МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ БУРЯТИЯ
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«БУРЯТСКИЙ РЕСПУБЛИКАНСКИИЙ ИНФОРМАЦИОННО-ЭКОНОМИЧЕСКИЙ ТЕХНИКУМ»
(ГБПОУ БРИЭТ)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для выполнения лабораторных работ
по профессиональному модулю

Эксплуатация объектов сетевой инфраструктуры

Раздел 1 Объекты сетевой инфраструктуры и операции над ними

Предназначены для обучающихся специальности
09.02.02 Компьютерные сети

г.Улан-Удэ
2018

Составитель:
Е.А. Тенгайкин©

Рассмотрено предметно-цикловой комиссией
информационных технологий
(название ЦК)

Протокол № 1 от « 30 » 08 2018г.

Председатель предметной цикловой
комиссии Бальчугова С.С. (ф.и.о)

Настоящие методические указания составлены в соответствии с рабочей программой и предназначены для обучающихся специальности СПО 09.02.02 Компьютерные сети при изучении ПМ.03 Эксплуатация объектов сетевой инфраструктуры. Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.02 Компьютерные сети (базовой подготовки) в части освоения основного вида профессиональной деятельности (ВПД): Эксплуатация объектов сетевой инфраструктуры и соответствующих профессиональных компетенций (ПК):

1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

3. Эксплуатация сетевых конфигураций.

4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования.

6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

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

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и профессиональной подготовке работников в областях, связанных с обслуживанием компьютерных сетей, при наличии среднего (полного) образования.

Содержание

Введение

Методические указания для выполнения лабораторных работ по профессиональному модулю Эксплуатация объектов сетевой инфраструктуры составлены в соответствии с рабочей программой ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Актуальность изучения МДК 03.01 Эксплуатация объектов сетевой инфраструктуры обусловлена тем, что данный МДК является частью основной профессиональной образовательной программы по специальности СПО 09.02.02 Компьютерные сети (базовой подготовки). Профессиональный модуль Эксплуатация объектов сетевой инфраструктуры логически взаимосвязан с профессиональными модулями и учебными дисциплинами специальности СПО 09.02.02 Компьютерные сети (базовой подготовки): основы электротехники, основы теории информации, технологии физического уровня передачи данных, архитектура аппаратных средств, операционные системы, основы программирования и баз данных, наладчик технологического оборудования, организация сетевого администрирования, проектирование сетевой инфраструктуры.

Техник компьютерных сетей - это специалист, который обслуживает компьютеры и обеспечивает бесперебойное функционирование офисной техники, компьютерных программ и информационных сетей в организации.

Работа техника компьютерных сетей связана с установкой, настройкой и эксплуатацией программного и аппаратного обеспечения с целью поддержания функционирования локальных компьютерных сетей.

Техник компьютерных сетей развёртывает и подключает сетевое оборудование и поддерживает его работу. В процессе работы он проводит диагностику и устраняет неисправность в работе одного или нескольких элементов локальной сети и сетевого оборудования, производит обмен информации по локальной корпоративной сети, выполняет профилактические работы, координирует работы по конфигурированию и эксплуатации компьютерных сетей, охватывая сегменты глобальной сети Интернет.

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

иметь практический опыт:

- обслуживания сетевой инфраструктуры, восстановление работоспособности сети после сбоя;
- удалённого администрирования и восстановления работоспособности сетевой инфраструктуры;
- организации бесперебойной работы системы по резервному копированию и восстановлению информации;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры;

уметь:

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- использовать схемы послеаварийного восстановления работоспособности сети эксплуатировать технические средства сетевой инфраструктуры;
- осуществлять диагностику и поиск неисправностей технических средств;
- выполнять действия по устранению неисправностей в части, касающейся полномочий техника;
- тестировать кабели и коммуникационные устройства;
- выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;
- правильно оформлять техническую документацию;
- наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;

- устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

знать:

- архитектуру и функции систем управления сетями, стандарты систем управления;
- задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;
- средства мониторинга и анализа локальных сетей;
- классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;
- правила эксплуатации технических средств сетевой инфраструктуры;
- расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;
- методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;
- основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности ИС, требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;
- основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

Выполнение лабораторных работ способствуют формированию:
Профессиональных компетенций:

ПК 1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей
ПК 2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях
ПК 3.	Использовать инструментальные средства для эксплуатации сетевых конфигураций
ПК 4.	Выполнять восстановление и резервное копирование информации ,участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети
ПК 5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль поступившего из ремонта оборудования
ПК 6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры

Общих компетенций

ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности
ОК 6.	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности

В результате выполнения лабораторных работ обучающиеся выполняют мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; учатся использовать схемы послеаварийного восстановления работоспособности сети и эксплуатировать технические средства сетевой инфраструктуры; осуществляют диагностику и поиск неисправностей технических средств; выполняют действия по устранению неисправностей в части, касающейся полномочий техника; тестируют кабели и коммуникационные устройства; выполняют замену расходных материалов и мелкий ремонт периферийного оборудования; правильно оформляют техническую документацию; наблюдают за трафиком и выполняют операции резервного копирования, восстановления данных;

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 1 «Ознакомление с программой CommView Remote Agent»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы диагностики настроек стека протоколов TCP/ IP; получить сведения о сетевом трафике.

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками программы CVR;
2. научить учащихся основным способам анализа сетевого трафика;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Программа CommView Remote Agent предназначена для наблюдения трафика в удалённой сети. Она позволяет пользователям программы CommView анализировать сетевой трафик на компьютере, где запущен Remote Agent, где бы физически этот компьютер ни был расположен.

Достаточно провести установку, несложную конфигурацию, и, CommView Remote Agent готов принять подключение со стороны CommView. Как только соединение будет установлено и произойдёт успешная проверка пароля, CommView Remote Agent сможет собирать трафик в своём сегменте сети и передавать его на CommView. Передаваемые пакеты "сжимаются" для уменьшения нагрузки на сеть и шифруются для обеспечения безопасной передачи по открытым сетям. Программа CommView оснащена гибким набором фильтров, чтобы отсеивать ненужные пакеты, минимизируя служебный TCP трафик между CommView и CommView Remote Agent.

CommView Remote Agent - незаменим для профессионалов в области сетевых технологий, программирования и безопасности, поможет решить широкий круг задач, таких как наблюдение многосегментных сетей или дистанционная отладка сетевых программ.

Порядок работы

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

Запустите VirtualBox. Включите виртуальный ПК с Windows XP.

1. Установка и настройка

CommView Remote Agent следует устанавливать на компьютер(ах), чей трафик вы намерены отслеживать. Как и CommView, он может захватывать пакеты, проходящие через любой сетевой интерфейс - сетевой адаптер или адаптер удалённого доступа. CommView Remote Agent можно устанавливать как на подключенные к сети, так и изолированные компьютеры.

Для установки программы под Windows NT/2000/XP требуются права администратора, после установки и конфигурирования программы - такой уровень привилегий для работы с ней не требуется. Не устанавливайте ОДНОВРЕМЕННО и CommView и CommView Remote Agent на одном и том же компьютере, поскольку это бессмысленно.

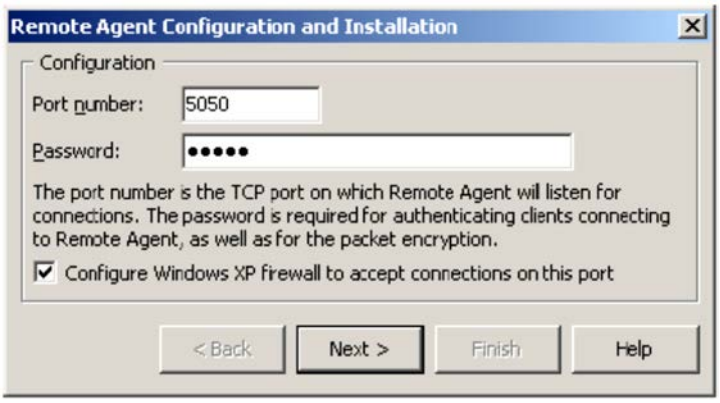
Установите программу CommView Remote Agent на виртуальный ПК с Windows XP.

2. Настройка программы

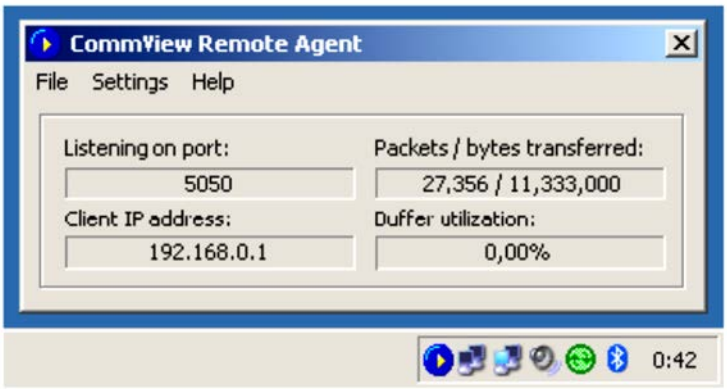
Для установки программы - запустите SETUP.EXE и следуйте инструкциям. Когда копирование необходимых файлов завершится, вы увидите окно Установки и Конфигурации (Installation and Configuration), где необходимо указать номер порта TCP и пароль доступа. По умолчанию выбран порт 5050, к нему будет подключаться клиентская программа CommView. Пароль требуется для идентификации клиента и последующей шифрации трафика.

Выбирайте **хороший** пароль (достаточно длинный, содержащий буквенно-цифровые комбинации, который трудно угадать), иначе, если кто-либо

посторонний угадает пароль, он получит ПОЛНЫЙ доступ к сетевому трафику данного компьютера.



Нажмите **Next**, чтобы продолжить, программа установит необходимые драйверы и произведёт первый запуск CommViewRemote Agent. Иконка программы появится в панели уведомлений, как показано на рисунке внизу. Для вызова окна приложения CommView Remote Agent, щёлкните по ней:



Поле **Status** показывает состояние программы: номер порта, на котором CommView Remote Agent ожидает подключения, IP адрес подключившегося клиента, статистику передачи пакетов, использование буфера. Поле **Service** содержит несколько настроечных кнопок. Изменить номер порта можно нажав **Change Port**. Изменить пароль можно нажав **Change Password**.

Приостановить и продолжить работу можно нажав соответственно кнопку **Pause** или **Resume**. Нажав на кнопку **About**, можно узнать общие сведения о программе. CommView Remote Agent способен устанавливать только одно клиентское подключение за раз.

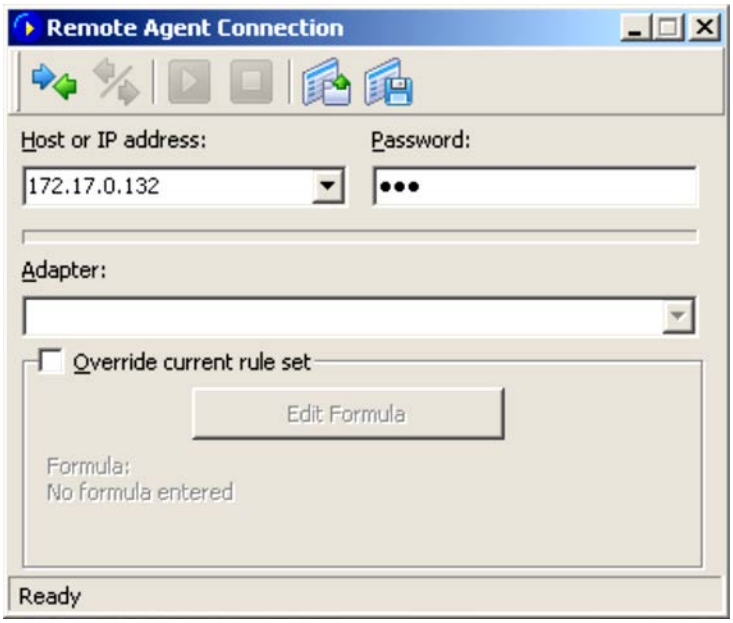
3. Наблюдение за трафиком

3.1. Включите виртуальную машину с сервером Windows Server 2008

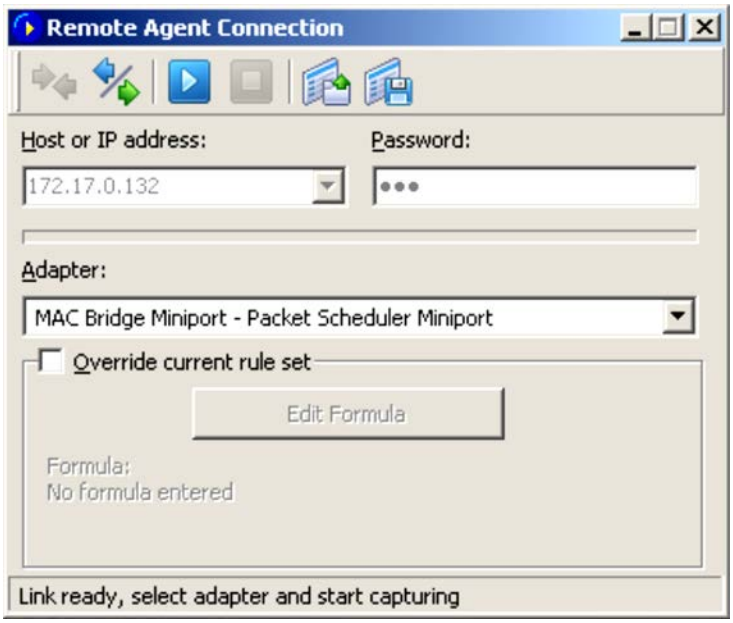
3.2. Установите программу CommView

3.3. Подключение CommView к CommView Remote Agent

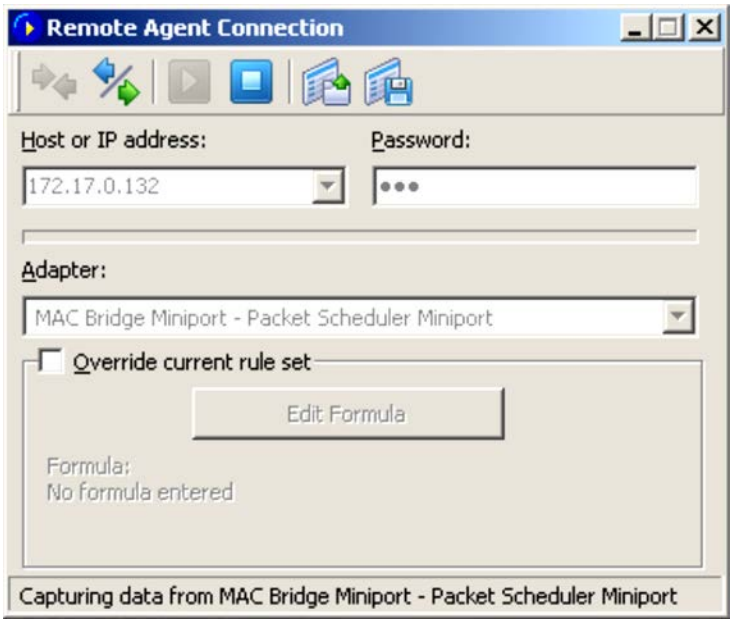
Чтобы включить режим удалённого наблюдения, выберите в меню **File (Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**. В дополнительной панели управления, появившейся под основной, укажите IP адрес компьютера, где запущен CommView Remote Agent, и нажмите кнопку **Connect** (Установить связь). Если вы работаете за брандмауэром (файрволом) или через прокси-сервер, или, если вы установили нестандартный номер порта на Remote Agent, вам придётся, нажав кнопку **Network Settings** (Сетевые установки), указать порт и/или ввести настройки прокси- сервера SOCKS5.



Во всплывающем окне укажите пароль доступа, заданный в установках Remote Agent. Если пароль указан верно, соединение будет сразу же установлено. Появится сообщение Link Ready(Связь подготовлена), а в списке доступных адаптеров появятся все имеющиеся на удалённом компьютере адаптеры.



Теперь необходимо установить правила в закладке **Rules(Правила)**. Важно настроить их так, чтобы не превысить пропускную способность канала связи между Remote Agent и CommView, иначе вы заметите существенное замедление реакции системы. Обязательно отфильтровывайте не интересующие вас пакеты (см. ниже). Когда всё готово, выберите в списке нужный адаптер и нажмите кнопку **Start Capture** (Начать сбор).



CommView начнёт сбор трафика удалённого компьютера, как если бы это был ваш локальный трафик, практически, нет разницы между этими двумя режимами работы CommView. Чтобы закончить удалённое наблюдение, нажмите кнопку **Stop Capture**. Можно или выбрать другой адаптер из списка или отключится от Remote Agent совсем, нажав кнопку **Disconnect.**

Чтобы вернуться в стандартный режим, выберите в меню **File(Файл)** => **Remote Monitoring Mode(Режим удалённого наблюдения)**, и дополнительная панель управления исчезнет.

Проверьте соединение между сервером и клиентской машиной с помощью команды ping.

Просмотрите содержимое анализа соединения в программе CommView на сервере:

1. Закройте окно Соединение с удаленным агентом
2. В окне программы CommView щелкните по вкладке Текущие IP-соединения (должна быть активна по умолчанию)
3. Двойным кликом мышки откройте локальный IP-адрес
4. В открывшемся окне справа выберите протокол и просмотрите информацию о соединении.
5. Запишите в тетрадь для лабораторных работ сл. Информацию:
    i. Какой версии протокол используется для соединения?
    ii. Какой размер фрейма?
    iii. Запишите номер IP-адреса ПК, чей трафик просматривается программой

Время выполнения работы 90 мин;

Контрольные вопросы

1. Может ли CommView быть использован для перехвата dial-up (RAS) трафика?
2. Что может "видеть" CommView, которая инсталлирована на компьютер с локальной сетью?
3.
4. Я подключен к LAN через switch и, когда я запускаю CommView, он ловит только пакеты, идущие к/от меня, я не вижу трафика других машин. Почему?
5. Я подключен к сети через hub, но не вижу чужого трафика, как если бы это был switch. Почему?
6. Может ли CommView собирать данные на адаптере, который не имеет своего IP-адреса?

7. Я работаю в локальной сети с большим объемом трафика, и поэтому мне сложно изучать отдельные пакеты, когда программа принимает сотни и тысячи пакетов в секунду, и старые пакеты быстро исчезают из циркулярного буфера. Можно с этим что-нибудь сделать?

8. Я подключен к сети через cable/xDSL-модем. Будет ли CommView осуществлять мониторинг трафика в этом случае?

9. Как установить захват пакетов по расписанию?

10. Возможен невидимый режим данной программы? Если да, то как его настроить?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

1. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.

2. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 2 «Создание схемы локальной сети программой LANState»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы возможности программ по сканированию локальных сетей.

В процессе занятия решаются следующие задачи:

3. познакомить с основными настройками и возможностями программы lanstate;

4. научить учащихся основным способам сканирования и управления сетевыми устройствами спомощью программы lanstate;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Программа 10-Strike LANState , позволяет осуществлять мониторинг сетевых служб и устройств, устранять неполадки в их работе, и сокращать простои.

Внезапные сбои в работе ответственных служб и протоколов сервера или активного сетевого оборудования часто оборачивается для компании немалыми убытками и подорванным доверием клиентов. В обязанности системного администратора входит задача своевременного обнаружения таких неполадок и их быстрого устранения. Но справиться с этой задачей без специальных программных инструментов подчас очень нелегко, и, можно сказать, невозможно. Решением проблемы автоматического мониторинга сети является программа 10-Strike LANState. Из под ее контроля не уйдет ни один сбой в работе сетевой службы или протокола. Программа вовремя обнаружит неполадку и сообщит о ней системному администратору.

В основе работы программы лежит механизм периодического выполнения задан-

ных проверок контролируемых служб и протоколов на серверах и другом сетевом оборудовании. О результате проверок системный администратор оповещается несколькими альтернативными способами: электронной почтой, SMS, звуковым сигналом. Кроме этого, программой ведется фиксация всех событий в журналах с подробной расшифровкой неполадок и временем их происшествия.

10-Strike LANState обладает возможностями мониторинга работы серверов баз данных, систем управления базами данных, значений некоторых параметров производительности сетевого оборудования (например, трафик на коммутаторах), а также оперативного доведения информации до системного администратора о достижении критических значений этих параметров. Для устранения неполадок программа может автоматически выполнить заданные администратором действия: перезагрузку служб и компьютеров, запустить программу или скрипт. Кроме этого, отличительной особенностью 10-Strike LANState является то, что она наглядно отображает контролируемые устройства в виде графической карты сети со связями и условными обозначениями (имеется веб-интерфейс). Карта призвана визуализировать результаты мониторинга, и позволяет быстро определить местонахождение сбойного устройства.

В новой версии 10-Strike LANState реализована возможность отслеживания изменений в списке установленного программного обеспечения на серверах и рабочих станциях локальной сети. Системный администратор будет оповещен о фактах установки пользователями новых программ и удаления старых.

