Федеральное агентство по образованию

Нижегородский Государственный Технический Университет

Кафедра: «Вычислительные системы и технологии»

Программное обеспечение

вычислительных сетей

**Лабораторная работа №3**

**Конфигурирование и использование сетевых служб**

**ОС Windows Server 2003**

Выполнил:

Студент группы 14-В-2

Носов А.В.

Проверил:

Кочешков А. А.

Нижний Новгород

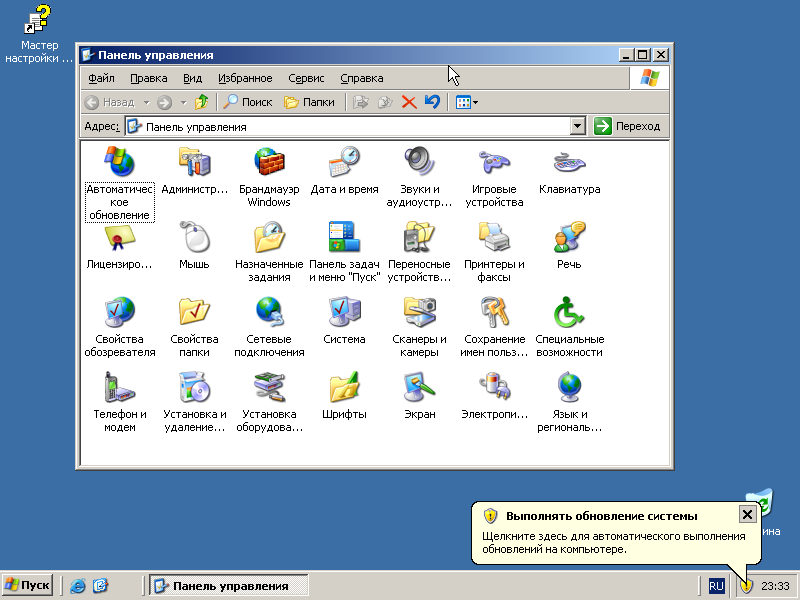
2017

**Цель:** Изучить состав и основные свойства сетевых служб ОС Windows Server, ознакомится со встроенными средствами управления, получить базовые навыки администрирования сетевой среды.

**I. Рассмотреть средства настройки системы средствами управляющей панели. Ознакомится с компонентами группы «Администрирование»**

***Задача:*** Рассмотреть средства настройки системы средствами управляющей панели.

***Выполнение:*** Панель управления ОС Windows Server содержит «стандартные» для настольных версий операционных систем апплеты панели управления. С помощью них возможно настроить сетевую подсистему ОС, графическую, звуковую и другие подсистемы. Помимо основных элементов панели, так же присутствуют специализированные апплеты.



*Рисунок 1. Вид панели управления в ОС Windows Server 2003*

Апплеты панели управления отличающиеся от набора апплетов для рабочих станций:

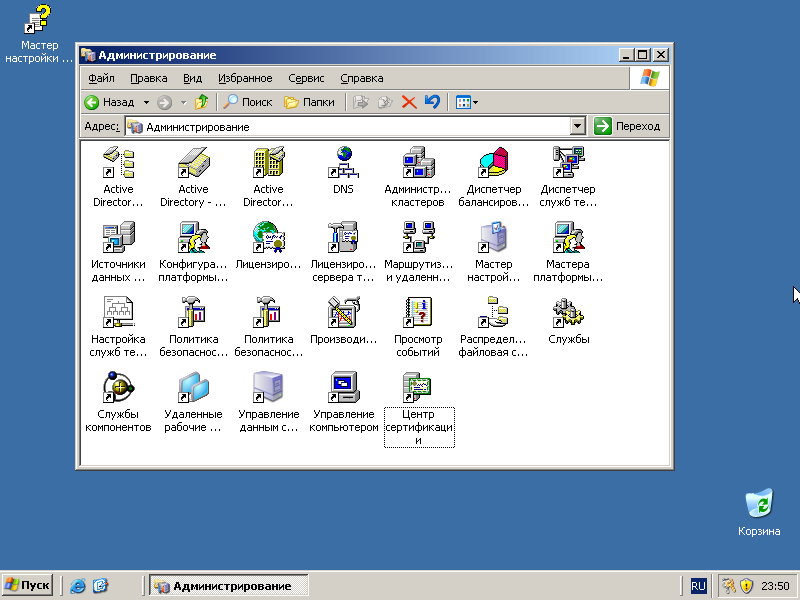
***Лицензирование.*** Используя этот апплет возможно изменить тип лицензирования (один раз), а так же удалить или добавить лицензию.

***Сохранение имён пользователей и паролей.*** Служба Single Sign-on автоматически определяет открытие вебсайта или приложения, защищённого паролем. Если пользователь ранее сохранил своё имя пользователя, пароль или другие учётные данные для этого вебсайта или программы в службе Single Sign-on, она автоматически выполнит вход в систему.

Microsoft Internet Explorer (32-разрядная версия) — единственный веб-браузер, поддерживаемый службой Single Sign-on.

**Ознакомится с компонентами группы «Администрирование»**

Раздел панели управления «Администрирование» содержит набор оснасток для управления сервером. Состав компонентов в разделе панели управления «Администрирование» зависит от сконфигурированных ролей сервера в сети.



*Рисунок 2. Вид раздела панели управления «Администрирование»*

Для сервера с установленными ролями контроллера домена ActiveDirectory и DNS-сервера в разделе «Администрирование» содержатся следующие компоненты:

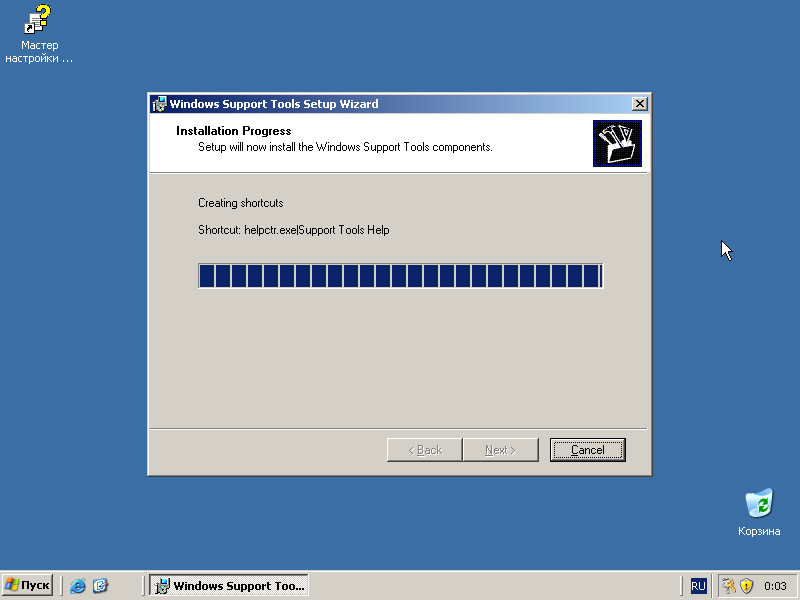
* Active Directory — домены и доверие (оснастка консоли ММС, которая используется для администрирования доверий домена, режимов работы домена и леса и суффиксов имён участников-пользователей).
* Active Directory — пользователи и компьютеры (оснастка консоли MMС, которая управляет пользователями, компьютерами и группами безопасности ActiveDirectory).
* Active Directory — сайты и службы (оснастка консоли MMC, которую можно использовать для администрирования репликации данных каталога).
* DNS — оснастка консоли ММС, которая управляет службой доменных имён
* Мастер настройки сервера - предоставляет центральный ресурс, из которого можно устанавливать или удалять роли сервера, доступные на сервере под управлением Windows Server 2003. Управлять ролью сервера после установки можно при помощи программы «Управление данным сервером».
* Политика безопасности контроллера домена (создание и управление политиками безопасности для объектов в домене).
* Управление данным сервером – обзор ролей и средства управления данным сервером
* и др.

***Выводы:*** По сравнению с настольными версиями операционных систем семейства Windows, серверные ОС обладают более расширенным функционалом. Дополнительные элементы панели управления появляются в разделе панели управления «Администрирование» после добавления той или иной роли серверу.

**II. Выполнить установку инструментального пакета администратора. Ознакомится с составом программ диагностики, с помощью утилит msinfo32, netdiag, browstat выполнить сбор данных и диагностику сети.**

***Задача:*** Выполнить установку инструментального пакета администратора.

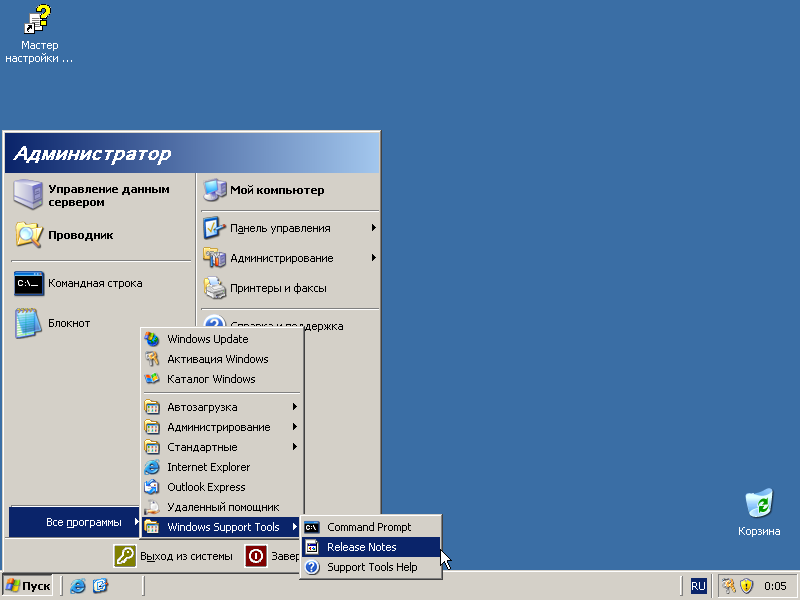
***Выполнение:*** Инструментальный пакет администратора представляет набор программ, устанавливаемых опционально на сервер. Пакет имеет название «Windows Support Tools». Дистрибутив содержащий все утилиты пакета администратора, располагается на установочном образе, в каталоге «*SUPPORT\TOOLS*» и имеет имя файла «*SUPTOOLS.msi»*.



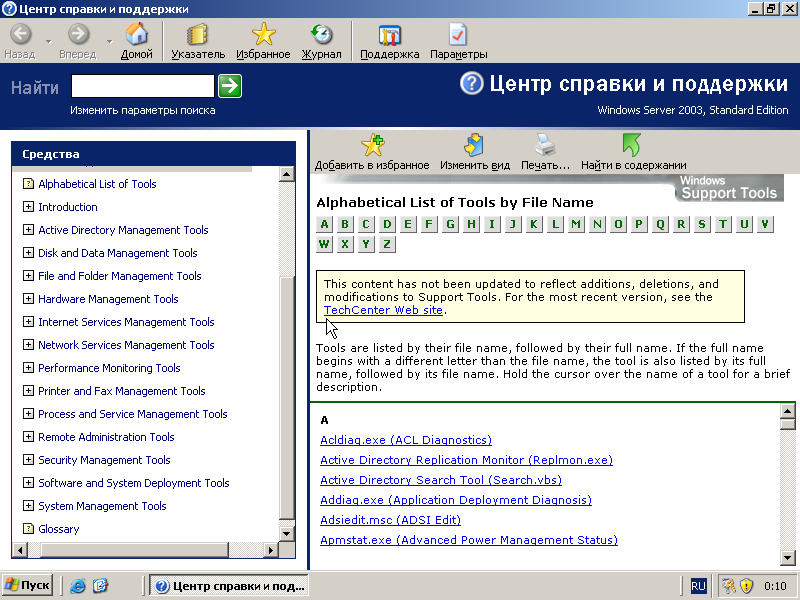
*Рисунок 3. Установка инструментального пакета администратора*

Данный пакет содержит в себе утилиты, которые облегчают поиск неисправностей в сетях и доменах на базе Windows Server 2003.

