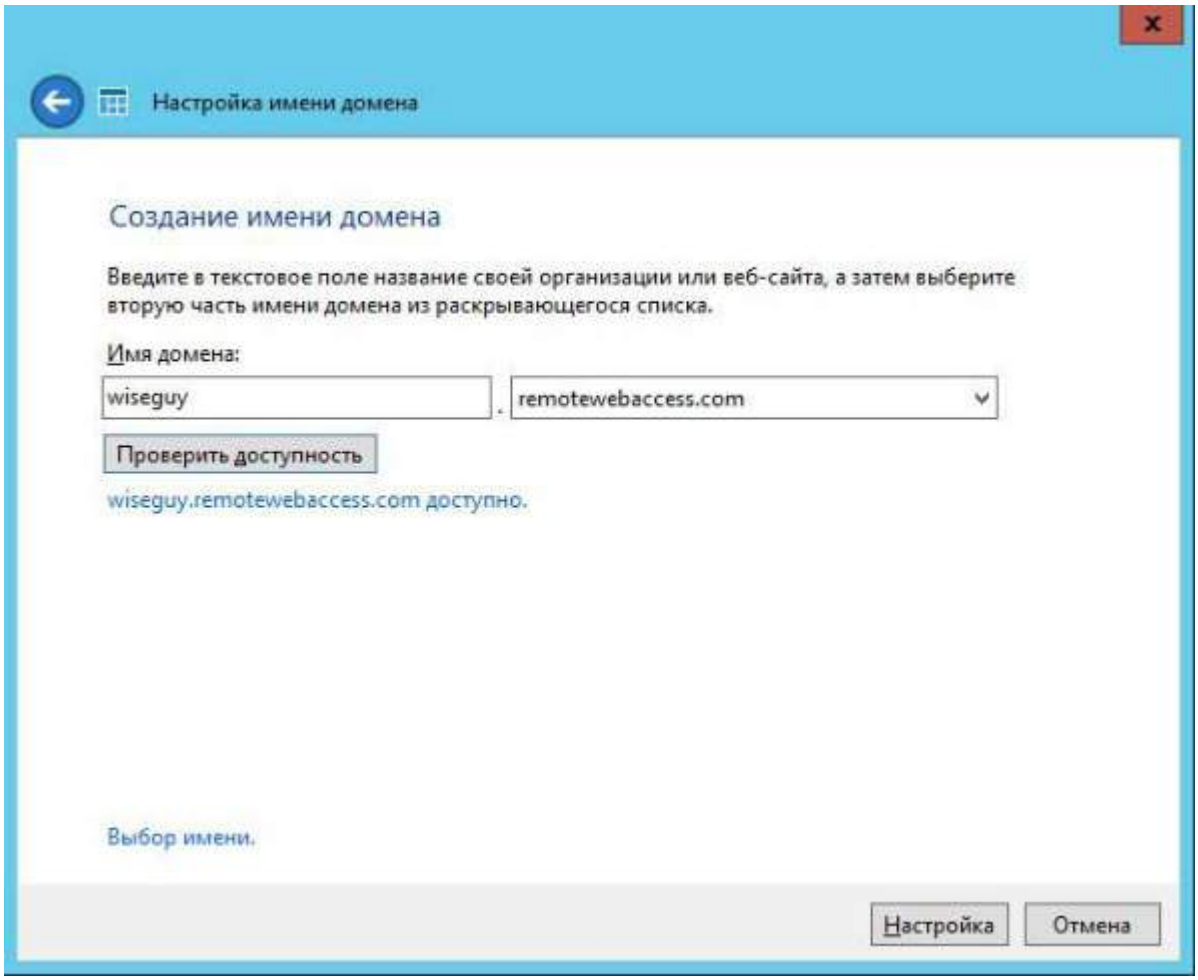


Рис.24 Создание имени домена

С именем домена разобрались. Продолжаем — далее.

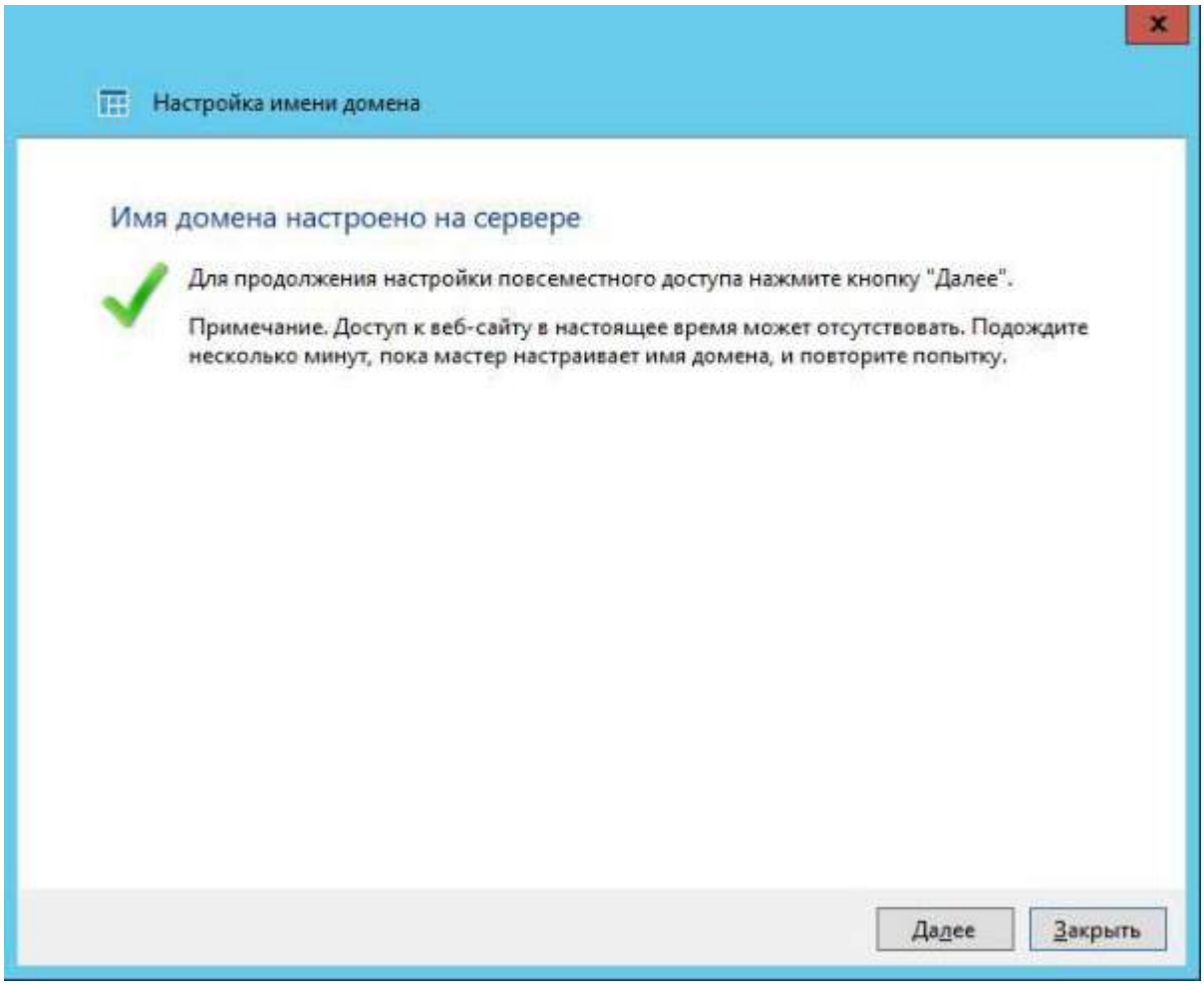


Рис.25 Окно завершения настройки имени домена

Выбираем какие именно возможности будут доступны.

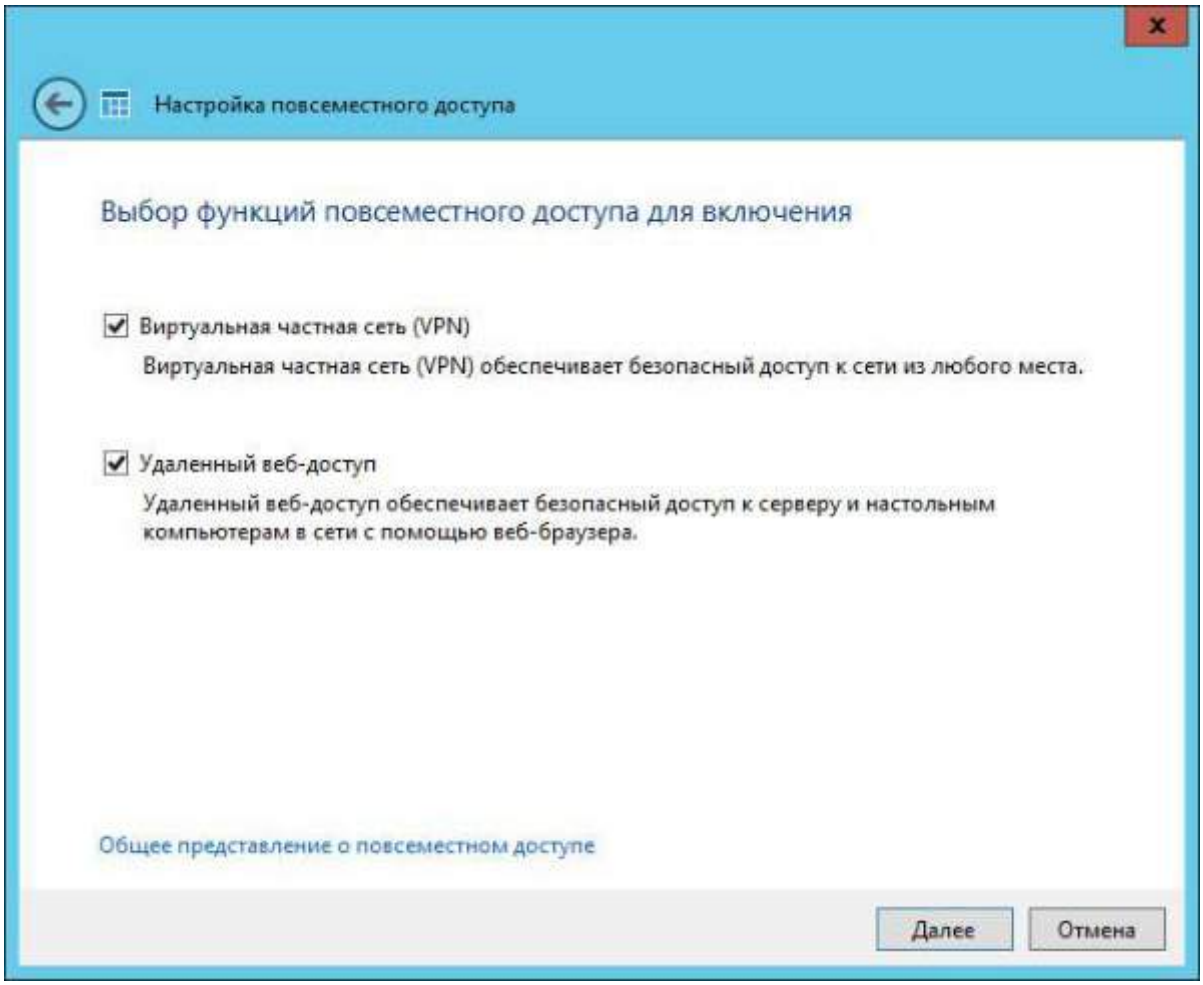


Рис.26 Выбор функций повсеместного доступа

Выбираем будет ли доступен удаленный доступ для текущих пользователей.

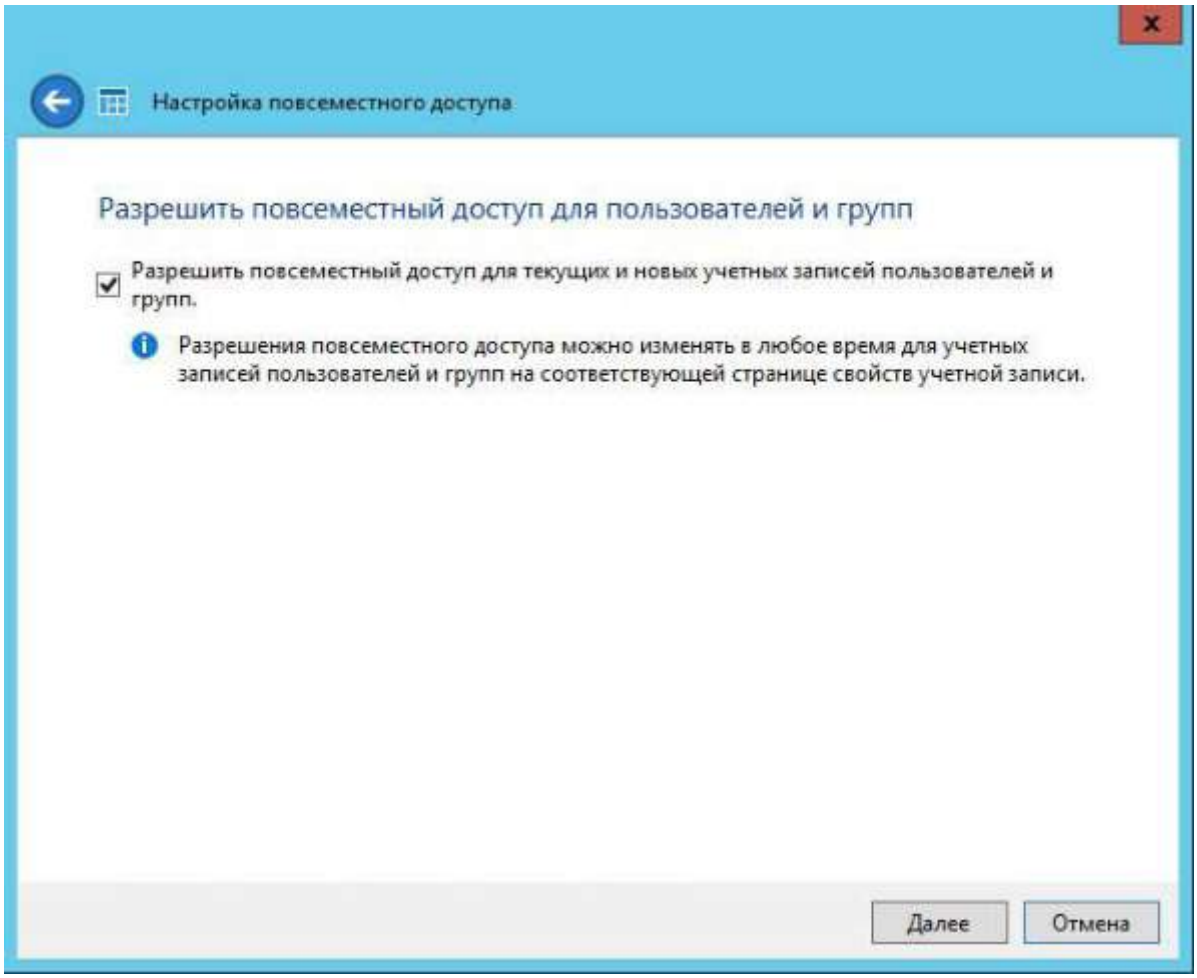


Рис.27 Повсеместный доступ для пользователей и групп

Подключение рабочих станций

Откроем панель мониторинга и перейдем на страницу подключение компьютеров, то увидим там лишь инструкцию к действию.

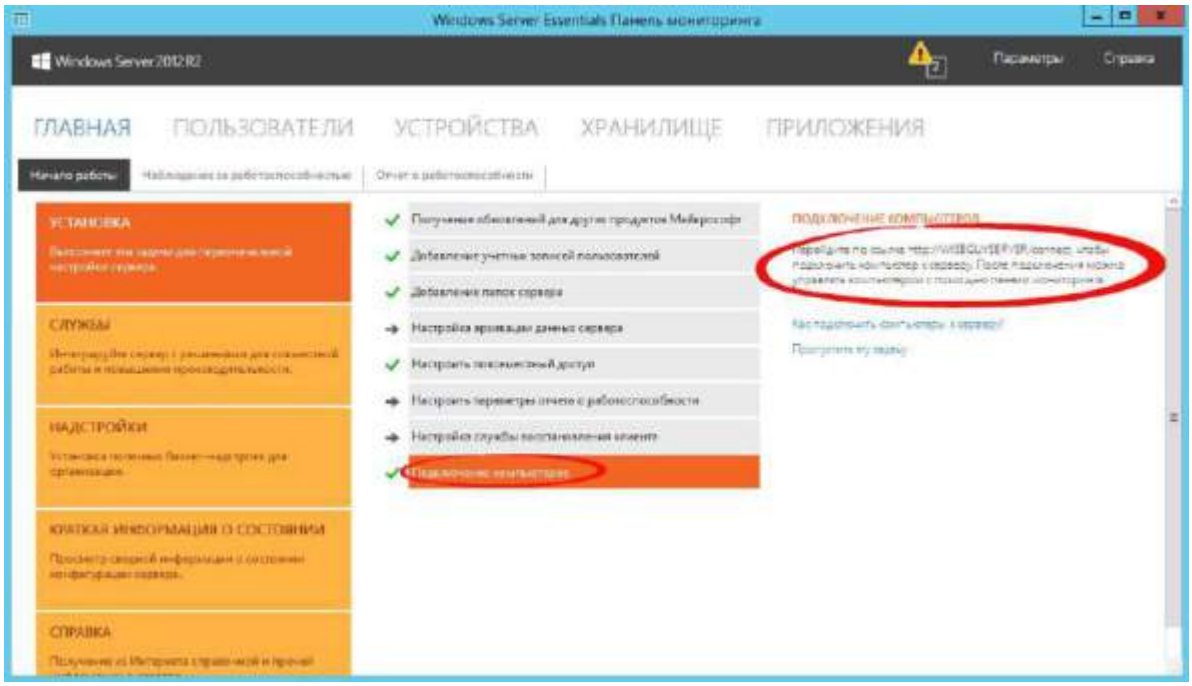


Рис.28 Инструкция к действию

Следуя инструкции на клиенте в браузере открываем страничку http://<Имя сервера>/connect. Нажимаем ссылку для скачивания.

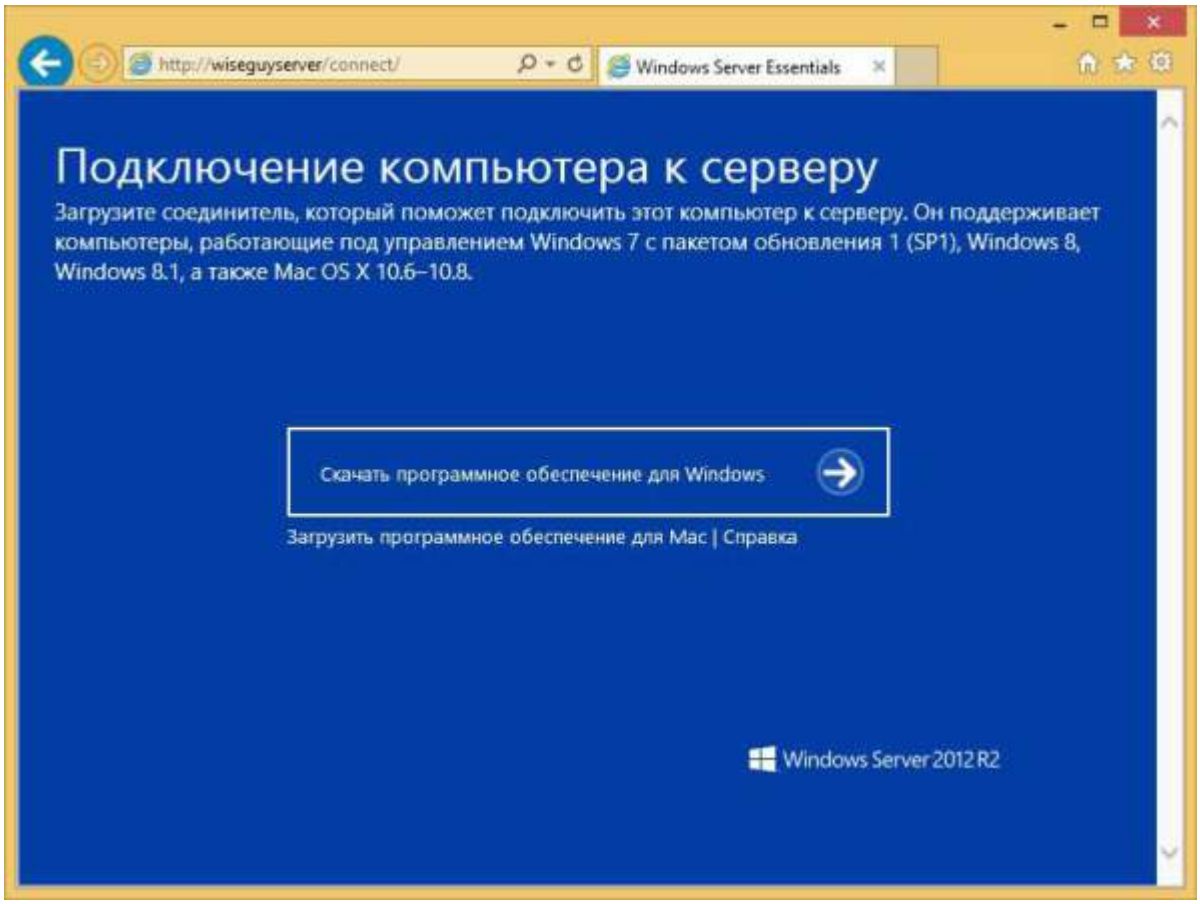


Рис.29 Подключение ПК к серверу

Выбираем выполнить.