Порядок работы

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

Часть I. Построение схемы сети

1. **Установите на свой компьютер программу LANState**
2. **Запустите программу.**
3. **Создание схемы сети автоматически**

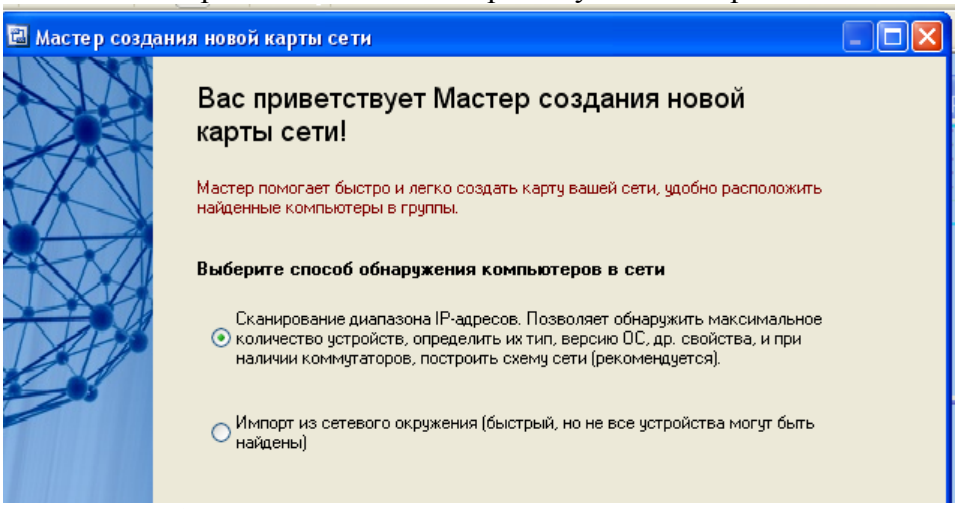
Начиная с версии 3.3, LANState поддерживает сканирование SNMP-устройств и может рисовать схему сети автоматически с созданием линий, соединяющих хосты. При этом номера портов коммутаторов проставляются в подписях к линиям.

Итак, как построим схему сети автоматически:

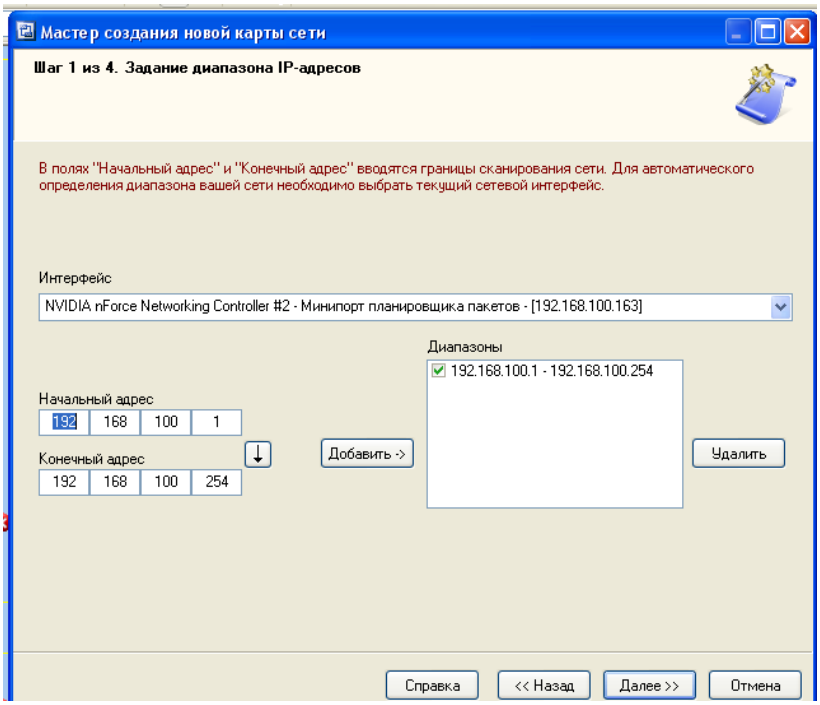
1. SNMP должен быть включен на коммутаторах. Программа должна быть разрешена в брандмауэре для успешной работы по протоколу SNMP.

2. Запустите **Мастер Создания Карты Сети (Файл – Мастер создания карты).**

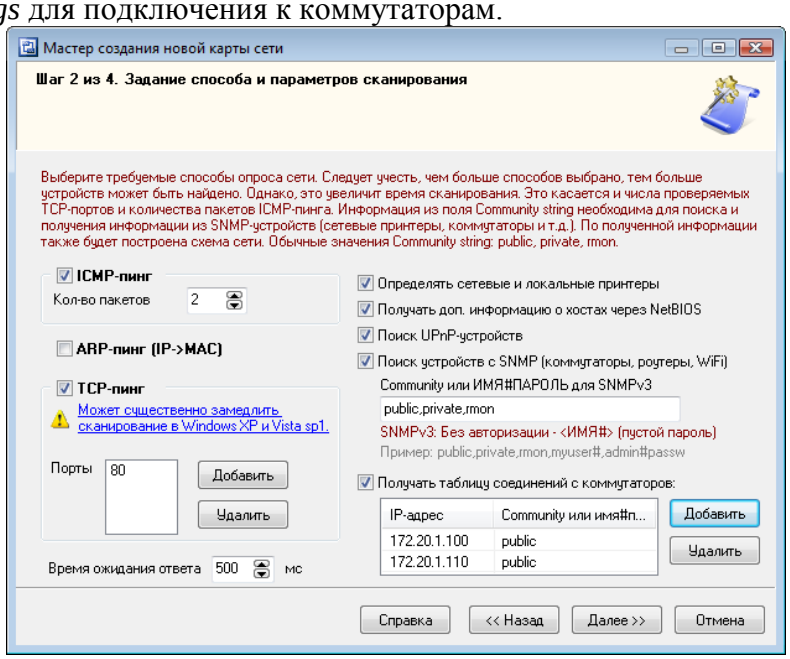
3. В открывшемся окне выберите пункт Сканирование диапазона IP-адресов



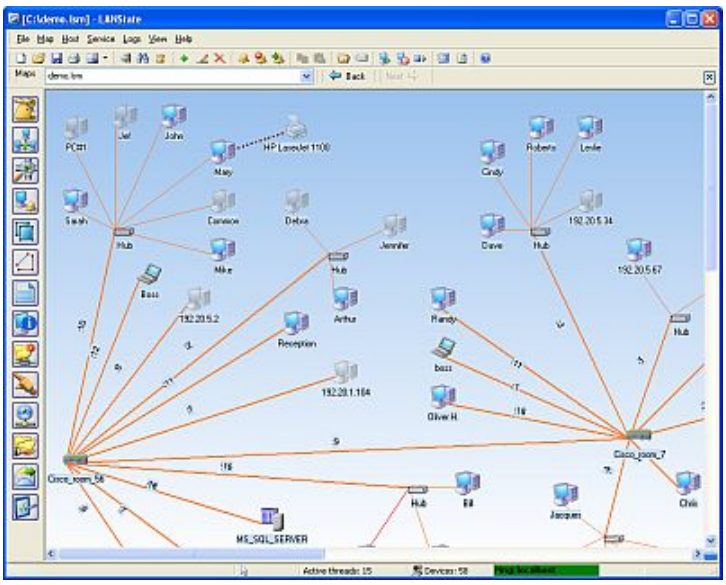
4. Выберите сканирование сети по диапазону IP-адресов. Укажите диапазоны (от 192.168.100.1 до 192.168.100.254) Устройства с SNMP должны находиться внутри указанных диапазонов.



4. Выберите методы сканирования и настройте их параметры. Не забудьте поставить галочку рядом с опцией "**Поиск устройств с SNMP...**" и укажите правильные *community strings* для подключения к коммутаторам.



5. После сканирования программа должна нарисовать схему сети. Если сканирование SNMP прошло успешно, соединения между сетевыми устройствами будут нарисованы автоматически. Передвиньте мышкой устройства для лучшего восприятия схемы.



6. Схема сети может быть выгружена в картинку, либо в схему Microsoft Visio (только в LANState Pro). Полученную схему сохраните в отдельный файл.

Часть II. Построение диаграмм сети

Краткие теоретические сведения

Программа построения диаграмм сети EDraw Network Diagrammer

При проектировании сетей иногда используется EDraw *Network* Diagrammer – *программа* создания диаграмм сети с большим количеством примеров и шаблонов.

Основные диаграммы:

- Топологические схемы сети
- Проектирование сетей Cisco
- Диаграммы кабельных сетей
- Диаграммы LAN (локальная компьютерная сеть)
- Диаграммы сетей WAN (глобальная сеть)

Сетевая диаграмма (*граф* сети) - графическое *отображение работ* проекта сети и их взаимосвязей. Отличием от блок-схемы является то, что *сетевая диаграмма* моделирует только логические зависимости между элементарными работами. Она не отображает входы, процессы и выходы.

Программа имеет как сходство с программой 10 Страйк: Схема Сети, так и принципиальные отличия. Например, в ней можно нарисовать не только изображение сети (рис. 1), но и изображение помещения, где эту *сеть* планируется установить (рис. 2).

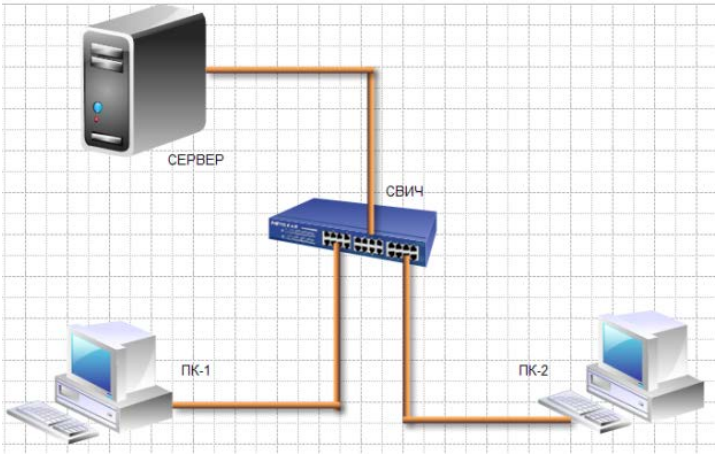


Рис. 1. Пример элементарной схемы сети, выполненной в EDraw Network Diagrammer

Задание 1

1. Постройте схему, изображенную на рисунке 1.
2. Для выбора компьютеров и мониторов из библиотеки (Libraries) нужно выбрать команду **Network-Computers and Monitors**, а для выбора кабелей – команду **Network and Peripherals**.

Задание 2 Нарисуйте схему помещения, изображенного на рисунке 2.

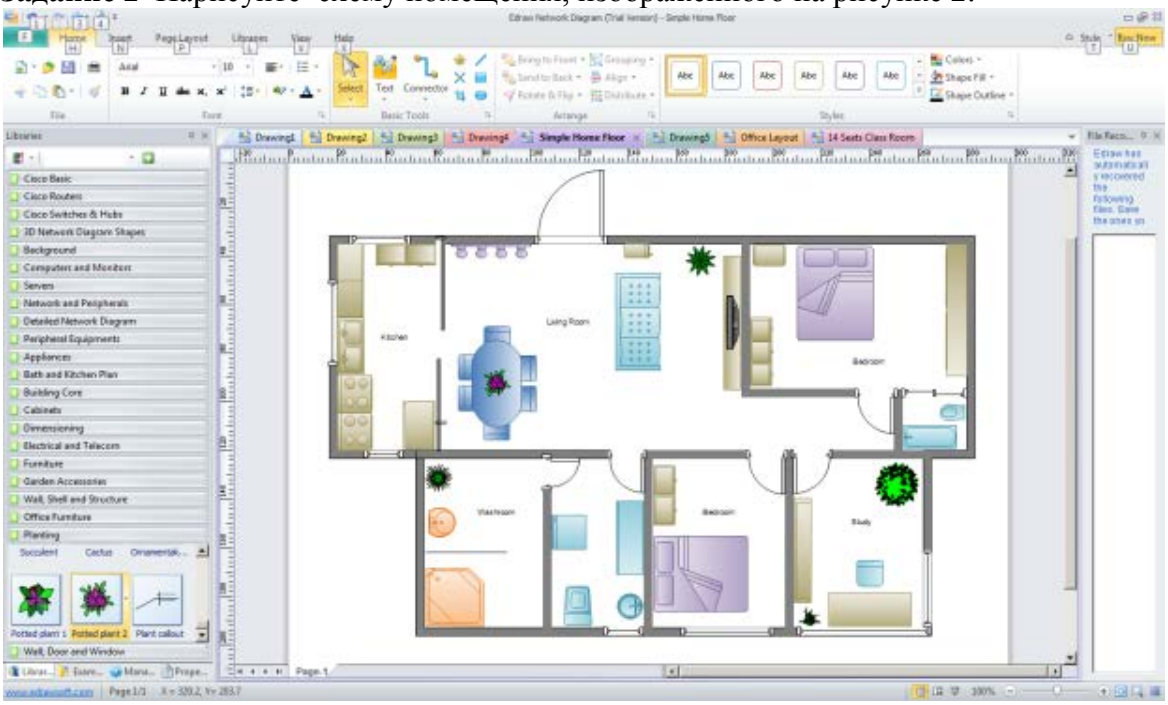


Рис.2. Изображение офисного помещения, нарисованного в EDraw Network Diagrammer

В этом случае из библиотеки нужно выбрать вариант **Floor Plans** (рис. 3).

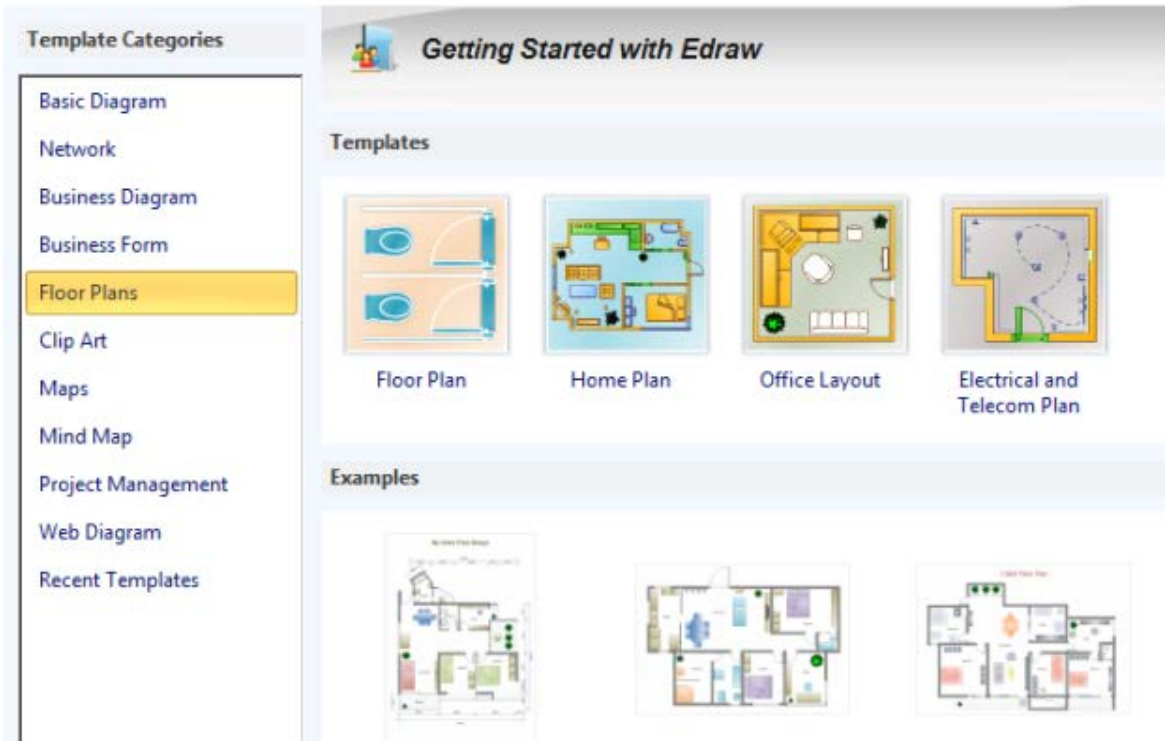


Рис 3. Различные схемы офисов, для размещения в них ПК

Задание 3. В программе EDraw Network Diagrammer повторите схему, показанную на рис.4. Поясните, что за устройства присутствуют в данной сети и как они работают.

Рис. 4. Схема сети небольшого офиса

Задание 3. Повторите рисунок, изображающий расположение компьютеров в компьютерном классе (рис.5).

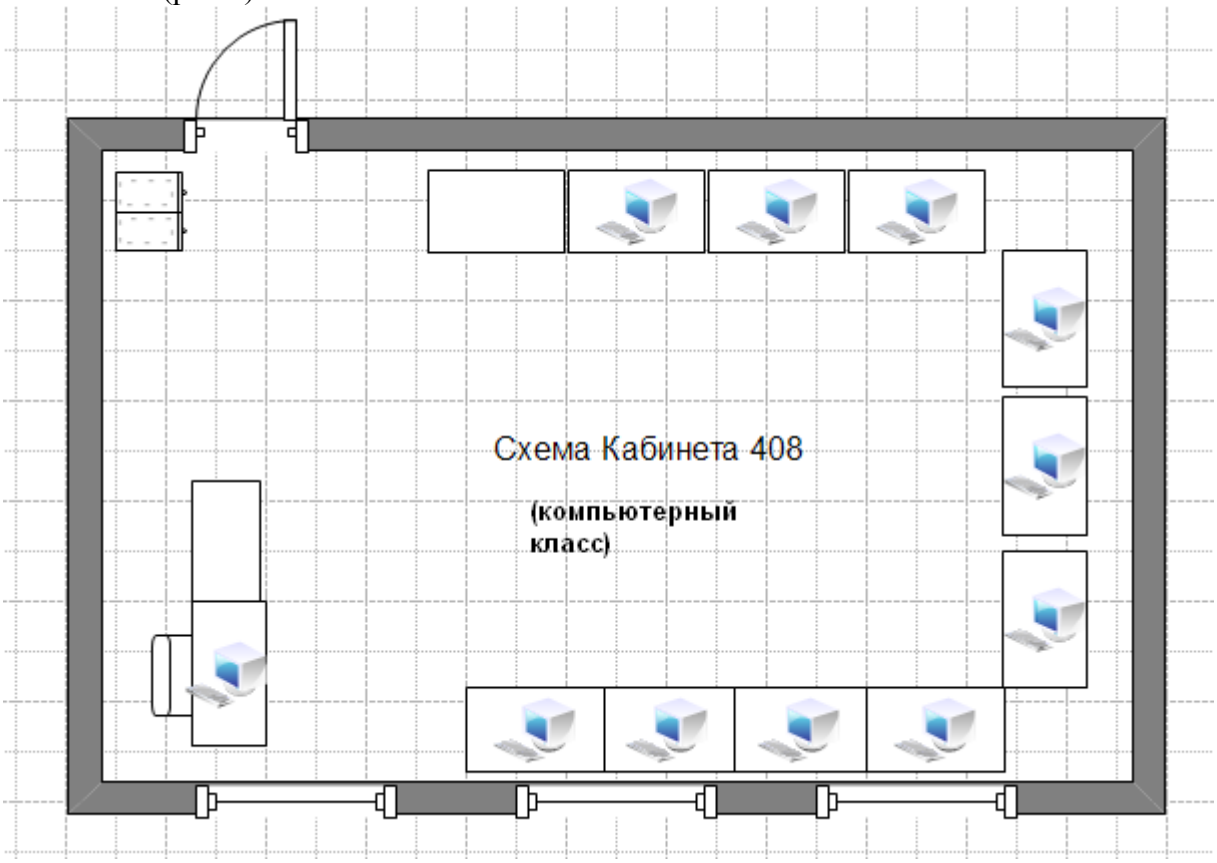


Рис. 5. Расположение компьютеров в компьютерном классе

Контрольное задание

Используя возможности программы **EDraw Network Diagrammer** создайте схему помещения и расположения компьютерной техники в кабинете № 402 (по аналогии с рис.

2. Время выполнения работы 90 мин;

Контрольные вопросы

1. Назовите основную функцию программы **10-Strike LANState**.
2. Перечислите сетевые функции программы **10-Strike LANState,** применимые к удаленным компьютерам.
3. Какие в программе **10-Strike LANState** реализованы полезные сервисные функции?
4. Вы просканировали сеть программой 10-Strike LANState , нашлись компьютеры, но связи не прорисованы. Почему?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.
2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно
3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 3 «Сканирование локальной сети с программой LanSurfer 2.0»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы диагностики сети программой LanSurfer.

В процессе занятия решаются следующие задачи:

5. познакомить с основными настройками программы LanSurfer;
6. научить учащихся основным способам диагностики сети программой LanSurfer;

Краткие теоретические и справочно-информационные материалы по теме занятия.