После установки пакета, в меню пуск в разделе программ появляется новое вложение «Windows Support Tools». Список утилит в данном пакете и справку по ним возможно найти в файле справки устанавливаемым вместе с утилитами. В данной справке, все команды разделены по категориям, в зависимости от их функциональности.



*Рисунок 4. Пункт «Windows Support Tools» в меню Пуск*



*Рисунок 5. Разделы справки по командам инструментального пакета*

Состав инструментального пакета приведён в таблице ниже.

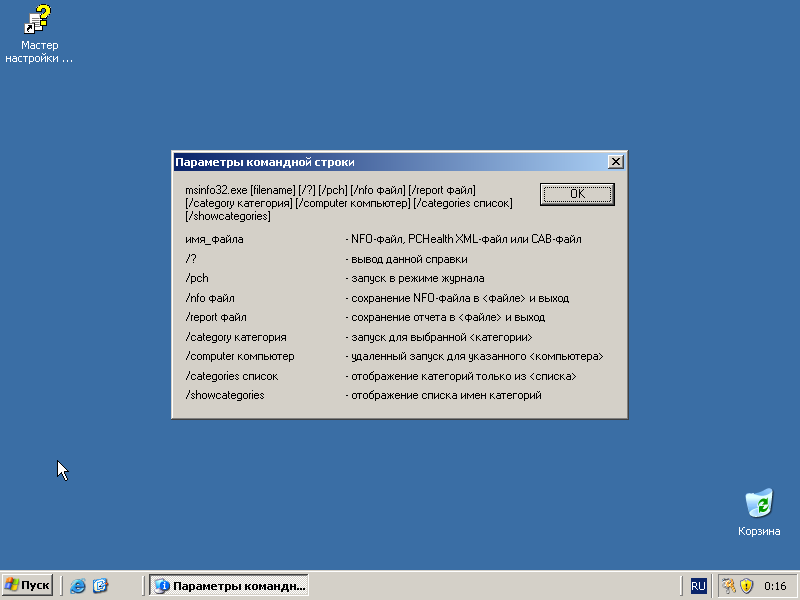
|  |  |
| --- | --- |
| **Задача** | **Инструменты** |
| Просмотр и редактирование объектов AD | ADSIEdit.msc, Ldp.exe, DsMod.exe, DsMove.exe, DsRm.exe, AdsVw.exe, ModifyUsers.vbs |
| Запросы к Active Directory | DsQuery.exe, DsGet.exe, Ldp.exe, Search.vbs, UserAccount.vbs, EnumProp.exe |
| Миграция и реструктуризация; работа с объектами AD | ADMT, MoveTree.exe, NetDom.exe, ClonePrincipal, DsAdd.exe, AddUsers.exe, GrpCpy.exe |
| Экспорт/импорт, пакетные операции | CSVDE.exe, LDIFDE.exe, AddUsers.exe, CreateUsers.vbs |
| Диагностика и обслуживание базы данных AD | NTDSutil.exe |
| Диагностика сети | NetDiag.exe, NSIookup.exe, DCdiag.exe, NLtest.exe, DNSCmd.exe, RPCPing |
| Репликация каталога AD | RepAdmin.exe, ReplMon.exe, DsaStat.exe, NTFRSutl.exe |
| Безопасность AD | ACLDiag.exe, DsACLs.exe, SDCheck.exe, KerbTray.exe, KList.exe |
| Безопасность системных объектов (файлов, общих ресурсов, реестра и т. д.) | SIDWalker, SublnACL.exe, ADMT |
| Групповые политики | GPOTool.exe, GPResult.exe, Group Policy Management Console (GPMC) |

***Задача:*** С помощью утилит msinfo32, netdiag, browstat выполнить сбор данных и диагностику сети.

***Выполнение:*** *msinfo32* – приложение позволяющее получить детальную информацию о системе в графическом режиме с выводом в файл. Позволяет так же получать информацию с удалённого компьютера.

*рис.3*

Из командной строки данную утилиту можно вызвать, только задав абсолютный путь. Из строки «Выполнить» команду можно вызвать, введя «msinfo32 /?», тогда будет выведено окно с параметрами, которые можно использовать с данной утилитой.



*Рисунок 6. Ключи запуска команды msinfo32*

Файл системной информации компьютера (*.nfo* файл экспорта системной информации) содержит следующие данные:

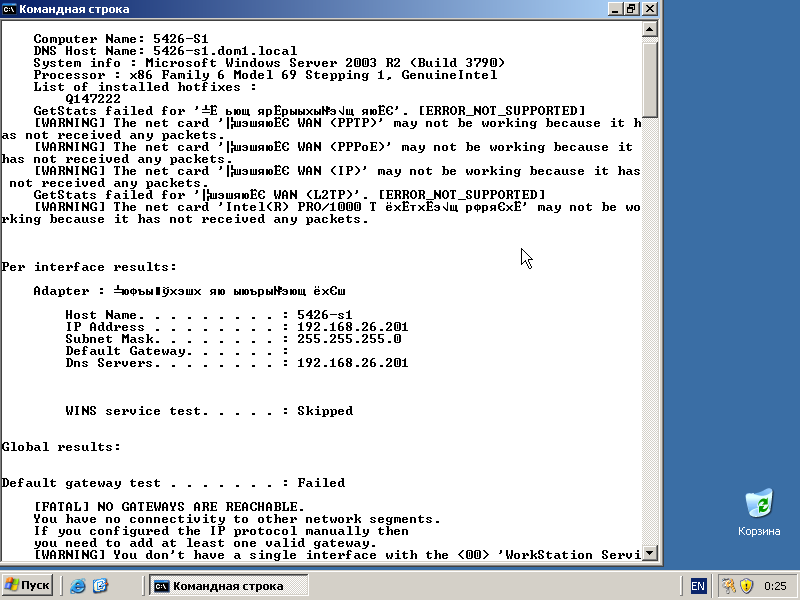
* Версия операционной системы, пакета обновлений и установленных исправлений
* Аппаратное обеспечение системы, включая объем оперативной памяти и тип центрального процессора

*рис.4*

* Версия BIOS системы
* Список конфликтов аппаратного обеспечения
* Список установленных устройств
* Список установленного программного обеспечения
* Драйверы системы (подписанные и неподписанные)
* Конфигурацию системных служб
* Информацию о конфигурации Internet Explorer

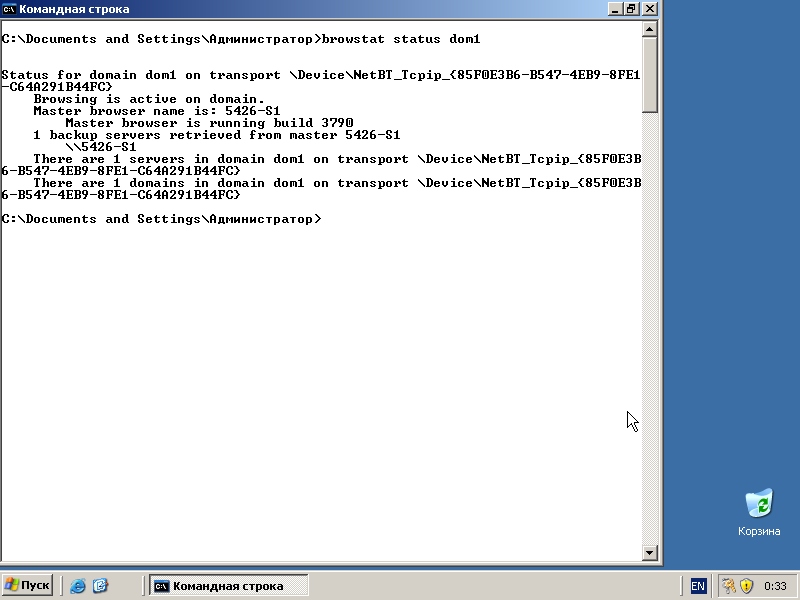
*Netdiag* – утилита для проверки работы сети. Результаты таких проверок и сведения о состоянии сети, могут использоваться для выявления проблем в сети и сетевых подключениях в компьютере или сервере.

С помощью данной утилиты есть возможность просмотреть информацию о работе сети. В целях эксперимента я с помощью данный команды выведу сокращённый вывод об ошибках



*Рисунок 7. Пример выполнения команды «netdiag /q»*

В состав инструментального пакета администратора входит утилита «browstat», позволяющая получить информацию о состоянии службы обозревателя сетевых ресурсов. Для получения информации об основных обозревателях домена необходимо использовать следующую команду: «*browstat status <домен>*» Так же возможно получить информацию относительно одного сервера указав его имя вместо домена.



*Рисунок 8. Пример выполнения команды «browstat status dom1»*

***Выводы:*** Инструментальный пакет администратора содержит множество утилит для конфигурации сервера. По каждой команде в пакете судзествует детальная справка разбитая по разделам. Одна из команд в пакете - команда «*browstat*», позволяющая узнать информацию о состоянии службы обозревателя сетевых ресурсов.

**III. Выбрать распределение сетевых сервисов DNS, WINS, DHCP по серверам. Установить соответствующую службу на выбранных серверах.**

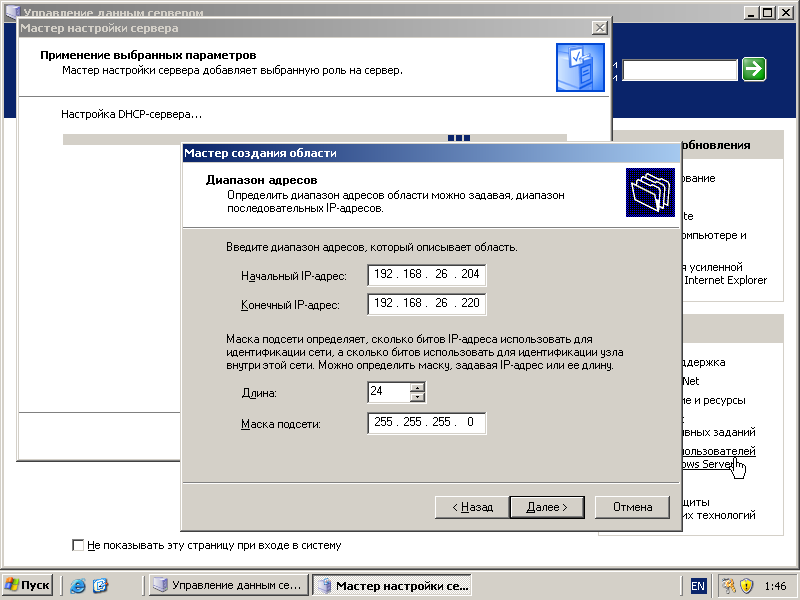
***Задача:*** Выбрать распределение сетевых сервисов DNS, WINS, DHCP по серверам.