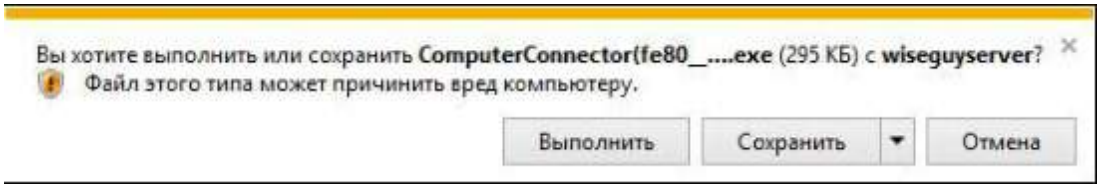


Рис.30 Выбираем выполнить

Принимаем лицензию и ждем

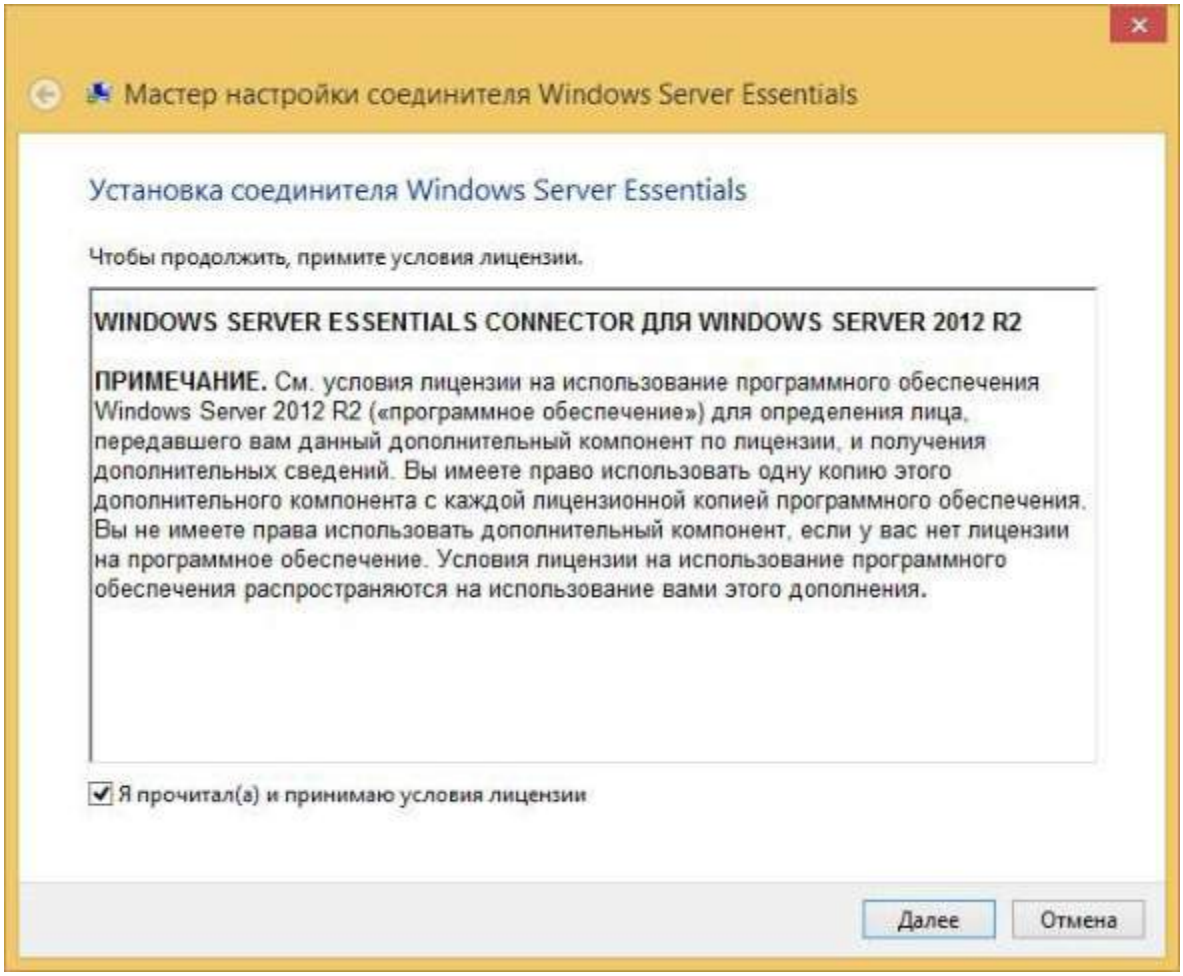


Рис. 31 Лицензионное соглашение

Вводим имя пользователя и пароль пользователя данного компьютера или администратора.

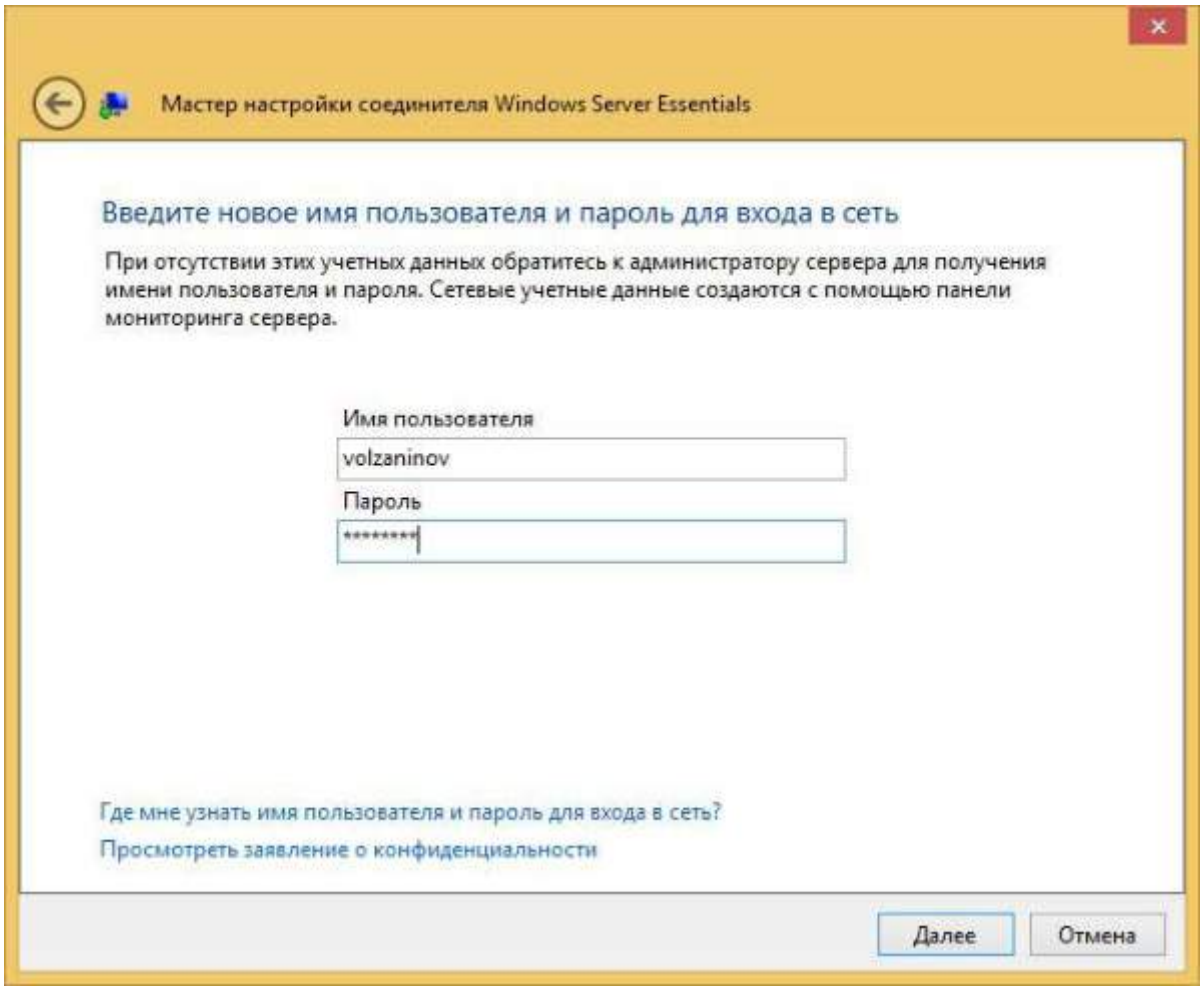


Рис.32 Окно ввода учетных данных

Перезагружаем сервер.

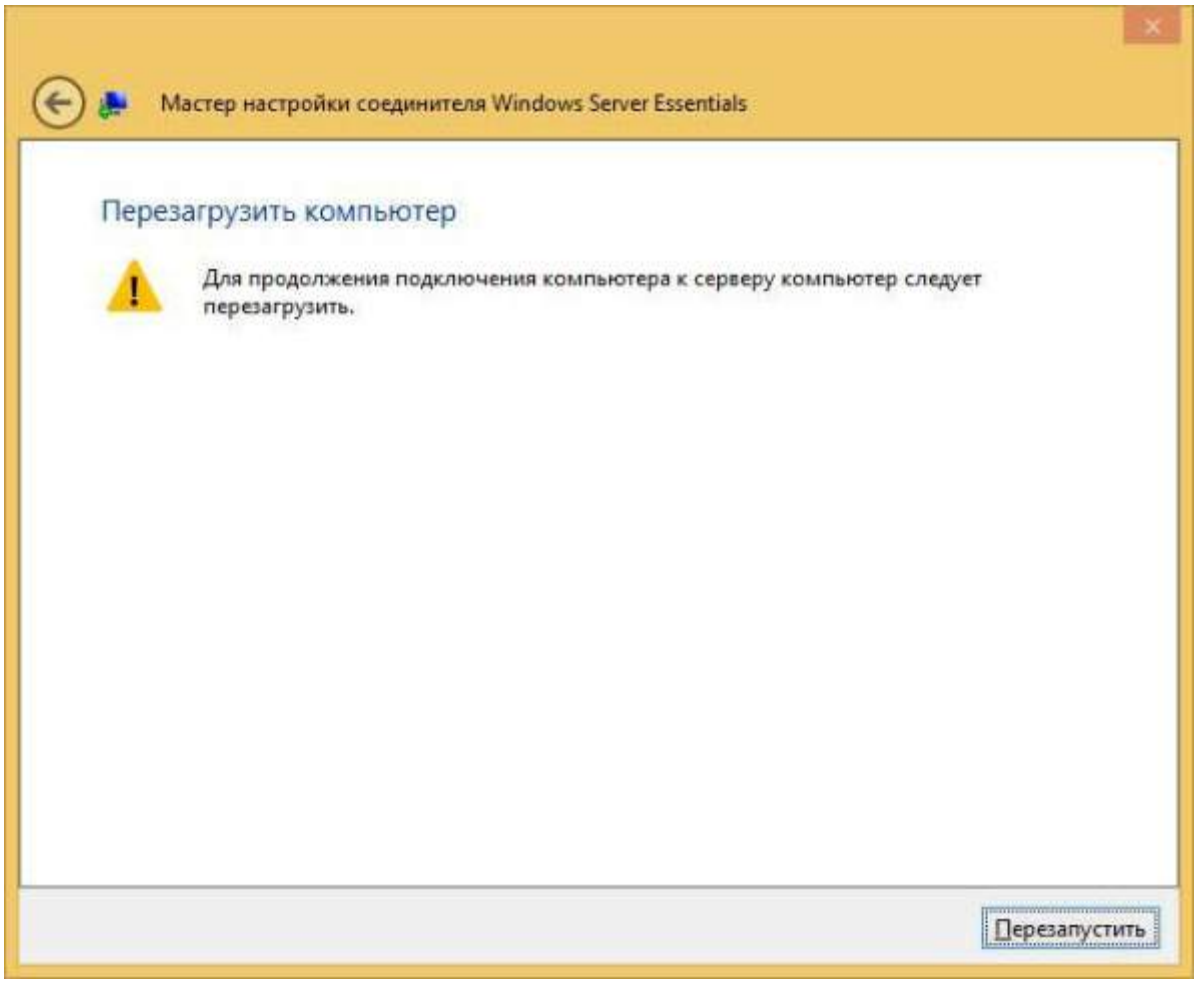


Рис. 33 Перезагрузка сервера

Выбираем, кто будет пользоваться компьютером.

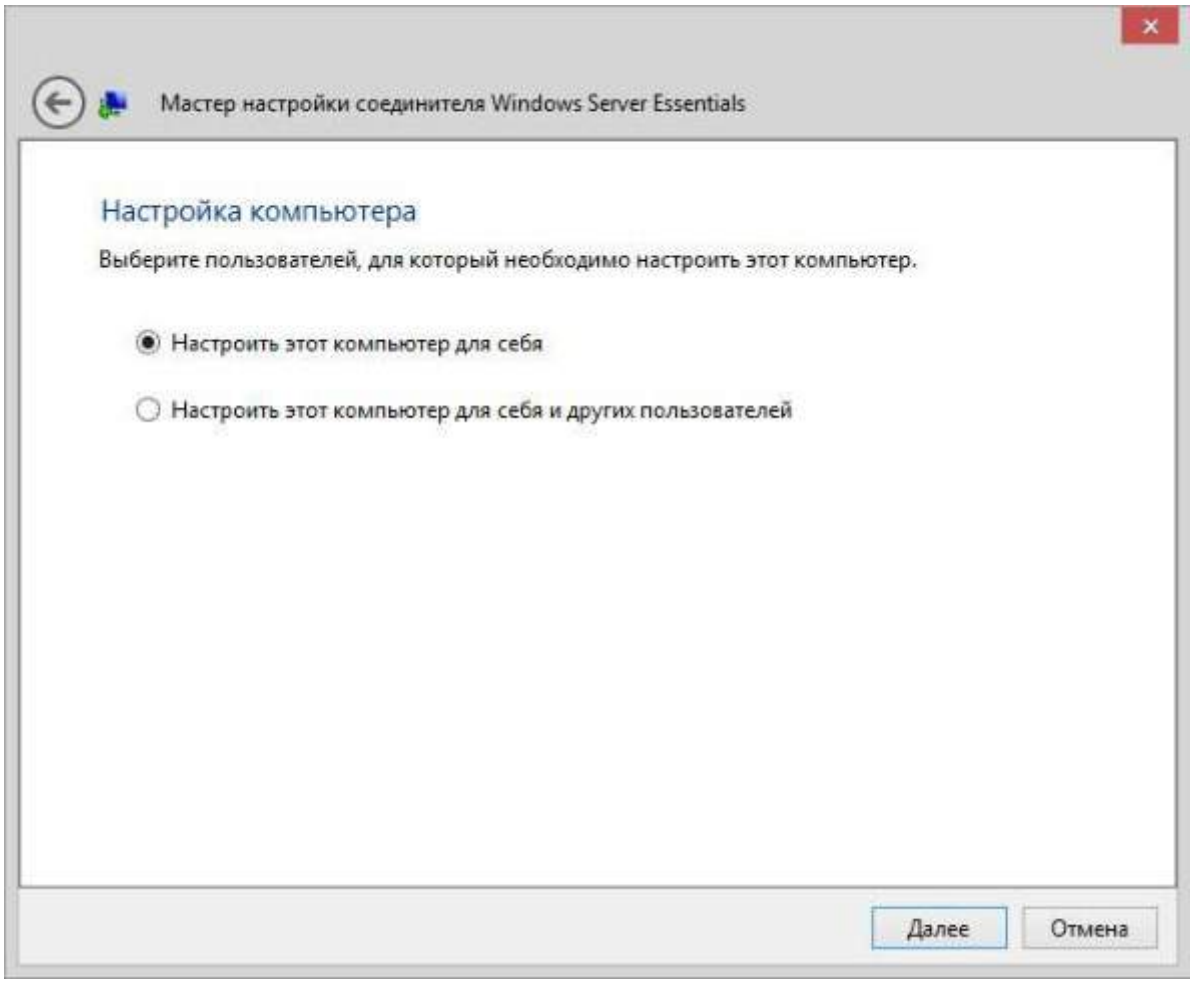


Рис. 34 Выбор пользователя для настройки ПК

Вводим описание компьютера.

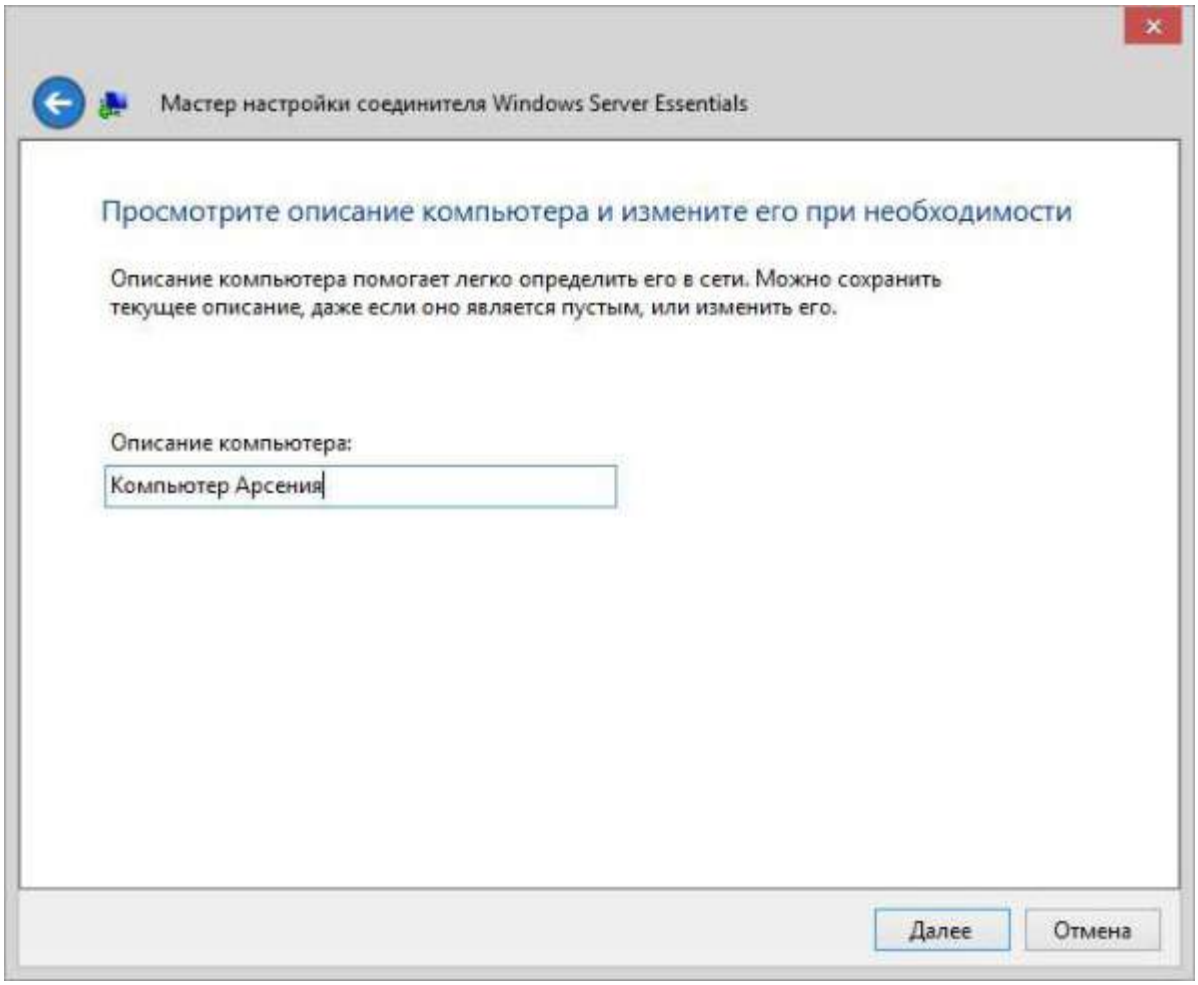


Рис. 35 Описание ПК

Параметры архивации.