LanSurfer предназначен для:

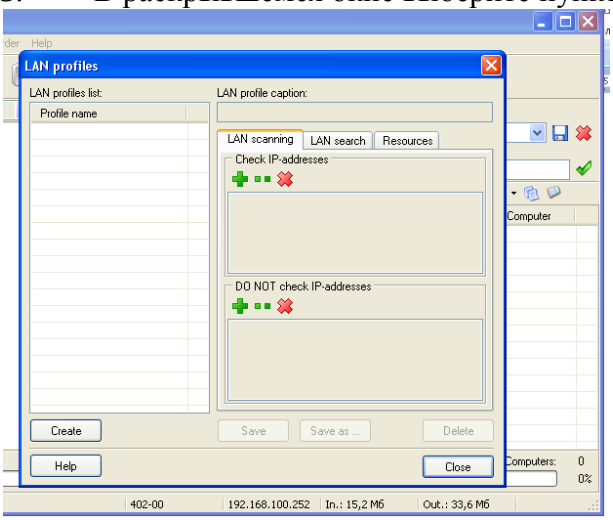
1. быстрого многопоточного сканирования компьютеров, расшаренных папок и серверов в локальной сети и составления списка сети, содержащего исчерпывающую информацию и компьютерах и ресурсах сети.
2. открытия ресурсов сети указанными пользователем приложениями.
3. вывода ресурсов сети, сходных по содержанию, вместе. (напр. видео или аудио папки) 4. быстрого многопоточного поиска файлов/папок в локальной сети (доступен расширенный поиск)
5. управления локальными расшаренными папками (на своем компьютере)
6. мониторинга и управления подключениями к локальным расшаренным папкам Полностью настраиваемый интерфейс с многоязычной поддержкой (с русским). Для

удобной работы широко используются профили (для хранения настроек). Например, можно создать профили сети, сканирования, поиска один раз и потом одним кликом переключаться между ними.

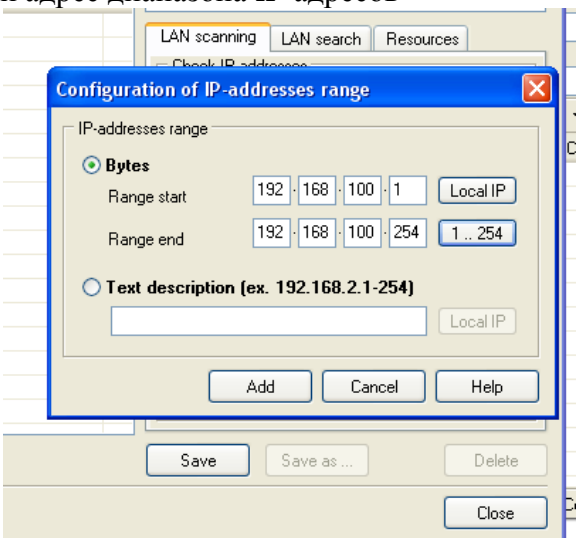
Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Установите программу **LanSurfer;**
3. После установки запустите программу.
4. Создайте LANprofiles. Для этого выберите пункт меню Options

5. В раскрывшемся окне выберите пункт LANprofiles



6. Щелкните мышкой по кнопке **Greate**
7. Вверху справа активируется строка ввода диапазона адресов для сканирования.
8. Щелкните кнопкой мыши по зеленому плюсу
9. Появиться окно, в котором необходимо ввести начальный IP-адрес и последний адрес диапазона IP-адресов

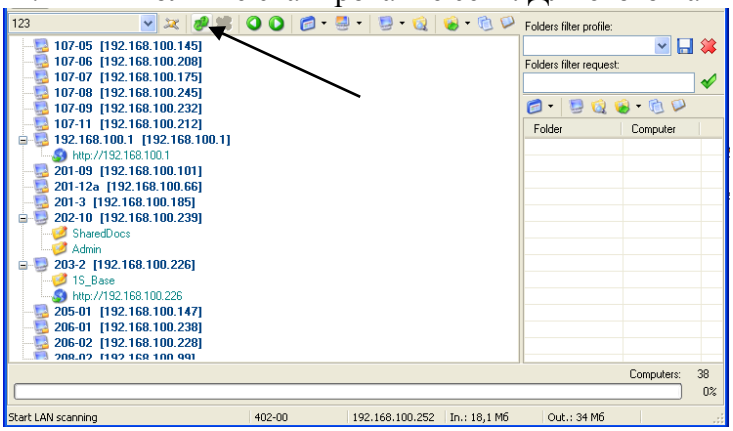


10. Введите диапазон адресов вручную или используя кнопки Local IP или 1..254
11. Нажмите кнопку ADD

12. Вверху в пункте Lanprofile caption введите имя вашего профиля и нажмите Save

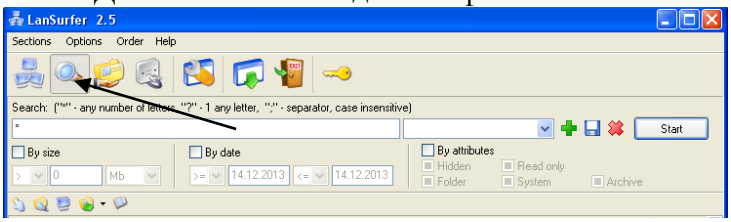
13. После этого выйдите из режима настройки профиля нажав кнопку Close

14. Выполните сканирование сети. Для этого нажмите кнопку StartLanScaning



15. После сканирования на экран выведется список ПК, серверов, маршрутизаторов, общедоступных папок.

16. Для поиска необходимого файла в сети используется Кнопка Search on Lan



17. В поисковой строке программы вводите имя файла и нажимаете кнопку Start

18. Ниже будет выведен список искомых файлов

Задание для самостоятельной работы

1. Создайте профиль для сканирования Моё сканирование
2. Укажите диапазон адресов от 192.168.100.1 до 192.168.100.254
3. Просканируйте сеть
4. Используя возможности программы найдите файл MyTestXSetup.exe
5. Перейдите в папку содержащий данный файл.

3. Время выполнения работы 90 мин;

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

5. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.

6. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 4 «Ознакомление программой SystemRescueCd 1.5.5»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы восстановления работы сервера специализированным диском SystemRescueCd.

В процессе занятия решаются следующие задачи:

7. познакомить с основными утилитами SystemRescueCd;
8. научить учащихся основным способам восстановления сервера используя SystemRescueCd;

Краткие теоретические и справочно-информационные материалы по теме занятия.

SystemRescueCd — это CD-образ, основанный на Linux, предоставляющий систему с минималистичным пользовательским интерфейсом и набором полезных программ. В комплект входят различные программы для восстановления данных, настройки сетевого соединения и веб-браузер. Наличие возможности настройки сети и веб-браузера часто бывают очень полезными, когда вам необходимо отыскать ответы на возникающие в процессе восстановления системы вопросы в Сети.

Несмотря на то, что **SystemRescueCd** предоставляет в распоряжение пользователя довольно хорошо настроенное рабочее окружение, не стоит его рассматривать как аналог таких дистрибутивов, как например, **Puppy Linux.**

От пользователя **SystemRescueCd** определённо требуется знание принципов работы компьютера и установленной на нём операционной системы, поскольку использование этого дистрибутива неопытными пользователями может привести к плачевным последствиям.

После загрузки, **SystemRescueCd** превращается в настоящий «швейцарский нож» с богатым набором разнообразных полезных приложений. Некоторые из этих приложений весьма схожи между собой по функциональности, однако, таким образом дистрибутиву удаётся предоставить большую свободу выбора пользователям: кому-то больше нравится работать в программами из командной строки, а кто-то предпочитает графический интерфейс.

Gparted позволяет создавать, удалять, копировать разделы жёсткого диска.

Partimage умеет целиком копировать разделы жёсткого диска в файлы или в разделы другого жёсткого диска. Если у вас есть куда скопировать исходные данные, над которыми вы собираетесь работать, скопируйте их. Это избавит вас от лишней головной боли, если что-то вдруг пойдёт не так.

Photorec позволяет выполнять восстановление media-данных, таких как фотографии или музыку. Она может работать с разнообразными носителями, вроде карт памяти, карманных компьютеров или мобильных телефонов.

ClamAV — отличный бесплатный антивирус, с помощью которого вы можете просканировать Windows-разделы в случае необходимости.

Также, в дистрибутиве имеется набор небольших программ, позволяющих выполнять восстановительные работы общего плана, например, **Grub**; программы для работы с архивами, текстовые редакторы, сетевые утилиты. В целом, **SystemRescueCd** содержит сотни полезных утилит.

На этапе загрузки вы можете выбрать загрузку различных floppy-образов, которые содержат разнообразные приложения для тестирования оборудования, менеджеры загрузки и **FreeDOS.**

Порядок работы

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

1. Запустите **SystemRescueCd**

2. Просмотрите основные программы SystemRescueCd

3. Используя встроенный антивирус ClamAV, проверьте папку Windows на наличие вирусов

4. Протестируйте встроенными средствами **SystemRescueCd** жесткий диск на наличие проблем.

4. Время выполнения работы 90 мин;

5. Контрольные вопросы

1. Перечислите основные аналоги программы SystemRescueCd

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 5 «Диагностика некоторых периферийных устройств ПК»

Цель работы: получение сведений по настройке пользовательского интерфейса периферийных устройств средствами операционной системы **Microsoft Windows.**

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками переферийных устройств
2. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Периферийные устройства персонального компьютера — это устройства, которые подключаются к компьютеру с помощью специальных разъёмов.

Операционная система **Microsoft Windows XP** позволяет настроить работу периферийных устройств индивидуально, с учетом требований конкретного пользователя. Настройка включает выбор параметров и характеристик видеосистемы, клавиатуры и мыши.

Рассмотрим настраиваемые конечным пользователем параметры основных периферийных устройств компьютера.

1. Видеосистема

В операционной системе **Microsoft Windows XP** предусмотрена возможность выбора графического режима и настройки параметров ***видеосистемы***

компьютера, *включающей монитор и видеоадаптер*.

Графическая информация в видеосистеме представлена в дискретной форме. В процессе кодирования изображения производится его пространственная дискретизация.

Пространственная дискретизация – перевод графического изображения из аналоговой формы в цифровой компьютерный формат путем разбивания изображения на отдельные маленькие фрагменты (точки), где каждому элементу *присваивается код цвета.*

Качество кодирования изображения зависит от двух параметров.

Во-первых, качество кодирования изображения тем выше, чем меньше размер точки и соответственно большее количество точек составляет изображение.

Во-вторых, чем большее количество цветов, то есть большее количество возможных состояний точки изображения, используется, тем более качественно кодируется изображение (каждая точка несет большее количество информации).

2. Клавиатура

Клавиатура – одно из важнейших устройств, используемое для ввода в систему команд и данных и представляющее собой небольшой компьютер.

Клавиатура ***состоит*** *из набора переключателей, объединенных в матрицу*. При нажатии клавиши *процессор*, установленный в самой клавиатуре, определяет координаты нажатой клавиши в матрице. Кроме того, *процессор клавиатуры*

определяет продолжительность нажатия и может обработать даже одновременное нажатие нескольких клавиш. В клавиатуре установлен *буфер* емкостью 16 байт, в который заносятся данные при слишком быстрых или одновременных нажатиях.

3. Манипулятор «мышь»

Очевидно, что манипулятор «мышь» - крайне важное устройство в составе персонального компьютера, поскольку вместе с клавиатурой постоянно используется для ввода информации и управления ею внутри компьютера.

По принципу действия мыши делятся на *оптико-механические* и *оптические*, а по своим управляющим возможностям – на *двухкнопочные* и *трехкнопочные*.

Основными компонентами мыши являются:

- корпус, который вы держите в руке и передвигаете по рабочему столу;
- датчик перемещения мыши;
- несколько кнопок для подачи или выбора команд;
- колесико прокрутки;
- кабель для соединения мыши с компьютером;
- разъем для подключения к компьютеру.

Несмотря на внешнее разнообразие, все устройства работают одинаково.

Встроенный в мышь *датчик* (*оптомеханический* или *оптический*) регистрирует перемещения устройства относительно опорной поверхности и преобразует их в электрические сигналы, которые по кабелю передаются в компьютер. Соответствующие электрические сигналы также генерируются в мыши при нажатии кнопок или вращении колесика прокрутки.

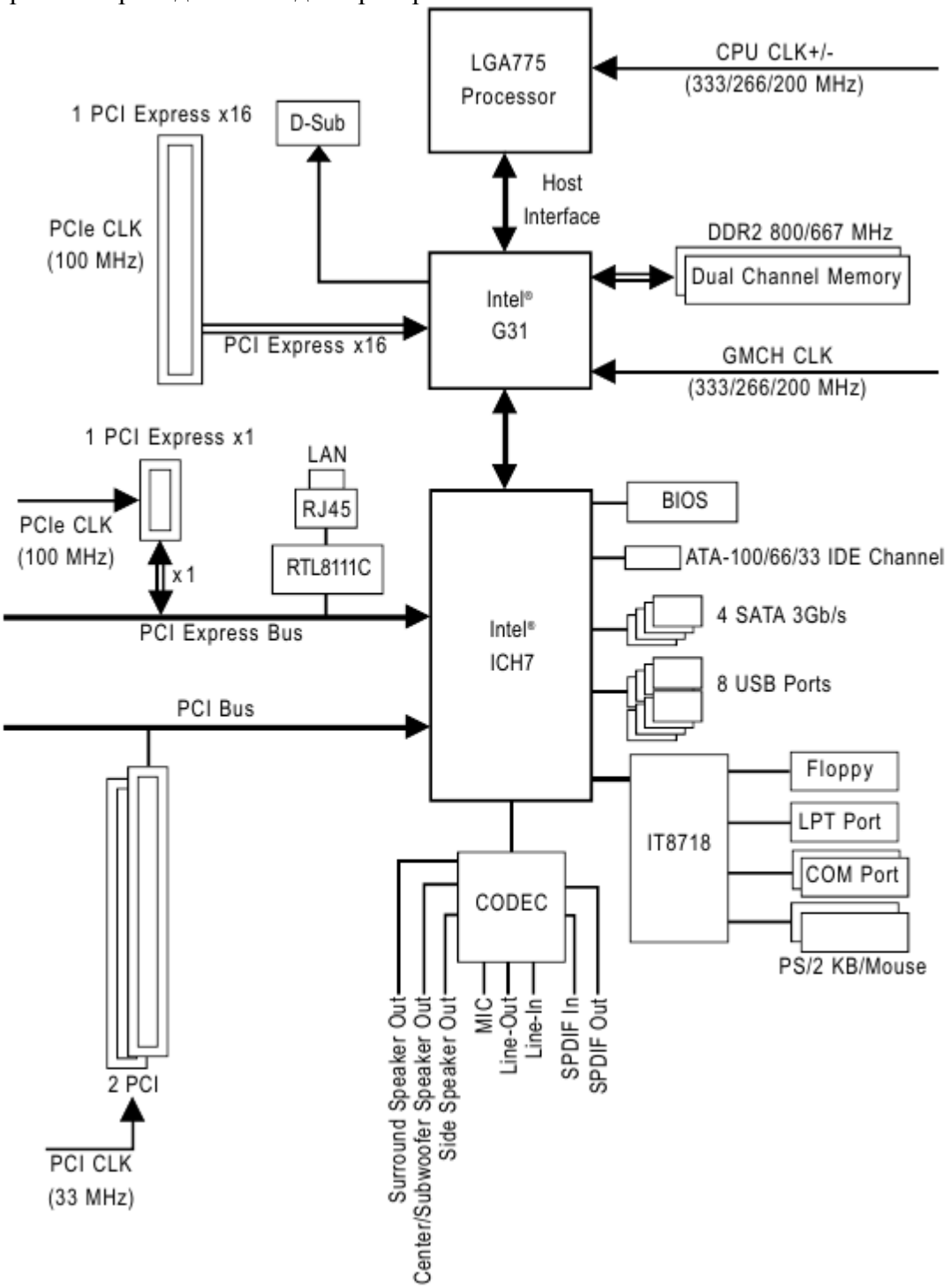
Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. **"Внутренние порты ПК. Изучение плат расширения ПК".**

Изучение производится на материнской плате ПК, т.к. на ней расположены все основные интерфейсы любого ПК.

Задание: изучить блок-диаграмму и компоновку материнской платы, зарисовать ее основные элементы в тетрадь, подписать их название/назначение. Зарисовать основные разъемы с подробным описанием каждого вывода разъема. Затем подключить необходимые/имеющиеся кабели к соответствующим местам материнской платы и предъявить ре-

зультат работы преподавателю для проверки.



Объясните блок-диаграмму материнской платы.

Задание 2

1. установить требуемые характеристики монитора: разрешение экрана, глубину цвета, частоту кадров, размер экранного шрифта;
2. вычислить объемы видеопамяти, необходимые для реализации заданной глубины цвета при различных разрешающих способностях экрана;
3. настроить требуемые параметры клавиатуры: интервал перед началом повтора символов, скорость повтора, скорость мерцания курсора;
4. настроить клавиши переключения языка клавиатуры;
5. настроить работу мыши: работу кнопок, указатель курсора, характеристики перемещения.

Время выполнения работы 90 мин;

Контрольные вопросы

1) В чем состоит суть метода пространственной дискретизации?

2) Объясните принцип формирования растрового изображения.

3) Какими параметрами задается графический режим, в котором изображения выводятся на экран монитора?

4) Как рассчитать количество цветов, отображаемых на экране монитора?

5) Какие компоненты входят в состав клавиатуры?

6) Опишите принцип действия клавиатуры.

7) Как в Microsoft Windows XP осуществляется поддержка различных языков?

8) Какими параметрами клавиатуры можно управлять в Microsoft Windows XP?

9) Перечислите основные компоненты мыши.

10) Опишите работу манипулятора «мышь».

11) Какие параметры мыши можно настроить в Microsoft Windows XP?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

7. Новожилов, Е.О. Компьютерные сети: учеб. пособие для студ. учреждений сред. проф. образования / Е.О.Новожилов, О.П.Новожилов. — 2-е издание перераб. и доп. — М. : Издательский центр «Академия», 2013. — 224 с.

8. Максимов, Н.В. Компьютерные сети: учебное пособие для студентов учреждений СПО [электронная версия]/ Н.В.Максимов, И.И.Попов. – 3-е изд., испр. и доп.,- М.: ФОРУМ, 2008. – 437 с.

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 6 «Исследование установки и настройки операционной системы Windows 2008 Server»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
2. научить учащихся основным способам настройки TCP/IP;

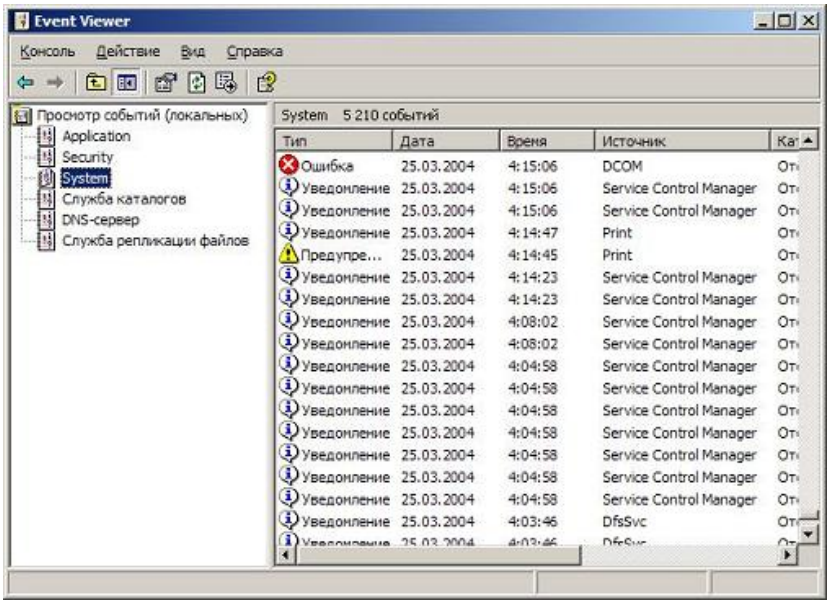
Краткие теоретические и справочно-информационные материалы по теме занятия.

Порядок работы

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

При запуске Windows Server автоматически запускается служба **Event Log** (Журнал событий).

Windows записывает все события в три журнала (или больше, если установлена служба Active Directory или DNS) и предоставляет возможность просматривать журналы с помощью утилиты **Event Viewer** (Просмотр событий).



Первое действие которое вы должны выполнить, при исследовании системы, просмотрите журналы событий на наличие ошибок. Если журнал содержит записи об ошибках, проанализируйте эти ошибки и постарайтесь решить проблему.

Программа установки устанавливает Windows Server в минимальной конфигурации, по соображениям безопасности. Изначально установлены только основные службы, обеспечивающие работоспособность ядра системы. В процессе настройки Windows Server, администратор может установить все необходимые службы и протоколы, обеспечивая при этом безопасный доступ к данным и ресурсам сервера.