***Выполнение:*** Для работы были созданы 4 виртуальных машины. На первой машине выбраны роли контроллера домена ActiveDirectory и DNS сервера. На второй машине выбрана роль DHCP-сервера, на третьей WINS сервера. На последней машине не установлено ролей.

|  |  |  |
| --- | --- | --- |
| **Роли** | **IPv4 адреса** | **Имена компьютеров** |
| Контроллер домена + DNS сервер | 192.168.26.201 | 5426-S1 |
| DHCP сервер | 192.168.26.202 | 5426-S2 |
| WINS сервер | 192.168.26.203 | 5426-S3 |
| Без роли (клиент) | 192.168.26.204 | 5426-S4 |

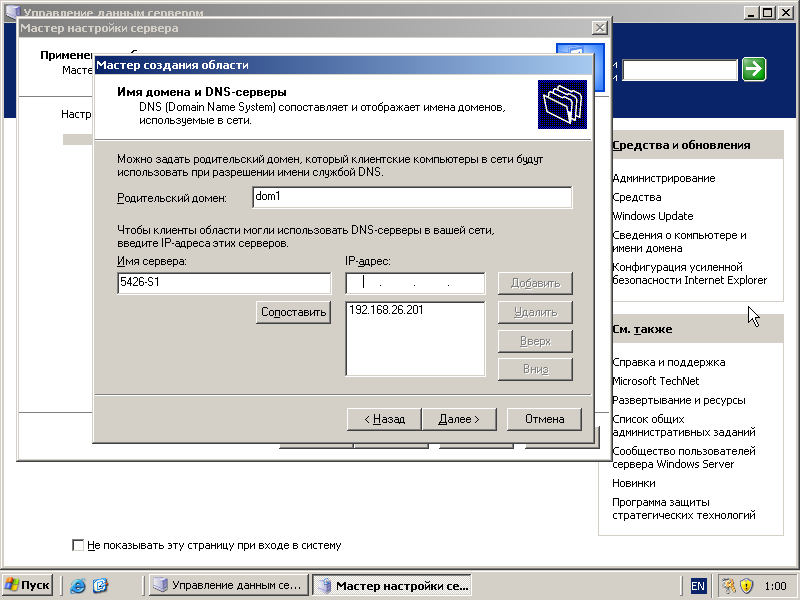
Роли контроллера домена и DNS сервера на первой машине были установлены во время выполнения лабораторной работы #2.

Установка роли DHCP сервер, производится с помощью мастера настройки сервера и производится автоматически. В процессе работы мастера настройки сервера открывается мастер создания области, которому необходимо сообщить параметры устанавливаемого сервера. Так, на первой странице необходимо указать имя и описание новой области. На следующей странице мастера ввести диапазоны адресов, которые описывают область. В моем случае пул адресов DHCP сервера будет состоять из адресов 192.168.26.204-192.168.26.220.



*Рисунок 10. Настройка диапазона адресов новой зоны DHCP*

На следующем шаге, описываются адреса которые необходимо исключить из диапазона адресов DHCP. Так как нет необходимости исключать адреса, оставляю поля пустыми. На следующей странице мастера необходимо выбрать срок действия адреса, выданного DHCP. Оставляю параметры по умолчанию. Далее, необходимо совершить переход по пункту настройки дополнительных параметров DHCP зоны, в результате чего, мастер запросит имя шлюза, которое будет сообщаться клиентам. Так как сеть изолированная, оставляю поле пустым. На следующем экране возможно задание домена и назначение адреса DNS серверу.



*Рисунок 10. Настройка адреса DNS сервера*

В данном окне мастера, есть смысл использовать разрешение по имени сервера, что позволит убедится в правильности IP адреса сервера DNS. На следующем экране указываются параметры для WINS сервера, но так как установка DHCP сервера производилась до установки WINS сервера и, поэтому сервер WINS ещё не был сконфигурирован, оставляю это поле пустым. После задания настроек WINS сервера, мастер преложит активировать область, после чего мастер завершит свою работу, а роль DHCP сервера станет активной для текущего сервера.

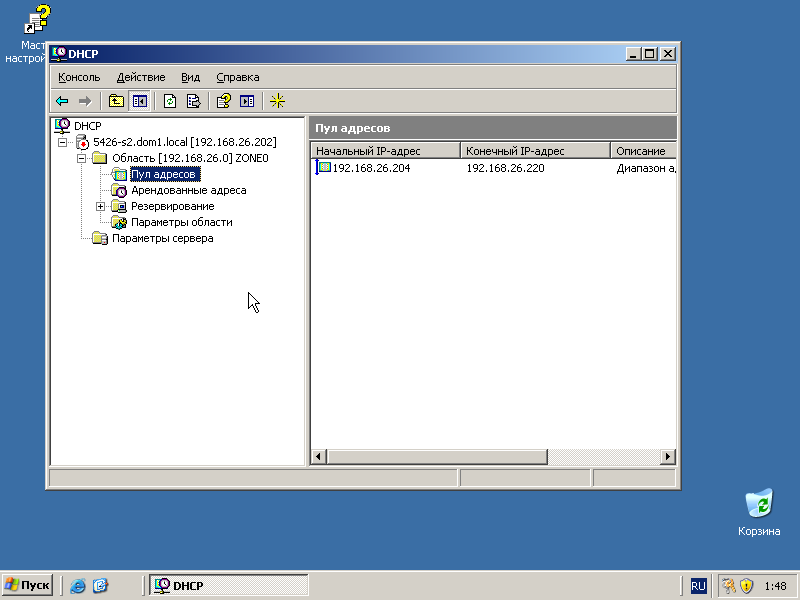
Установка роли WINS сервера, так же как и DHCP, производится с помощью мастера настройки сервера. Мастер произвёл копирование файлов. Для установки потребовался установочный диск Windows Server 2003R2. Мастер установки WINS сервера не нуждается в дополнительных параметрах от администратора, поэтому установка производится автоматически.

Сервер без роли в сети, выполняющий роль клиента, был сконфигурирован в лабораторной работе #2, и поэтому не нуждается в настройке.

**IV. Конфигурирование и использование DHCP. На DHCP сервере использовать консоль администратора DHCP. Выполнить начальное конфигурирование, описать области адресов, авторизовать сервер в ActiveDirectory. На клиентах сконфигурировать свойства протокола TCP/IP для доступа к DHCP серверу. С помощью команды ipconfig получить отчёт о настройке TCP/IP. Выполнить освобождение и обновление IP адреса. Проверить регистрацию на сервере.**

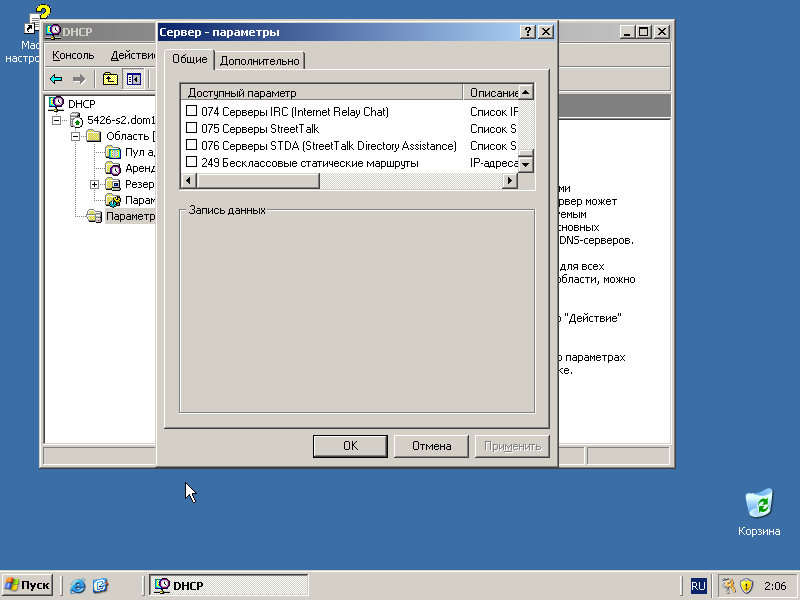
***Задача:*** Конфигурирование и использование DHCP. На DHCP сервере использовать консоль администратора DHCP. Выполнить начальное конфигурирование, описать области адресов, авторизовать сервер в ActiveDirectory.

***Выполнение:*** После установки DHCP сервера, в разделе панели управления «Администрирование» появился новый компонент «DHCP». Для того что бы просмотреть области DHCP сервера, необходимо развернуть узел «Область» в оснастке консоли управления «DHCP».



*Рисунок 11. Оснастка консоли управления DHCP сервера при просмотре пула адресов зоны*

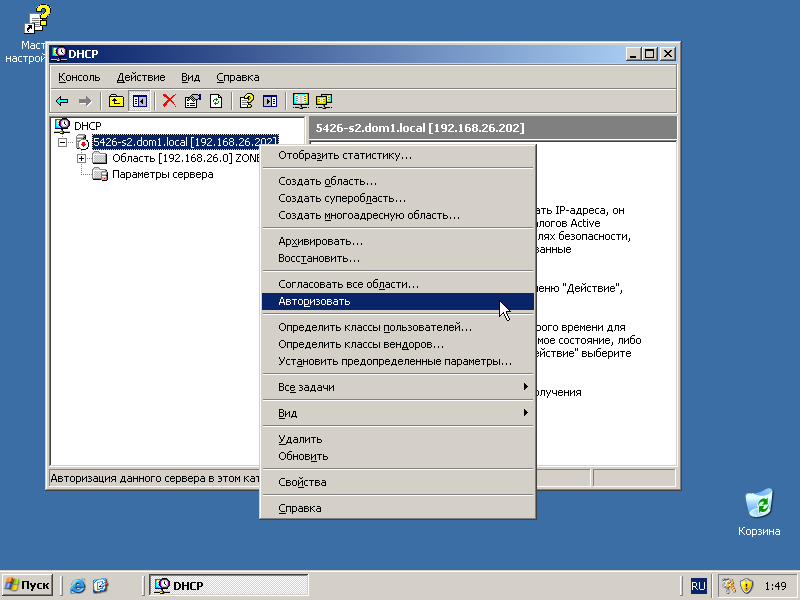
Так как в процессе установки DHCP сервера был запущен мастер создания области, в результате чего начальная область создана, начальная конфигурация DHCP сервера уже выполнена. Для DCHP сервера возможна более тонкая настройка путём редактирования дополнительных параметров в окне «Сервер - параметры». В данном окне присутствуют более чем 50 параметров для конфигурирования.



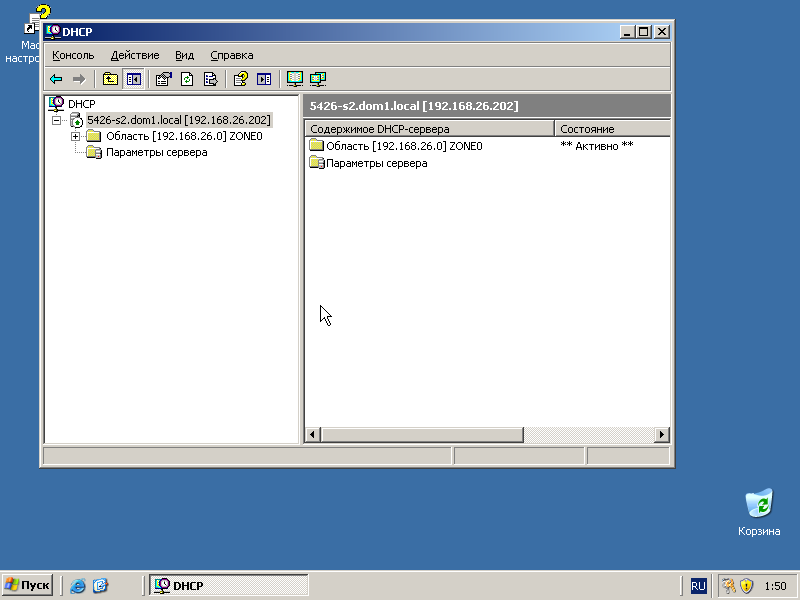
*Рисунок 12. Окно дополнительных параметров DHCP сервера*

До того как сервер DHCP начнёт функционировать его необходимо авторизировать в базе ActiveDirectory. Делается это в целях безопасности, для того что бы в сети работали только авторизованные DHCP сервера.

Для авторизации DHCP сервера необходимо выполнить правый клик по разделу сервера, после чего выполнить пункт контекстного меню «Авторизировать». При успешной авторизации значок рядом с иконкой сервера поменяется с красной стрелки вниз на зелёную стрелку вверх.