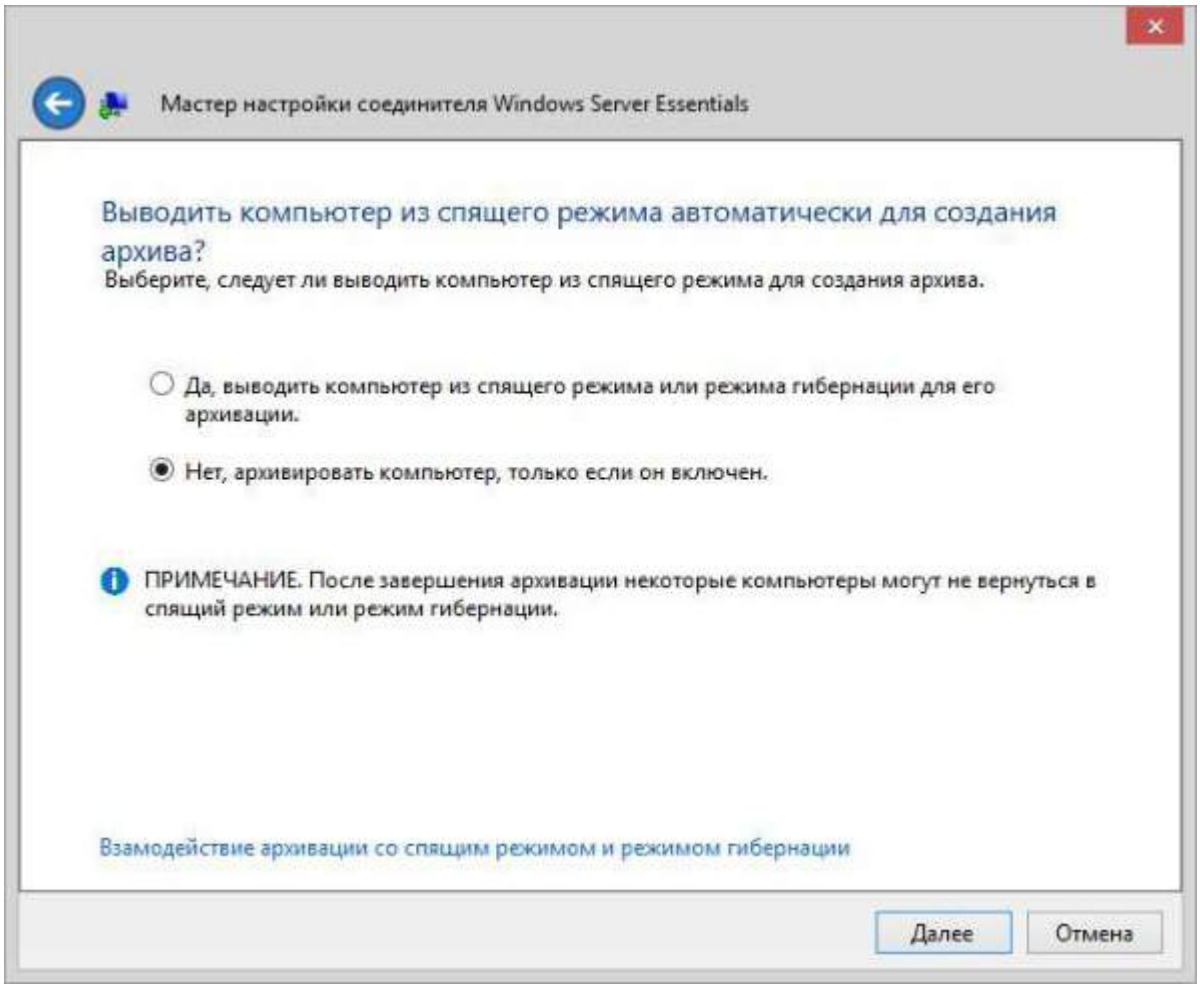


Рис. 36 Параметры архивации

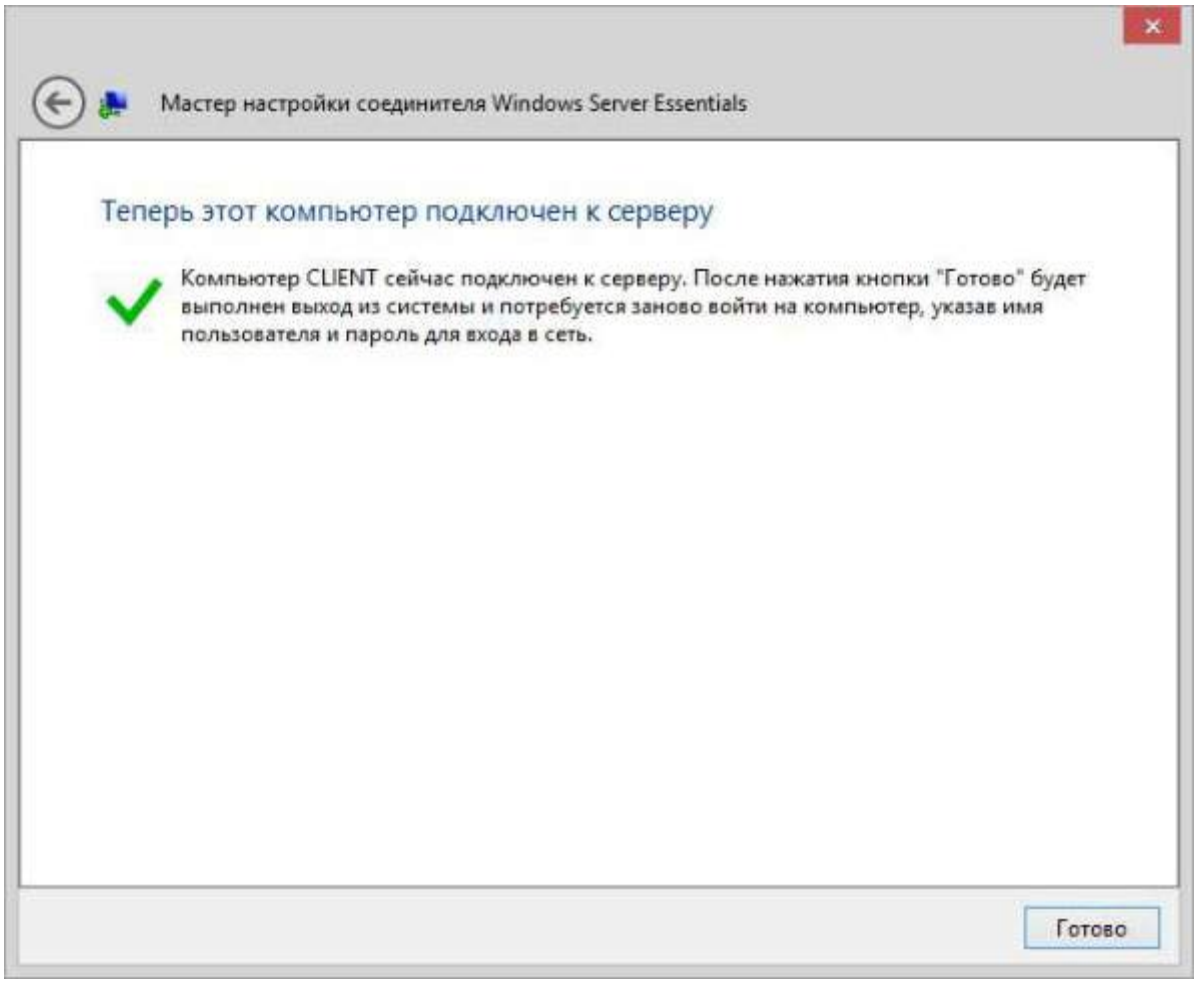


Рис. 37 ПК подключен к серверу

После этого заходим на компьютер под учетной записью пользователя.

ПРАКТИЧЕСКАЯ РАБОТА №37.
Установка System Center 2012 R2 Virtual Machine Manager

Цель работы:
Получение практических навыков по установке System Center 2012 R2 Virtual Machine Manager

Перед установкой

Virtual Machine Manager не является единым продуктом, а состоит из нескольких компонентов. Сюда входят сам сервер управления VMM, консоль управления, сервер библиотеки и сервер БД. Также стоит упомянуть о Web-портале самообслуживания, который имеет прямое отношение к VMM, хотя начиная с SP1 входит в состав App Controller и устанавливается отдельно.

Компоненты VMM могут быть как установлены все вместе, так и разнесены по разным серверам в различных сочетаниях, для распределения нагрузки. Так например, я планирую использовать для установки две машины — одна под сервер управления и библиотеку, другая под базу данных.

Установка System Center 2012 R2 Virtual Machine Manager возможна на Windows Server 2012\2012 R2 редакций Standart и Datacenter. Также для установки сервера управления требуется установить Windows Assessment and Deployment Kit (ADK).

В качестве сервера БД для VMM 2012 R2 можно использовать любую 64-разрядную версию SQL Server 2008 R2 SP2\2012\2012 R2 редакций Standart или Enterprise.

Сервер, на который устанавливается VMM, обязательно должен быть членом домена Active Directory. Если сервер управления и сервер БД находятся в разных доменах Active Directory, то между этими доменами должны быть установлены двусторонние доверительные отношения. Имя сервера не должно превышать 15 символов, и в нем не должно быть дефисов, то есть сервер можно назвать **SCVMM**, но нельзя **SC-VMM.**

И немного об аппаратных требованиях. По документации Microsoft минимальной конфигурацией для развертывания VMM являются 64-разрядный Pentium 4 2,8 ГГц и 2 ГБ ОЗУ. При установке сервера управления на виртуальную машину Hyper-V с использованием динамической памяти, стартовый объем ОЗУ должен быть не меньше 2 ГБ.

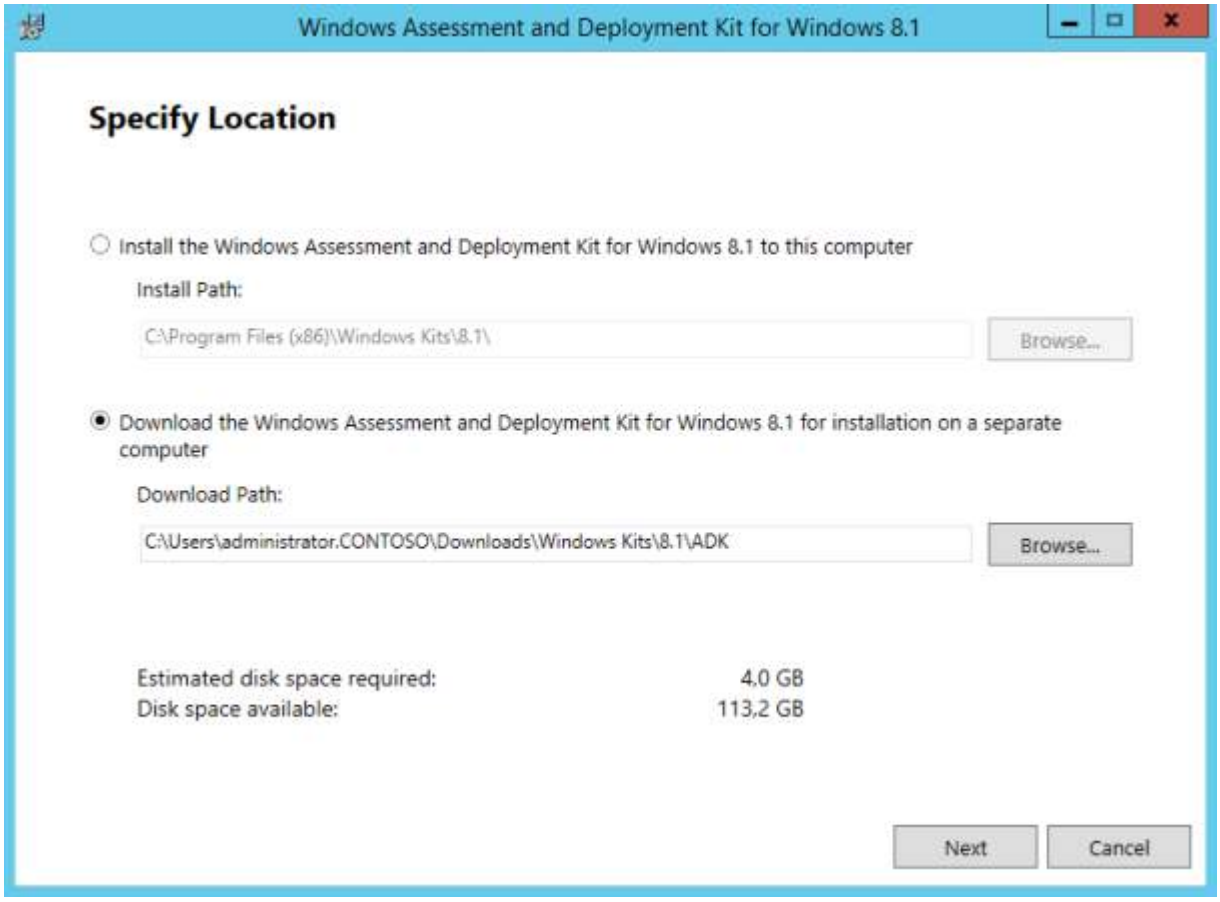
Также для установки VMM потребуется минимум 2 ГБ дискового пространства для установки отдельно от сервера БД, или 80 Гб с учетом БД. Если же сервер управления планируется использовать и как библиотеку, то следует выделить дополнительное место под хранение объектов (виртуальных дисков, ISO-образов и т.п.).

Более подробно системные требования к компонентам System Center 2012 можно посмотреть здесь, а мы перейдем к установке. Я выбрал сценарий развертывания с раздельным сервером БД, поэтому установка будет производится на две виртуальные машины. Сервер управления будет установлен на машину SC1, а сервер БД — на SC2.

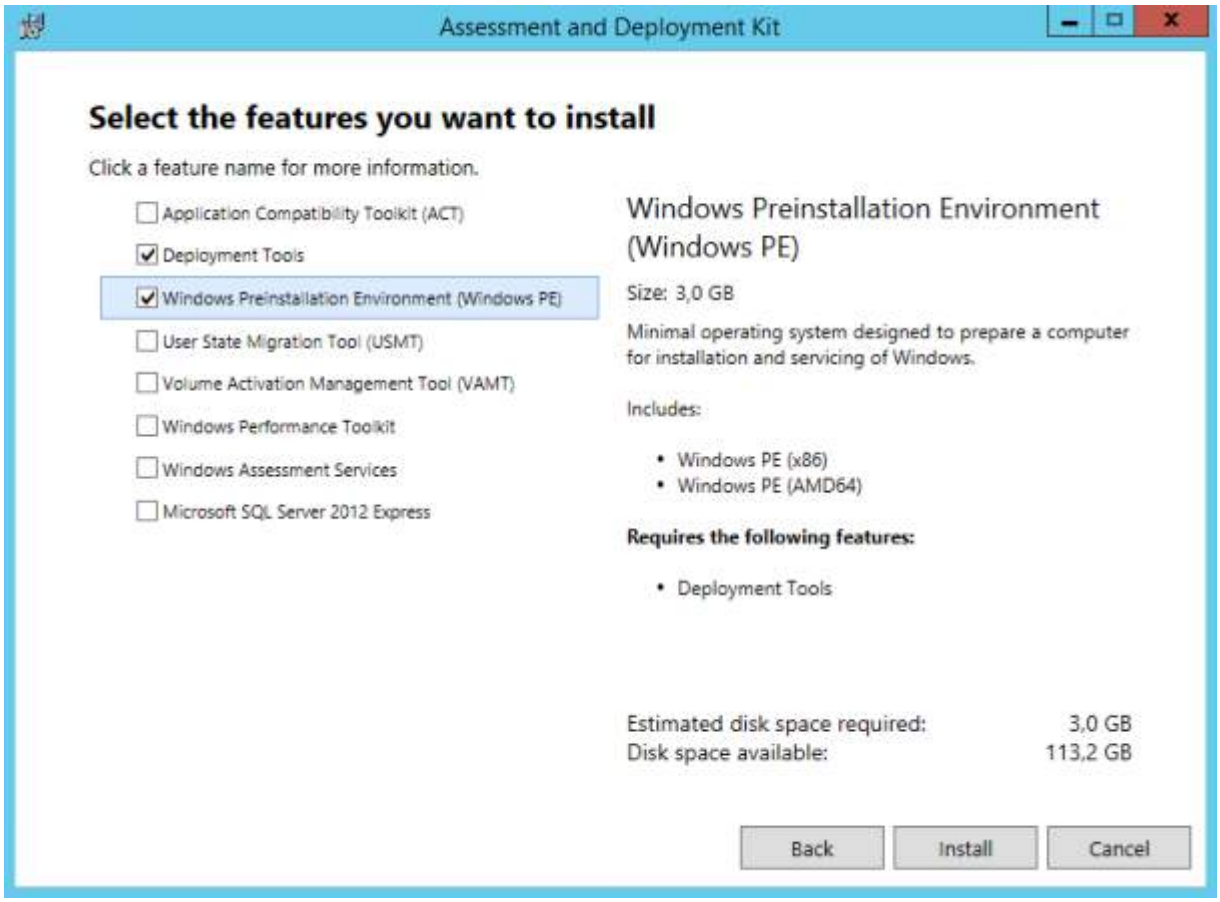
Установка ADK

Переходим на SC1 и скачиваем Windows Assessment and Deployment Kit (ADK) for Windows 8.1. Обратите внимание, что по ссылке скачивается небольшой файлик, который затем загружает и устанавливает все остальное. Как вариант,

можно предварительно загрузить файлы установки в указанную папку, а потом перенести их на сервер и запустить установку.

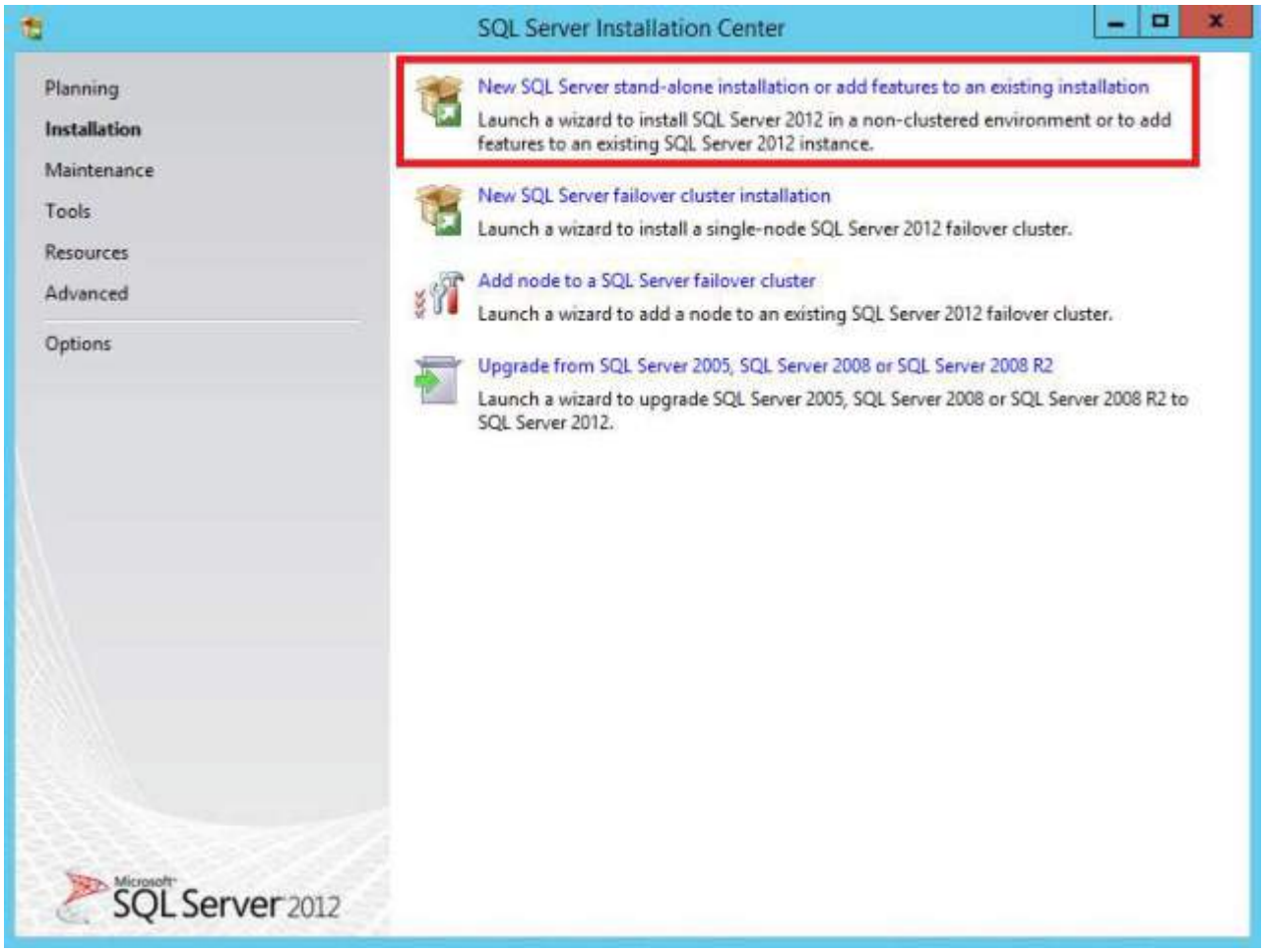


Из всего набора ADK для VMM необходимо установить только Deployment Tools и Windows PE.