К процессу первоначальной настройки Windows Server относятся: настройка набора компонентов Windows, настройка основных системных параметров Windows, установка дополнительных драйверов и устройств, установка дополнительных программ, установка пакетов обновлений и отдельных обновлений. Все эти операции желательно произвести сразу после установки.

Проверка параметров безопасности.

После установки операционной системы Windows Server проверьте следующие параметры безопасности сервера и при необходимости установите их:

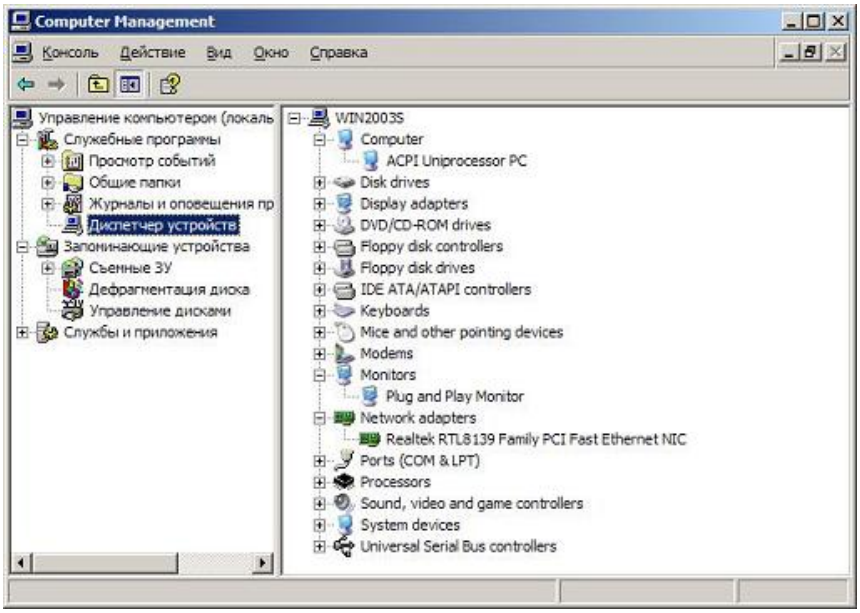
- Просмотр параметров запуска служб. Откройте окно Управление компьютером. В папке Службы узла Службы и приложения измените Тип запуска для служб таким образом, чтобы автоматически запускались только необходимые серверу службы. Кроме того, подтвердите, что все автоматически запускающиеся службы могут запускаться без вмешательства пользователя или без нескольких попыток.
- Просмотрите сведения о параметрах безопасности по умолчанию. В операционных системах семейства Windows Server по умолчанию включена конфигурация усиленной безопасности Internet Explorer. Параметры этой настройки позволяют повысить уровень безопасности компьютера, ограничивая возможность воздействия на него через

веб-сайты злоумышленников. В связи с этим при наличии соответствующего уровня безопасности может оказаться, что некоторые веб-сайты в процессе просмотра в Интернете и интранет-сетях отображаются в Internet Explorer с ошибками. Кроме того, при попытке доступа к сетевым ресурсам, таким как файлы общих папок UNC, может быть предложено ввести учетные данные. В значения параметров расширенной настройки безопасности можно вносить изменения.

- Просмотр открытых сетевых портов. Чтобы обеспечить защиту от несанкционированного доступа к серверам, закройте порты, которые не нужны системе для правильного функционирования. С помощью команды netstat можно просмотреть порты. Кроме того, полезно использовать сканер внешнего порта и сравнить полученные результаты с результатами выполнения команды netstat. До запуска сканера порта, в случае если он влияет на поведение системы или отключает существующие триггеры для обнаружения вторжения, необходимо уведомить об этом других системных администраторов.
- Переименование или отключение учетной записи администратора; установка или просмотр разрешений и учетных записей, относящихся к данному серверу. Переименуйте или отключите учетную запись администратора, созданную во время установки (ее нельзя удалить). Для настройки, задач архивирования, работы и использования сервера установите соответствующие учетные записи и разрешения. Для пользователей и администраторов ограничьте доступ до необходимого минимума. Например, для тех, кто выполняет только задачи архивирования, используйте группу Операторы архива. Кроме того, установите политики, необходимые для поддержки пользователями надежных паролей.
- Определение применяемых к серверу изменений системы безопасности. Связанные с безопасностью вопросы меняются в зависимости от решаемых сервером задач. Например, возникает вопрос о том, какой тип доступа необходим и каковы возможные последствия несанкционированного доступа к файловому серверу, которому нужен доступ к заданному файлу или папке. Для веб-сервера эти вопросы относятся к используемым веб-приложениям, связанным с их использованием рискам и настройкам, которые могут помочь снизить вероятность этих рисков.
- Настройка параметров аудита, установка системной защиты и антивирусного сканера. Просмотрите и примените параметры аудита, в том числе для событий безопасности, что позволит отслеживать все изменения в системе и защищать программное обеспечение от нежелательных изменений.
- Проверка правильности установки брандмауэра. Брандмауэр - это система безопасности, действующая как защитный барьер между сетью и внешним миром.

Проверка работоспособности устройств.

Программа установки Windows Server хорошо определяет и конфигурирует устройства, но не может решать проблемы связанные с отсутствием драйверов или конфликтом ресурсов. Для проверки работоспособности оборудования компьютера используйте **Диспетчер устройств** (Device Manager), который входит в состав службы **Управление компьютером** (Computer Management) из меню **Администрирование**.



В правой части окна **Computer Management** представлен список всех устройств, обнаруженных системой на вашем компьютере.

Все неработающие устройства помечены восклицательным знаком, указывающим на наличие проблем этого устройства.

Отключенные устройства помечены красным крестиком поверх значка.

При наличии конфликтов попробуйте изменить параметры устройства или обновить его драйвер. Чтобы просмотреть параметры устройства, выберите нужное устройство из списка и нажмите правую кнопку мышки. В контекстном меню выберите пункт **Свойства.**

Для установки оборудования, не поддерживающего Plug and Play, можно использовать **Мастер установки оборудования**, который можно запустить из **Панели управления**, выбрав компонент **Установка оборудования.**

Настройка основных системных параметров Windows.

После установки Windows Server системные параметры настроены на стандартные значения, обеспечивающие оптимальную работу устройств и служб. Вы можете изменить стандартные настройки системных параметров в зависимости от персональных параметров вашей сети и конфигурации вашего компьютера.

- **Задание размера журнала и параметров перезаписи для окна просмотра событий**. Определите размер журнала событий и параметры перезаписи в соответствии со своими требованиями и требованиями безопасности.

Чтобы установить параметры журнала событий выполните следующее: Запустите программу **Просмотр событий.**

- o В дереве консоли выберите журнал, параметры которого требуется установить.
- o В меню **Действие** выберите команду **Свойства.**
- o На вкладке **Общие** установите требуемые параметры.

- **Проверка оптимизации сервера**. Настройте параметры оптимизации сервера в соответствии с ролью, которую компьютер будет играть в организации.

Чтобы настроить параметры памяти данного компьютера

- o Откройте компонент **Сетевые подключения**.
- o Щелкните правой кнопкой мыши значок **Подключение по локальной сети** и выберите команду**Свойства.**

- В списке **Компоненты**, используемые этим подключением дважды щелкните компонент **Служба доступа к файлам и принтерам сетей Microsoft.**
- Обратите внимание, что по умолчанию в группе Критерии оптимизации выбран вариант макс. пропускная способность доступа к общим файлам. Чтобы отключить это вариант и уменьшить объем подкачки, установите переключатель в положение макс. пропускная способность для сетевых приложений.

- **Проверка настроек IP, DNS, WINS и шлюза по умолчанию**. Воспользуйтесь средствами администрирования для настройки и проверки сетевых параметров. Имеется также возможность открыть окно командной строки и ввести ipconfig /all, а затем проверить отображаемые настройки. Дополнительную информацию по настройке протокола TCP/IP можно посмотреть в разделе Установка и настройка сетевых протоколов Windows XP Professional данного курса. Об изменении настроек служб DNS и WINS будет рассказано позже.
- **Определение параметров файлов подкачки и дампов памяти**. Задайте размер и расположение файла на основе размеров памяти и использования сервера. Чтобы изменить параметры виртуальной памяти
  - Откройте окно **Управление компьютером.**
  - В дереве консоли щелкните правой кнопкой элемент **Управление компьютером** (локальным) и выберите команду **Свойства.**
  - На вкладке **Дополнительно** в группе Быстродействие нажмите кнопку **Параметры.**
  - В группе Виртуальная память нажмите кнопку **Изменить.**
  - В списке Диск выберите диск, содержащий файл подкачки, размер которого необходимо изменить.
  - Установите переключатель Размер файла подкачки для выбранного диска в положение Особый размер и введите новый размер файла подкачки в поле Исходный размер (МБ) или в поле Максимальный размер (МБ), а затем нажмите кнопку Установить. Нажмите кнопку **OK.**

Кроме того, следует задать параметры операционной системы, которые будут использоваться при внезапной ее остановке (например, параметры дампов памяти). Чтобы задать действия, выполняемые при внезапной остановке системы

- На панели управления откройте компонент **Система.**
- На вкладке **Дополнительно** в группе **Загрузка и восстановление** нажмите кнопку **Настройка.**
- В группе **Загрузка системы** установите флажок **Отображать варианты восстановления** и введите число секунд, в течение которых должен отображаться список параметров восстановления, прежде чем будет задействован параметр восстановления по умолчанию.
- В группе **Отказ системы** установите флажки, соответствующие действиям, которые должна будет выполнять система Windows при возникновении STOP-ошибки:
  - Если флажок Записать событие в системный журнал установлен, сведения о событии будут записаны в системный журнал.На компьютерах, управляемых системой Windows XP, можно включить или отключить эту возможность. Однако на компьютерах с операционными системами семейства Windows Server 2003 эту возможность отключить нельзя. Windows всегда записывает данные о событии в системный журнал.
  - Если установлен флажок Отправить административное оповещение, системный администратор будет оповещен о появлении STOP-ошибки. Для отправки администратору сообщения об ошибке по сети в системе Windows используется команда net send.
  - Если установлен флажок Выполнить автоматическую перезагрузку, система Windows автоматически перезапустит компьютер.
- В группе **Запись отладочной информации** выберите тип сведений, которые система Windows должна будет записывать в случае возникновения системной ошиб-

ки.

- Малый дамп памяти. Этот параметр задает запись минимального набора сведений, необходимых для определения причины неполадок. Для выбора этого параметра требуется, чтобы размер файла подкачки составлял как минимум 2 МБ на загрузочном томе компьютера. В этом режиме Windows создает новый файл (размером 64 КБ или 128 КБ) при каждой внезапной остановке системы. Такие файлы будут храниться в папке, заданной в поле Папка малого дампа.
- Дамп памяти ядра. Этот параметр записывает только память ядра; при этом сохраняется больше данных, чем в режиме малого дампа памяти, и на это требуется меньше времени, чем в режиме полного дампа памяти, при внезапной остановке системы. Файл будет сохранен в папке, указанной в поле Файл дампа памяти. Выбирая этот параметр, необходимо иметь на загрузочном томе достаточно большой файл подкачки. Необходимый размер файла зависит от размера ОЗУ компьютера, хотя максимальный объем места на диске, доступный для дампа памяти ядра, должен составлять 32 МБ. На 64-разрядных системах максимальный объем пространства, необходимый для дампа памяти ядра, должен быть равен объему ОЗУ плюс 128 МБ). Рекомендуемые размеры приведены в следующей таблице

Размер ОЗУ	Файл подкачки не должен быть меньше
256 МБ – 1 373 МБ	1,5-кратного размера ОЗУ
1 374 МБ и больше	32-разрядная система: 2 ГБ плюс 16 МБ 64-разрядная система: размер ОЗУ плюс 128 МБ

-
- Полный дамп памяти. Этот параметр недоступен на компьютерах с объемом ОЗУ более 2 ГБ. В этом режиме записывается все содержимое системной памяти при внезапной остановке системы. При выборе этого параметра необходимо иметь файл подкачки на загрузочном томе, равный физической оперативной памяти плюс одиннадцать мегабайт (МБ). Файл будет сохранен в папке, указанной в поле Файл дампа памяти.

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 7 «Исследование настройки сети в операционной системе Windows 2003 Server»

Цель работы: В результате выполнения лабораторной работы обучающиеся изучат способы диагностики настроек стека протоколов TCP/ IP; получить сведения о настройке TCP/IP для работы с DHCP сервером.

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
2. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Когда команда **ipconfig** выполняется с параметром **/all**, она выдает подробный отчет о конфигурации всех интерфейсов, включая все настроенные последовательные порты. Результаты выполнения команды **ipconfig /all**можно перенаправить в файл и вставить в другие документы. Можно также использовать эти результаты для проверки конфигурации TCP/IP на всех компьютерах сети и для выявления причин неполадок TCP/IP-сети.

Устраняя неполадки сетевых соединений TCP/IP, начинайте с проверки конфигурации TCP/IP на компьютере, на котором возникли эти неполадки. Если компьютер настроен на использование DHCP и получает конфигурацию от DHCP-сервера, можно инициировать обновление аренды, выполнив команду **ipconfig /renew.**

Когда выполняется команда **ipconfig /renew**, все сетевые адаптеры компьютера, на котором используется DHCP (за исключением тех, которые настроены вручную), пытаются связаться с DHCP-сервером и обновить имеющиеся или получить новые конфигурации. Можно также выполнить команду **ipconfig** с параметром **/release**, чтобы немедленно освободить текущую конфигурацию DHCP для узла.

Команда **ping** позволяет проверить работоспособность IP-соединения. С помощью команды **ping** можно отправить эхо-запрос ICMP нужному узлу, используя его имя или IP-адрес. Используйте команду **ping** всегда, когда требуется проверить, может ли узел подключиться к сети TCP/IP и ее ресурсам. Команду **ping** можно также использовать для выявления неполадок сетевых устройств и неправильных конфигураций.

Как правило, рекомендуется проверять наличие маршрута между локальным компьютером и узлом сети, обращаясь сначала к узлу с помощью команды **ping** и его IP-адреса. Для этого выполните следующую команду:

ping*IP_адрес*

Протокол ARP (Address Resolution Protocol) позволяет узлам определять аппаратные адреса сетевых интерфейсов других узлов, расположенных в той же физической сети, по IP-адресам этих узлов. Для более эффективного использования ARP каждый компьютер кэширует сопоставления IP-адресов с аппаратными адресами, устраняя тем самым повторяющиеся широковещательные запросы ARP.

Для просмотра и изменения таблицы ARP на локальном компьютере можно использовать команду **arp**. Команда**arp** служит для просмотра кэша ARP и устранения неполадок с разрешением адресов.

Порядок работы

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

1. Просмотрим сетевые настройки в данный момент командой *ipconfig*

2. Настроим сетевые параметры:

- IP-адрес сервера: 192.168.0.151
- Маска сети: 255.255.255.0
- Шлюз: 192.168.0.151
- DNS-сервер: 8.8.8.8
- DNS-сервер (второй): 8.8.4.4 (не обязательно, но рассмотрим)

Чтобы посмотреть какие интерфейсы присутствуют в системе, выполните команду:

netsh interface ipv4 show interfaces

Запомните число, указанное в графе «Инд» (**в английской версии «*Idx*»)** для сетевого адаптера, которому вы хотите установить **статический IP адрес**. В данном случае, в сервере только один сетевой интерфейс. Если на Вашем компьютере более одного сетевого адаптера, запишите номер, соответствующий нужному сетевому адаптеру.

В командной строке введите в одну строку:

netsh interface ipv4 set address name="Подключение по локальной сети" source=static address=192.168.0.151 mask=255.255.255.0 gateway=192.168.0.151

Чтобы не писать длинное название интерфейса **«Подключение по локальной сети»**, можно воспользоваться его идентификатором (в нашем случае 21). Тогда команда изменится на:

netsh interface ipv4 set address name="21" source=static address=192.168.0.151 mask=255.255.255.0 gateway=192.168.0.151

Проверяем сетевые настройки кодандой

ifconfig

Для настройки DNS (**name-21** — это наш сетевой идентификатор)

netsh interface ipv4 add dnsserver name="21" address=8.8.8.8index=1

Проверим настройки

ipconfig /all

Если Вам нужен второй DNS-сервер, укажите параметр index=2

netsh interface ipv4 add dnsserver name="21" address=8.8.4.4index=2

Все эти действия можно реализовать с помощью скрипта первичной настройки **sconfig**

config

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе вы-

полнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 8 «Исследование использования точки доступа»

Цель работы: Изучить принципы построения сетей Wi-Fi внутри помещений; построить сеть и настроить оборудование указанной сети.

Изучить влияние изменения схем множественного доступа, модуляции и кодирования на реальную скорость передачи информации в сети Wi-Fi, построенной по топологии BSS. Ознакомиться с программным обеспечением CommView for Wi-Fi, предназначенным для анализа пакетов, передаваемых по радиоинтерфейсу в беспроводной локальной сети IEEE 802.11.

В процессе занятия решаются следующие задачи:

3. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
4. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Описание принципов построения сетей Wi-Fi

Сети на базе оборудования 802.11 можно строить в соответствии с несколькими топологиями:

1. Топология “точка – множество точек”. В терминологии Wi-Fi данная топология носит название Базовая Зона Обслуживания (*Basic Service Set – BSS*). В данном варианте построения все пользовательские станции находятся в зоне действия станции, называемой точкой доступа (*Access Point – AP*). Все пакеты, передаваемые одной станцией из сети для другой, поступают сначала на точку доступа, а затем на станцию-получателя. При дальнейшем конфигурировании точки доступа такую топологию будем называть **Инфраструктурой** (*Infrastructure*).
2. Топология “точка-точка”. В терминологии Wi-Fi данная топология носит название Независимая Базовая Зона Обслуживания (*Independent Basic Service Set – IBSS*). Соединения такого типа устанавливают между станциями пользователей без использования точки доступа. Теоретически в данную сеть может входить неограниченное количество пользовательских станций. Такая топология называется также *ad-hoc*. Соединения, установленные в соответствии с данной топологией, носят ограниченный во времени, эпизодический характер. Чаще всего эту топологию используют при передаче какой-либо информации с одного компьютера на другой при отсутствии установленной точки доступа.
3. Топология Расширенная Зона Обслуживания (*Extended Service Set*). При данном построении сеть содержит несколько точек доступа, которые взаимодействуют как с пользовательскими станциями в зоне обслуживания, так и с другими точками доступа.

В данной работе рассмотрим построение BSS. В качестве оборудования используем точку доступа D-Link AirPlus XtremeG DWL-AP2100, а также несколько сетевых плат (пользовательских станций) D-Link AirPlus XtremeG DWL-G520. Характеристики указанного оборудования представлены в приведенных ниже таблицах.

Табл. 1 Технические характеристики беспроводного адаптера D-Link AirPlus XtremeG DWL-G520

Поддерживаемые стандарты	IEEE 802.11 IEEE 802.11b IEEE 802.11g
Дальность действия	Внутри помещений – до 100 м Снаружи помещений – до 400 м
Рабочие температуры	0° C - 55° C
Диапазон частот	2,4 ГГц – 2,462 ГГц
Скорости передачи данных	54 Мбит/с 48 Мбит/с 36 Мбит/с 24 Мбит/с 22 Мбит/с 18 Мбит/с 12 Мбит/с 11 Мбит/с 9 Мбит/с 6 Мбит/с 5.5 Мбит/с 2 Мбит/с 1 Мбит/с
Чувствительность приемника при вероятности ошибочных пакетов < 8% и при размере пакета 1024 байт	54 Мбит/с OFDM, -71 дБм 48 Мбит/с OFDM, -72 дБм 36 Мбит/с OFDM, -77 дБм 24 Мбит/с OFDM, -80 дБм 22 Мбит/с PBCC, -80 дБм 18 Мбит/с OFDM, -82 дБм 12 Мбит/с OFDM, -86 дБм 11 Мбит/с CCK, -84 дБм 9 Мбит/с OFDM, -87 дБм 6 Мбит/с OFDM, -89 дБм 5.5 Мбит/с CCK, -87 дБм 2 Мбит/с QPSK, -90 дБм 1 Мбит/с BPSK, -92 дБм
Мощность излучения	802.11b - 14 дБм 802.11g – 16 дБм
Ток потребления	Режим энергосбережения – 28 мА Режим ожидания – 4,66 мА Режим передачи – 248 мА
Вид модуляции	OFDM, CCK, QPSK, BPSK

Табл. 2 Технические характеристики точки доступа D-Link AirPlus XtremeG DWL-2100AP

Поддерживаемые стандарты	IEEE 802.11g IEEE 802.11 IEEE 802.11b IEEE 802.3 IEEE 802.3u
Дальность действия	Внутри помещений – до 100 м Снаружи помещений – до 400 м
Рабочие температуры	0° C - 55° C
Диапазон частот	2,4 ГГц – 2,4835 ГГц
Скорости передачи данных по радиоканалу	54 Мбит/с 48 Мбит/с 36 Мбит/с 24 Мбит/с 22 Мбит/с 18 Мбит/с 12 Мбит/с 11 Мбит/с 9 Мбит/с 6 Мбит/с 5.5 Мбит/с 2 Мбит/с 1 Мбит/с
Чувствительность приемника	54 Мбит/с OFDM, 10% PER, -66 дБм 48 Мбит/с OFDM, 10% PER, -71 дБм 36 Мбит/с OFDM, 10% PER, -76 дБм 24 Мбит/с OFDM, 10% PER, -80 дБм 18 Мбит/с OFDM, 10% PER, -83 дБм 12 Мбит/с OFDM, 10% PER, -85 дБм 11 Мбит/с CCK, 8% PER, -83 дБм 9 Мбит/с OFDM, 10% PER, -86 дБм 6 Мбит/с OFDM, 10% PER, -87 дБм 5.5 Мбит/с CCK, 8% PER, -85 дБм 2 Мбит/с QPSK, 8% PER, -89 дБм 1 Мбит/с BPSK, 8% PER, -90 дБм
Мощность излучения	802.11b - 14 дБм 802.11g – 16 дБм
Коэффициент усиления антенны	2 дБм

Порядок работы

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

Настройка точки доступа

Для настройки точки доступа можно использовать специальное программное обеспечение, поставляемое на диске, который прилагается к точке доступа при ее покупке. Однако для удобства пользователей точка доступа может быть сконфигурирована с помощью программы Internet Explorer (или любого другого Интернет браузера). Во втором случае возможна и удаленная настройка точки доступа.