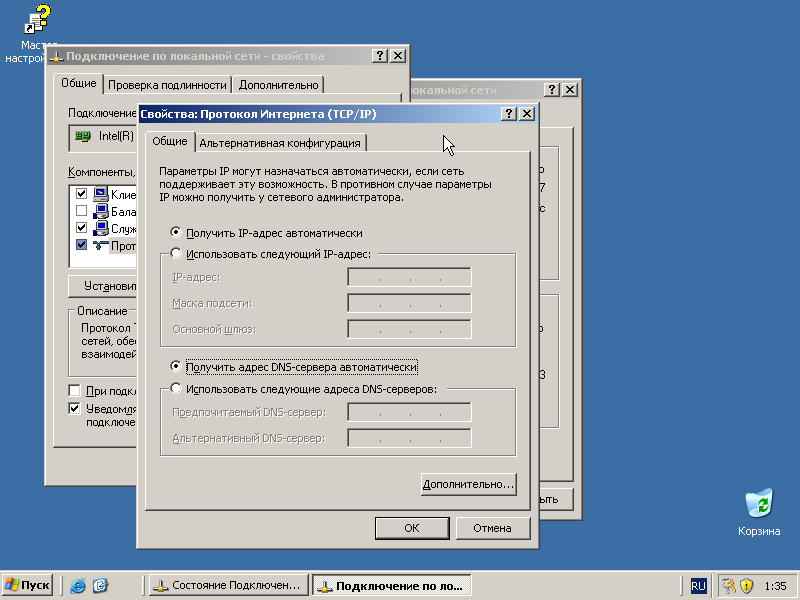
*Рисунок 13. Авторизация DHCP сервера*



*Рисунок 14. Авторизированный DHCP сервер*

***Задача:*** На клиентах сконфигурировать свойства протокола TCP/IP для доступа к DHCP серверу.

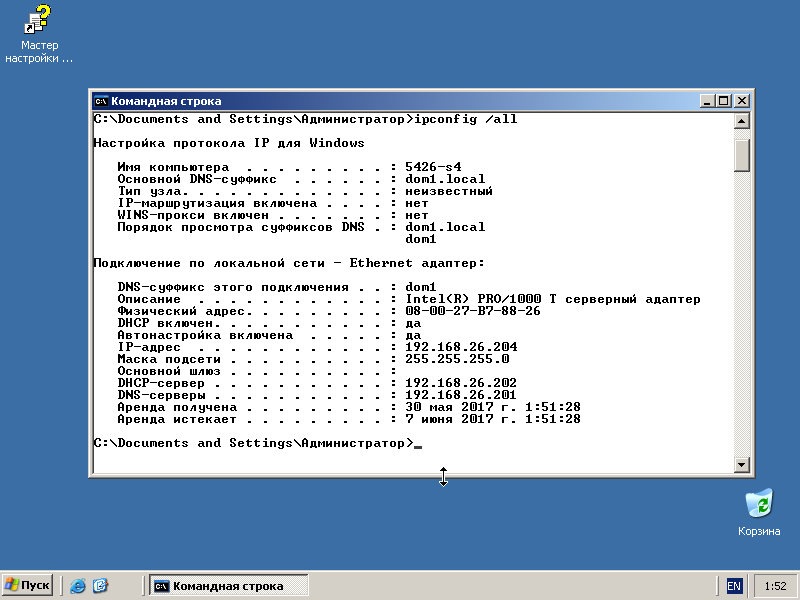
Для того что бы компьютеры-клиенты в сети могли использовать DCHP сервер в сети, их необходимо правильно сконфигурировать, путем выставления опции автоматического получения параметров TCP/IP протокола в активное состояние. В окне изменения параметров стека протоколов TCP/IP был выбран пункт «Получить IP адрес автоматически», а так же пункт «Получить адрес DNS сервера автоматически».

****

*Рисунок 15. Конфигурирование клиентов для использования DHCP сервера*

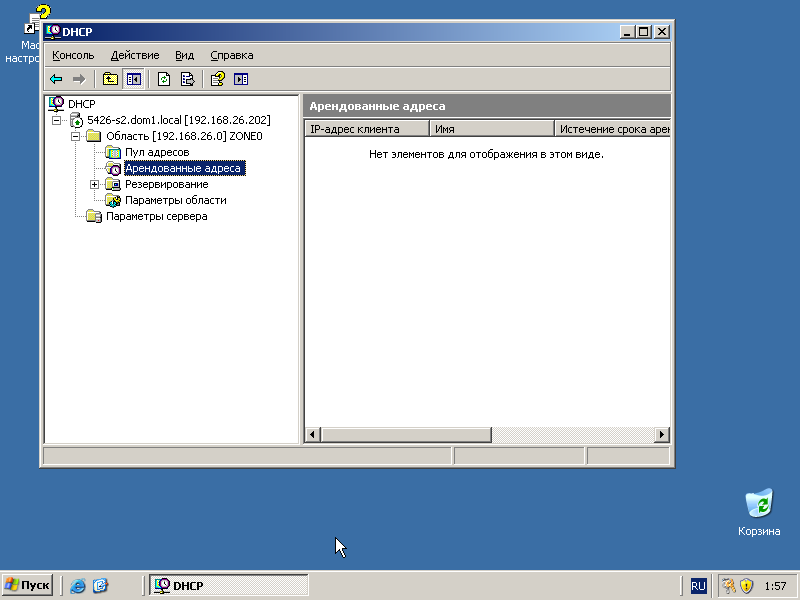
***Задача:*** С помощью команды *ipconfig* получить отчёт о настройке TCP/IP. Выполнить освобождение и обновление IP адреса. Проверить регистрацию на сервере.

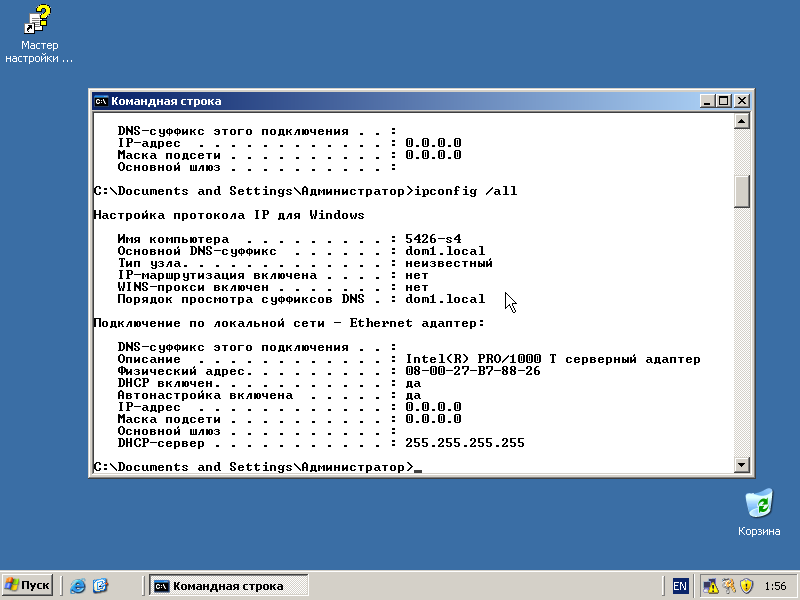
***Выполнение:*** Для проверки правильности настройки параметров DHCP сервером возможно использовать команду «*ipconfig /all*» которая отобразит список подключений данного компьютера. В результате её выполнения было выявлено, что IP адрес, адрес DNS сервера были получены с помощью сервера DCHP в сети. Так же в выводе команды *ipconfig* указаны срок аренды адреса.



*Рисунок 16. Проверка получения клиентом IP адреска с DHCP клиента*

Для освобождения IP адреса используется команда «*ipconfig /release*». После её выполнения состояние адаптеров возможно просмотреть командой «*ipconfig /all*». Так же арендованные адреса возможно просмотреть в оснастке управления сервером DHCP.

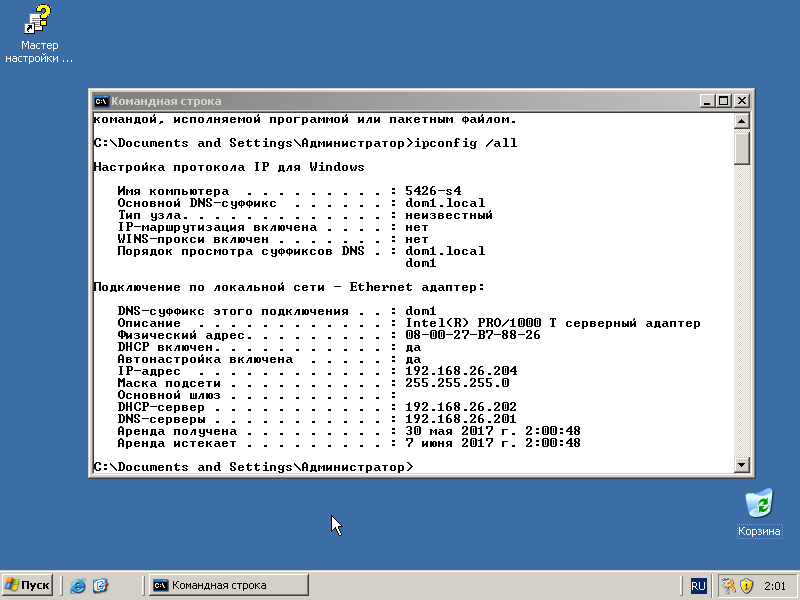


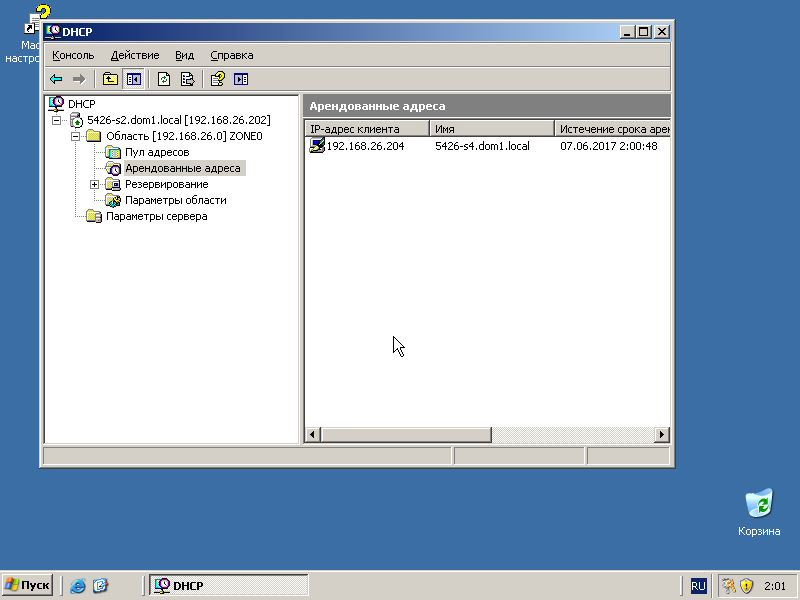


*Рисунок 17. Проверка освобождения IP адреса клиентом*

В результате выполнения команды IP адрес сетевого интерфейса стал равным «*0.0.0.0*», что говорит о несконфигурированном интерфейсе. В оснастке управления сервером DHCP в разделе «Арендованные адреса» так же отсутствуют записи.

Для получения нового IP адреса необходимо выполнить команду «*ipconfig /renew*». Просмотреть результаты выполнения команды можно с помощью вызова утилиты «*ipconfig»* с ключом «/*all*».