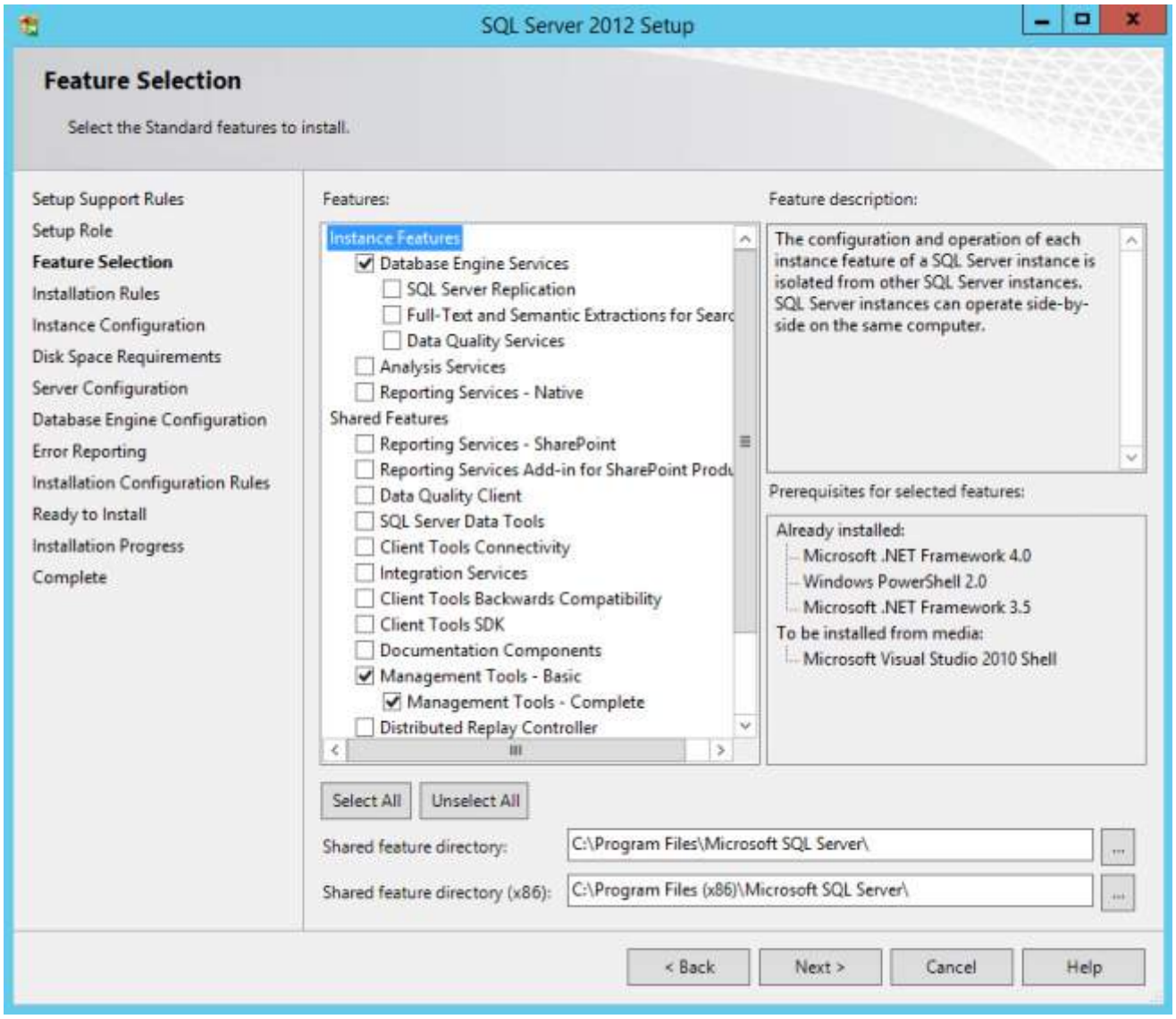


Установка SQL Server

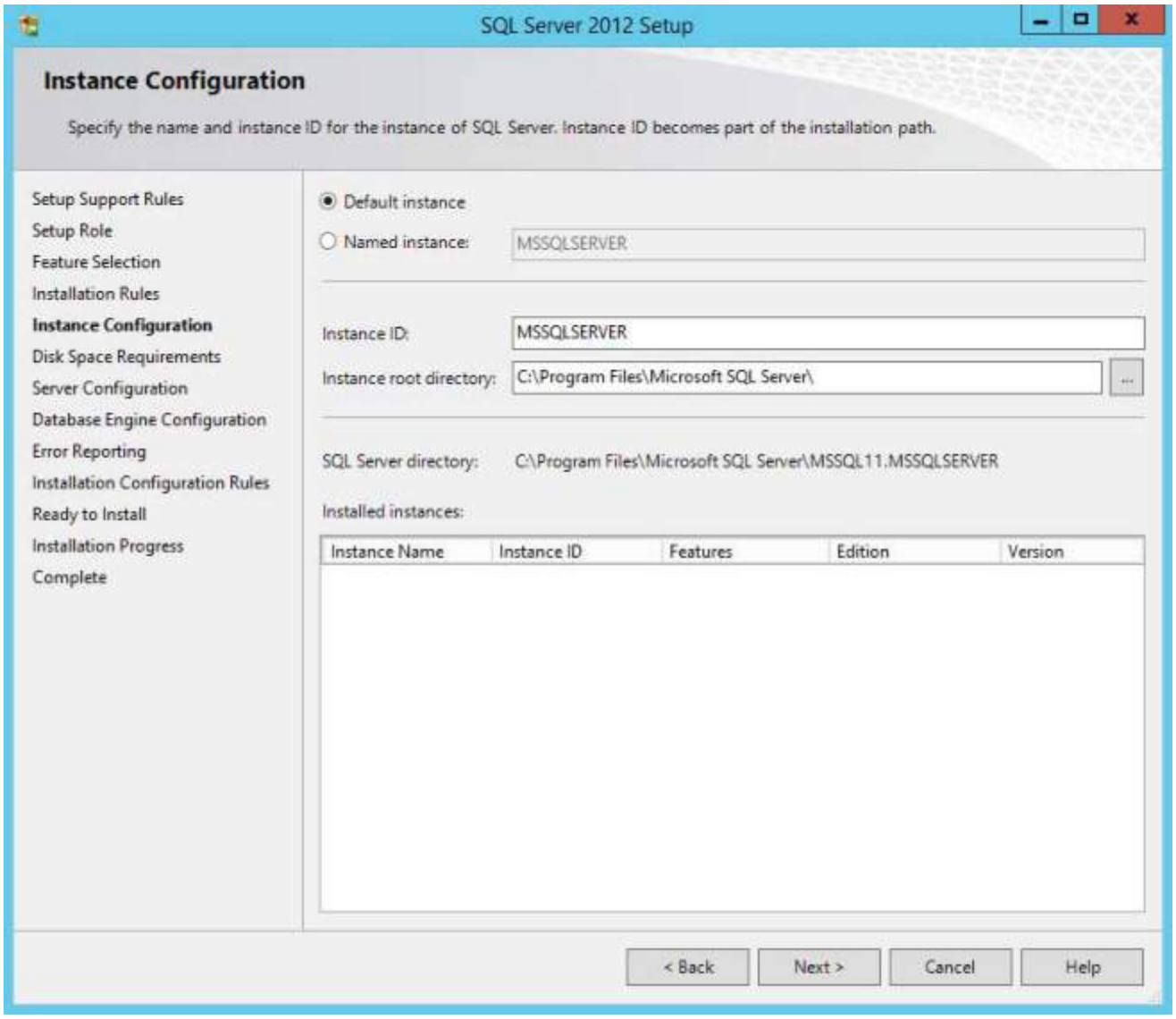
Будем устанавливать дистрибутив SQL Server 2012 SP1. Запускаем инсталлятор и выбираем тип установки одиночный сервер (stand-alone).



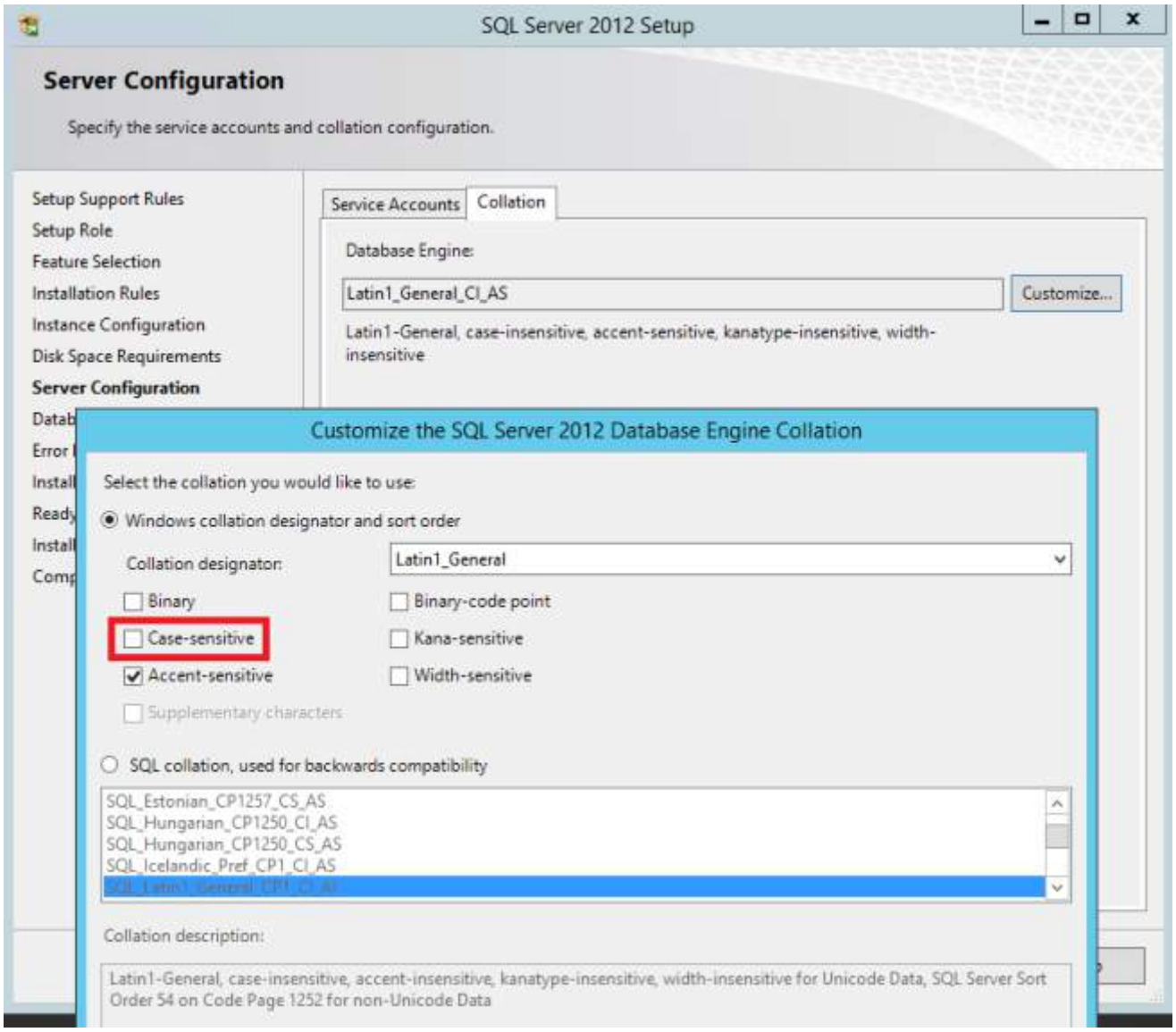
Выбираем установку компонентов **Database Engine Services** и **Management Tools — Complete**.



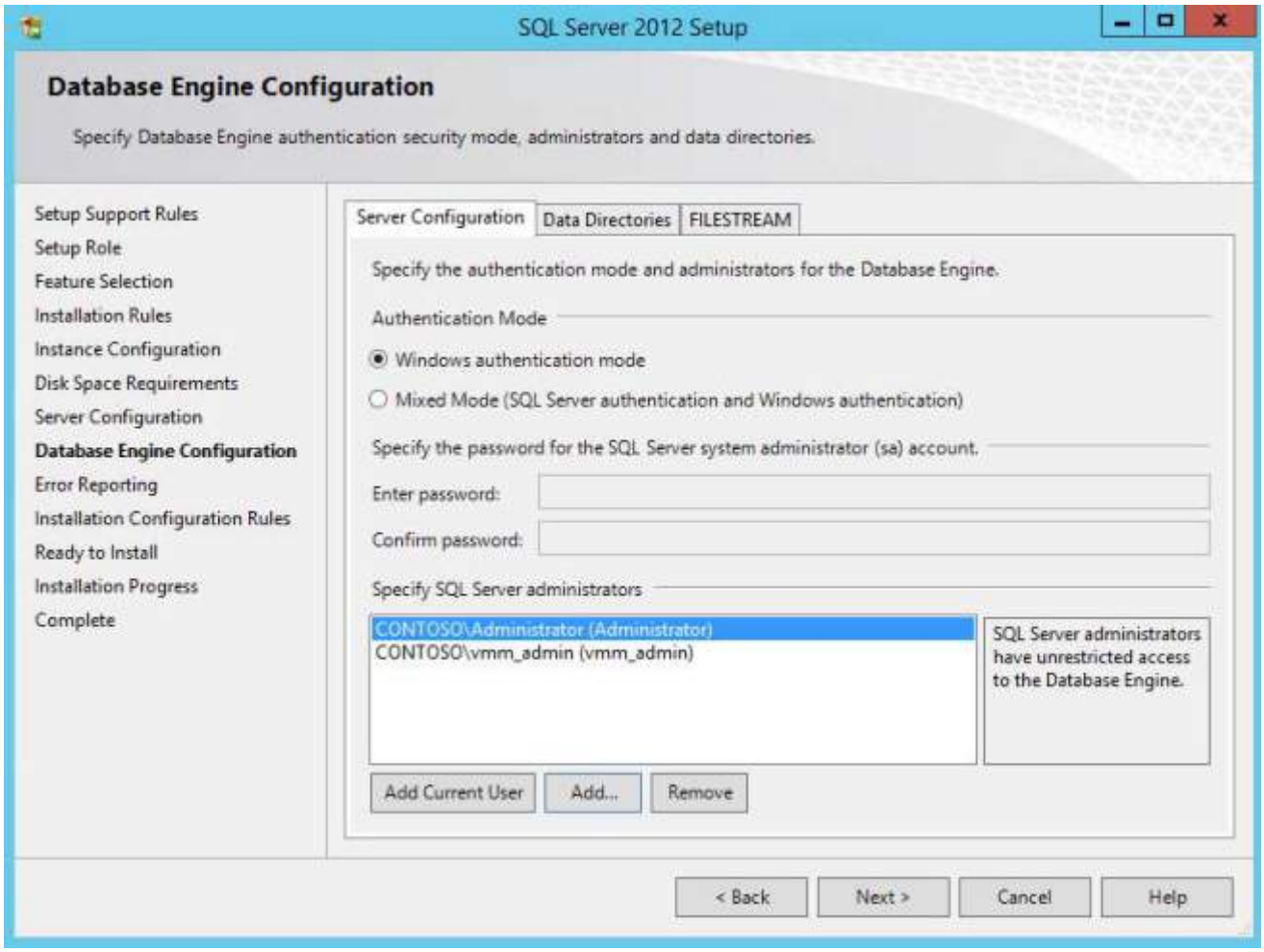
Выбираем установку Default instance с настройками по умолчанию, хотя при желании можно установить и именованный экземпляр SQL Server.



Обязательным требованием для VMM является использование экземпляра SQL Server без учета регистра символов при сортировке. Поэтому на пункте Server Configuration переходим на вкладку Collation, жмем кнопку Customize и проверяем наличие отсутствия галочки в пункте Case-Sensitive. Это важный момент, изменить порядок сортировки после установки SQL Server крайне сложно.

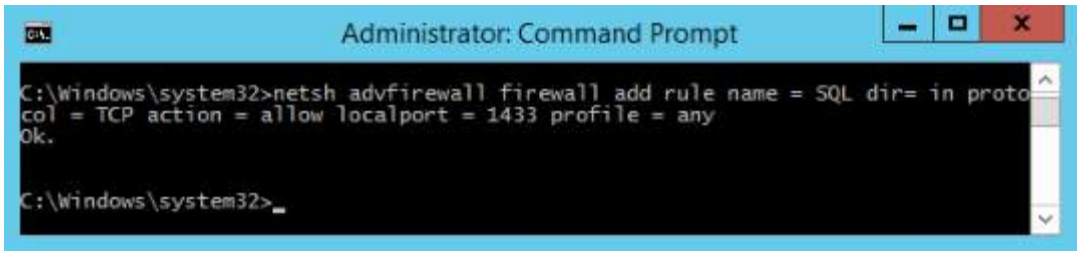


Выбираем режим аутентификации Windows authentication mode и добавляем в список администраторов пользователя vmm_admin. Под этим пользователем сервер управления VMM будет подключаться к базе данных.



И после окончания установки открываем для входящего трафика на файерволле порт 1433 TCP, который использует дефолтный экземпляр SQL Server. Сделать это можно из графической оснастки, либо в командной консоли командой:

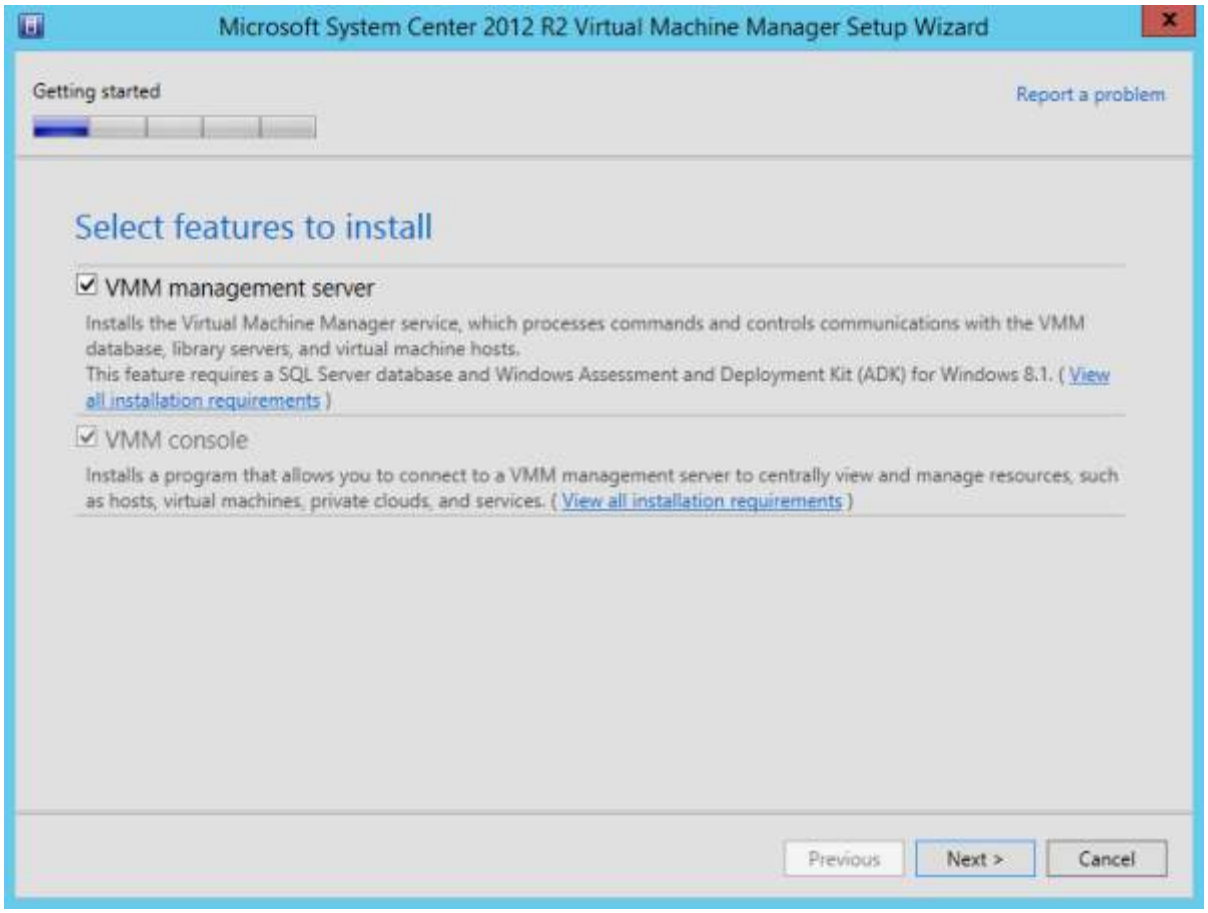
netsh advfirewall firewall add rule name = SQL dir = in protocol = TCP action = allow localport = 1433 profile = any