В этой работе в качестве браузера будем использовать Internet Explorer. В компьютере, используемом для настройки, обязательно наличие сетевой Ethernet платы, так как конфигурирование производят по Ethernet интерфейсу. При этом в настройках TCP/IP стека данной сетевой платы должен быть указан IP адрес, принадлежащий той же подсети, в которой находится IP адрес точки доступа. По умолчанию продуктам D-Link присваи-

вают следующий IP адрес: 192.168.0.50. Следовательно, IP адрес сетевой платы, к которой подключают точку доступа, должен быть вида 192.168.0.XXX, где XXX – любое число в диапазоне от 1 до 255 (кроме 50).

После согласования IP адресов точки доступа и сетевой платы можно приступать непосредственно к настройке AP. Для этого необходимо запустить программу MS Internet Explorer, находящуюся на рабочем столе и ввести в поле адреса следующий адрес: **http://192.168.0.50,** при этом на экране появляется окно, изображенное на рис. 1.

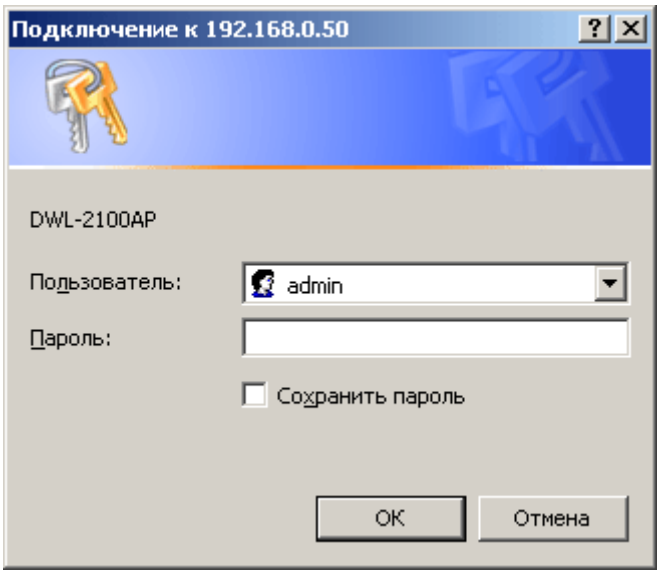


Рис. 1 Окно ввода пароля

Введите имя пользователя **admin**, а поле пароля оставьте пустым. После этого на экране появится следующее окно (см. рис. 2).

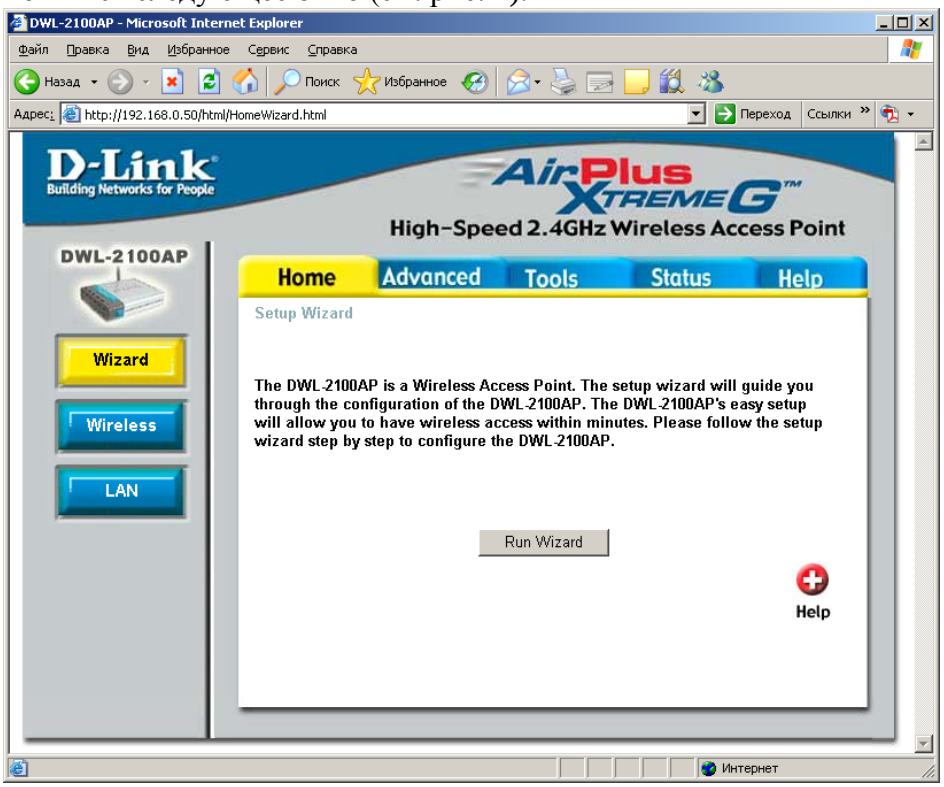


Рис. 2 Окно первоначальной настройки точки доступа

Для настройки точки доступа начните с нажатия на кнопку **Wireless** (*Настройки беспроводного интерфейса*). При этом на экране появится окно, изображенное на рис. 3.

В данном окне можно указать следующие параметры настройки:

1. **Wireless Band** (*диапазон частот*). В данном случае точка доступа работает в диапазоне частот 2,4 ГГц, определенном спецификациями IEEE 802.11b и g.
2. **Mode** (*режим работы*). Существует возможность выбора одного из пяти режимов работы:
   a. **Access Point** (*Точка Доступа*) – этот режим предполагает работу устройства непосредственно в качестве точки доступа.
   b. **Wireless Client** (*Беспроводной Клиент*) – режим работы, в котором точка доступа выступает в качестве обычной пользовательской станции. При этом требуется указать MAC адрес удаленной точки доступа, к которой будет подключена данная точка доступа, настроенная в режим станции пользователя.
   c. **WDS** (*Беспроводной Мост*) – режим работы, позволяющий объединить две или более беспроводных локальных сети. При этом функции беспроводного моста аналогичны функциям обычного моста, применяемого в проводной сети Ethernet. Этот режим используют для построения сети простейшего типа по топологии ESS.
   d. **WDS with AP** (*Мост, работающий с точкой доступа*) – этот режим используют для создания сложных сетей по топологии ESS. Соединяясь, точки доступа образуют сеть типа точка – множество точек, в центре которой находится AP, работающая в режиме WDS with AP.
   e. **Repeater** (*Повторитель*) – режим работы, применяемый для расширения зоны обслуживания какой-либо точки доступа. Повторитель использует протоколы физического уровня модели OSI.

3. **SSID** (*идентификатор зоны обслуживания*). Точка доступа передает данный идентификатор в кадрах маяка, который принимают все пользовательские станции в зоне обслуживания. По SSID абонентские станции могут выбрать сеть, к которой они хотят подключиться. Именно этот идентификатор высвечивается в окне поиска доступных точек доступа при настройке абонентских станций. Другими словами он представляет собой «название» зоны обслуживания сети Wi-Fi.

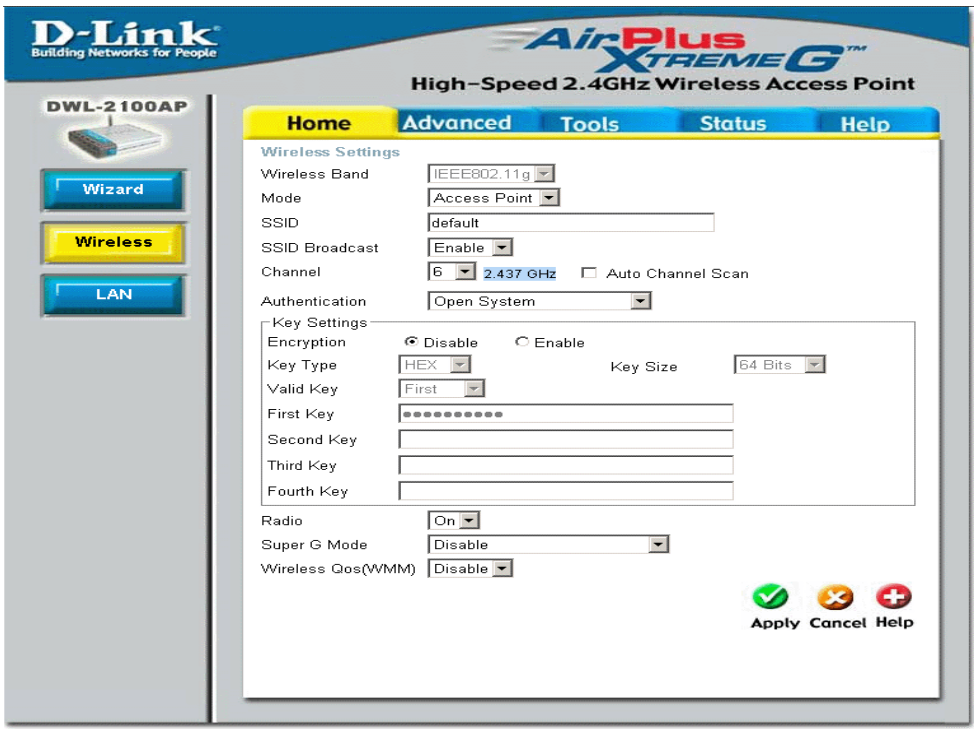


Рис. 3 Настройка беспроводного интерфейса

4. **SSID Broadcast** (*широковещание SSID*). Включает или отключает передачу SSID в широковещательном режиме.

5. **Channel** (*канал*). В данном поле задается номер канала, на который настроена точка доступа. Пользователь может выбрать один из 13 стандартных каналов, указанных в спецификациях 802.11g и предназначены для использования в Европе. Центральная частота канала указана рядом с выпадающим списком. Также канал может быть задан автоматически, после сканирования диапазона на наличие других точек доступа Wi-Fi, работающих рядом. Для этого следует отметить поле **Auto Channel Scan** (*автоматическое сканирование каналов*).

При выборе канала вручную необходимо учитывать другие точки доступа, которые работают поблизости. Для того чтобы посмотреть, какие точки доступа включены рядом, можно использовать ПО CommView for Wi-Fi или другие программные продукты (например NetStumbler). Просматривать все каналы диапазона позволяют также программы настройки некоторых беспроводных адаптеров. При этом следует избегать установленного по умолчанию канала 6, так как именно на этом канале наиболее вероятна работа других точек доступа.

6. **Authentication** (*аутентификация*). В данном поле требуется указать тип аутентификации, которая будет применяться при установлении соединения. На выбор пользователя предоставляются как методы аутентификации, предложенные в первоначальной спецификации стандарта IEEE 802.11 (**Open System** – *открытая*, **Shared Key** – *с помощью совместно используемых ключей*), так и методы, предложенные в более поздней спецификации по безопасности IEEE 802.11i (WPA-EAP и WPA-PSK).

Т.к. методы аутентификации и шифрования, описанные в первоначальной спецификации стандарта показали значительное количество уязвимостей, то для более надежной защиты и аутентификации в беспроводной локальной сети рекомендуется устанавливать методы WPA.

7. **Key Settings** (*настройка ключей шифрования*), **Radius Server Settings** (*настройка сервера аутентификации RADIUS*) или **PassPhrase Settings** (*настройка пароля для WPA*).

Для различных режимов защиты, выбранных в предыдущем поле, необходимо ввести разные настройки. Настройка ключей шифрования используется при выборе открытой аутентификации или аутентификации с совместно используемыми ключами.

Для того чтобы включить или отключить шифрование в одном из указанных режимов необходимо выбрать соответствующее поле рядом с отметкой **Encryption** (*шифрование*). При включении функции шифрования данных пользователю необходимо задать ключ шифрования. При этом ключи, указанные на точке доступа и на пользовательской станции должны быть одинаковыми. В окне, изображенном на рис. 3, можно указать формат ключа **HEX** (*шестнадцатеричный формат*) или **ASCII** (*формат ASCII*), длину ключа **Key Length** (*64, 128 или 256 бит*) и, наконец, сам ключ. Всего может быть задано до 4 различных ключей в полях **Key 1** – **Key 4**.

При использовании WPA-EAP (а также WPA2-EAP или WPA2-EAP) необходимо настроить сервер RADIUS.

При использовании WPA-PSK (а также WPA2-PSK или WPA2-PSK) необходимо выбрать пароль (в поле **PassPhrase**), а также указать период смены группового ключа в поле **Group Key Update Interval**.

8. **Radio** (*беспроводной модуль*). Позволяет включать или отключать радиомодуль точки доступа.

9. **Super G Mode** (*режим Super G*). Включение режима работы точки доступа с повышенной скоростью. Работа точки доступа в данном режиме выходит за рамки спецификаций стандарта IEEE 802.11.

10. **Wireless QoS (WMM)** (*поддержка QoS*). Позволяет включить или отключить поддержку спецификации IEEE 802.11e, вводящей приоритеты обслуживания станций и различные типы трафика для обеспечения качества обслуживания, необходимого при передаче мультимедиа трафика.

После того как все параметры в данном окне указаны, нажмите на кнопку **Apply** (*применить настройки*). Далее нажмите на кнопку **LAN** (*настройки локальной сети*). При этом на экране появится окно, представленное на рис. 4.

В этом окне требуется указать IP адрес, маску подсети (**Subnet Mask**) и адрес шлюза по умолчанию (**Default Gateway**), если выбран статический режим назначения адресов **Static (Manual)**. В режиме динамического назначения адресов **Dynamic DHCP** они будут назначены автоматически.

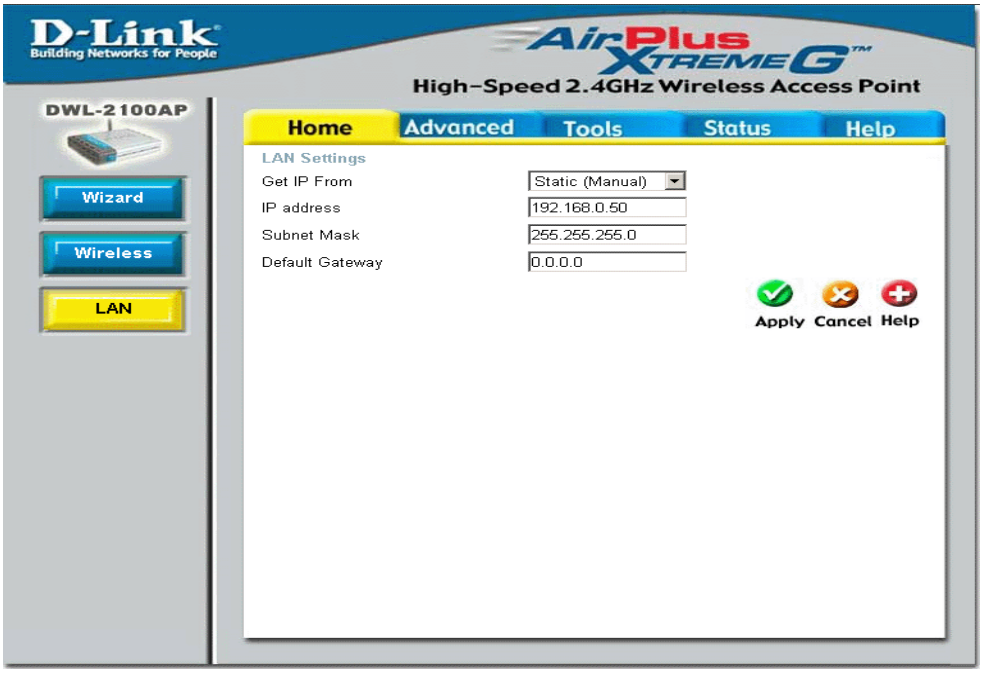


Рис. 4 Настройка локальной сети

После того как все параметры в данном окне указаны, нажмите на кнопку **Apply** (*применить настройки*). Далее перейдите к вкладке **Advanced** (*расширенные настройки*). Первая кнопка во вкладке **Advanced** позволяет настроить параметры, влияющие на производительность сети Wi-Fi (**Performance**).

Окно **Performance** представлено на рис. 5. В этом окне задают следующие параметры:

1. **Wireless Band** (*диапазон частот*). В данном случае точка доступа работает в диапазоне частот 2,4 ГГц, определенном спецификациями IEEE 802.11 b и g.

2. **Data Rates** (*скорости передачи*)

a. AUTO (*автоматически*) – при установке данного параметра скорость передачи устанавливается точкой доступа автоматически.

b. Одна из перечисленных скоростей передачи.

3. **Beacon Interval** (*маячковый интервал*) – номинальный период следования кадров маяка в мс. Рекомендованное значение для этого параметра составляет 100 мс.

4. **DTIM Interval** (*интервал Delivery Traffic Indication Message*) – установка счетчика окон для прослушивания широковещательных и групповых сообщений в маячковых интервалах. По умолчанию для данного счетчика устанавливают значение, равное 1.

5. **Fragment Length** (*длина фрагмента*) – значение длины пакета в байтах, при превышении которой данный пакет будет фрагментирован. По умолчанию эта длина составляет 2346 байт.

6. **RTS Length** (*длина пакета, при которой происходит активация механизма RTS/CTS*). Устанавливает минимальное значение длины кадра в байтах, для передачи которого будет использован механизм RTS/CTS. Рекомендованное значение для этого параметра составляет 2432 байта.

7. **Transmit Power** (*мощность излучения*) – используют для установки одной из возможных мощностей излучения. В данной точке доступа предусмотрены пять градаций мощности излучения: самый высокий уровень, половина, четверть, одна восьмая от максимального уровня или самый низкий.

8. **802.11g Only** (*только физический уровень 802.11g*) – позволяет включить в точке доступа режим использования только физического уровня IEEE 802.11g.

9. **Preamble** (*преамбулы*) – позволяет установить режим использования преамбул. Устанавливаются либо короткие и длинные преамбулы, либо только длинные.

При установке скорости передачи следует иметь в виду, что выбор наиболее высокой скорости передачи не всегда приводит к максимизации реальной скорости передачи данных. Это связано с тем, что при выборе более высокой скорости передачи снижается помехоустойчивость системы в целом (за счет применения модуляции с большим числом позиций и ухудшения параметров помехоустойчивого кодирования). Поэтому на практике при установке скорости 54 Мбит/с реальная скорость передачи информации может оказаться меньше, чем при установке скорости, например, в 48 Мбит/с.

Рис. 5 Окно настроек производительности

После того как все параметры в данном окне указаны, нажмите на кнопку **Apply** (*применить настройки*). Далее нажмите на кнопку **Filter** (*фильтрация*) для настройки фильтрации по MAC адресам (см. рис. 6).

В данном окне можно задать параметры фильтрации по MAC адресам, которая является одним из эффективных методов повышения безопасности в беспроводной сети. Для того чтобы отметить каким станциям разрешено, а каким запрещено подключаться к точке доступа, введите их MAC адреса в поле **MAC Address**, а затем в поле **Access Control** (*управление доступом*) отметьте запрет или разрешение на подключение к сети.

После того как список MAC адресов заполнен и каждому их них определен соответствующий статус, нажмите на кнопку **Apply** (*применить настройки*). Затем перейдите к вкладке **WLAN Partition** (*сегментация беспроводной локальной сети*). В открывшемся окне можно запретить или разрешить станциям, подключенным к данной точке доступа, обмениваться информацией друг с другом (поле **Internal Station Connection**). Также можно запретить или разрешить пользователям сети Ethernet, получать доступ к беспроводным станциям (поле **Ethernet to WLAN Access**). При этом доступ беспроводных станций к станциям сети Ethernet останется в любом случае открытым.