*Рисунок 18. Проверка обновления IP адреса клиента с DHCP сервера*

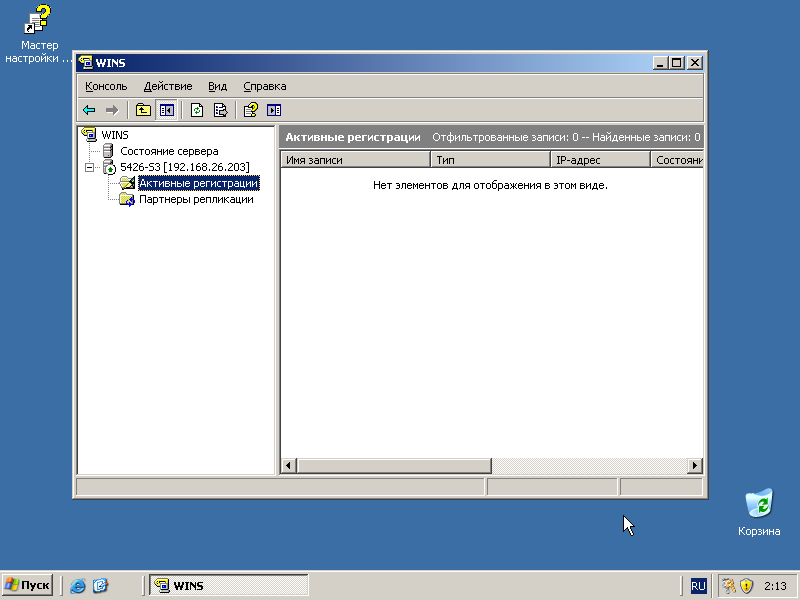
В результате выполнения обновления адреса на сетевом интерфейсе, был получен новый IP адрес, адрес DNS сервера с DHCP сервера, что было зафиксировано путём выполнения команды «*ipconfig /all*» на клиенте и в оснастке управления DHCP сервера на сервере.

***Выводы:*** Настройка DHCP сервера заключается в правильной настройки его зоны. Для DHCP сервера так же существует множество дополнительных параметров зоны, настроить которые возможно в окне настроек сервера DHCP. Клиенты конфигурируются на получение адреса от DHCP сервера с помощью установки опции «Получить IP адрес автоматически». Команда *ipconfig* позволяет отобразить состояние сетевого интерфейса, высвободить адрес, или запросить его заново с DHCP сервера.

**V. Конфигурирование и использование WINS. На WINS сервере использовать консоль администратора WINS. На клиентах сконфигурировать свойства протокола TCP/IP для доступа к WINS серверу. Проверить регистрацию на сервере. Используя команду nbtstat, получить информацию о работе NetBIOS по разрешению имён.**

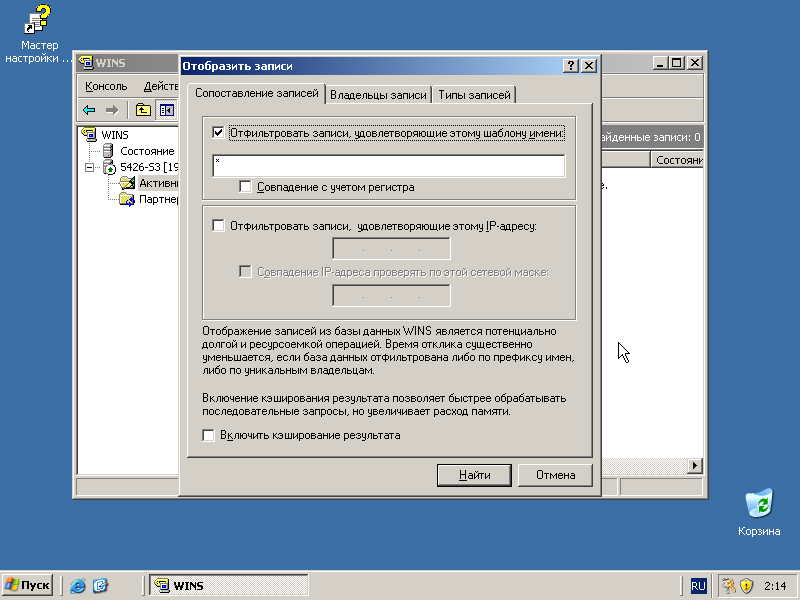
***Задача:*** Конфигурирование и использование WINS. На WINS сервере использовать консоль администратора WINS.

***Выполнение:*** После установки WINS сервера в панели управления в разделе «Администрирование» появился новый пункт «WINS». Этот компонент представляет собой оснастку консоли для управления WINS сервером.



*Рисунок 19. Консоль управления сервером WINS*

Для того что бы отобразить текущий список регистраций необходимо выполнить действие «Отобразить записи...», при выполнение которого откроется окно фильтра. Для того что бы отобразить все записи необходимо применить фильтр по имени с шаблоном «\*» т.е все имена.

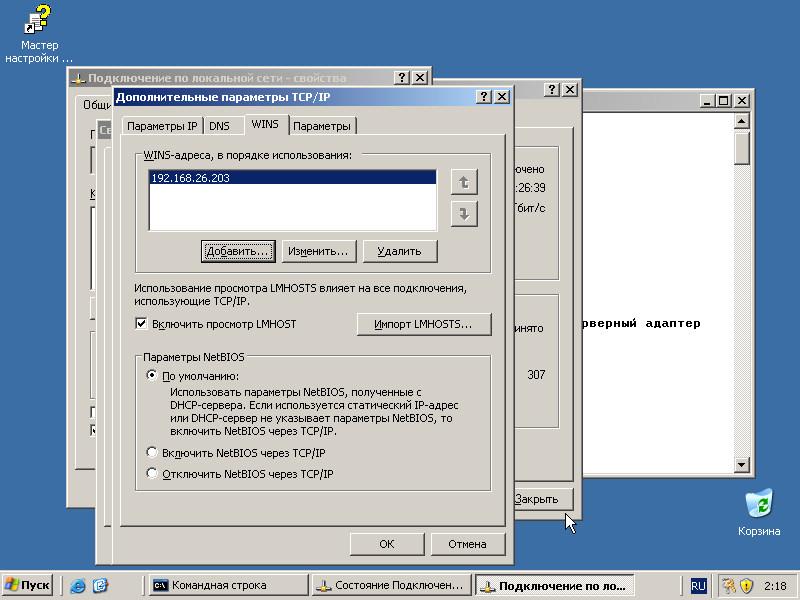


*Рисунок 20. Окно фильтрации записей регистрации WINS*

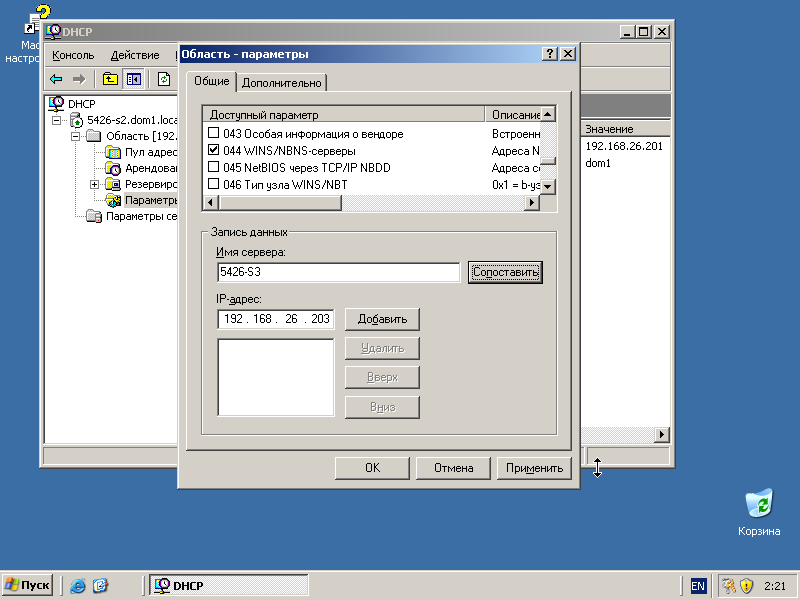
***Задача:*** На клиентах сконфигурировать свойства протокола TCP/IP для доступа к WINS серверу. Проверить регистрацию на сервере.

На компьютерах клиентах настройки WINS находится в дополнительных параметрах стека протоколов TCP/IP на вкладке WINS.

Для того что бы не выполнять настройку WINS сервера на всех клиентах сети возможно настройки автоматическую выдачу адреса WINS сервера DHCP сервером. Для этого необходимо настроить параметры зоны в консоли управления сервером DHCP. После настройки зоны DHCP сервера нужно обновить адреса на клиентах командой «*ipconfig /renew*» после чего адрес WINS сервера на клиентских машинах сконфигурируется автоматически.

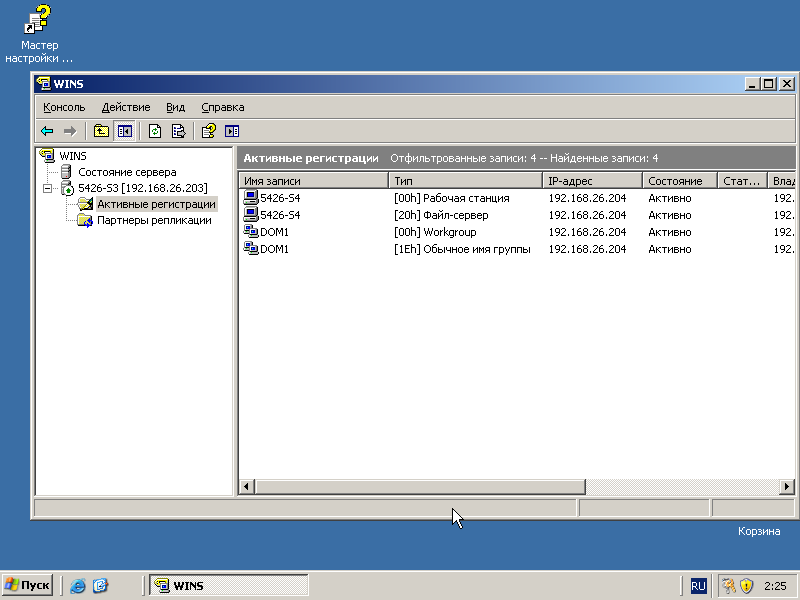


*Рисунок 21. Окно настройки клиентов на использование WINS сервера*



*Рисунок 22. Окно настройки дополнительных параметров WINS*

Каждая регистрация компьютера на сервере WINS может быть просмотрена с помощью консоли управления WINS. Для примера, выведу список компьютеров зарегистрированных на сервере WINS с помощью фильтра по имени «\*».

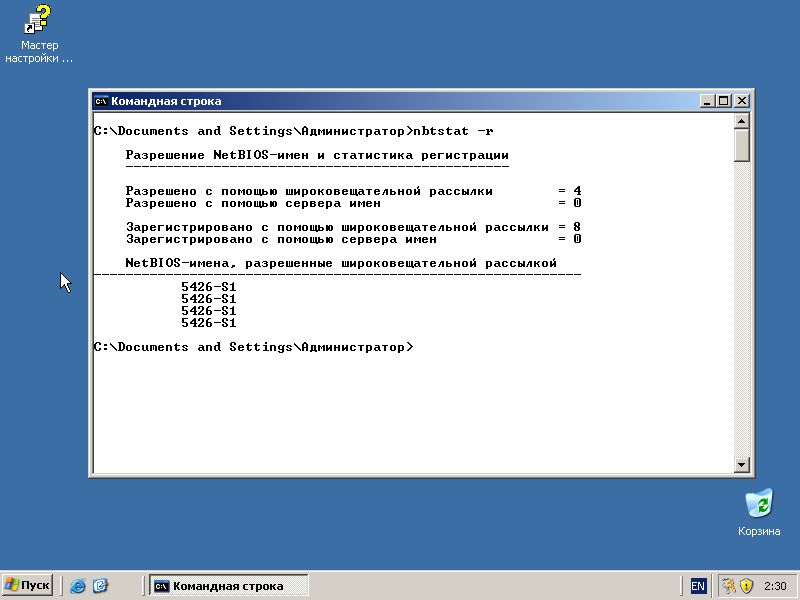


*Рисунок 23. Список регистраций на сервере WINS*

***Задача:*** Используя команду nbtstat, получить информацию о работе NetBIOS по разрешению имён.

***Выполнение:*** Утилита *nbtstat.exe* имеется в составе всех версий операционных систем семейства Windows и используется для получения информации о подключениях с использованием протокола NETBIOS через TCP/IP или NBT (Network BIOS over TCT/IP).

Команда nbstat с ключом –r позволяет вывести статистику разрешения имён, с помощью рассылки и WINS сервера. В результате выполнения было выявлено что ни одно имя узла не было получено с помощью сервера имён.