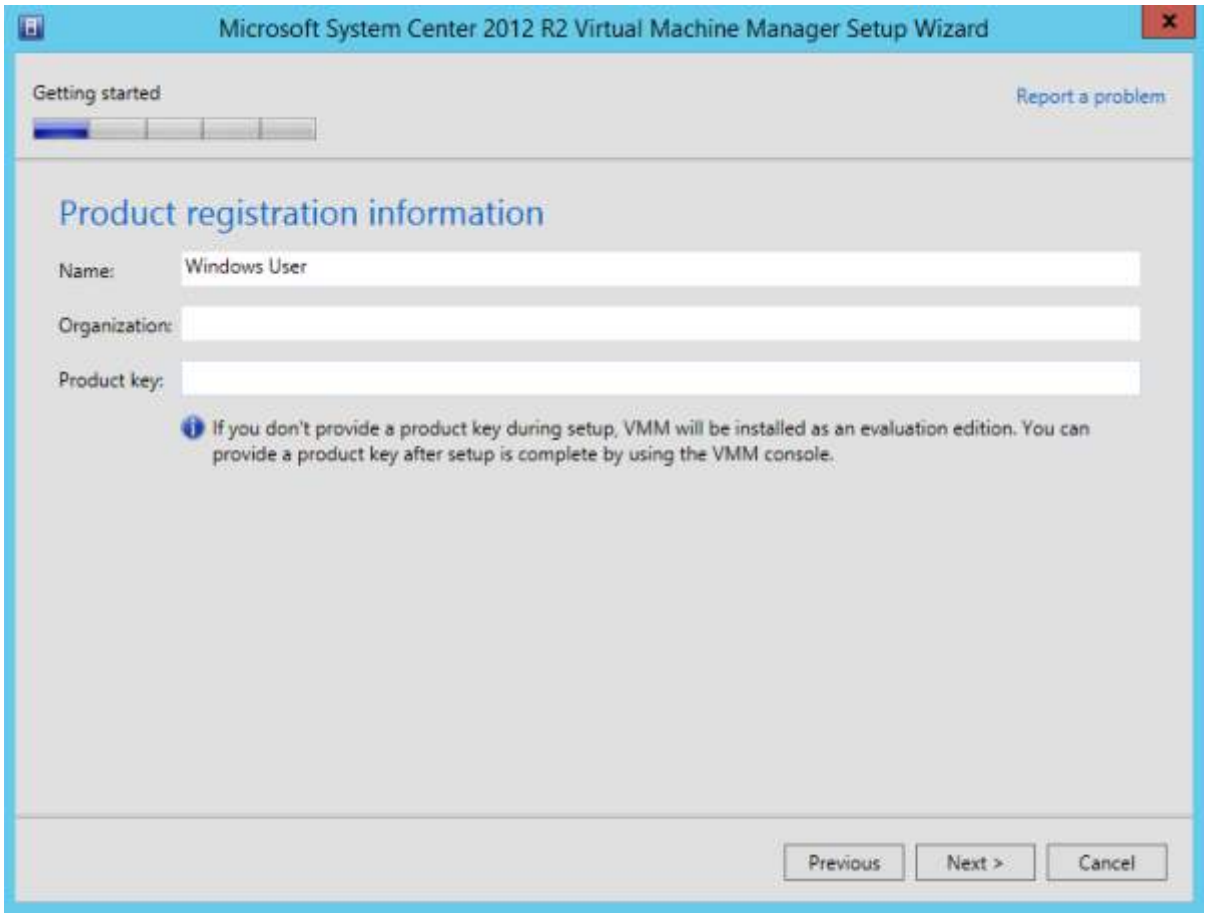
Установка Virtual Machine Manager

Запускаем инсталлятор и жмем Install.

Выбираем для установки компонент **VMM management server**.



Указываем имя пользователя и регистрационные данные. Ключ продукта не обязательно вводить при установке, это можно сделать и потом.

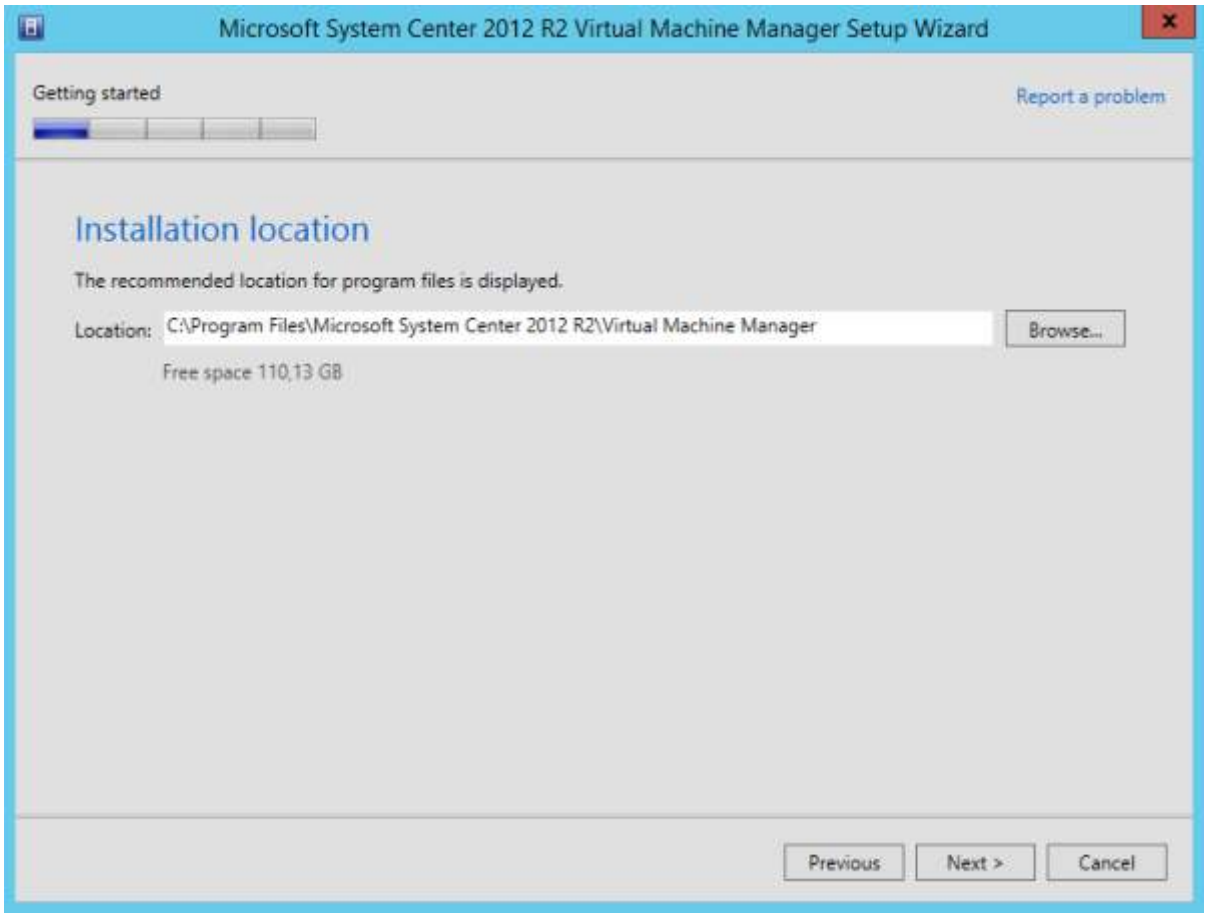


Соглашаемся с лицензионным соглашением.

И отказываемся от участия в программе повышения качества обслуживания (CEIP).

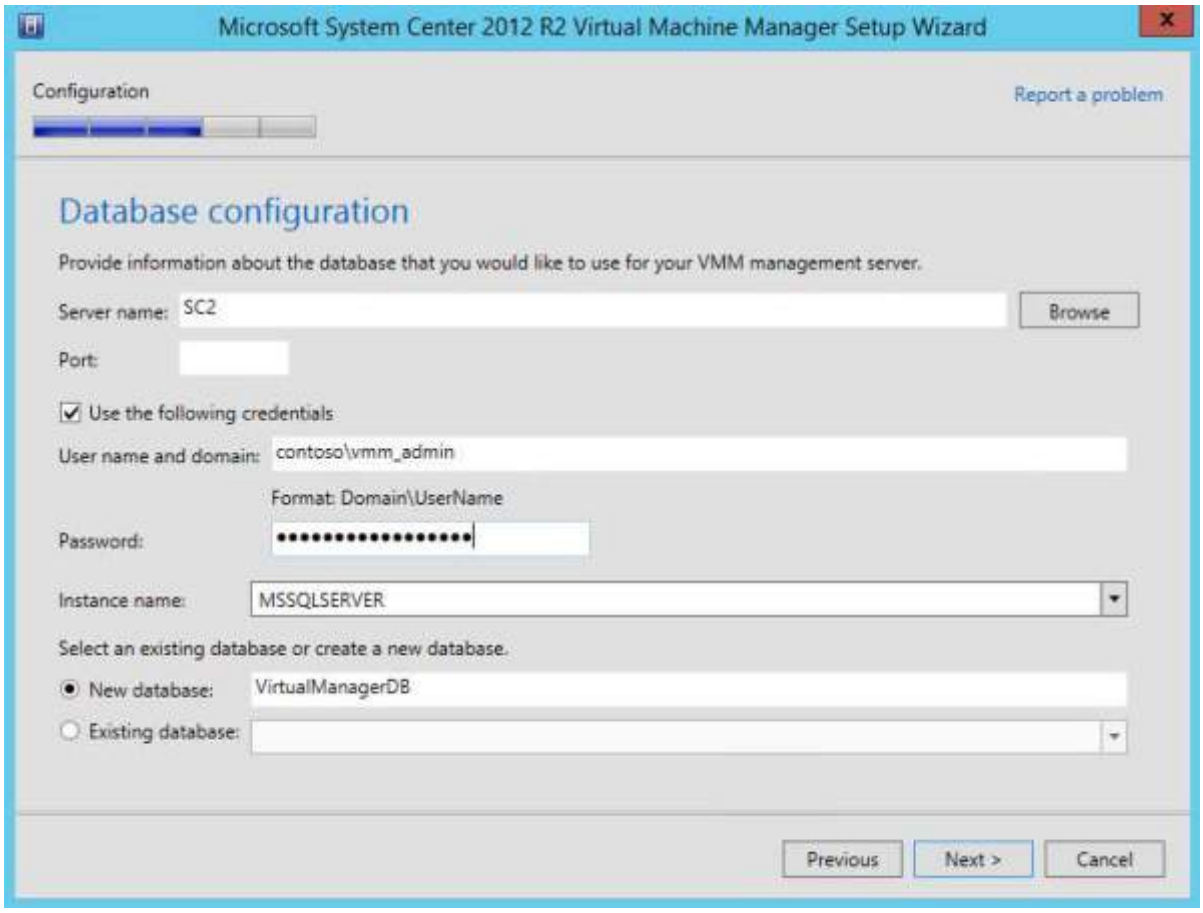
Включаем автоматическое обновление VMM.

Указываем папку для установки.



На следующем этапе производится сбор сведений и проверка на соответствие необходимым требованиям. Если система не соответствует требованиям, то установка может быть прервана. В нашем случае выдано предупреждение о недостаточном объеме памяти, что позволяет продолжить установку.

Дальше идет настройка подключения к базе данных. Выбираем сервер SC2 с портом по умолчанию, указываем учетные данные пользователя vmm_admin, под которыми будет производится подключение к базе. Затем выбираем дефолтный экземпляр сервера и указываем создание новой базы данных.



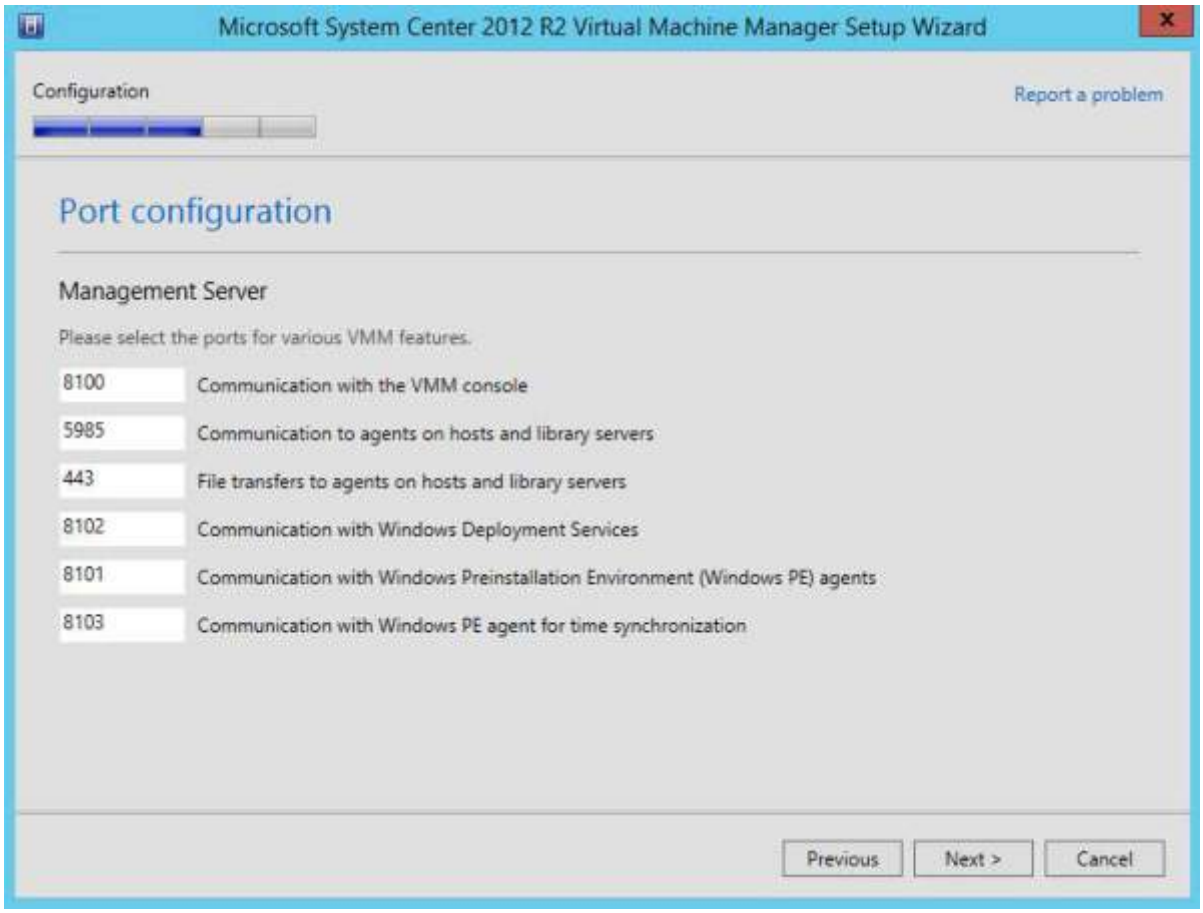
Настраиваем учетную запись, под которой будет работать служба VMM. Можно выбрать системный аккаунт Local System, либо указать доменную учетную запись. При выборе надо учитывать, что изменить учетную запись службы VMM после установки будет невозможно, для этого потребуется полная переустановка. Если указывается доменная учетная запись, то она должна входить в группу локальных администраторов на данном компьютере.

Дальше идет выбор варианта управления ключами. С помощью этих ключей VMM шифрует некоторые данные в базе (напр. учетные записи и пароли RunAs User). При локальном хранении ключей шифрование этих данных будет привязано к конкретному компьютеру, на котором установлена служба VMM, и к учетной записи этой службы. Соответственно при переносе VMM на другой сервер данные будут потеряны.

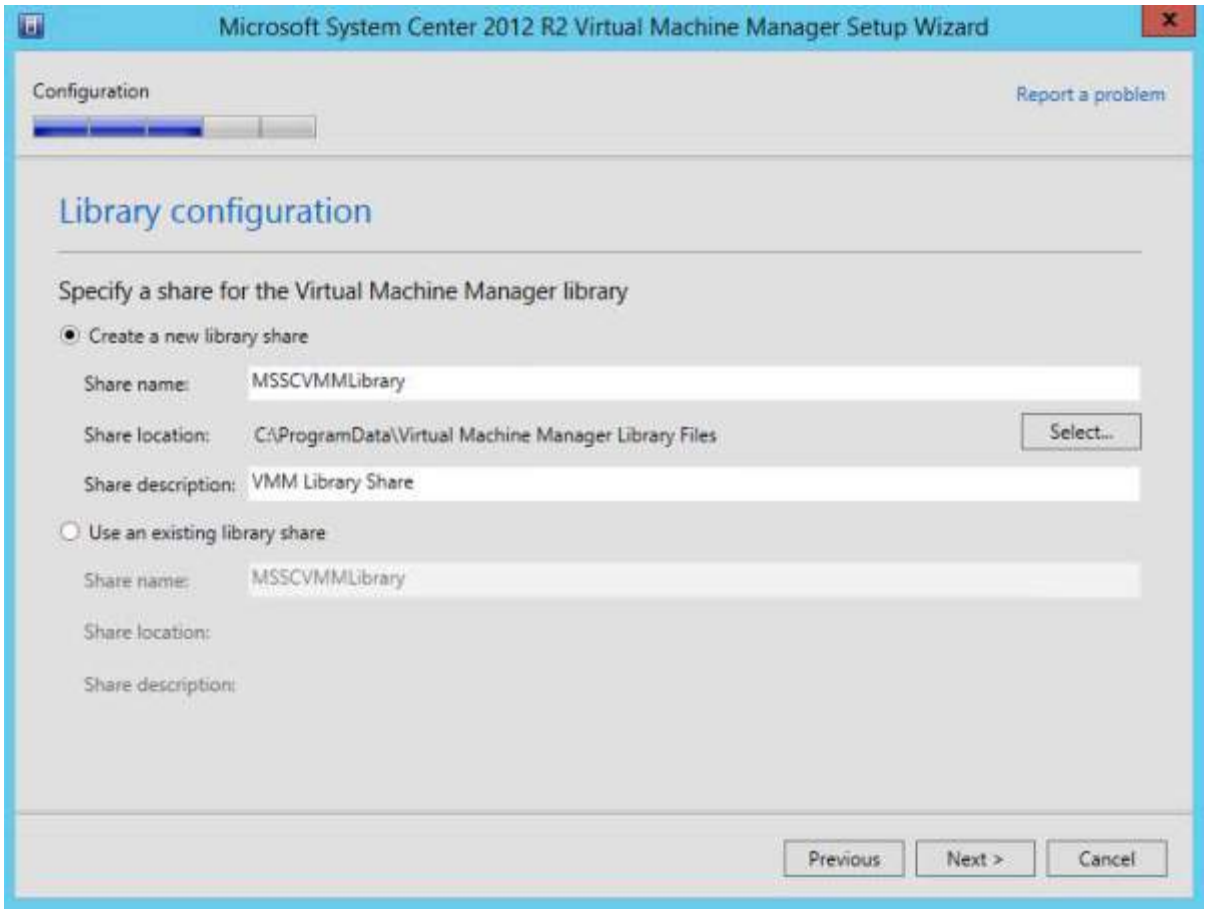
Распределенное управление ключами (Distributed Key Management) позволяет сохранить ключи в Active Directory, поэтому в случае переноса службы зашифрованные данные сохраняются и будут доступны с другого компьютера. В этом случае перед установкой VMM необходимо создать в Active Directory специальный контейнер для хранения ключей. Контейнер может быть типа такого "CN=SCVMM,DC=contoso,DC=com", создать его можно с помощью редактора ADSIEdit.

Для production правильно будет создать для VMM в домене управляемую сервисную учетную запись (Managed Service Account), а ключи хранить в Active Directory. Для развертывания в лабораторной среде можно оставить Local System и хранить ключи локально, что я и сделаю.