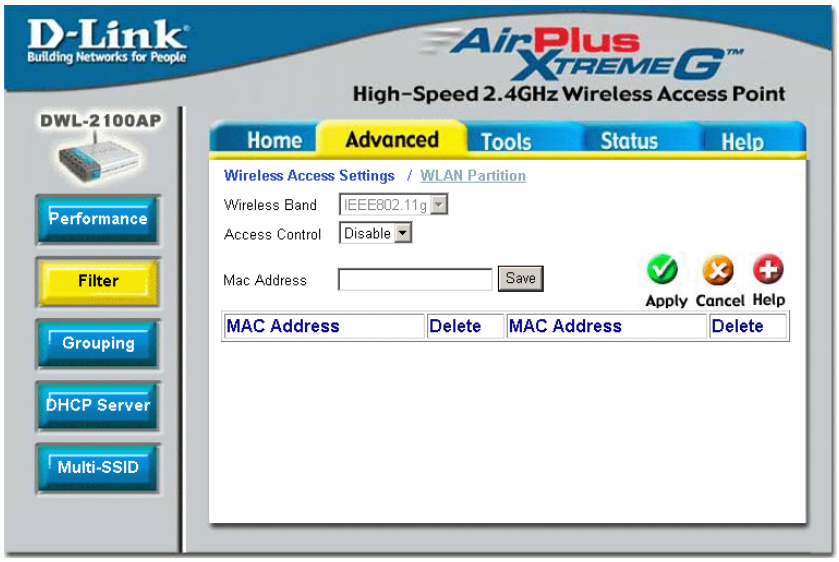


Рис. 6 Настройки фильтрации по MAC адресам

Далее можно приступить к настройкам балансировки нагрузки в беспроводной сети и ее интеграции с проводной Ethernet сетью. Для этого необходимо нажать на кнопку **Grouping** (*группирование*).

В данном окне (рис. 7) можно включить или отключить балансировку нагрузки для точки доступа. Режим балансировки нагрузки не определен в спецификациях стандарта IEEE 802.11, однако многие производители (например Cisco) включают его в свои точки доступа.

При настройке балансировки нагрузки можно воспользоваться ограничением количества подключаемых к точке доступа абонентских станций (поле **User Limit**). В поле **Link Integrate** (*интеграция*) возможно включить или отключить такой режим работы точки доступа, при котором в случае потери соединения Ethernet она также отключит все установившие с ней соединение абонентские станции. Для того чтобы посмотреть состояние канала Ethernet можно воспользоваться полем **Ethernet Link Status**, находящемся в этом же окне.

Настроив режим балансировки нагрузки, нажмите на кнопку **DHCP Server** (*настройка DHCP сервера*). При этом на экране появится окно, представленное на рис. 8.

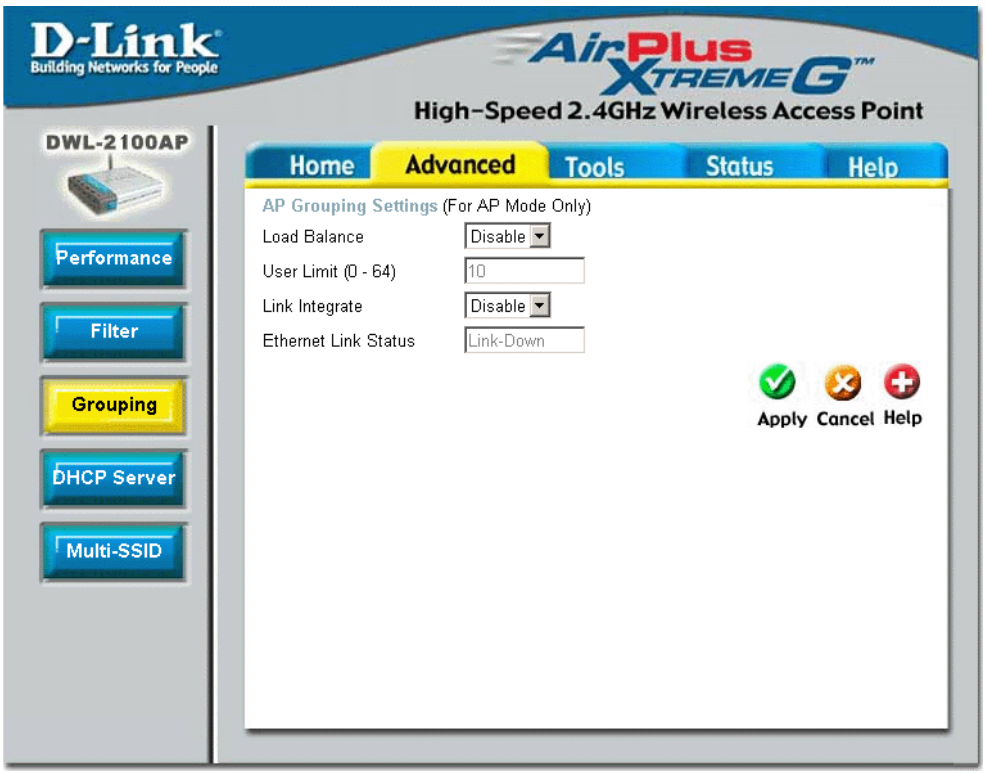


Рис. 7 Настройка группирования точки доступа

Точка доступа D-Link DWL-2100AP включает два режима работы, предназначенных для автоматического назначения IP адресов абонентским станциям. Первый режим называется **Dynamic Pool** и предполагает динамическое назначение IP адресов и их смену. Второй режим называется **Static Pool** и предполагает, что для каждой абонентской станции на точке доступа задается определенный IP адрес. Таким образом, в статическом режиме работы станции всегда присваивается один и тот же IP адрес.

В динамическом режиме необходимо задать диапазон IP адресов, которые будут назначаться подключающимся станциям. Для этого надо указать начальный IP адрес в поле **IP Assigned From**, а также количество адресов, которые DHCP сервер будет использовать при работе (поле **The Range of Pool**). Далее требуется задать маску подсети в поле **Subnet Mask**, IP адрес шлюза – в поле **Gateway**, адреса Wins и DNS серверов (в полях **Wins** и **DNS**, соответственно), имя домена в поле **Domain Name** и время смены назначенного станции IP адреса (поле **Lease Time**).

В статическом режиме указываются такие же параметры, однако, для каждой из абонентских станций в отдельности. Указание конкретной абонентской станции осуществляется путем введения ее MAC адреса в поле **Assigned MAC Address**.

Список станций, подключенных к точке доступа в настоящий момент времени (с указанием IP адресов), можно просмотреть во вкладке **Current IP Mapping List**.

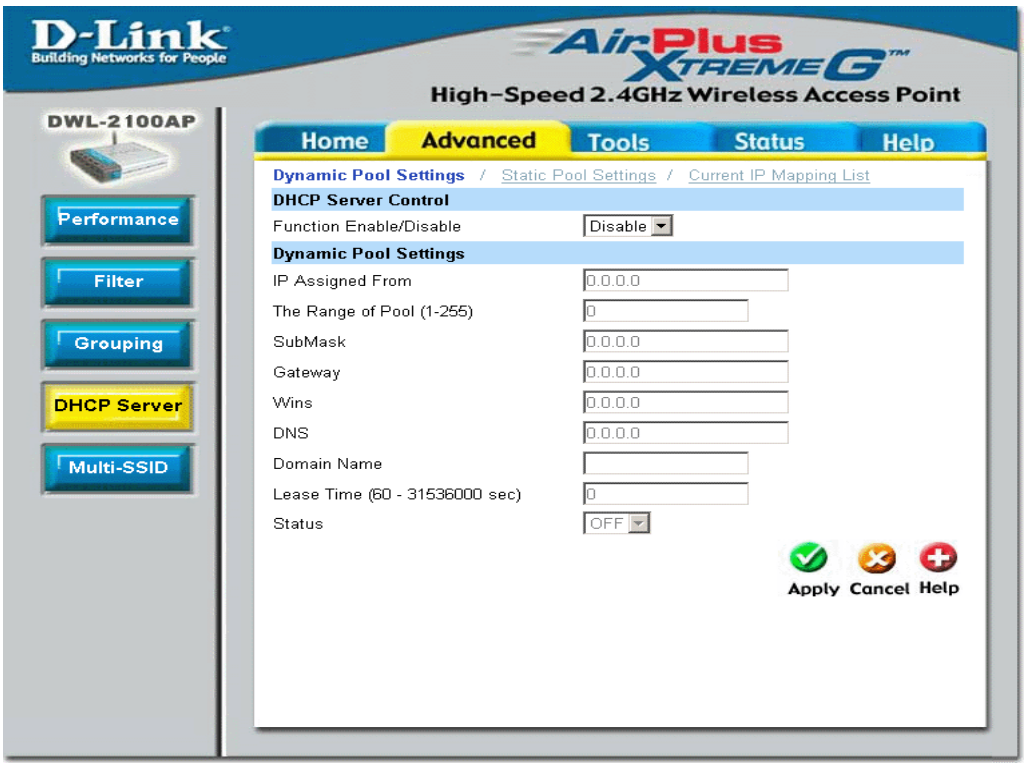


Рис. 8 Настройка DHCP сервера

Окончив настройку DHCP сервера точки доступа, нажмите на кнопку **Multi-SSID**. При этом на экране появится окно, изображенное на рис. 9.

Режим Multi-SSID позволяет эффективно разделять станции, находящиеся в зоне обслуживания точки доступа, на группы. В каждой из групп может быть установлен собственный уровень безопасности. Например, режим Multi-SSID часто используется для разделения абонентских станций сотрудников компании и пришедших клиентов.

В рассматриваемом режиме работы точка доступа образует до 7 виртуальных зон обслуживания вдобавок к основной рабочей зоне. При этом для каждой из зон обслуживания можно задать собственный SSID и уровень безопасности. При этом абонент, производящий сканирование доступных точек доступа, будет видеть только основной SSID, а все вторичные SSID будут от него скрыты. Таким образом, подключиться к одной из вторичных зон обслуживания сможет только абонент, знающий SSID вторичной зоны.

Настройка параметров Multi-SSID производится в окне, показанном на рис. 9. В поле **Index** выбирается номер зоны обслуживания. В поле **Security** задается тип шифрования-аутентификации для выбранной зоны обслуживания. Уровень безопасности основной зоны обслуживании не может быть изменен в этом окне.

Настроив при необходимости режим Milti-SSID, перейдите к вкладке **Tools** (*инструменты*).

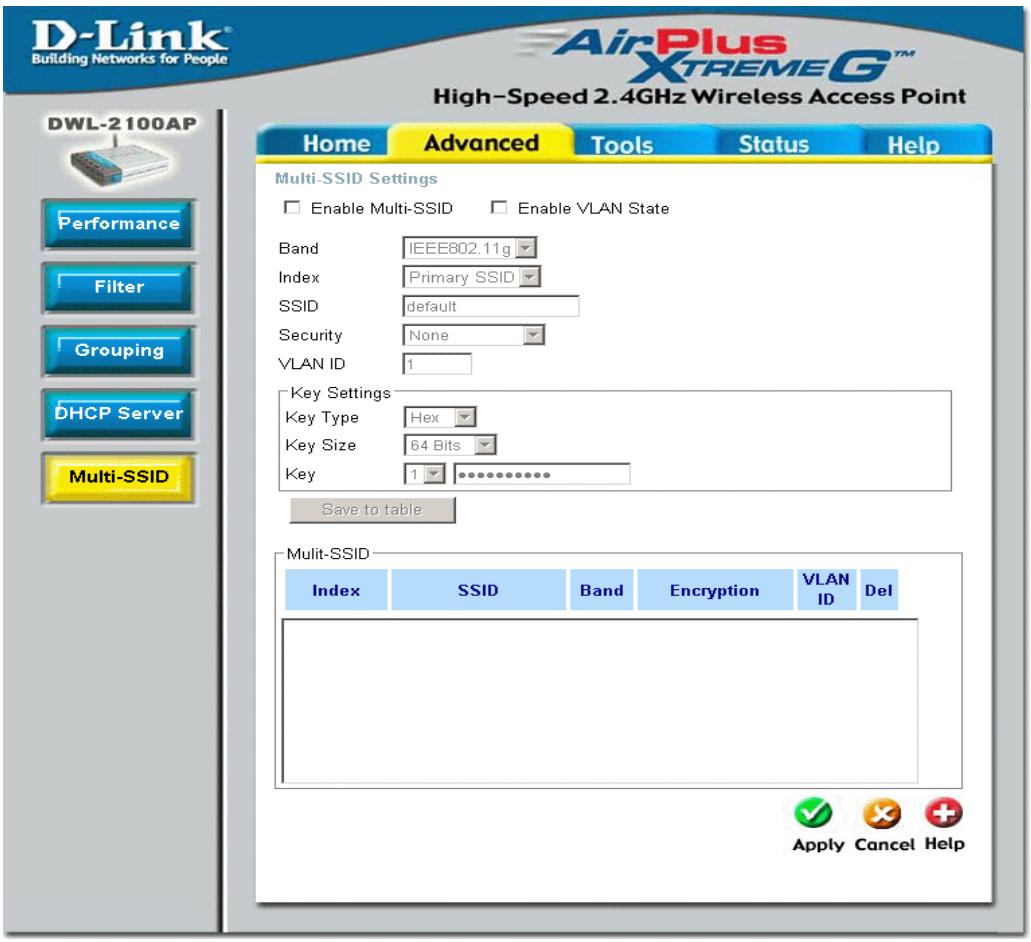


Рис. 9 Настройка режима Multi-SSID

Во вкладке **Tools** можно изменить способ администрирования точки доступа (нажав на кнопку **Admin**), применить настройки точки доступа или сбросить их до значений, установленных производителем (нажав на кнопку **System**), обновить прошивку устройства (нажав на кнопку **Firmware**) или сохранить/загрузить все настройки устройства (нажав на кнопку **Cfg File**).

Во вкладке **Status** (*состояние*) можно просмотреть информацию обо всех текущих настройках точки доступа (нажав на кнопку **Device Info**), статистическую информацию о пакетах (нажав на кнопку **Stats**), информацию о подключенных в настоящий момент к точке доступа станциях (нажав на кнопку **Client Info**), а также отчет по работе точки доступа с момента ее включения (нажав на кнопку **Log**).

Вкладка **Help** (*помощь*) содержит исчерпывающую информацию обо всех возможностях точки доступа и ее настройке.

Окончив настройку точки доступа, перейдите к настройке станций пользователя.

Конфигурирование станции пользователя

Настройку станции пользователя осуществляют специальной программой конфигурирования, которая имеет название D-Link AirPlus XtremeG Wireless Utility. При запуске данной программы появится окно, изображенное на рис. 10.

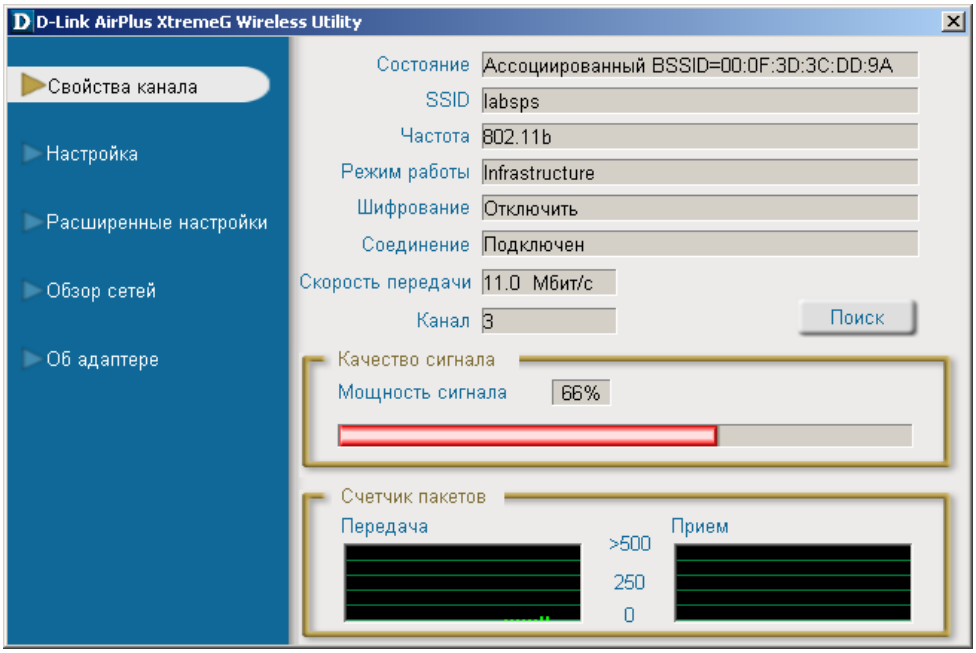


Рис. 10 Окно информации о канале в программе конфигурирования станции пользователя

В данном окне отображается следующая информация:

- О состоянии подключения адаптера (в данном примере адаптер ассоциирован с точкой доступа, имеющей MAC адрес 00-0F-3D-3C-DD-9A; также видно, что сеть построена по принципу BSS – имеется одна точка доступа, к которой подключают все пользовательские станции).
- Об идентификаторе зоны обслуживания (поле **SSID**).
- Об используемом физическом уровне (в данном примере 802.11b).
- О режиме работы (инфраструктура – Infrastructure).
- Об используемом типе шифрования.
- О скорости передачи в канале (в данном примере 11 Мбит/с).
- О номере канала, на который настроена станция пользователя (в данном примере используется 3 радиоканал).

Также в этом окне отображают три индикатора: индикатор мощности сигнала, индикаторы количества переданных пакетов и отправленных пакетов. Индикаторы количества пакетов начинают показывать какие-либо значения при передаче или приеме пакетов.

Если при запуске программы конфигурирования станция пользователя не ассоциирована с какой-либо точкой доступа автоматически, необходимо произвести настройку ее параметров. Для этого следует вызвать закладку **Настройка** в левой части окна программы. После этого появится окно, изображенное на рис. 11.

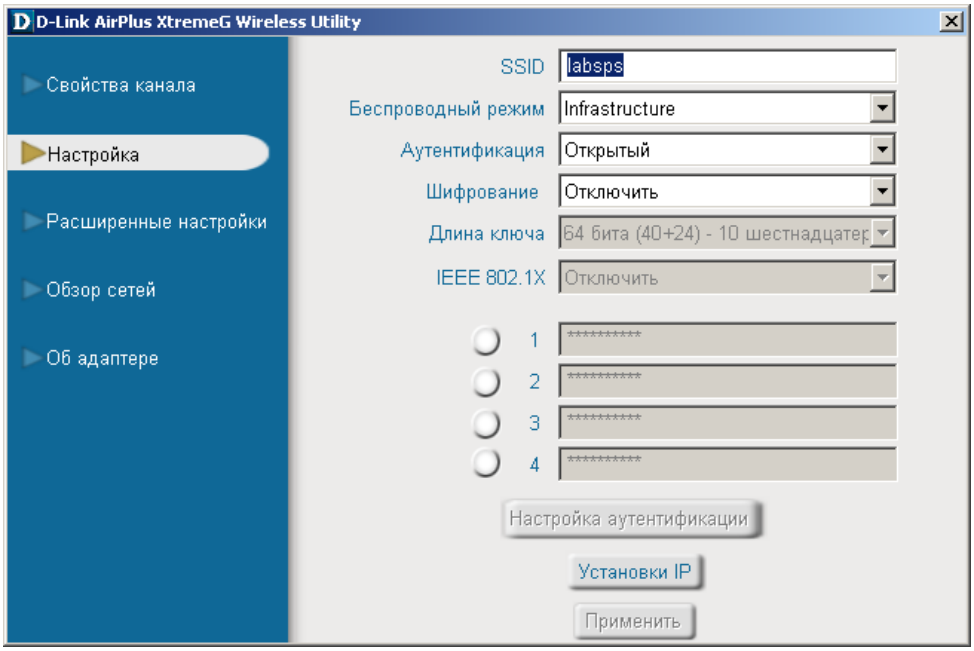


Рис. 11 Окно настройки адаптера в программе конфигурирования станции пользователя

В данном окне необходимо произвести следующие настройки:

1. Задать идентификатор зоны обслуживания **SSID**, аналогичный тому, который был задан для точки доступа, если построена сеть BSS. Если на точке доступа включен режим Multi-SSID, то вместо основного SSID может быть введен вторичный.
2. Задать режим работы станции: либо она работает в сети с точкой доступа (топология BSS) – тогда необходимо выбрать пункт **Infrastructure**, либо без точки доступа (топология IBSS) – тогда необходимо выбрать пункт **Ad-hoc**.
3. Указать тип аутентификации. В режиме BSS этот тип должен совпадать с установленным на точке доступа.
4. Указать тип шифрования. В режиме BSS этот тип должен совпадать с установленным на точке доступа.
5. Настроить параметры выбранного режима аутентификации и шифрования. (Для настройки используйте описание режимов аутентификации и шифрования, приведенное для точки доступа).
6. Настроить параметры IP адресации, нажав на кнопку **Установки IP**. При включении DHCP сервера на точке доступа указывать IP адрес адаптера не следует.