*Рисунок 24. Статистика разрешения NetBIOS имён*

Для того что бы проверить использование сервера имён, необходимо сгенерировать трафик, который использует WINS сервер. NetBIOS-имена разрешаются с помощью WINS-сервера, поэтому необходимо использовать некоторую команду с указанием узла в виде NetBIOS имени. Для этого возможно использовать команду nbtstat –a которая производит вывод таблиц имён узла, указанного с помощью NetBIOS-имени.

*рис.20*

Поле чего, просмотрев статистику использования WINS сервера было обнаружено что происходило 1 обращение к серверу. Это значит, что сервер работает правильно, без сбоев.

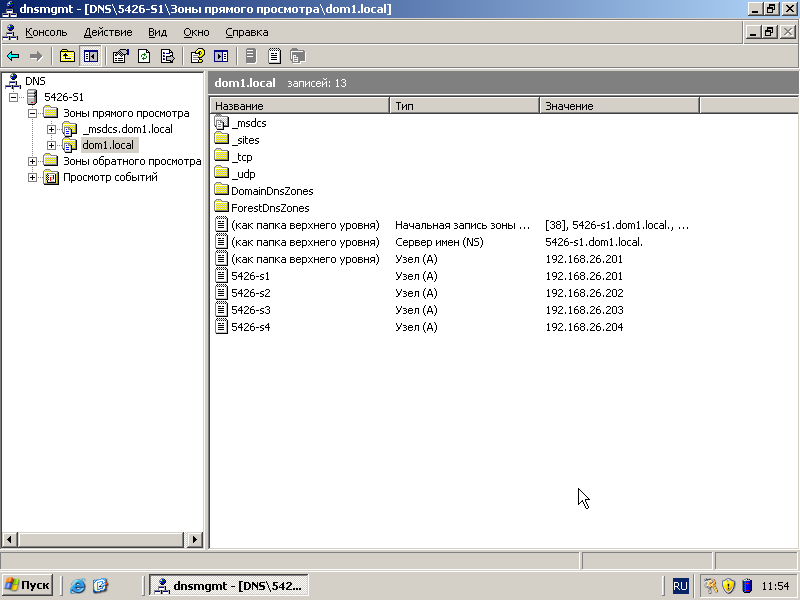
***Выводы:*** Установка и конфигурирование WINS сервера крайне проста. Для настройки клиентов на использование WINS сервера возможно воспользоваться графическим интерфейсом пользователя на каждой машине либо же задать выдачу IP адреса WINS сервера в параметрах DHCP сервера. В ОС Windows Server 2003R2 имеется встроенная системная утилита nbtstat, которая позволяет получать информацию о подключениях с использованием протокола NetBIOS.

*рис.21*

**VI. Конфигурирование и использование DNS. На DNS сервере использовать консоль администратора DNS. Составить отчёт о текущих записях DNS имён. На клиентах сконфигурировать свойства протокола TCP/IP для доступа к DNS серверу. Используя команду ipconfig, получить информацию о работе клиента по регистрации и разрешению имён. Выполнить перерегистрацию. Использовать команды nslookup, dnscmd (SupportTools) для получения информации о DNS сервере.**

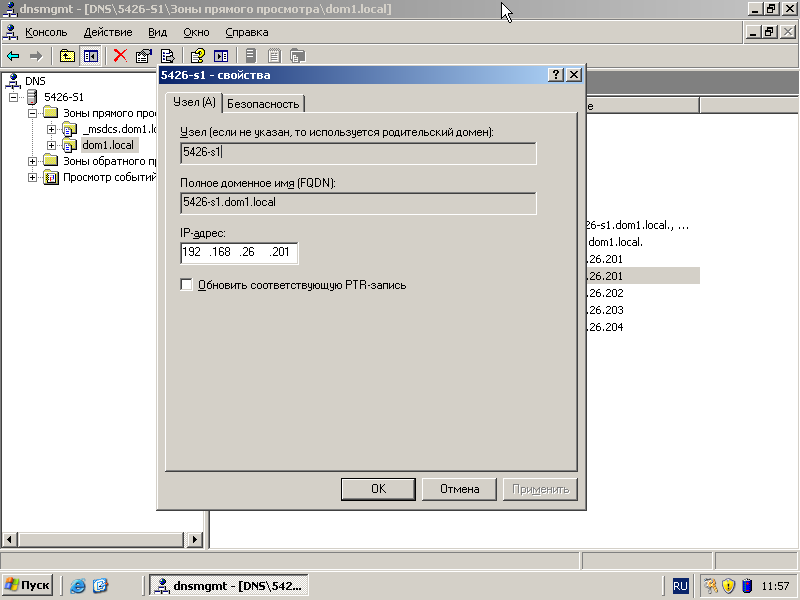
***Задача:*** Конфигурирование и использование DNS. На DNS сервере использовать консоль администратора DNS. Составить отчёт о текущих записях DNS имён.

***Выполнение:*** Так же как и при установке других ролей серверов, после установки DNS сервера в панели управления в разделе «Администрирование» появился новый компонент «DNS». Данный компонент позволяет управлять и просматривать состояние DNS сервера. При распределении ролей по серверам, было решено устанавливать DNS сервер рядом с контроллером домена ActiveDirectory.



*Рисунок 25. Список записей регистрации узлов на DNS сервере*

Список текущих записей в DNS сервере возможно просмотреть использовав оснастку консоли управления DNS. Так в подразделе «Зоны прямого просмотра» указаны имена зарегистрированные на сервере. В результате просмотра данного раздела консоли управления было выявлено что имена всех компьютеров в сети зарегистрированы на сервере DNS. Для каждой записи возможно просмотреть имя узла, полное доменное имя FQDN и IP адрес узла.

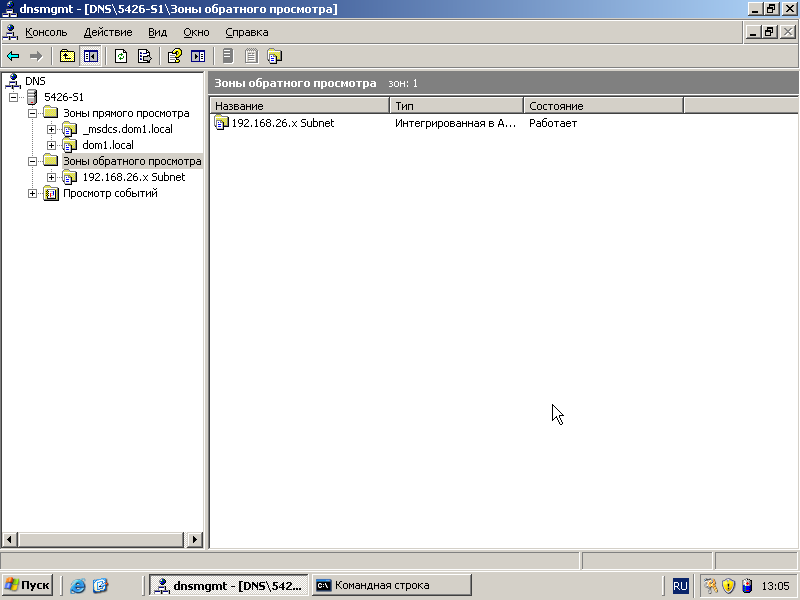


*Рисунок 26. Окно свойств записи регистрации*

Зоны обратного просмотра служат для разрешения IP-адресов в имена устройств. Несмотря на то что зоны обратного просмотра не являются обязательными в большинстве сетей, они могут оказаться полезными для определённых приложений безопасности, нуждающихся в подтверждении по IP-адресу.

Для создания зоны обратного просмотра возможно воспользоваться командной строкой или консолью сервера DNS. Добавление зоны обратного просмотра в командной строке выполняется с помощью команды *dnscmd* из пакета *SupportTools* с ключом /*ZoneAdd*. В качестве параметра используется имя домена «*in-addr.arpa*» в обратном формате. В графическом интерфейсе консоли DNS добавление осуществляется с помощью мастера создания зоны, имя домена «*in-addr.arpa*» указывается в прямом формате.

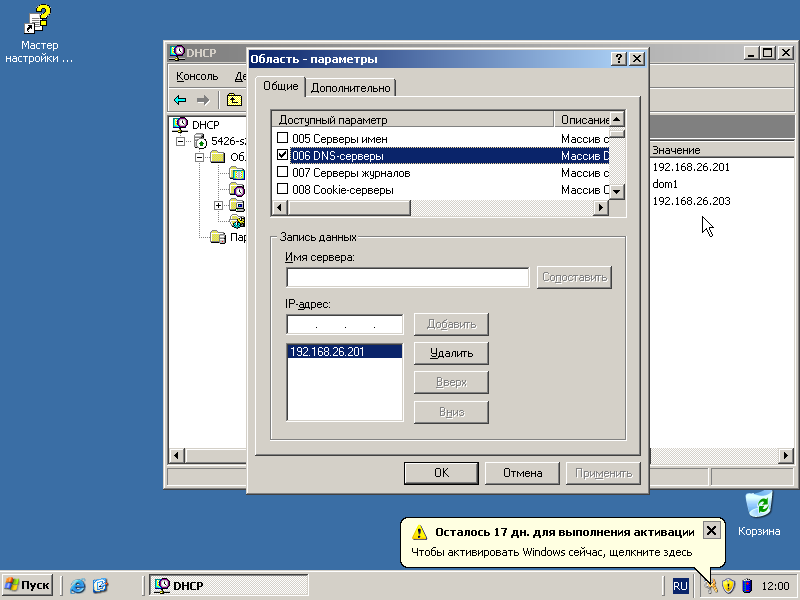
Создам зону обратного просмотра в консоли управления DNS сервером. После запуска мастера добавления новой зоны и выполнения всех его шагов в оснастке консоли управления DNS появилась новая зона обратного просмотра «*192.168.26.x Subnet*». Для проверки работоспособности зоны обратного просмотра, выполню с клиента команду «*ping -a 192.168.26.203*», ключ -а означает разрешение имени по адресу. В результате выполнения имя было разрешено верно.



*Рисунок 27. Окно просмотра зоны обратного просмотра*

***Задача:*** На клиентах сконфигурировать свойства протокола TCP/IP для доступа к DNS серверу.

***Выполнение:*** Для доступа к DNS серверу c компьютеров клиентов необходимо совершить настройку стека протоколов TCP/IP. Для того что бы назначить DNS сервер нужно указать его IP адрес в окне настройки стека протоколов TCP/IP. Для клиентов в сети возможно автоматически получать IP адрес DNS сервера, для этого на клиентах включается получение параметров сети с помощью DHCP сервера, а на самом DHCP сервере включается компонент передачи адреса DNS сервера, с помощью консоли управления DHCP в параметрах зоны.