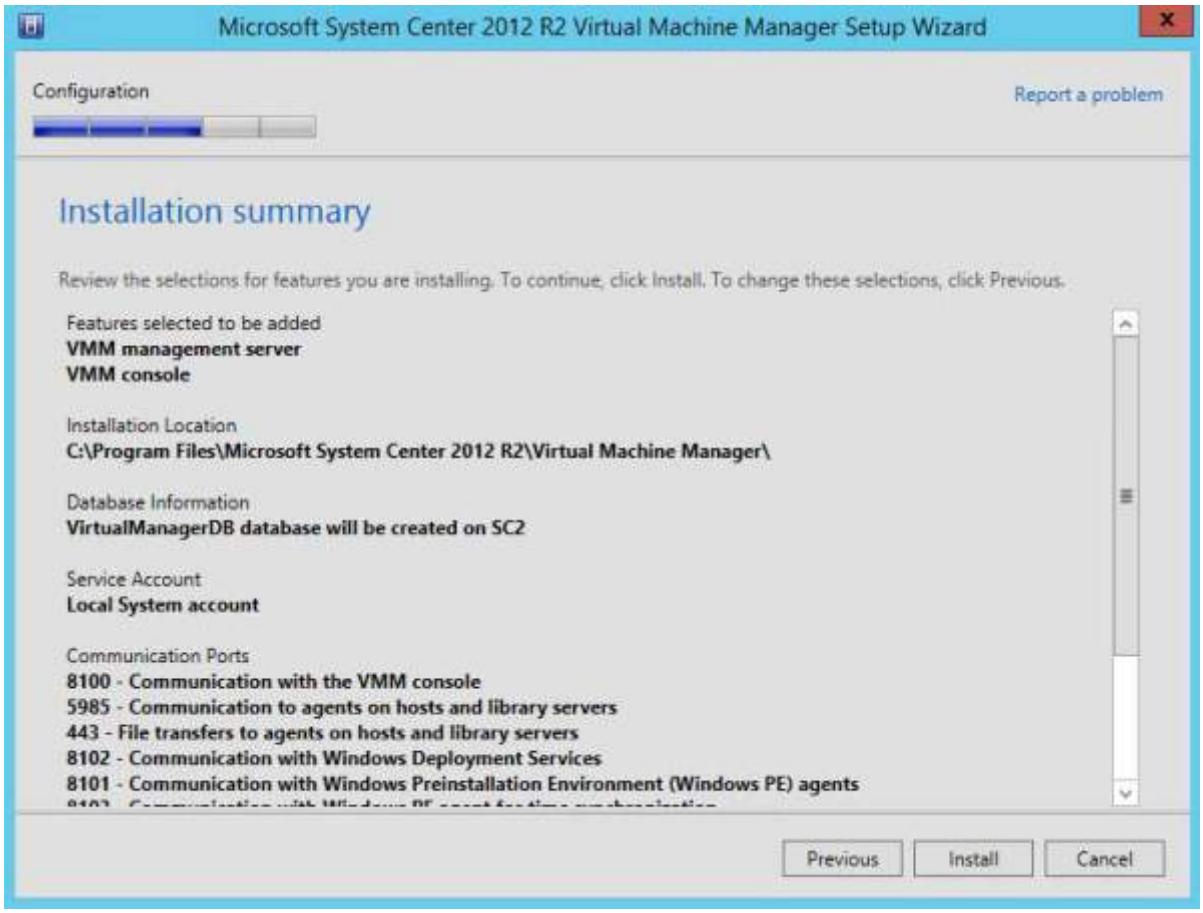
Дальше идет настройка портов. Без необходимости их лучше не менять.



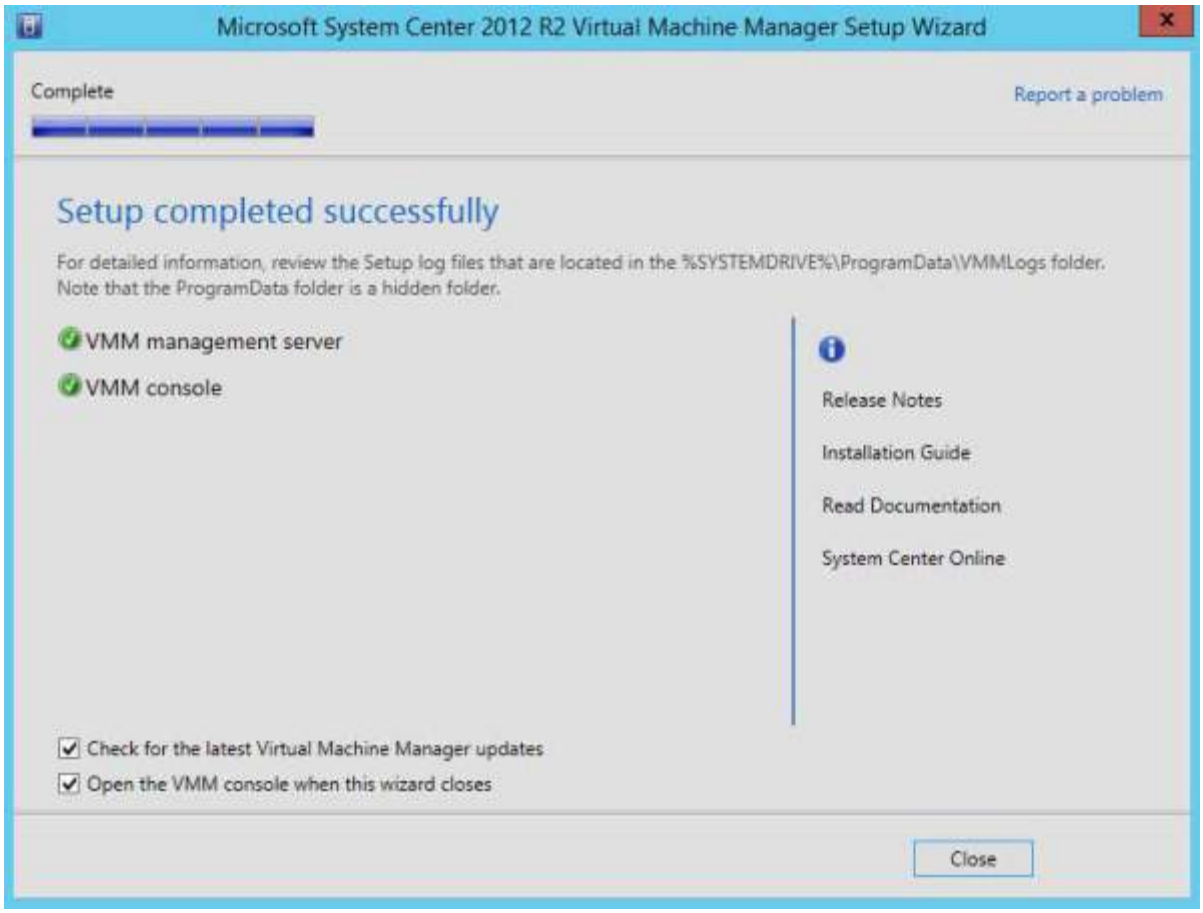
Указываем имя и место для файловой шары под библиотеку. Как вариант, библиотеку VMM можно разместить на отдельном файловом сервере.



Проверяем суммарную информацию и жмем Install, запуская процесс установки.



Несколько минут ожидания, и финальный экран с сообщением об успешном завершении установки.



System Center 2012 R2 Virtual Machine Manager установлен и можно приступать к его использованию — подключать хосты, создавать облака, развертывать сервисы и многое другое.

ПРАКТИЧЕСКАЯ РАБОТА №38.
АНТИВИРУС КАСПЕРСКОГО ДЛЯ MICROSOFT ISA SERVER. УСТАНОВКА, НАСТРОЙКА, УПРАВЛЕНИЕ

Цель: ознакомиться с процессом инсталляции, принципами работы и управления Антивирусом Касперского для Microsoft ISA Server 2000

Программное обеспечение:

- операционная система
  - Microsoft Windows 2000 Server SP 4 или выше
  - Microsoft Windows 2000 Advanced Server SP 4 или выше
- Microsoft ISA Server 2000 в режиме Integrated (должен использоваться в качестве прокси-сервера)
- Microsoft Internet Explorer версии 5.0 или выше (настроенный на работу с Microsoft ISA Server 2000)

- Антивирус Касперского для Microsoft ISA Server

На компьютере преподавателя должен быть установлен веб-сервер (например Internet Information Server) и открыта папка с общим доступом Test_virus_ISA с правами на чтение, доступ к тексту сценария, обзор, запуск сценария для всех пользователей локальной сети по протоколам HTTP и FTP.

Содержание работы:

1. Изучить процесс установки Антивируса Касперского для Microsoft ISA Server
2. Ознакомиться с назначением и функциями Антивируса Касперского для Microsoft ISA Server
3. Ознакомиться с возможностями управления Антивирусом Касперского для Microsoft ISA Server через консоль ISA Management
4. Выполнить задания к лабораторной работе

Методические указания к лабораторной работе

Антивирус Касперского для Microsoft ISA Server 2000 - система антивирусного контроля над файлами, передаваемыми по протоколам HTTP и FTP через брандмауэр Microsoft Internet Security and Acceleration Server.

Антивирус Касперского для MS ISA-серверов выполняет функции фильтра, который перехватывает данные, передаваемые по протоколам HTTP и FTP, выделяет из них контролируемые объекты, анализирует их на наличие вирусов и блокирует проникновение в локальную сеть зараженных файлов и веб-документов.

Приложение обеспечивает выполнение следующих функций:

- Антивирусную проверку и обработку потоков данных, поступающих из сети Интернет
- Генерацию потока данных из вылеченных файлов для передачи клиенту, запросившему поток
- Обновление антивирусных баз через Интернет, как автоматическое согласно заданному расписанию, так и в ручном режиме
- Сбор статистической информации о работе приложения и просмотр статистики через стандартные механизмы операционной системы Windows
- Управление лицензионными ключами

Антивирус Касперского поддерживает следующие протоколы передачи данных:

- HTTP 1.0 и 1.1 (RFC 2616)
- FTP (RFC 959, 2389, Extensions to FTP)

- FTP over HTTP

Состав приложения

В состав приложения входят следующие компоненты:

- **Фильтры потоков** - интегрируются в MS ISA-сервер как плагины
- **Антивирусное ядро** - устанавливается в систему как служба
- **Средства администрирования** - представляют собой встраиваемую оснастку. Управление Антивирусом Касперского для Microsoft ISA Server осуществляется через интерфейс, встроенный в ISA Management

Поддерживаемые операционные системы

Антивирус Касперского функционирует совместно с продуктом Microsoft Internet Security and Acceleration Server 2000 с установленным Service Pack 2 или выше на следующих платформах:

- Microsoft Windows 2000 Server с установленным Service Pack 4 или выше
- Microsoft Windows 2000 Advanced Server с установленным Service Pack 4 или выше

Установка

В процессе установки приложения автоматически определяется режим работы ISA-сервера. В руководстве к ISA-серверам описаны три возможных режима работы:

- Firewall
- Proxy
- Integrated

В консоли MS ISA-сервера предусмотрен ряд стандартных фильтров, которые позволяют контролировать входящие потоки данных. Для протоколов HTTP это HTTP Redirector Filter. Протоколы FTP контролируются через FTP Access Filter (не используется в режиме Proxy). Антивирус Касперского для MS ISA-серверов использует настройки по умолчанию указанных фильтров, чтобы получать исходный поток данных для его последующей проверки.

Перед тем как устанавливать Антивирус Касперского для ISA-серверов, убедитесь, что стандартные фильтры HTTP Redirector Filter и FTP Access Filter не отключены или не перенаправляют потоки данных, минуя антивирусную фильтрацию. Это может привести к отключению антивирусной защиты сервера. Управление фильтрами потоков осуществляется через стандартное окно управления ISA Management.

Процедура установки Антивируса Касперского для Microsoft ISA Server на ISA-сервер выполняется стандартно, как для большинства приложений Windows. Можно выбрать как полную, так и выборочную установку продукта, а также восстановить некорректную установку Антивируса Касперского для Microsoft ISA Server.

Программа установки устанавливает Антивирус Касперского для Microsoft ISA Server в соответствии с текущим режимом работы ISA-сервера. Сразу же после установки приложение готово к запуску процесса проверки потоков данных, поскольку необходимые общие параметры уже заданы.

Средство управления - оснастка управления Антивирус Касперского для Microsoft ISA Server встраивается в ISA Management в секцию **Extensions**.

- FTP-фильтр Антивируса Касперского
- Web-фильтр Антивируса Касперского
- HTTP-фильтр Антивируса Касперского

Добавление тех или иных фильтров зависит от режима ISA - сервера.

В установленном приложении автоматически создается пользователь **default**, группа пользователей **default** и политика **default**, так как наличие хотя бы одной группы пользователей и одной антивирусной политики, назначаемой этой группе, является необходимым условием для функционирования Антивируса Касперского.

Результат установки

Основные файлы Антивируса Касперского для Microsoft ISA Server помещаются в каталог, заданный при установке, по умолчанию - в папку Program Files\Kaspersky Lab\ Kaspersky Anti-Virus for ISA Server на системном диске. В этом каталоге также расположены служебные папки:

- Bases - каталог хранилища антивирусных баз
- Logs - каталог хранения журналов событий
- StoreDir
- TaskQueue - каталог хранения очереди объектов для проверки
- Temp - каталог для временных файлов

Принципы работы

Антивирус Касперского для Microsoft ISA Server производит антивирусную проверку трафика HTTP проходящего через ISA-сервер. Оптимизацию антивирусной проверки HTTP-трафика можно осуществить путем изменения следующих настроек:

- Максимальное время проверки первого пакета данных в секундах
- Максимальный интервал между отправками данных клиенту в секундах
- Количество данных в процентах, не отправляемых клиенту до завершения проверки
- Разрешить дозагрузку файлов

Антивирус Касперского для Microsoft ISA Server производит антивирусную проверку трафика FTP проходящего через ISA сервер. Оптимизацию антивирусной проверки FTP можно проводить с помощью изменения настройки **Количество данных, полученных сервером до того, как первый пакет с данными отправляется клиенту**.

Также существует возможность общей настройки антивирусной проверки путем включения или выключения следующих параметров:

- Лечить объекты, если возможно
- Проверять архивы
- Проверять упакованные и исполняемые файлы

Управление группами клиентов

В каждую группу включены клиенты внутренней сети, к которым могут быть применены одинаковые политики. Каждый клиент может входить в одну или несколько групп.

К клиентам группы **default** автоматически относятся все клиенты ISA-сервера, не внесенные ни в какую другую группу.

Если клиент входит одновременно в несколько групп, то для него производится антивирусная проверка в соответствии с группой, обладающей наименее строгими условиями проверки.

Внедрение политик антивирусной проверки

Для каждой группы клиентов может быть задана своя политика. В политиках определяются дополнительные параметры фильтрации входящего потока данных, которые позволяют задавать различные правила для разных групп клиентов и, тем самым, могут ускорить процесс антивирусной проверки.

Каждой группе может соответствовать только одна политика. Например, если группе **Администраторы** назначена политика **Администраторы**, то ей не могут соответствовать другие политики.

Настройка диагностики работы приложения

Антивирус Касперского для ISA Server позволяет проводить полную диагностику своей работы для любого из MS ISA-серверов, на которых он установлен, и фиксировать ее результаты в следующих файлах журналов:

- Kavisa<ДАТА>.log - журнал Антивируса Касперского для Microsoft ISA Server, содержащий информацию о работе приложения в заданном объеме на определенную дату. В качестве <ДАТА> в названии файла приводится дата его создания в формате ГодМесяцЧисло. В случае если в момент дополнения журнала он будет открыт администратором на редактирование, Антивирус Касперского сформирует новый файл с дополнительным постфиксом к его имени.
- Viruslog<ДАТА>.log - журнал Антивируса Касперского для ISA Server, включающий информацию об обнаруженных вредоносных объектах.

Для любой из классификаций сообщений можно выбрать уровень детализации:

- **Не выводить** - не записывать в журналы никакой информации
- **Минимальный** - фиксировать в журналах только основные события (например, запуск и остановка приложения и т. д.)
- **Средний** - записывать помимо основных событий ряд дополнительных, характеризующих работу Антивируса более детально (например, сообщение об ошибке соединения с сервером обновлений)
- **Максимальный** - выводить в журналы максимально полную информацию о работе приложения, за исключением отладочных сообщений
- **Отладочный** - записывать в журналы всю информацию, в том числе и отладочную

По умолчанию для всех сообщений установлен минимальный уровень детализации.

Обновление антивирусных баз

Обновление антивирусных баз может выполняться автоматически с заданным периодом обновления или вручную администратором. Возможны два способа получения антивирусных баз:

- через Интернет по FTP- или HTTP-протоколу с серверов обновлений Лаборатории Касперского
- из локального или сетевого каталога

Управление обновлением антивирусных баз осуществляется на закладке **Обновление** диалогового окна **Свойства Антивируса Касперского для MS ISA-сервера**.

Настройка уведомлений пользователей

Если приложение обнаруживает в потоке данных инфицированный файл, который невозможно вылечить, соединение разрывается, и пользователь, запросивший эти данные, получает HTML-страницу с сообщением об обнаружении вируса.

Сообщения формируются только в том случае, если вредоносный объект был обнаружен Web-фильтром Антивируса Касперского или HTTP-фильтром Антивируса Касперского

Можно отредактировать сообщения, направляемые пользователю, на закладке **HTTP** диалогового окна **Свойства Антивируса Касперского для ISA-сервера**. Максимальная длина сообщения 10240 байт. Кодовая страница win1251.

Сбор и просмотр статистической информации

Просмотр и управление сбором статистической информации о работе Антивируса Касперского осуществляется через стандартные счетчики производительности Windows, доступные через консоль **Производительность (Пуск, Настройка, Панель управления, Администрирование, Системный монитор)**

Оценка работы приложения проводится по следующим параметрам:

- всего вылеченных объектов
- всего зараженных (невылеченных) объектов
- всего испорченных объектов
- всего непроверенных объектов
- всего ошибок проверки
- всего подозрительных объектов
- всего прерванных проверок
- всего проверено объектов
- всего чистых объектов
- длина очереди задания
- объем обработанного Антивирусом Касперского трафика в килобайтах
- число обычных, прямых и сложных загрузок данных каждым из фильтров Антивируса Касперского (FTP- , HTTP- и Web-фильтр).

Чтобы выбрать, какие сведения будут отражаться в статистике, необходимо добавить соответствующие счетчики для объекта **HTTP**

Уведомление администратора посредством ISA Server Alerts

Встроенные средства ISA Server Alerts позволяют различными способами (запись в системный журнал, уведомление почтовым сообщением и т.д.)

информировать администратора о критических событиях, возникающих при работе какого-либо из установленных на ISA-сервере приложений. Для Антивируса Касперского для ISA-сервера также предусмотрен ряд важных событий, возникновение которых требует немедленной реакции администратора системы, например, событие **До истечения срока действия лицензии осталось 14 дней**. Набор таких событий пополняет существующий список событий ISA-сервера сразу после установки приложения на сервер. Способ доставки уведомления для каждого из событий можно настроить самостоятельно.

Управление лицензионными ключами

Управление лицензионными ключами осуществляется на закладке **Лицензирование** диалогового окна **Свойства Антивируса Касперского для ISA Server**. Лицензионный ключ необходим для полнофункциональной работы Антивируса Касперского для ISA Server. Если лицензионный ключ отсутствует или не соответствует данному приложению, Антивирус Касперского для ISA Server не будет работать. По истечении срока действия лицензии, Антивирус Касперского для ISA Server сохраняет свою функциональность за исключением возможности обновления антивирусных баз. Потоки данных по-прежнему подвергаются антивирусной фильтрации.

Задание

1. Запустите Internet Explorer, проверьте доступность содержимого папки Test_virus_ISA по протоколам HTTP, FTP. Адрес веб-сервера и путь к папке Test_virus_ISA уточните у преподавателя.
2. Откройте консоль ISA Management, секцию **Monitoring**, директорию **Session** и убедитесь, что веб-сессии проходят через ISA-сервер. Также убедитесь. что Internet Explorer настроен на работу через ISA-сервер.
3. Установите локально Антивирус Касперского для ISA Server на Ваш ISA-сервер. Место расположения дистрибутива и ключевого файла уточните у преподавателя. Перезагрузите компьютер.
4. Убедитесь, что установка Антивируса Касперского для ISA Server прошла успешно, в ISA Management в секции **Extensions** добавилась оснастка **Антивирус Касперского**. Запишите в протокол лабораторной работы, какие службы добавились, и какие процессы и фильтры запускаются при старте Антивируса Касперского для ISA Server.
5. Ознакомьтесь с настройками Антивируса Касперского для ISA Server. Запишите в протокол лабораторной работы, какое количество экземпляров антивирусного ядра запускается одновременно по умолчанию, какие параметры антивирусной проверки можно задавать в Антивирусе Касперского для ISA Server
6. Настройте сбор статистики по работе Антивируса Касперского для ISA Server через стандартные счетчики Windows. Создайте и запустите счетчик

Всего зараженных объектов. Перечислите в протоколе лабораторной работы все доступные счетчики, связанные с Антивирусом Касперского для ISA Server.