После выполнения описанных выше настроек нажмите на кнопку **Расширенные настройки**. При этом на экране появится окно, представленное на рис. 12.

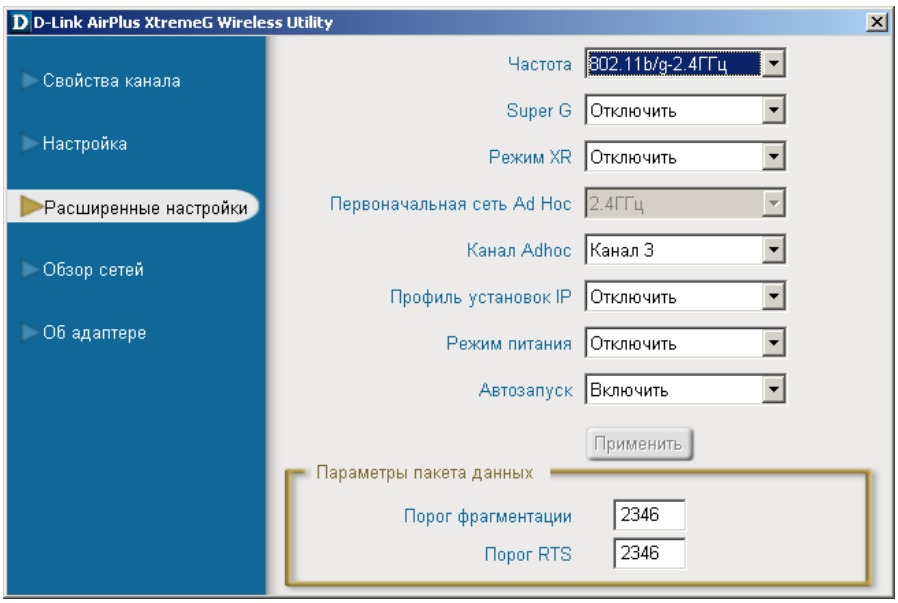


Рис. 12 Окно расширенных настроек в программе конфигурирования станции пользователя

В данном окне можно установить следующие параметры:

1. Установить частотный диапазон, используемый адаптером. Адаптеры, используемые в лаборатории, работают в частотном диапазоне 2.4 ГГц, описанном в спецификациях IEEE 802.11 b и g.
2. Установить режимы **Super G** и **XR**. Оба этих режима предназначены для повышения пропускной способности сети Wi-Fi, однако при этом они выходят за рамки спецификаций стандарта IEEE 802.11. Поэтому в указанных режимах работы станции пользователя могут быть совместимы не со всеми точками доступа различных производителей. При работе в сети, построенной на оборудовании различных производителей, рекомендуется не включать данные режимы.
3. Задать канал для работы станции пользователя в режиме Ad-Hoc Возможен выбор одного из 13 каналов.
4. Задать режим питания адаптера:
   a. Режим постоянного доступа
   b. Режим наивысшей экономии питания
   c. Режим экономии питания.
5. Установить порог фрагментации и порог применения процедуры RTS/CTS (см. аналогичные настройки в точке доступа).

В любой момент времени пользователь может просканировать диапазон частот и найти все точки доступа, работающие рядом. Для этого необходимо нажать на кнопку **Обзор сетей**, после чего на экране появится окно, изображенное на рис. 13.

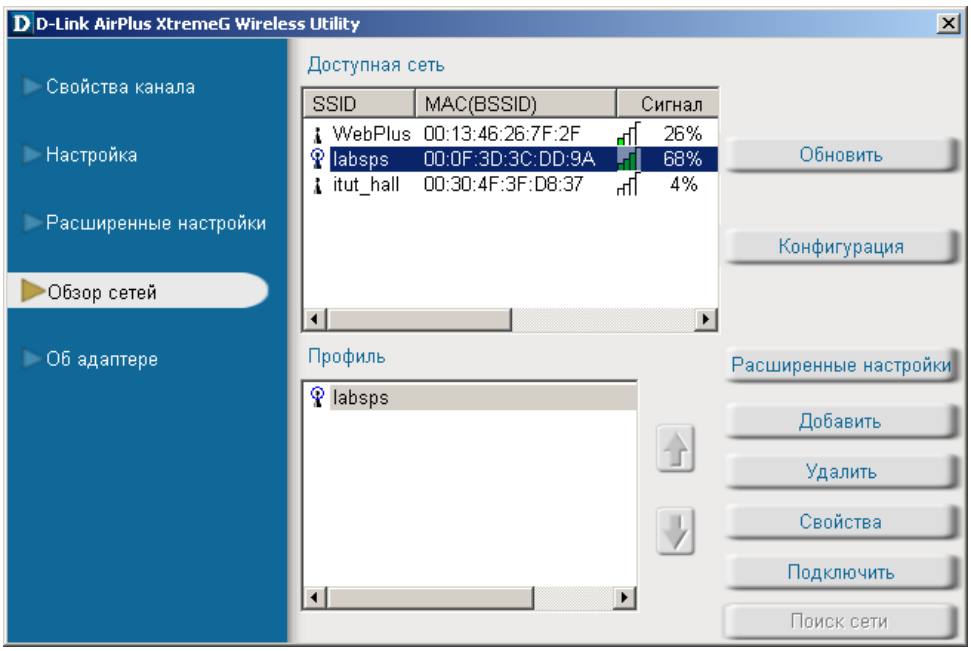


Рис. 13 Окно обзора доступных беспроводных сетей в программе конфигурирования станции пользователя

В этом окне показаны две области. Первая – область доступных сетей, отображающая все точки доступа и станции пользователей, в зоне действия которых находится данная станция. Справа от этой области расположены две кнопки: **Обновить** (которая позволяет обновлять информацию обо всех устройствах Wi-Fi, в зоне действия которых находится данная станция) и кнопа **Конфигурация** (которая позволяет просмотреть информацию о найденной точке доступа).

Вторая область, расположенная ниже, – область профилей. В этой области можно создавать профили для конкретных подключений. Профиль – это набор параметров, с которыми пользовательская станция будет подключаться к другой станции (в режиме ad-hoc) или точке доступа (в режиме infrastructure). Профиль включает в себя все опции, которые задавались в рассмотренных ранее окнах настроек пользовательской станции. Справа, расположены кнопки, позволяющие управлять профилями, а также выполнить подключение к выбранной точке доступа или другой станции.

Для просмотра информации о версии драйвера устройства, а также его MAC адресе нажмите на кнопку **Об адаптере**. При этом на экране появится окно, представленное на рис. 14

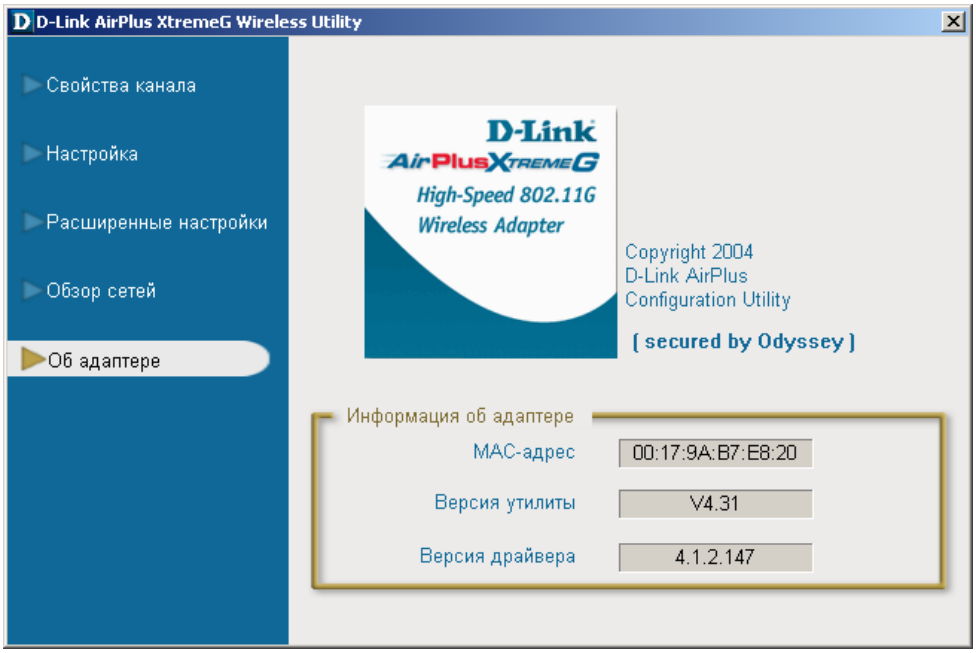


Рис. 14 Окно информации об адаптере в программе конфигурирования станции пользователя

Задание 2

Задание к выполнению

Проанализировать изменение реальной скорости передачи данных в беспроводной локальной сети Wi-Fi, построенной по топологии BSS, при изменении схем модуляции, кодирования и множественного доступа на физическом уровне стандарта IEEE 802.11.

Указания к выполнению работы

Пользуясь описанием выше настроить параметры точки доступа, заданные преподавателем. Установить соединение двух абонентских станций с точкой доступа. Пользуясь описанием, приведенным в приложении, подготовить станцию с установленным сетевым анализатором CommView for Wi-Fi к работе. Произвести сканирование диапазона (смотри *Приложение*), найти точку доступа, используемую для организации беспроводной локальной сети в лаборатории, и начать захват пакетов, передаваемых по найденному радиоканалу.

Установите на точке доступа скорость передачи 54 Мбит/с. На компьютере с анализатором протокола Wi-Fi откройте окно *Статистика*. Одновременно начните пересылку заданного файла с одной абонентской станции, подключенной к точке доступа, на другую абонентскую станцию. В окне статистики CommView for Wi-Fi замеряйте реальную скорость передачи файла в беспроводной локальной сети. Сохраните файл отчета вместе с графиками, пользуясь вкладкой *Отчет* в окне *Статистика*.

Повторите аналогичные измерения для других скоростей передачи, приведенных в табл. 3, передавая тот же файл, который использовали ранее.

Табл. 3

Задание	Скорость на АР
1	54 Мбит/с
2	36 Мбит/с
3	24 Мбит/с
4	11 Мбит/с
5	5,5 Мбит/с
6	1 Мбит/с

Приложение. Описание основных принципов работы с ПО CommView for Wi-Fi.

CommView for WiFi - это специальная версия ПО CommView, созданная для захвата и анализа сетевых пакетов в беспроводных сетях стандарта 802.11a/b/g. Она получает информацию от беспроводного сетевого адаптера и декодирует анализируемые данные.

С помощью CommView for Wi-Fi можно просматривать список сетевых соединений, IP-статистику и исследовать отдельные пакеты. Пакеты можно дешифровать с использованием пользовательских ключей WEP или WPA-PSK и декодировать вплоть до самого низкого уровня с полным анализом распространенных протоколов. Предоставляется полный доступ к необработанным данным. Перехваченные пакеты могут быть сохранены в файле для последующего анализа. Гибкая система фильтров позволяет отбрасывать ненужные пакеты или перехватывать только те пакеты, которые необходимы. Настраиваемые предупреждения позволяют сообщать пользователю о важных событиях, таких как подозрительные пакеты, высокая загрузка сети или неизвестные адреса.

CommView for WiFi – это полнофункциональный и доступный инструмент для администраторов беспроводных сетей, специалистов в области сетевой безопасности, сетевых программистов или тех, кто хочет видеть всю картину трафика в беспроводной сети. Эта программа работает в Windows 2000/XP/2003 и ей необходим совместимый беспроводной сетевой адаптер.

Для выполнения лабораторной работы необходимо ознакомиться со следующими функциями ПО:

- Сканирование
- Захват пакетов
- Обзор статистики захваченных пакетов

Сканирование

Для начала сканирования выберите пункт меню ***Файл > Начать захват***. На экране появится окно изображенное на рис. 15.

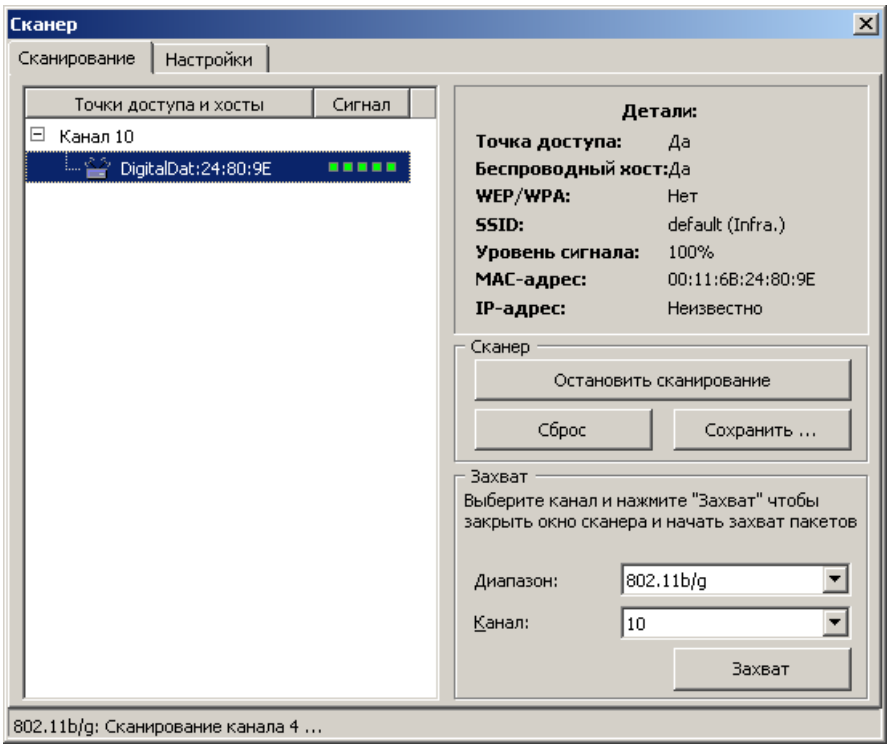


Рис. 15 Начальное окно сканирования доступных радиоканалов

В данном окне можно просканировать эфир на предмет сигналов от станций Wi-Fi, а также выбрать канал для мониторинга. Для начала мониторинга нажмите на кнопку **Начать сканирование**. Процесс сканирования циклический, т. е. программа “слушает” сигналы на первом канале, потом переключается на следующий канал и т. д., пока не достигнет последнего канала, после чего начнется новый цикл сканирования. Процесс сканирования будет остановлен нажатием кнопки **Остановить Сканирование**. Чтобы убрать всю собранную информацию, нажмите на кнопку **Сброс**. Чтобы сохранить отчет о сканировании в формате HTML, нажмите на кнопку **Сохранить**. Если сканирование закончено и стало известно, на каком канале необходимо осуществлять сбор пакетов, то в выпадающем списке **Диапазон** выберите диапазон (802.11b/g), а затем в выпадающем списке **Канал** выберите требуемый канал для захвата и нажмите на кнопку **Захват**.

Для того чтобы настроить более тонкие параметры сканирования выберите вкладку **Настройки**. На экране появится окно, изображенное на рис. 16.

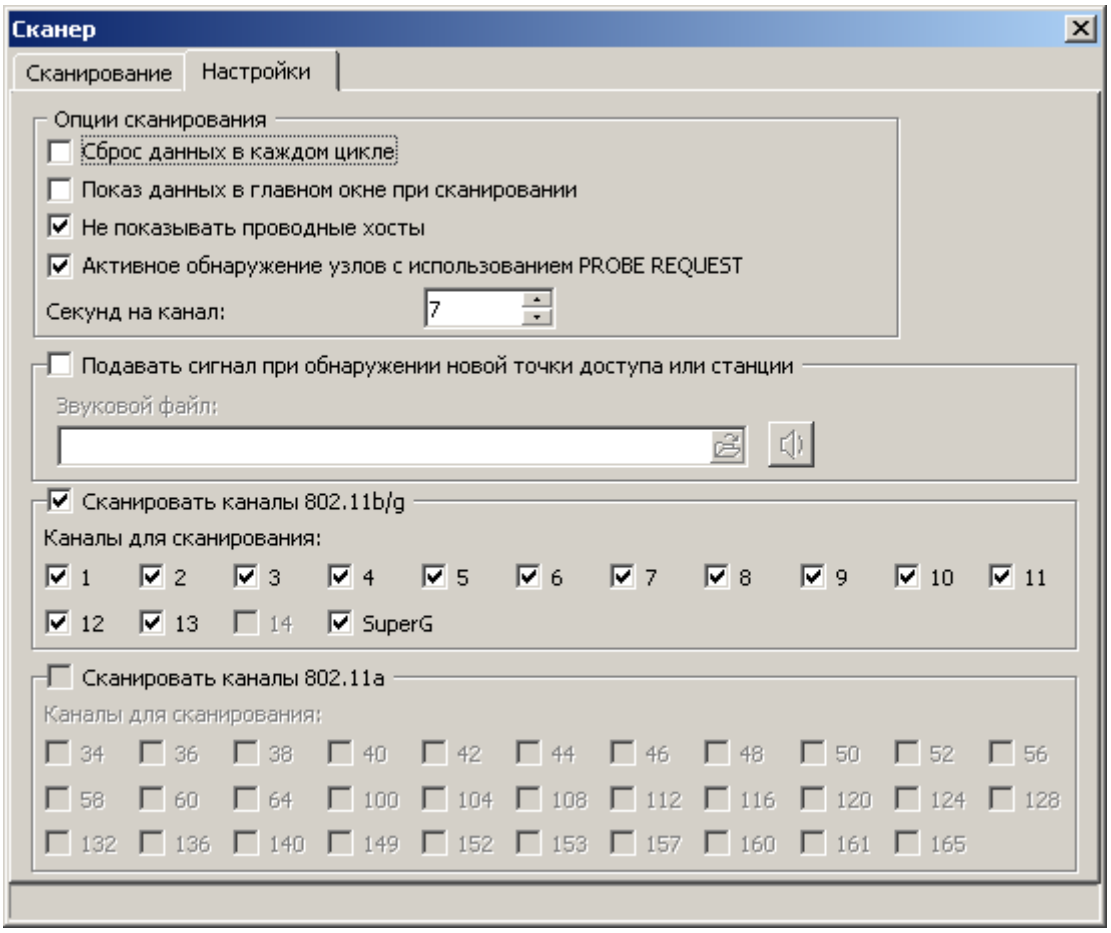


Рис. 16 Окно расширенных настроек сканирования

В этом окне можно задавать следующие параметры:

- **Сброс данных в каждом цикле** – если это поле отмечено, то перед началом нового цикла сканирования будет произведен сброс всех собранных ранее данных.
- **Показ данных в главном окне при сканировании** – показать пакеты, которые были перехвачены во время сканирования в главном окне программы (в закладках **Узлы**, **Каналы**, **Пакеты** и **Текущие IP-соединения**). Если опция выключена, пакеты, перехваченные во время работы сканера, нигде не будут зафиксированы.
- **Не показывать проводные хосты** – показывать только беспроводные хосты и точки доступа. Если опция выключена, сканер покажет проводные и беспроводные хосты просканированного сегмента. Помните, что включение этой опции может сделать

беспроводные хосты невидимыми, поскольку программа должна перехватить несколько пакетов для того, чтобы установить, является ли данный хост проводным или беспроводным.

- **Активное обнаружение узлов с использованием PROBE REQUEST** – позволяет периодически отправлять пакеты PROBE REQUEST. Эти пакеты помогают обнаруживать те точки доступа, которые не передают свой SSID (идентификатор зоны обслуживания).
- **Секунд на канал** – позволяет задать временной интервал, в течение которого сканер будет опрашивать один канал.
- **Подавать сигнал при обнаружении новой точки доступа или станции** – выбрать звуковой WAV-файл, который будет проигран при обнаружении новой точки доступа или станции. Для проверки WAV-файла нажмите на кнопку, расположенную справа от поля выбора файла.
- **Сканировать каналы 802.11b/g** и **Сканировать каналы 802.11a** – позволяет выбрать те или иные каналы из диапазона, которые будут просканированы. В любом из диапазонов требуется выбрать хотя бы один канал. Если сетевая плата, используемая для мониторинга, не поддерживает работу на физическом уровне 802.11a, то все каналы диапазона 5 ГГц будет неактивны.

Обзор статистики захваченных пакетов

Для того чтобы просмотреть статистику по захваченным пакетам, выберите пункт меню **Вид > Статистика**. При этом на экране появится окно, представленное на рис. 17.