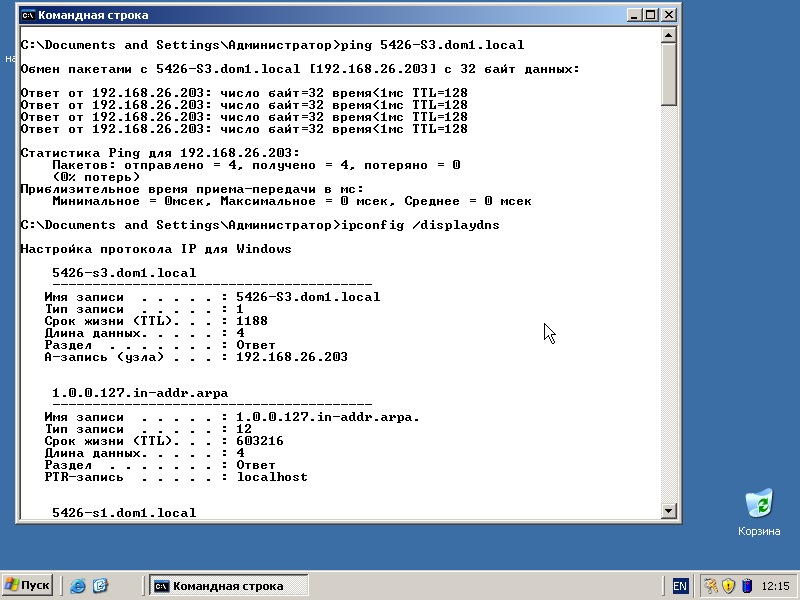


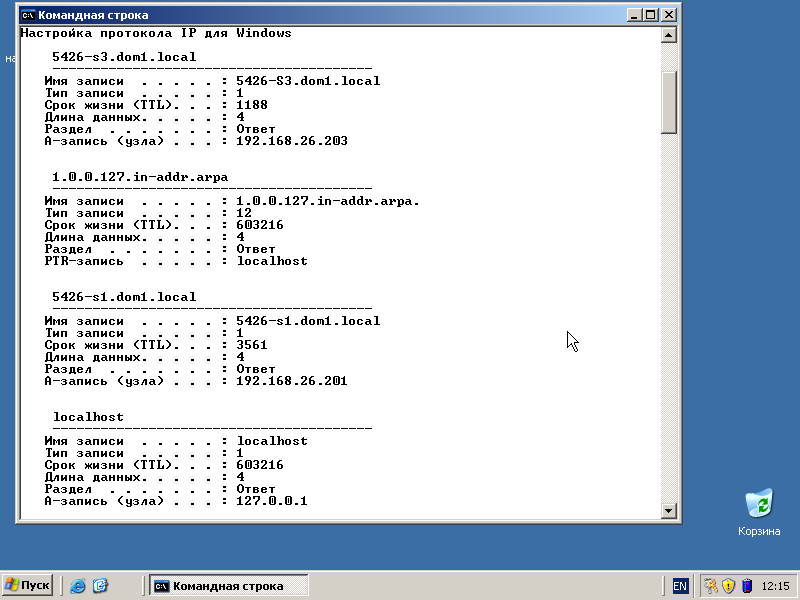
*Рисунок 28. Окно дополнительных параметров DHCP сервера*

***Задача:*** Используя команду ipconfig, получить информацию о работе клиента по регистрации и разрешению имён. Выполнить перерегистрацию.

***Выполнение:*** Для уменьшения нагрузки на сеть, на локальных машинах присутствует кэш DNS имён. При первом разрешении имени оно сохраняется в локальный кэш на определённое время. Проверка состояния DNS сервера осуществляется с помощью любой команды, которая будет запрашивать у DNS сервера разрешение имени. Простейшая команда, которую возможно использовать - команда ping.

При исполнение команды «*ping 5426-S3.dom1.local*», было установлено что связь с узлом 5425-S3 c узла 5426-S4 присутствует. Так как обращение к компьютеру было произведено с помощью DNS имени, команде необходимо разрешить его в IP адрес. Состояние записей кэша DNS на клиенте просматривается с помощью ключа «*/displaydns»* команды *ipconfig*. В результате выполнения команды «*ipconfig /displaydns*» было выявлено, что имя 5426-S3.dom1.local было добавлено в кэш.





*Рисунок 29. Разрешение DNS имени и результирующая запись в DNS кэше*

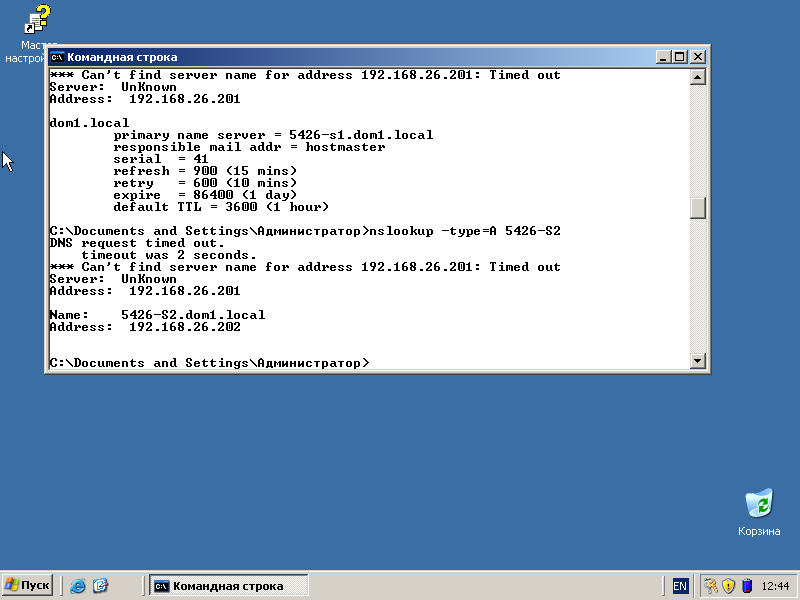
Для проверки использования кэша DNS который действует 15 минут, отключу удалённый узел 5426-S3. После выполнения запроса ping к узлу 5426-S3 по его DSN имени (5426-S3.dom1.local) было выявлено что связь отсутствует, но связь полного имени узла и его IP адреса осталась.

Для того, что бы кэш DNS содержал правильные записи, его содержимое необходимо сбросить. Это возможно сделать с помощью ключа «*/flushdns*» команды ipconfig. Если, после совершения операции очистки кэша выполнить запрос ping то, программа выдаст сообщение о том что узел невозможно найти. При этом в кэше DNS попадает запись о несуществующем сервере. Что бы произвести регистрацию машины на сервере DNS, возможно выполнить команду ipconfig с ключом «*/registerdns*».

Верну машину *5426-S3* в сеть, и выполню команду «*/registerdns*». В результате чего будет выполнена регистрация записей ресурсов DNS для всех адаптеров компьютера. Регистрация была проверена с помощью консоли управления DNS сервера. Выполнение запроса ping на узел 5426-S3.dom1.local показало успешное восстановление имени удалённого узла в кэше DSN локального компьютера.

***Задача:*** Использовать команды nslookup, dnscmd (SupportTools) для получения информации о DNS сервере.

***Выполнение:*** nslookup (name server lookup поиск на сервере имён) — [утилита](https://ru.wikipedia.org/wiki/%D0%A3%D1%82%D0%B8%D0%BB%D0%B8%D1%82%D0%B0), предоставляющая пользователю [интерфейс командной строки](https://ru.wikipedia.org/wiki/%D0%98%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D0%BA%D0%BE%D0%BC%D0%B0%D0%BD%D0%B4%D0%BD%D0%BE%D0%B9_%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%B8) для обращения к системе [DNS](https://ru.wikipedia.org/wiki/DNS) ([DNS-клиент](https://ru.wikipedia.org/wiki/DNS-%D0%BA%D0%BB%D0%B8%D0%B5%D0%BD%D1%82)). Позволяет задавать различные типы запросов и опрашивать произвольно указываемые [сервера](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_(%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)). При запуске без параметров переходит в интерактивный режим. Выполнив команду указав тип запроса A команда nslookup выведет IP адрес узла указанного имени.



*Рисунок 30. Пример выполнения запроса «nslookup -type=A 5426-S2.dom1.local»*

В качестве типа записи можно указать A(IP адрес), ANY(Вся доступная информация), HINFO(Информация о аппаратной части) и другие.

Утилита dnscmd доступна в пакете Support Tools. dnscmd позволяет диагностировать и исправлять ошибки в конфигурации, а так же выполнять широкий диапазон действий по администрированию сервера DNS.

Команда dnscmd имеет следующий синтаксис:

*dnscmd [server] <операция> [параметры] [аргументы]*

В этом синтаксисе необходимо указать имя сервера DNS, управление которым будет осуществляться, или команду, которая будет отправлена локальному серверу. Существует множество различных операций, которые можно выполнять с помощью утилиты dnscmd.

Операция *clearcache* позволяет удалять все кэшированные записи ресурсов из кэша сервера DNS. Эта операция оказывается полезной, когда сервер DNS перенаправляет запрос другому серверу DNS, возвращающему неправильный ответ. Даже если исправить адрес на сервере DNS, поддерживающем данную запись, локальный сервер DNS сохранит кэшированный некорректный ответ и будет предоставлять клиентам именно его.

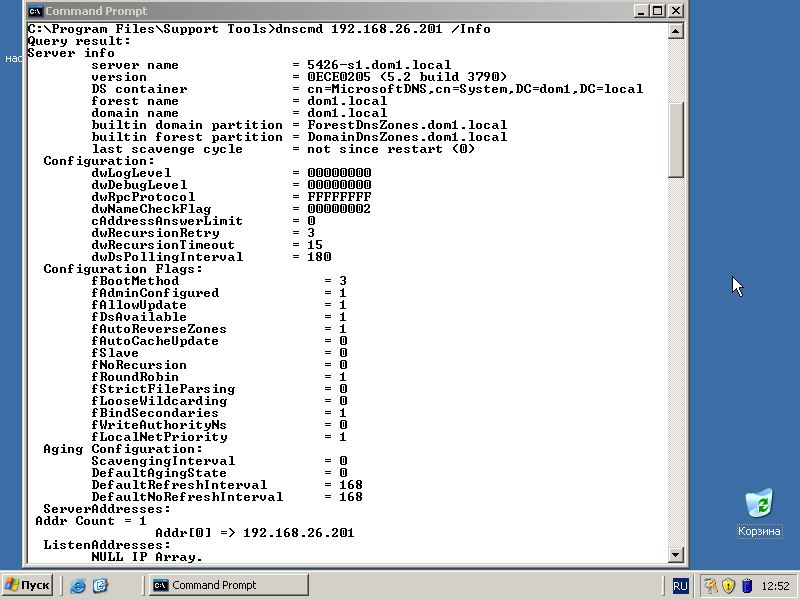
Операция *statistics* позволяет получить большой объем информации о сервере DNS, включая:

* запросы, отправленные и полученные;
* типы полученных запросов (A, NS, MX, PTR);
* попытки передачи зон и частота успешных попыток;
* ссылки на WINS;
* статистику динамических обновлений (безопасные обновления, типы записей);
* статистику производительности записи.

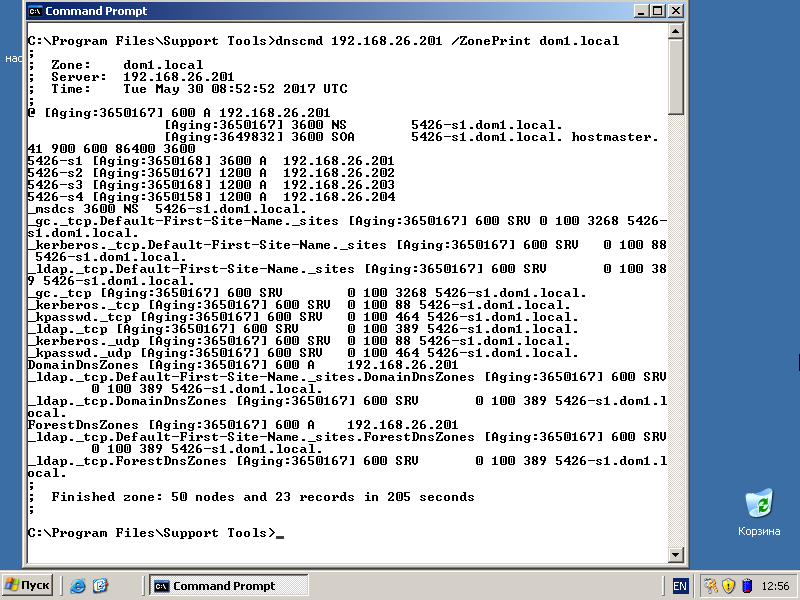
Так же существует ключ /ZonePrint который позволяет получить подробную информацию о зоне. С помощью ключа /info можно получить информацию о DNS сервере.