7. Настройте получение уведомлений администратором средствами ISA Alert с параметрами по умолчанию для событий Антивируса Касперского для ISA Server. Запишите в протокол лабораторной работы доступные уведомления для Антивируса Касперского для ISA Server.
8. Настройте параметры обновления антивирусных баз Антивируса Касперского для ISA Server на получение обновлений из указанного преподавателем источника. Произведите обновление антивирусных баз. Перечислите в протоколе лабораторной работы, какие данные можно задавать для получения обновления антивирусных баз.
9. Запустите Internet Explorer, попытайтесь скачать файлы, содержащиеся в папке Test_virus_ISA и во вложенных в нее папках по протоколу HTTP. Проанализируйте файл журнала обнаруженных вредоносных объектов. Перечислите в протоколе лабораторной работы, какие файлы были вылечены.
10. Запустите Internet Explorer, попытайтесь скачать файлы, содержащиеся в папке Test_virus_ISA и во вложенных в нее папках по протоколу FTP. Проанализируйте файл журнала обнаруженных вредоносных объектов. Перечислите в протоколе лабораторной работы, какие файлы были пропущены.
11. Отключите Web-фильтр Антивируса Касперского и перезапустите службы ISA-сервер. Запустите Internet Explorer, попытайтесь скачать файлы, содержащиеся в папке Test_virus_ISA и во вложенных в нее папках по протоколам FTP и HTTP.
12. Добавьте в группу **default** нового клиента - свой компьютер. Отредактируйте политику **default** таким образом, чтобы исключить машину на которой расположен веб-сервер из проверки Антивируса Касперского для ISA Server. Скопируйте все файлы из ресурса Test_virus_ISA по протоколу HTTP. Сохраните файл журнала, распечатайте его и предоставьте файл журнала при сдаче лабораторной работы. Перечислите в протоколе лабораторной работы, какие объекты и по каким признакам можно исключать из антивирусной проверки.
13. Вручную перезапустите службу **Антивирус Касперского для Microsoft ISA Server**. Опишите в протоколе лабораторной работы, что произойдет при этом с Антивирусом Касперского для Microsoft ISA Server.

Контрольные вопросы

1. Какие фильтры будут установлены Антивирусом Касперского для Microsoft ISA Server при установке последнего на Microsoft ISA Server, работающий в режиме Proxy?
2. Каким образом буду проверяться архивы при отключенном механизме распаковки архивов в Антивирусе Касперского для Microsoft ISA Server?

3. По протоколу HTTP идет загрузка архива, содержащего инфицированный объект, поддающийся лечению и чистый файл. Что произойдет с таким архивом?
4. В каком случае не формируется уведомление пользователю при обнаружении вредоносного объекта?

ПРАКТИЧЕСКАЯ РАБОТА №39-40.
АНТИВИРУС КАСПЕРСКОГО 5.5 ДЛЯ MS EXCHANGE SERVER. УСТАНОВКА, НАСТРОЙКА, УПРАВЛЕНИЕ

Цель работы: **ознакомиться с процессом инсталляции, принципами работы и управления Антивирусом Касперского 5.5 для MS Exchange Server.**

Программное обеспечение:

- операционная система
  - Microsoft Windows 2000 Server (первый компьютер - почтовый сервер)
  - Microsoft Windows 2000 Professional Service Pack 2 и выше; Microsoft Internet Explorer версии 5.0 и выше (второй компьютер - рабочая станция)
  - Microsoft Windows XP Professional (второй компьютер - рабочая станция)
- MTA
  - Microsoft Exchange Server 2000 Service Pack 2 (первый компьютер - почтовый сервер)
- почтовый клиент
  - Outlook Express 5.0 или выше
  - Microsoft Outlook 2000 или выше
- Антивирус Касперского 5.5 для MS Exchange Server

На первом компьютере (почтовом сервере) необходимо создать папку с общим доступом KAV и учетные записи USER и USERADMIN.

Почтовый клиент на первом компьютере (почтовом сервере) должен быть настроен на обработку почты пользователя USERADMIN, на втором компьютере (рабочей станции) - пользователя USER, в обоих случаях будет использован протокол IMAP.

Содержание работы:

1. Изучить процесс установки Антивируса Касперского 5.5 для MS Exchange Server
2. Ознакомиться с назначением и функциями Антивируса Касперского 5.5 для MS Exchange Server

3. Ознакомиться с возможностями управления Антивирусом Касперского 5.5 для MS Exchange Server
4. Ознакомиться с возможностями управления Антивирусом Касперского 5.5 для MS Exchange Server через Консоль администрирования
5. Выполнить задания к лабораторной работе
6. Защитить лабораторную работу, ответив на контрольные вопросы

Методические указания к лабораторной работе

Антивирус Касперского для MS Exchange Server предназначен для антивирусной защиты почтовых ящиков и общих папок на Microsoft Exchange Server, а также для антивирусной проверки проходящего почтового трафика.

Исходя из назначения Антивирус Касперского для MS Exchange Server выполняет следующие основные функции:

- Постоянную проверку входящих и исходящих сообщений, их атрибутов и вложений
- Проверку по требованию хранилищ и общих папок (в фоновом режиме)
- Обнаружение и обезвреживание вредоносного кода в проверяемых объектах
- Обновление антивирусных баз и модулей приложения (автоматическое и по требованию)
- Уведомление отправителя, получателя и администратора о сообщении, содержащем вредоносный объект
- Регистрацию событий и запись информации о них в отчеты
- Фиксирование возникновения эпидемий (увеличение количества инфицированных сообщений в общем потоке проверяемых сообщений за определенный промежуток времени) и уведомление о них
- Управление лицензионными ключами (установка, удаление, проверка, автоматическая замена)

Состав и принцип работы

Антивирус Касперского для MS Exchange Server состоит из следующих компонентов:

- **Сервер безопасности** - обеспечивает антивирусную функциональность и обновление антивирусных баз, удаленное управление, настройки, а также выполняет функции хранения информации
- **Консоль управления** - модуль управления, выполнен в виде компонента расширения к Microsoft Management Console (MMC), обеспечивающего доступ к административным сервисам приложения Антивирус Касперского для MS Exchange Server, позволяет осуществлять удаленную настройку и управление серверной частью Антивируса

Архитектура Сервера безопасности

Сервер безопасности Антивируса Касперского для MS Exchange Server, состоит из следующих основных подсистем:

- **Перехватчик почтовых сообщений** - осуществляет перехват объектов, поступающих на Microsoft Exchange Server, и направляет их в подсистему антивирусной проверки. Компонент встраивается в процессы Microsoft Exchange Server по технологии VSAPI 2.0 и 2.5.
- **Подсистема антивирусной проверки** - осуществляет антивирусную проверку объектов. Компонент представляет собой несколько процессов, в каждом из которых находится по одному антивирусному ядру. Он также включает в себя хранилище временных объектов для проверки в оперативной памяти.
- **Модуль внутреннего управления продуктом и контроля целостности** - запускается отдельным процессом и является службой Microsoft Windows. Данная служба запускается автоматически и не зависит от состояния Microsoft Exchange Server (запущен, остановлен), что позволяет управлять Сервером безопасности, даже если Microsoft Exchange Server остановлен.

Поддерживаемые операционные системы

Антивирус Касперского для MS Exchange Server может быть интегрирован в следующие версии Microsoft Exchange Server:

- Microsoft Exchange 2000 Server Enterprise Edition с установленным Service Pack 2 или выше
- Microsoft Exchange 2000 Server Standard Edition с установленным Service Pack 2 или выше
- Microsoft Exchange Server 2003 Enterprise Edition или выше
- Microsoft Exchange Server 2003 Standard Edition или выше

Консоль управления Антивируса Касперского для Microsoft Exchange Server может быть установлена на следующие операционные системы:

- Microsoft Windows 2000 с установленным Service Pack 4 или выше
- Microsoft Windows XP
- Microsoft Windows Server 2003

Установка

Процесс инсталляции Антивируса Касперского для MS Exchange Server аналогичен процессу инсталляции продуктов Лаборатории Касперского для Microsoft Windows. Сразу после запуска дистрибутива запускается мастер установки приложения, с помощью которого производится пошаговая установка Антивируса Касперского для MS Exchange Server. В процессе установки пользователю предлагается: ознакомиться и согласиться с условиями лицензионного соглашения, осуществить выбор типа установки: полная или выборочная, а также установить лицензионный ключ к данному приложению. В случае выбора полной установки (по умолчанию) происходит установка

Сервера безопасности и Консоли управления. Выборочная установка используется в случаях, когда необходимо установить только средство управления - Консоль управления.

Завешается работа мастера установки Антивируса Касперского для MS Exchange Server предложением включить антивирусную защиту сервера автоматически сразу после завершения установки, либо сделать это позже вручную - через Консоль управления Антивирусом. По умолчанию в качестве защищаемых хранилищ будут выбраны все сформированные на сервере хранилища. Если в установленном лицензионном ключе указано максимальное количество защищаемых почтовых ящиков меньшее, чем сформировано в хранилищах сервера, перед запуском антивирусной защиты необходимо снять защиту с части хранилищ.

Результаты установки

Основные файлы Антивируса Касперского для Microsoft Exchange Server помещаются в каталог, заданный при установке, по умолчанию - Program Files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server на системном диске, в этом каталоге также расположены служебные папки:

- BackUp - каталог хранения резервных копий антивирусных баз
- Bases - каталог хранилища антивирусных баз
- Logs - каталог хранения журналов событий Антивируса Касперского for MS Exchange Server
- QB - каталог резервного хранилища
- Reports - каталог хранилища отчетов
- Store - служебный каталог, в котором сохраняются файлы, размер которых больше 1 Мб, для дальнейшей антивирусной проверки
- Tmp - каталог хранилища временных файлов

Принципы работы

Производительность антивирусной защиты

Антивирус Касперского для MS Exchange Server предоставляет возможность регулировать производительность работы приложения в зависимости от объема и характера проходящего через Exchange-сервер почтового трафика и системных характеристик компьютера: объема оперативной памяти, быстродействия, количества процессоров. Настройка параметров производительности может осуществляться как в автоматическом режиме, так и вручную

Фоновая проверка

Антивирус Касперского для MS Exchange Server осуществляет проверку хранящейся на сервере почты и содержимого общих папок. Проверяются все общие папки и защищаемые хранилища (mailbox storages). При этом

обрабатываются сообщения, которые не были проверены с использованием текущей версии антивирусных баз. Программа проверяет тело сообщения и присоединенные к нему файлы в соответствии с общими параметрами антивирусной проверки. Если фоновая проверка хранилищ отключена, хранящиеся на сервере сообщения проверяются только при запросе их пользователем непосредственно перед доставкой.

Уровни защиты

В Антивирусе Касперского для Microsoft Exchange Server предусмотрены следующие уровни защиты:

- **Стандартная антивирусная защита** - защита от всех известных вредоносных программ. Данный уровень установлен по умолчанию.
- **Расширенная антивирусная защита** - защита от всех известных вредоносных программ и потенциально опасных программ
- **Избыточная антивирусная защита** - защита от всех известных вредоносных программ, потенциально опасных программ и хакерских утилит

Настройка диагностики работы приложения

Антивирус Касперского для MS Exchange Server позволяет проводить полную диагностику своей работы и регистрировать зафиксированные события в журнале приложений операционной системы Windows и в собственных журналах. Журналы событий Антивируса Касперского для MS Exchange Server ведутся в двух форматах и в зависимости от формата имеют следующую структуру имен:

- Kavscmesrv<ДАТА>.log - основной журнал событий приложения. В качестве <ДАТА> в названии файла приводится дата его создания в формате ГГГГММДД.

  Если в момент заполнения журнала он недоступен для записи, например, открыт администратором на редактирование, Антивирус Касперского сформирует новый файл с дополнительным постфиксом к его имени.

- kavscmesrv.raw<ДАТА>.log и store.raw<ДАТА>.log - журналы, содержащие информацию в неотформатированном виде. Событие регистрируется в raw-журнале, если по каким-либо причинам его не удалось записать в основной журнал.

  Объем и полнота информации, выводимой в журналы, зависит от установленных в параметрах приложения уровней диагностики для каждого из модулей программы. Если модуль состоит из нескольких компонентов, уровень диагностики устанавливается для каждого компонента отдельно.

Предусмотрены следующие уровни диагностики:

- **Не выводить** - не записывать в журналы никакой информации.
- **Минимальный** - фиксировать в журналах только основные события.
- **Средний** - записывать помимо основных событий ряд дополнительных, характеризующих работу Антивируса более детально.
- **Максимальный** - выводить в журналы максимально полную информацию о работе модуля, за исключением отладочных сообщений.
- **Отладочный** - записывать в журналы всю информацию, в том числе и отладочную

Обновления антивирусных баз. Источники обновлений

Источником обновлений могут выступать:

- **Сервера обновлений Лаборатории Касперского** - в этом случае обновление происходит по протоколам HTTP/FTP
- **HTTP-, FTP-сервер или сетевой каталог** - источником является задаваемый сетевой ресурс, HTTP, FTP либо UNC

Загрузка обновлений происходит либо по расписанию, либо вручную. Настроить параметры доступа к сетевым HTTP/FTP ресурсам можно, нажав на гиперссылке **Антивирусные обновления** в панели результатов.

По нажатию открывается окно **Настройка**, в котором предлагается указать режим доступа к FTP ресурсам (пассивный либо активный), тайм-аут соединения (промежуток ожидания ответа на запрос к серверу), а также задать параметры настройки доступа к прокси-серверу.

Если управление работой установленных на компьютерах сети приложений Лаборатории Касперского осуществляется при помощи системы централизованного управления Kaspersky Administration Kit 5.0, то получаемые Сервером администрирования обновления антивирусных баз размещаются в папке общего доступа. В таком случае возможно использовать данную папку в качестве источника обновлений для Антивируса Касперского для MS Exchange Server.

Работа с инфицированными и подозрительными объектами

Во избежание потери важной информации, перед выполнением каких бы то ни было действий с зараженными объектами, будь то попытка лечения или удаление, они помещаются в специальное резервное хранилище, откуда при необходимости могут быть извлечены.

Уведомления

Приложение Антивирус Касперского для MS Exchange Server предоставляет возможность оповещать об обнаруженных при антивирусной проверке зараженных объектах.

Предусмотрено уведомление о событиях следующих типов:

- обнаружен зараженный объект
- обнаружен подозрительный объект
- обнаружен поврежденный объект

Для каждого типа событий формируется уведомление соответствующего типа.

Контроль вирусной активности

Антивирус Касперского для Microsoft Exchange Server позволяет фиксировать степень вирусной активности в проверяемом почтовом трафике, почтовых ящиках и общих папках Microsoft Exchange Server с помощью счетчиков вирусной активности и уведомлять об этом администратора. Вирусная активность определяется на основании данных антивирусной защиты Microsoft Exchange Server и позволяет фиксировать события следующих типов:

- Обнаружен зараженный объект
- Обнаружен подозрительный объект
- Обнаружен поврежденный объект
- Один и тот же вирус обнаружен несколько раз

При установке Сервера безопасности в объекте **Счетчики вирусных эпидемий** создается встроенный **Счетчик вирусной эпидемии**. Для реализации функции отсылки уведомлений **Счетчика вирусных эпидемий** устанавливается порог вирусной активности - максимально допустимое количество событий заданного типа (например, **Обнаружен зараженный объект**) в течение ограниченного временного интервала. Если вирусная активность превышает установленный порог, Сервер безопасности рассылает уведомление о данном событии на заданные почтовые адреса (обычно, на адрес администратора), с целью уведомления администратора о произошедшем событии.

Отчеты об антивирусной проверке

Отчет об антивирусной проверке проходящего почтового трафика, почтовых ящиков и общих папок Microsoft Exchange Server формируется автоматически, в соответствии с расписанием, или по запросу и может быть сохранен по умолчанию в каталоге Program Files\Kaspersky Lab\Kaspersky Anti-Virus for Microsoft Exchange Server\reports, а также отправлен по электронной почте.

При установке Сервера безопасности создается встроенный шаблон отчета. На основании этого шаблона - **Отчет об антивирусной проверке** - формируется отчет о результатах антивирусной проверки почтового сервера первого числа каждого месяца за прошедшие 30 дней.

Задание

1. Запустите почтовые клиенты на рабочей стации и файловом сервере. Обменяйтесь тестовыми почтовыми сообщениями, чтобы убедиться в работоспособности Microsoft Exchange Server и почтовых клиентов.
2. Установите Антивирус Касперского для MS Exchange Server на почтовый сервер. Место расположения дистрибутива и ключевого файла уточните у преподавателя.
3. Перезагрузите почтовый сервер. Откройте консоль управления Антивирусом Касперского для MS Exchange Server и подключитесь к Серверу безопасности Антивируса Касперского для MS Exchange Server, который установлен на Вашем почтовом сервере. Запишите в протокол лабораторной работы службы, процессы, папки, которые добавились после установки Антивирус Касперского для MS Exchange Server.
4. Ознакомьтесь с настройками Сервера безопасности доступными по гиперссылке **Общие параметры**. Перечислите модули системы и доступные им уровни диагностики, запишите название защищаемого хранилища почтовых ящиков и название защищаемого хранилища общих папок.
5. Ознакомьтесь с настройками Сервера безопасности доступными по гиперссылке **Антивирусная защита**. Запишите в протокол лабораторной работы, какие действия возможны с зараженными объектами, подозрительными объектами, защищенными / поврежденными объектами, также укажите, какие действия выполняются по умолчанию над этими объектами.
6. Ознакомьтесь с настройками Севера безопасности доступными по гиперссылке **Антивирусные обновления**. Запишите в протокол лабораторной работы, какие данные о антивирусных базах можно узнать по этой гиперссылке.
7. Настройте параметры обновления антивирусных баз Антивируса Касперского для MS Exchange Server на получение обновлений из указанного преподавателем источника. Произведите обновление антивирусных баз. Запишите в протокол лабораторной работы, какие данные на закладке **Параметры соединения** можно задавать для получения обновлений антивирусных баз.
8. Настройте и активируйте получение уведомлений **О зараженном объекте** таким образом, чтобы почтовое уведомление приходило получателю и отправителю, а сообщение NET SEND приходило на рабочую станцию. Убедитесь, в правильности настроек с помощью отправки тестового сообщения. Запишите в протокол лабораторной работы содержание тестового сообщения NET SEND, которое пришло на рабочую станцию.
9. Аналогично настройте уведомления **О поврежденном объекте** и **О подозрительном объекте**.

10. Изучите возможности создания отчетов Севера безопасности с помощью объекта **Шаблоны отчетов**. Запишите в протокол лабораторной работы параметры формирования отчетов.
11. Настройте и активируйте получение **Отчета о вирусной активности** таким образом, чтобы отчет высылался пользователю **USER** за 10 минут до конца пары. Сохраните полученный отчет и предоставьте файл отчета во время сдачи лабораторной работы.
12. Изучите настройки объекта **Счетчики вирусных эпидемий**. Измените настройки существующего счетчика вирусной эпидемий таким образом, чтобы он срабатывал при следующих условиях: один вирус обнаружен 5 раз за одну минуту. Активируйте счетчик. Запишите в протокол лабораторной работы, на какие типы событий могут создаваться **Счетчики вирусных эпидемий**.
13. Создайте на своем компьютере папку с названием test_virus. Скопируйте в нее содержимое папки test_virus2. Место расположения папки test_virus2 уточните у преподавателя.
14. Сформируйте и отправьте три письма с темами Test1, Test2, Test3 на адрес пользователя USER, в копию поставьте адрес общей папки KAV. К первому письму прикрепите все файлы из папки test_virus2 с расширением .com, ко второму письму - с расширением .zip, к третьему - с расширением .rar.
15. На рабочей станции запустите почтовый клиент и получите почту пользователя USER. Проанализируйте полученные письма Test1, Test2, Test3, их вложения и полученные уведомления. В протоколе лабораторной работы объясните, почему не были проверены файлы прикрепленные письмам Test2, Test3.
16. Измените, настройки антивирусной защиты Сервера безопасности таким образом, чтобы вложения писем Test2, Test3 были проверены. Сформируйте заново письма Test2, Test3 изменив тему писем на Test2v2, Test3v2, прикрепите необходимые файлы и отошлите на адрес пользователя USER, в копию поставьте адрес общей папки KAV. Запишите в протокол лабораторной работы изменения, которые Вы внесли в настройки **Антивирусной защиты** Сервера безопасности.
17. На рабочей стации станции запустите почтовый клиент и получите почту пользователя USER. Проанализируйте полученные письма Test2v2, Test3v2, их вложения и полученные уведомления. В протоколе лабораторной работы объясните, почему не были проверены файлы pass_eicar.rar и pass_eicar.zip, прикрепленные к письмам Test2v2, Test3v2.
18. Сформируйте письма с темами Test2v3, Test3v3 прикрепите к ним файлы pass_eicar.rar и pass_eicar.zip. Укажите в теле письма пароль к этим файлам, т. е. просто наберите в теле письма 1 и оправьте сформированные письма.
19. Получите почту пользователя USER. Проанализируйте полученные письма Test2v3, Test3v3 и их вложения, а также полученные уведомления.

20. Изучите настройки объекта **Резервное хранилище**, ознакомьтесь с его содержимым. Перечислите в протоколе лабораторной работы возможные поля, доступные при создании фильтров для этого объекта.
21. Создайте фильтр по статусу **Подозрительный** для **Резервного хранилища**. Перечислите в протоколе лабораторной работы, какие действия можно производить над файлами, помещенными в **Резервное хранилище**.
22. Создайте отчет об антивирусной проверке вручную. Сохраните полученный на почтовый ящик отчет (см. пункт 11). Ознакомьтесь с содержимым этих отчетов. Опишите в протоколе лабораторной работы, в чем разница между этими отчетами.

Контрольные вопросы

1. Какие пути доставки уведомлений существуют в Антивирус Касперского 5.5 для MS Exchange Server?
2. Почему рекомендуется не отсылать уведомления о найденном вирусе отправителю инфицированного сообщения?
3. Куда и в каком виде по умолчанию сохраняются файлы отчета?
4. Что произойдет с Антивирусом Касперского для MS Exchange Server при нарушении целостности файлов антивирусных баз?

ПРАКТИЧЕСКАЯ РАБОТА №41-42
ОСНОВНЫЕ ПРИЗНАКИ ПРИСУТСТВИЯ ВРЕДОНОСНЫХ ПРОГРАММ И МЕТОДЫ ПО УСТРАНЕНИЮ ПОСЛЕДСТВИЙ ВИРУСНЫХ ЗАРАЖЕНИЙ

Цель работы: **получить навыки обнаружения на компьютере вредоносных программ, изучить основные методы по устранению последствий вирусных инцидентов без использования антивирусного программного обеспечения**.

Основные сведения

Программное обеспечение:

- операционная система
  - Microsoft Windows XP Professional

Содержание работы:

1. Ознакомиться с определением вируса и вредоносных программ
2. Ознакомиться с типами вредоносных программ и их описанием
3. Ознакомиться с жизненными циклами различных типов вредоносных программ
4. Ознакомиться с действиями червей при заражении компьютера

5. Ознакомиться с возможностями лечения компьютеров без использования антивирусного программного обеспечения
6. Выполнить задания к лабораторной работе
7. Защитить лабораторную работу, ответив на контрольные вопросы

Методические указания к лабораторной работе

Определения компьютерного вируса - исторически проблемный вопрос, поскольку достаточно сложно дать четкое определение вируса, очертив при этом свойства, присущие только вирусам и не характерные для других программ. Наоборот, давая жесткое определение вируса как программы, обладающей определенными свойствами практически сразу же можно найти пример вируса, таковыми свойствами не обладающего.

Приведем определение вируса согласно ГОСТ Р 51198-98

Вирус - *программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам*

Еще одна проблема, связанная с определением компьютерного вируса кроется в том, что сегодня под вирусом чаще всего понимается не "традиционный" вирус, а практически любая вредоносная программа. Это приводит к путанице в терминологии, осложненной еще и тем, что сегодня практически любой антивирус способен выявлять все типы вредоносных программ, таким образом ассоциация "вредоносная программа-вирус" становится все более устойчивой.

Вредоносная программа - *компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе (КС), либо для скрытого нецелевого использования ресурсов КС, либо иного воздействия, препятствующего нормальному функционированию КС. К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви и др*.

Вирусы

К вирусам относятся:

- **Загрузочные вирусы** - вирусы, заражающие загрузочные сектора постоянных и сменных носителей
- **Файловые вирусы** - вирусы, заражающие файлы
- **Макровирусы** - вирусы, написанные на языке макрокоманд и исполняемые в среде какого-либо приложения. В подавляющем большинстве случаев речь идет о макросах в документах Microsoft Office

- **Скрипт-вирусы** - вирусы, исполняемые в среде определенной командной оболочки: раньше - bat-файлы в командной оболочке DOS, сейчас чаще VBS- и Java-скрипты в командной оболочке Windows Scripting Host (WSH)

Отдельно стоит сказать пару слов о макровирусах. Большинство электронных документов создаются и обрабатываются в формате MS Office, инструмент VBA (Visual Basic for Application), который можно использовать для создания макровирусов поставляется вместе с приложением MS Office. Такое положение дел приводит к тому, что на сегодняшний день макровирусы - наиболее часто встречающийся тип вирусов. Однако борьба с ними не вызывает особых проблем и сводится к изучению тела вредоносного макроса с помощью того же VBA на предмет выполняемых операций, контролю стартовых макросов AutoOpen, AutoClose, AutoSave, глобальных макросов FileOpen, FileSaveAs, FileSave, FileClose и ряда стандартных операций, таких как вызов API-функций, выполнения команд Shell и т. д. Процедура лечение макровирусов сводится к удалению тела макроса из документов и шаблонов MS Office.

Сетевые черви

Червь (сетевой червь) - *тип вредоносных программ, распространяющихся по сетевым каналам, способных к автономному преодолению систем защиты автоматизированных и компьютерных систем, а также к созданию и дальнейшему распространению своих копий, не всегда совпадающих с оригиналом, осуществлению иного вредоносного воздействия*

В зависимости от путей проникновения в операционную систему черви делятся на:

- **Почтовые черви** (Mail-Worm) - черви, распространяющиеся в формате сообщений электронной почты
- **IM черви** (IM-Worm) - черви, использующие Интернет-пейджеры
- **P2P черви** (P2P-Worm) - черви, распространяющееся при помощи пиринговых (peer-to-peer) файлообменных сетей
- **Сетевые черви** (Net-Worm) - прочие сетевые черви, среди которых имеет смысл дополнительно выделить Интернет-черви и LAN-черви
  - **Интернет черви** - черви, использующие для распространения протоколы Интернет. Преимущественно этот тип червей распространяется с использованием неправильной обработки некоторыми приложениями базовых пакетов стека протоколов tcp/ip
  - **LAN черви** - черви, распространяющиеся по протоколам локальных сетей

Трояны

Троян *(троянский конь) - тип вредоносных программ, основной целью которых является вредоносное воздействие по отношению к компьютерной системе. Трояны отличаются отсутствием механизма создания собственных копий*

Некоторые трояны способны к автономному преодолению систем защиты КС, с целью проникновения и заражения системы. В общем случае, троян попадает в

систему вместе с вирусом либо червем, в результате неосмотрительных действий пользователя или же активных действий злоумышленника. Наиболее распространены следующие виды троянов:

- **Клавиатурные шпионы** (Trojan-SPY) - трояны, постоянно находящиеся в памяти и сохраняющие все данные поступающие от клавиатуры с целью последующей передачи этих данных злоумышленнику. Обычно таким образом злоумышленник пытается узнать пароли или другую конфиденциальную информацию
- **Похитители паролей** (Trojan-PSW) - трояны, также предназначенные для получения паролей, но не использующие слежение за клавиатурой. Обычно в таких троянах реализованы способы извлечения паролей из файлов, в которых эти пароли хранятся различными приложениями
- **Утилиты удаленного управления** (Backdoor) - трояны, обеспечивающие полный удаленный контроль над компьютером пользователя. Существуют легальные утилиты такого же свойства, но они отличаются тем, что сообщают о своем назначении при установке или же снабжены документацией, в которой описаны их функции. Троянские утилиты удаленного управления, напротив, никак не выдают своего реального назначения, так что пользователь и не подозревает о том, что его компьютер подконтролен злоумышленнику. Наиболее популярная утилита удаленного управления - Back Orifice
- **Анонимные smtp-сервера и прокси** (Trojan-Proxy) - трояны, выполняющие функции почтовых серверов или прокси и использующиеся в первом случае для спам-рассылок, а во втором для заметания следов хакерами
- **Модификаторы настроек браузера** (Trojan-Cliker) - трояны, которые меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, для организации несанкционированных обращений к Интернет-ресурсам
- **Инсталляторы прочих вредоносных программ** (Trojan-Dropper) - трояны, представляющие возможность злоумышленнику производить скрытую установку других программ
- **Загрузчики вредоносных программ** (Trojan Downloader) - трояны, предназначенные для загрузки на компьютер-жертву новых версий вредоносных программ, или рекламных систем
- **Уведомители об успешной атаке** (Trojan-Notifier) - трояны данного типа предназначены для сообщения своему "хозяину" о зараженном компьютере
- **"Бомбы" в архивах** (ARCBomb) - трояны, представляющие собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные - зависание или существенное замедление работы компьютера, заполнение диска большим количеством "пустых" данных
- **Логические бомбы** - чаще не столько трояны, сколько троянские составляющие червей и вирусов, суть работы которых состоит в том, чтобы

при определенных условиях (дата, время суток, действия пользователя, команда извне) произвести определенное действие: например, уничтожение данных

- **Утилиты дозвона** - сравнительно новый тип троянов, представляющий собой утилиты dial-up доступа в Интернет через платные почтовые службы. Такие трояны прописываются в системе как утилиты дозвона по умолчанию и влекут за собой крупные счета за пользование Интернетом

Жизненный цикл вредоносных программ

Процесс размножения вирусов может быть условно разделен на несколько стадий:

1. Активация вируса
2. Поиск объектов для заражения
3. Подготовка вирусных копий
4. Внедрение вирусных копий

Так же как для вирусов, жизненный цикл **червей** можно разделить на определенные стадии:

1. Проникновение в систему
2. Активация
3. Поиск "жертв"
4. Подготовка копий
5. Распространение копий

У **троянов** вследствие отсутствия функций размножения и распространения, их жизненный цикл меньше чем у вирусов - всего три стадии:

1. Проникновение на компьютер
2. Активация
3. Выполнение заложенных функций

Это, само собой, не означает малого времени жизни троянов. Напротив, троян может незаметно находиться в памяти компьютера длительное время, никак не выдавая своего присутствия, до тех пор, пока не выполнит свою вредоносную функцию будет обнаружен антивирусными средствами.

Основные пути проникновения в систему и активации

Существует утверждение - любую вредоносную программу пользователь может победить самостоятельно, т. е. не прибегая к использованию антивирусных программ. Это действительно так, за успешными действия любой антивирусной программы стоит труд вирусных аналитиков, которые по сути дела вручную разбираются с алгоритмами работы новых вирусов, выделяют сигнатуры, описывают алгоритм работы вируса.

Сигнатура вируса - *в широком смысле, информация, позволяющая однозначно определить наличие данного вируса в файле или ином коде*

Примерами сигнатур являются: уникальная последовательность байт, присутствующая в данном вирусе и не встречающаяся в других программах; контрольная сумма такой последовательности

Таким образом, антивирусную программу можно рассматривать как средство автоматизации борьбы с вирусами. Следует заметить, что анализ вирусов требует от пользователя владения большим объемом специфических знаний в области программирования, работы операционных систем и т. д. Современные вредоносные программы используют сложные технологии маскировки и защиты своих копий, которые обуславливают необходимость применение специальных средств для их анализа.

Процесс подготовки вредоносной программой своих копий для распространения может существенно отличаться от простого копирования. Авторы наиболее сложных в технологическом плане вирусов стараются сделать разные копии максимально непохожими для усложнения их обнаружения антивирусными средствами. Как следствие, составление сигнатуры для такого вируса крайне затруднено.

При создании копий для маскировки могут применяться следующие технологии:

- **Шифрование** - вирус состоит из двух функциональных блоков: собственно вируса и шифратора. Каждая копия вируса состоит из шифратора, случайного ключа и вирусного блока, зашифрованного этим ключом
- **Метаморфизм** - создание различных копий вируса путем замены групп команд на эквивалентные, перестановки местами блоков кода, вставки между значащими кусками кода "мусорных" команд, которые практически ничего не делают

Сочетание этих двух технологий приводит к появлению следующих типов вирусов.

- **Шифрованный вирус** - вирус, использующий простое шифрование со случайным ключом и неизменный шифратор. Такие вирусы легко обнаруживаются по сигнатуре шифратора
- **Метаморфный вирус** - вирус, применяющий метаморфизм ко всему своему телу для создания новых копий
- **Полиморфный вирус** - вирус, использующий метаморфный шифратор для шифрования основного тела вируса со случайным ключом. При этом часть информации, используемой для получения новых копий шифратора также может быть зашифрована. Например, вирус может реализовывать несколько

алгоритмов шифрования и при создании новой копии менять не только команды шифратора, но и сам алгоритм

Рассматривая современные вирусные угрозы необходимо отметить, что более 90% процентов вирусных угроз в последнее время связаны с червями. Наиболее многочисленную группу в этом классе вредоносных программ составляют почтовые черви. Интернет-черви также являются заметным явлением, но не столько из-за количества, сколько из-за качества: эпидемии, вызванные Интернет-червями зачастую отличаются высокой скоростью распространения и большими масштабами. IRC и P2P черви встречаются достаточно редко, чаще IRC и P2P служат альтернативными каналами распространения для почтовых и Интернет-червей. Распространение через LAN также используется преимущественно как дополнительный способ распространения.

Кроме того, на этапе активации червей можно разделить на две большие группы отличающиеся как по технологиям активации, так и по срокам жизни:

- Для активации необходимо активное участие пользователя
- Для активации участие пользователя не требуется вовсе либо достаточно лишь пассивного участия

Активация сетевого червя без участия пользователя всегда означает, что червь использует бреши в безопасности программного обеспечении компьютера. Это приводит к очень быстрому распространению червя внутри корпоративной сети с большим числом станций, существенно увеличивает загрузку каналов связи и может полностью парализовать сеть. Именно этот метод активации использовали черви Lovesan и Sasser. Под пассивным участием пользователя понимается, например, просмотр писем в почтовом клиенте, при котором пользователь не открывает вложенные файлы, но его компьютер тем не менее оказывается зараженным.

Активное участие пользователя в активации червя означает, что пользователь был введен в заблуждение методами социальной инженерии. В большинстве случаев основным фактором служит форма подачи инфицированного сообщения: оно может имитировать письмо от знакомого человека (включая электронный адрес, если знакомый уже заражен), служебное сообщение от почтовой системы или же что-либо подобное, столь же часто встречающееся в потоке обычной корреспонденции.

При заражении компьютера черви обычно производят следующие действия:

- Создают исполняемый файл с расширением .exe с произвольным именем или именем очень похожим на имя системных файлов Windows. В некоторых червях могут использоваться технологии присущие вирусам, в таком случае черви инфицируют уже существующий файл приложения (например WSOCK32.DLL) или заменяют его на свой файл (например I-Worm.MTX

записывает одну из своих процедур в файл WSOCK32.DLL таким образом, что она перехватывает отсылку данных в Интернет (процедура send). В результате червь в зараженной библиотеке WSOCK32.DLL получал управление каждый раз, когда данные отправляются в Интернет).

- Кроме этого, вместе с добавлением в систему исполняемых файлов, в ряде случаев черви помещают в систему файлы библиотек, которые обычно выполняют функции Backdoor компонентов (например один из клонов червя MyDoom - I-Worm.Mydoom.aa создавал системном каталоге Windows файл tcp5424.dll, являющийся Backdoor-компонентом и регистрировал его в системном реестре: HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32 {Default} = "%SysDir%\tcp5424.dll")
- Вредоносная программа может вносить изменения в системные файлы win.ini и system.ini. Например Email-Worm.Win32.Toil при установке в заражаемой системе копирует себя в папку Windows со случайным именем и записывает в файл system.ini следующие значения:
- [boot]
  shell=Explorer.exe %имя червя%

  что обеспечивает ему автозапуск при каждой перезагрузке Windows (но только под Win9x/Me).

  Email-Worm.Win32.Atak.h в процессе инсталляции копирует себя с именем dec25.exe в системный каталог Windows и модифицирует файл win.ini для своего последующего запуска - добавляет полный путь к файлу dec25.exe в ключ run секции [windows]:

  [windows]
  run=%SystemDir%\dec25.exe)

  Следует так же отметить, что в файле system.ini кроме секции [boot] вредоносные программы могут использовать секцию [Drivers]

- Вредоносные программы могут вносить изменения в следующие ветки реестра:
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion в ключи Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce - для того чтобы система запускала созданные червем файлы
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion в ключ Run.

  Например, Email-Worm.Win32.Bagle.ax после запуска копирует себя в системный каталог Windows, после чего регистрирует в реестре скопированный файл: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "Sysformat"="%System%\sysformat.exe

- HKEY_CLASSES_ROOT\exefile\shell\open\command

  Например вирус I-Worm.Navidad. вносил следующие изменения:

  HKEY_CLASSES_ROOT\exefile\shell\open\command {Default} = %SystemDir%\wintask.exe %1 %*)

  Таким образом запуск всех exe-файлов проходил через обращение к инфицированному файлу wintask.exe. В результате, если файл wintask.exe удалялся до правки реестра, операционная система теряла возможность запускать файлы с расширением .exe.

- HKEY_CLASSES_ROOT\txtfile\shell\open\command

  Например Email-Worm.Win32.LovGate.ad изменяет ключ системного реестра HKCR\txtfile\shell\open\command {default}="Update_OB.exe %1", таким образом, чтобы при открытии текстовых файлов получать управление.

- Кроме выше перечисленных ветвей и ключей реестра вредоносные программы могут вносить изменения и в другие ветки и ключи реестра, например:

  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WOW\boot
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Drivers32
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\WinLogon
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AeDebug

Устранение последствий заражения

В связи с тем, что черви практически не используют технологии шифрования и метаморфизма для маскировки своих копий, борьба с ним вручную несколько упрощается и сводится к следующему алгоритму действий:

1. Анализ и выявление с помощью **Диспетчера задач Windows** подозрительных процессов
2. Анализ открытых портов с помощью команды Netstat
3. Выгрузка подозрительных процессов
4. Анализ реестра с помощью утилиты Regedit.exe в выше перечисленных ветках и ключах
5. Восстановление и правка ключей реестра

6. Поиск инфицированных файлов по имени на основе данных анализа процессов операционной системы и данных анализа реестра
7. Удаления или замена инфицированных файлов
8. Перегрузка системы

Контрольный анализ процессов, ключей реестра, открытых портов. Если подозрительных процессов не обнаружено, ключи реестра не изменились, значит, процедуру дезинфекции компьютера можно считать успешной, в противном случае алгоритм придется повторить.

Тем не менее, учитывая тот факт, что современные черви могут использовать технологии присущие вирусам, устанавливать backdoor-компоненты, затрудняя, тем самым, процедуру анализа и обнаружения своих файлов, для полной уверенности компьютер после дезинфекции вручную настоятельно рекомендуется осуществить проверку антивирусным средством. Следует также отметить, что бороться вручную с вредоносными программами можно только постфактум - после того, как они поразили компьютер, в то же время использование антивирусного программного обеспечения в подавляющем большинстве случаев не допустит активации вредоносной программы на компьютере.

Задание

1. Запустите **Диспетчер задач Windows** и проанализируйте список запущенных процессов, нагрузку, которую они оказывают на ЦП. Запишите в протокол лабораторной работы название подозрительных процессов. Объясните, на основании чего были сделаны такие выводы.
2. Используя **Диспетчер задач Windows** выгрузите подозрительные процессы.
3. Запустите интерфейс командной строки Windows. Ознакомьтесь с ключами команды netstat. Получите статистку текущих сетевых подключений Вашего компьютера с параметрами отображение всех подключений и ожидающих портов, отображение последовательности компонентов участвующих в создании подключения, отображение исполняемого файла, участвующего в создании каждого подключения, или слушающего порт. Сохраните статистику в файл с названием netstat.log. Запишите протокол лабораторной работы формат команды для этого действия. Проанализирует данные netstat.log. Запишите в протокол лабораторной работы подозрительные открытые порты и приложения их использующие. Объясните, на основании чего были сделаны такие выводы.
4. Запустите утилиту работы с реестром Windows. Проанализируйте содержимое перечисленных в теоретической части веток и ключей реестра.
5. При необходимости внесите изменения в параметры ключей с целью удалить подозрительные записи, созданные вредоносной программой. Запишите в протокол лабораторной работы все внесенные изменения.

6. Проанализируйте содержание файла win.ini на предмет подозрительных записей. При необходимости внесите корректировки в файл win.ini. Запишите в протокол лабораторной работы вносимые корректировки.
7. Проанализируйте файл system.ini на предмет подозрительных записей. При необходимости внесите корректировки в файл system.ini. Запишите в протокол лабораторной работы вносимые корректировки
8. Используя стандартные средства поиска, найдите файлы, которые порождали подозрительные процессы и удалите их. Запишите в протокол лабораторной работы имена этих файлов.
9. Перегрузите компьютер, выполните пункты 1-6, чтобы убедиться, что удаление вредоносной программы прошло успешно, в оперативной памяти нет подозрительных процессов, ключи реестра не изменились, на компьютере отсутствуют подозрительно открытые порты.

Контрольные вопросы

1. Объясните в чем разница между шифрованным и полиморфным вирусом?
2. Достаточно ли для защиты от заражения вредоносной программой установить файлам разрешения только для чтения? Обоснуйте ответ.
3. Объясните в чем отличие понятий вирус и вредоносная программа.