В выводе команды dnscmd с ключом /ZonePrint указываются протоколы, например:

* *\_ldap.\_tcp – облегченный протокол доступа к каталогам*
* *\_kerberos.\_tcp – протокол аутентификации*
* *\_gc.\_tcp – запись о контроллере домена*



*Рисунок 31. Пример получения информации о DNS сервере с помощью команды dnscmd.*



*Рисунок 32. Пример получения информации о зоне DNS сервера с помощью команды dnscmd.*

***Выводы:*** DNS сервер был настроен на одной машине вместе с контроллером домена ActiveDirectory. Управление DNS сервером производится с помощью консоли управления DNS, а так же используя команды nslookup, dnscmd и другие. Так же была создана и протестирована зона обратного просмотра DNS сервера, необходимая для получения имени по IP адресу.

**VII. Рассмотреть состав установленных служб и способы управления службами. Выбрать и описать свойства активных служб, связанных с сетевыми функциями, определить их взаимозависимости. Предложить варианты для сокращения состава используемых служб в зависимости от требуемых функций сервера.**

***Задача:*** Рассмотреть состав установленных служб и способы управления службами. Выбрать и описать свойства активных служб, связанных с сетевыми функциями, определить их взаимозависимости.

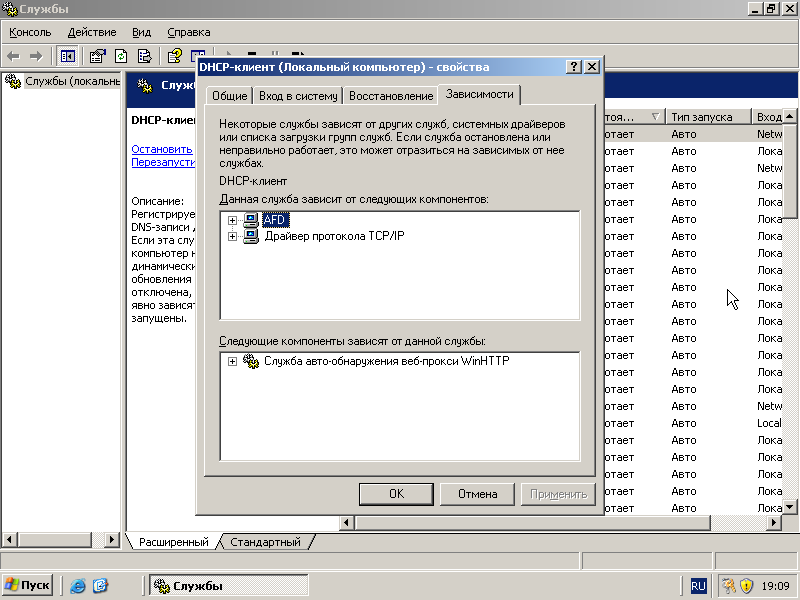
***Выполнение:*** Локальные службы управляются с помощью оснастки консоли ММС «Службы». Для каждой из служб в списке возможно установить тип запуска, остановить или запустить службу, просмотреть зависимости. Рассмотрю активные службы на узле 5426-S2 (выполняет роль DHCP сервера).

* DHCP-клиент – регистрирует и обновляет IP-адреса и DNS-записи для этого компьютера. Если эта служба остановлена, этот компьютер не сможет получать динамические IP-адреса и выполнять обновления DNS.
* DHCP-сервер – выполняет настройку TCP/IP для клиентов DHCP, включая динамическое назначение IP-адресов, указание WINS-серверов и DNS-серверов, настройку специфических DNS-имён. Если эта служба остановлена, DHCP-сервер не будет выполнять настройку TCP/IP для клиентов.

*рис.32*

* DNS-клиент – разрешает для данного компьютера DNS-имена в адреса и помещает их в кэш. Если служба остановлена, не удастся разрешить DNS-имена и разместить службу каталогов Active Directory контроллеров домена.
* DNS-сервер – позволяет клиентам DNS выполнять разрешение DNS-имён, отвечая на запросы о DNS-именах и на запросы обновления DNS. Если эта служба остановлена, обновления информации DNS не выполняются.
* Telnet – позволяет удалённому пользователю входить в систему и запускать программы, поддерживает различных клиентов TCP/IP Telnet, включая компьютеры с операционными системами UNIX и Windows.
* WINS – обеспечивает разрешение NetBIOS-имён для клиентов TCP/IP, обнаруживая сетевые службы, использующие NetBIOS-имена. Если эта служба остановлена, функционирование сетевых служб NetBIOS может быть нарушено.
* Брандмауэр Windows/Общий доступ к Интернету (ICS) – обеспечивает поддержку служб трансляции адресов, адресации и разрешения имён или предотвращает вторжение служб в домашней сети или сети небольшого офиса.
* Диспетчер подключений удалённого доступа – создаёт сетевое подключение.
* Запуск серверных процессов DCOM – обеспечивает запуск для служб DCOM.
* Локатор удалённого вызова процедур (RPC) – позволяет клиентам службы удалённого вызова процедур (RPC) использовать семейство RpcNs\* API для обнаружения RPC-серверов. Если эта служба остановлена или отключена, клиенты RPC, использующие RpcNs\* API, могут быть неспособны обнаруживать серверы или даже начать работу. Интерфейсы RpcNs\* API не используются внутри Windows.
* Обозреватель компьютеров – обслуживает список компьютеров в сети и выдаёт его программам по запросу. Если служба остановлена, список не будет создан или обновлён.
* Рабочая станция – обеспечивает поддержку сетевых подключений и связь.
* Сервер – обеспечивает поддержку общего доступа к файлам, принтерам и именованным каналам для данного компьютера через сетевое подключение.
* Сетевые подключения – Это способность ПК подключаться к сети
* Службы IPSEC – обеспечивает безопасность подключений между клиентами и серверами в сетях TCP/IP. Если эта служба остановлена, безопасность подключений TCP/IP между клиентами и серверами в сети может быть нарушена.
* Удалённый вызов процедур (RPC) – обеспечивает сопоставление конечных точек и служит диспетчером управления службы COM. Если эта служба остановлена или отключена, программы, использующие службу COM или службы удалённого вызова процедур (RPC), не смогут работать.
* Сетевой вход в систему - Обеспечивает безопасный канал связи между компьютером и контроллером домена для проверки подлинности пользователей и служб.
* Удалённый реестр - Позволяет удаленным пользователям изменять параметры реестра на компьютере.
* Модуль поддержки NetBIOS через TCP/IP - Включает поддержку службы NetBIOS через TCP/IP (NetBT) и разрешения NetBIOS-имен в адреса.

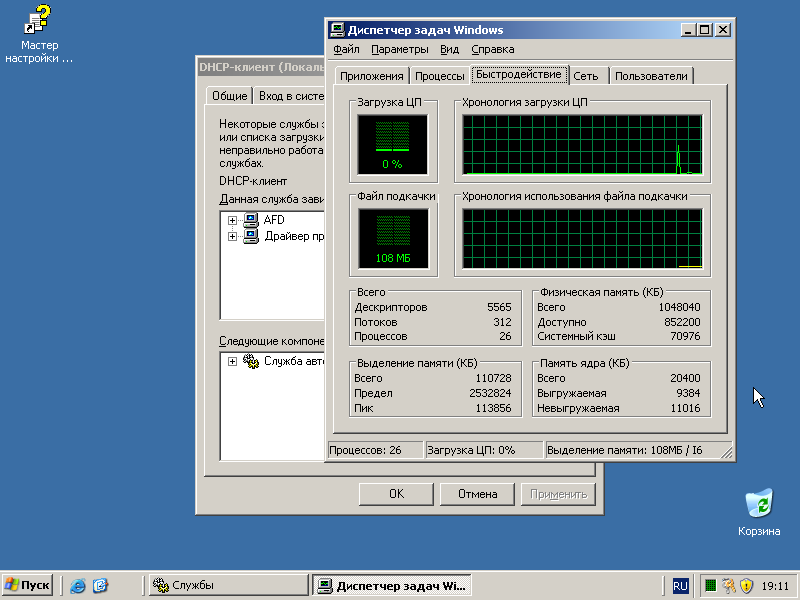
Для каждой службы возможно определить зависимости. Для их определения необходимо зайти на вкладку «Зависимости» в окне свойств службы. На вкладке «Зависимости» отображены компоненты которые зависят от данное службы, и, компоненты которые нужны для запуска данной службы.



*Рисунок 33. Окно зависимостей службы DHCP-клиента*

***Задача:*** Предложить варианты для сокращения состава используемых служб в зависимости от требуемых функций сервера.

***Выполнение:*** При начальном состоянии узла 5426-S2 (DHCP сервер) активно 26 процессов, выделено 108МБ памяти, открыто 5565 дескрипторов, 312 потоков.

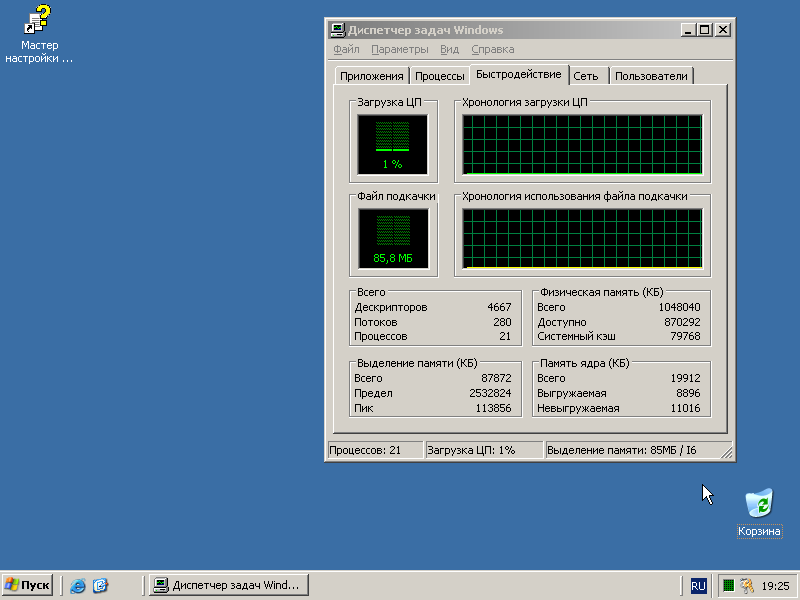


*Рисунок 34. Потребление ресурсов до оптимизации*

После просмотра списка активных служб было принято решение отключить следующие службы:

* Windows Audio - сервер не использует звуковых эффектов
* Автоматическое обновление - поддержка Windows Server 2003 прекращена и обновления не выпускаются.
* Диспетчер очереди печати - принтер не подключён
* Определение оборудования оболочки - в функции автозапуска содержимого со схемных носителей нет необходимости на сервере
* Служба регистрации ошибок - поддержка Windows Server 2003 прекращена, от службы нет практической пользы
* Справка и поддержка - отключение центра справки для экономии памяти
* Удалённый реестр - управление сервером происходит локально + безопасность

В результате отключения вышеперечисленных служб исполняемых процессов стало 21, выделяемой памяти 85МБ, открытых дескрипторов 4667, а потоков 280. Для администратора визуально производительность сервера не увеличилась, но, например, в системах с небольшим количеством оперативной памяти разница может быть существенна.



*Рисунок 35. Потребление ресурсов после оптимизации*

***Выводы:*** На не настроенном сервере включено некоторое количество служб, в которых нет необходимости на сервере. Если правильно оценить важность тех или иных служб, можно принять решение об отключении некоторых из них. Все службы управляются с помощью оснастки консоли ММС «Службы», где возможно управлять состоянием той или иной службы, а также просмотреть наличие зависимостей данной службы от других и других служб от данной.

**Выводы**

В результате выполнения лабораторной работы были сконфигурированы 4 сервера на основе ОС Microsoft Windows Server 2003 R2. На первом сервере были сконфигурированы роли контроллера домена ActiveDirectory и DNS сервера. На втором сервере была сконфигурирована роль DHCP сервера с выдачей IP адресов WINS и DNS серверов. На третьей машине была установлена роль WINS сервера (сервера разрешения NetBIOS имён). Четвёртая машина выступала как клиент в рассматриваемом домене. Была проведена начальная конфигурация каждого из серверов. Правильность настройки была проверена для каждого из компонентов отдельно.