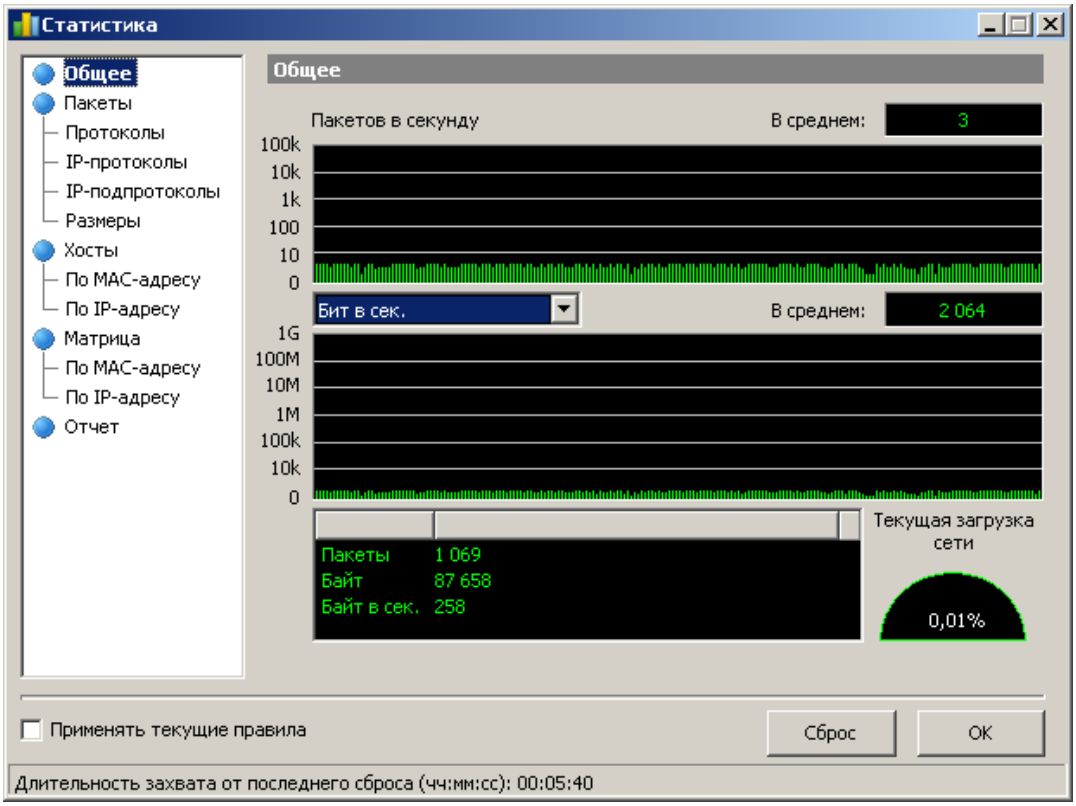


Рис. 17 Главное окно статистики по пакетам

В этом окне можно ознакомиться с такими параметрами сетевой статистики сегмента LAN, как количество пакетов в секунду, байтов в секунду или распределение протоколов Ethernet, IP и субпротоколов. Дважды щелкнув по диаграммам, их можно скопи-

ровать в буфер обмена Windows. Для удобства просмотра секторных диаграмм их можно вращать с помощью двух небольших кнопок в правом нижнем углу.

Данные каждой страницы можно сохранить или в формате bitmap или в текстовом файле CSV. Для этого воспользуйтесь контекстным меню или просто перетащите объект мышкой. Выбрав пункт меню **Отчет**, можно создавать автоматические отчеты в формате HTML или текстовом формате CSV.

Сетевая статистика может строиться на базе всех пакетов, проходящих через адаптер, или с учетом правил, установленных на данный момент. Если требуется, чтобы в статистике учитывались лишь текущие правила, следует отметить флаг **Применить текущие правила.**

Вкладка “Общее”

Вкладка общее (см. рис. 17) содержит гистограммы вида "Пакетов в секунду" и "Байт/бит в секунду", индикатор использования пропускной способности (удельный трафик, деленный на номинальную скорость сетевого адаптера или модемного соединения), а также общее количество пакетов и байт, переданных по выбранному каналу с начала захвата пакетов.

Вкладка “Протоколы”

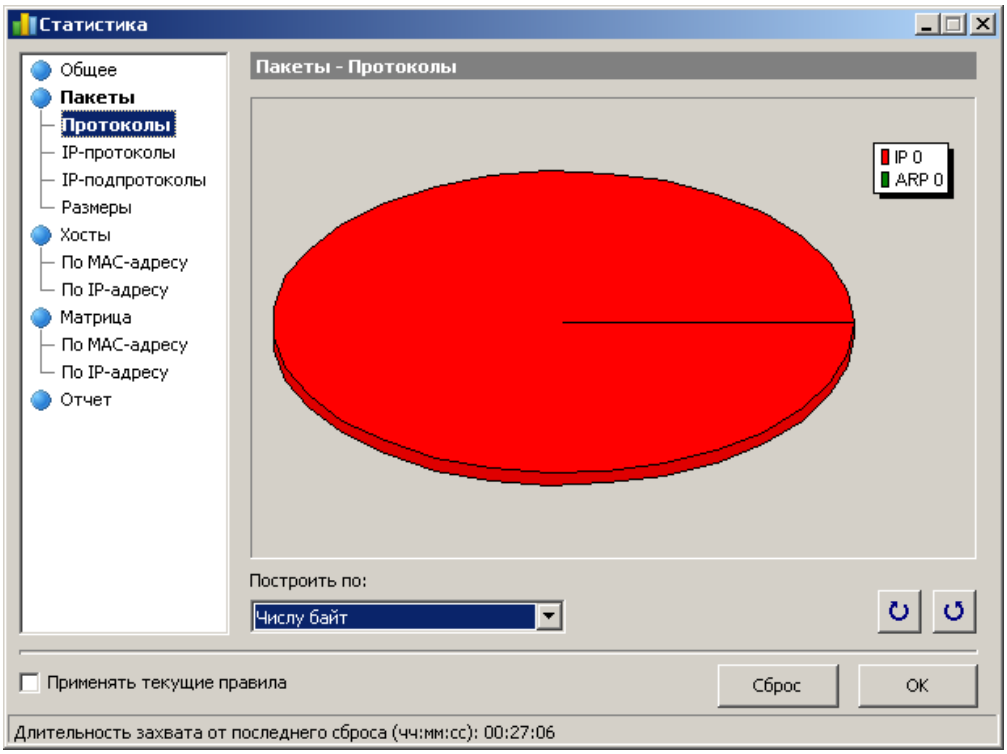


Рис. 18 Вкладка “Протоколы” в окне просмотра статистики

В этой вкладке отображается диаграмма распределения Ethernet-протоколов: ARP, IP, SNAP, SPX и т. д. В выпадающем меню **Построить по:** можно выбрать способ формирования диаграммы: по числу пакетов или по числу байт. Диаграмму можно вращать с помощью кнопок, находящихся в нижней части окна.

Вкладка “IP-протоколы”

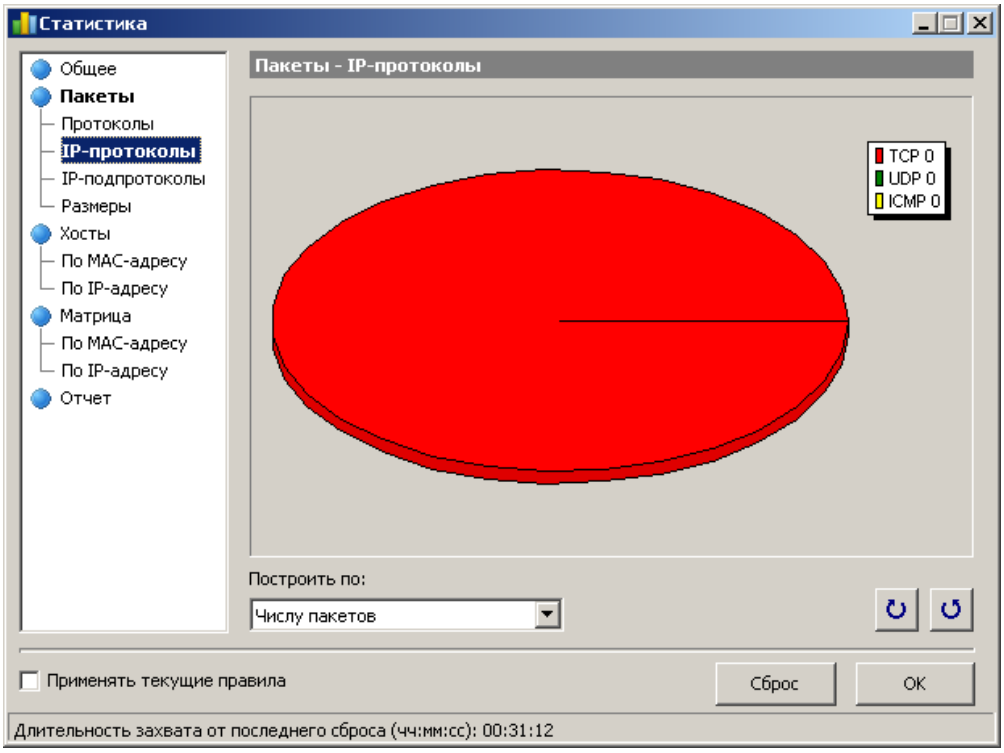


Рис. 19 Вкладка “IP-протоколы” в окне просмотра статистики

В данной вкладке отображается распределение IP-протоколов: TCP, UDP, ICMP. В выпадающем меню **Построить по:** можно выбрать способ формирования диаграммы: по числу пакетов или по числу байт. Диаграмму можно вращать с помощью кнопок, находящихся в нижней части окна.

Вкладка “IP-подпротоколы”

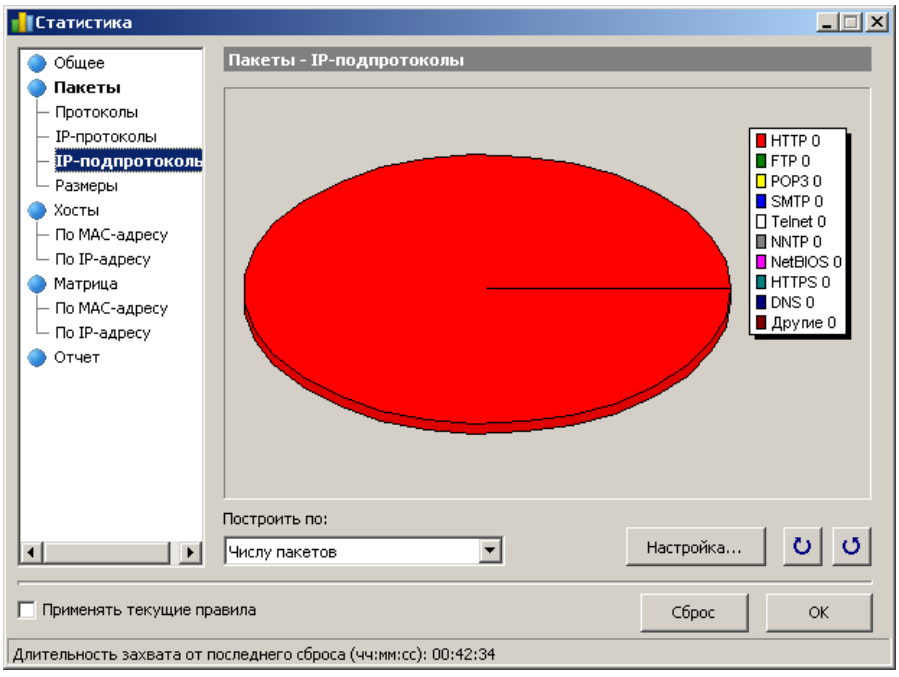


Рис. 20 Вкладка “IP-подпротоколы” в окне просмотра статистики

В данной вкладке отображается распределение основных IP-протоколов уровня

приложения: HTTP, FTP, POP3, SMTP, Telnet, NNTP, NetBIOS, HTTPS и DNS. Чтобы добавить другие протоколы, нажмите на кнопку **Настройка**. При этом на экране появится окно, изображенное на рис. 21.

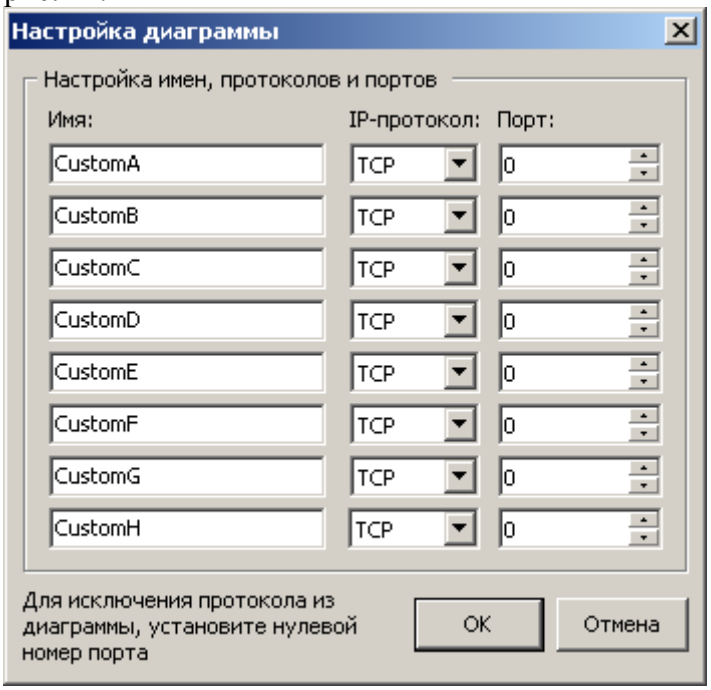


Рис. 21 Окно добавления пользовательских протоколов в диаграмму IP-подпротоколов

Здесь можно указать до восьми протоколов, вводя их название, тип протокола (TCP/UDP) и номер порта.

В выпадающем меню **Построить по:** можно выбрать способ формирования диаграммы: по числу пакетов или по числу байт. Диаграмму можно вращать с помощью кнопок, находящихся в нижней части окна.

Вкладка “Размеры”

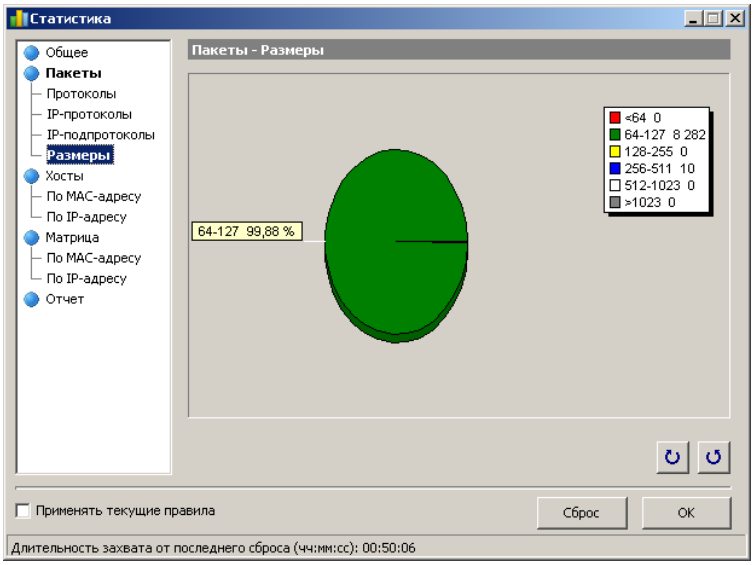


Рис. 22 Вкладка “Размеры” в окне просмотра статистики

В данной вкладке отображается диаграмма распределения размера пакетов. Диаграмму можно вращать с помощью кнопок, находящихся в нижней части окна.

Хосты по MAC-адресу

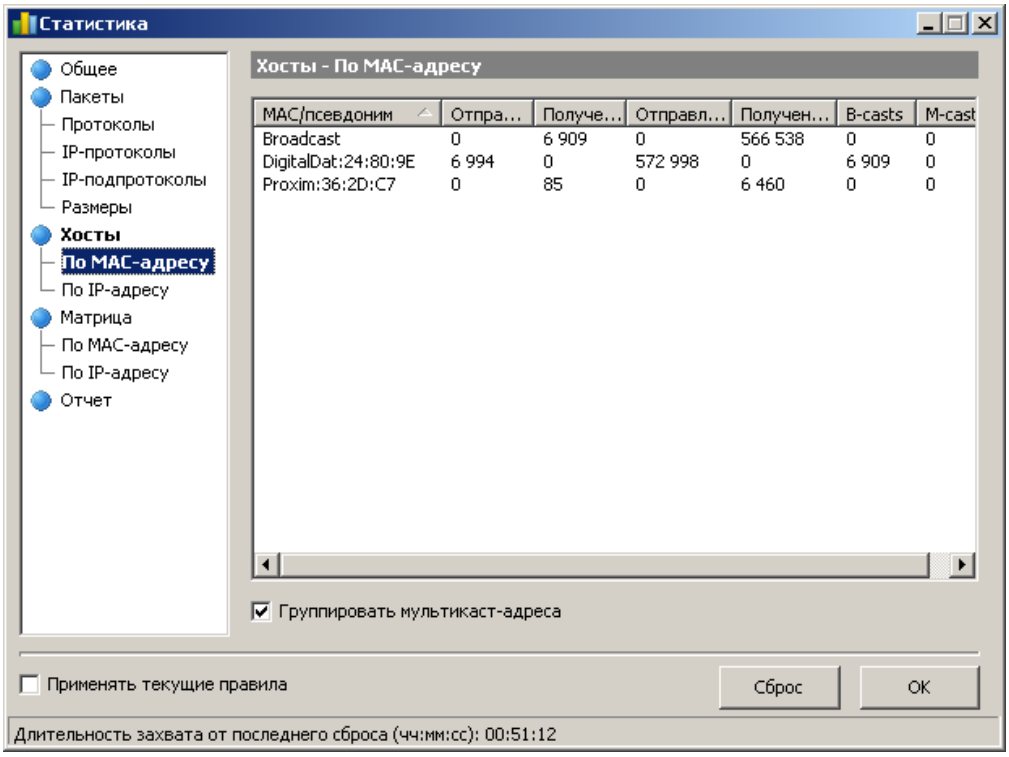


Рис. 23 Вкладка “Хосты по MAC адресу” в окне просмотра статистики

Данная вкладка содержит список активных LAN-хостов, упорядоченных по MAC-адресам, со статистикой передачи данных. MAC-адресам можно присвоить имена (псевдонимы). Если в сети очень много групповых пакетов (multicast) и таблица **Хосты по MAC адресу** слишком перегружена данными, то можно сгруппировать их в одну строку. Эту опцию включают флажком **Группировать мультикаст-адреса**. Обратите внимание, что группироваться будут только вновь получаемые пакеты. Данные, полученные до момента включения данной опции, не будут сгруппированы.

Хосты по IP-адресу

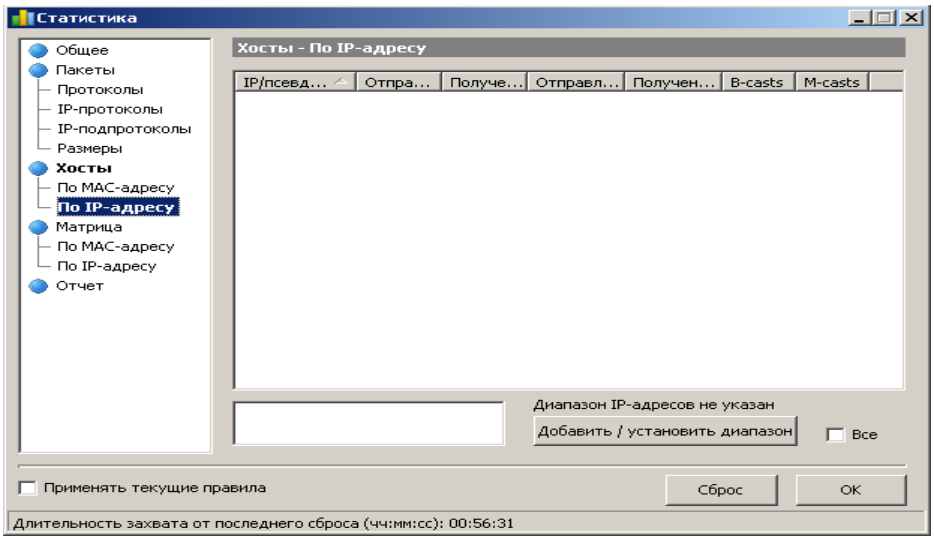


Рис. 24 Вкладка “Хосты по IP адресу” в окне просмотра статистики

В данной вкладке отображается список активных LAN-хостов, упорядоченных по IP-адресам, со статистикой передачи данных. Поскольку IP-пакеты, накапливаемые про-

граммой, могут приходить с неограниченного числа IP-адресов (как внутренних, так и внешних), то по умолчанию данная закладка не отображает никакой статистики. Чтобы ее отобразить, необходимо задать диапазон IP-адресов в соответствующем поле. Задаваемый диапазон должен принадлежать вашей сети. Можно задать несколько диапазонов, но общее число IP-адресов не может превышать 1000. Чтобы удалить диапазон, щелкните по нему правой кнопкой мыши и выберите соответствующую команду (**Удалить диапазон**, **Удалить все диапазоны**). IP-адресам также можно присвоить имена (псевдонимы).

Матрица по MAC-адресу

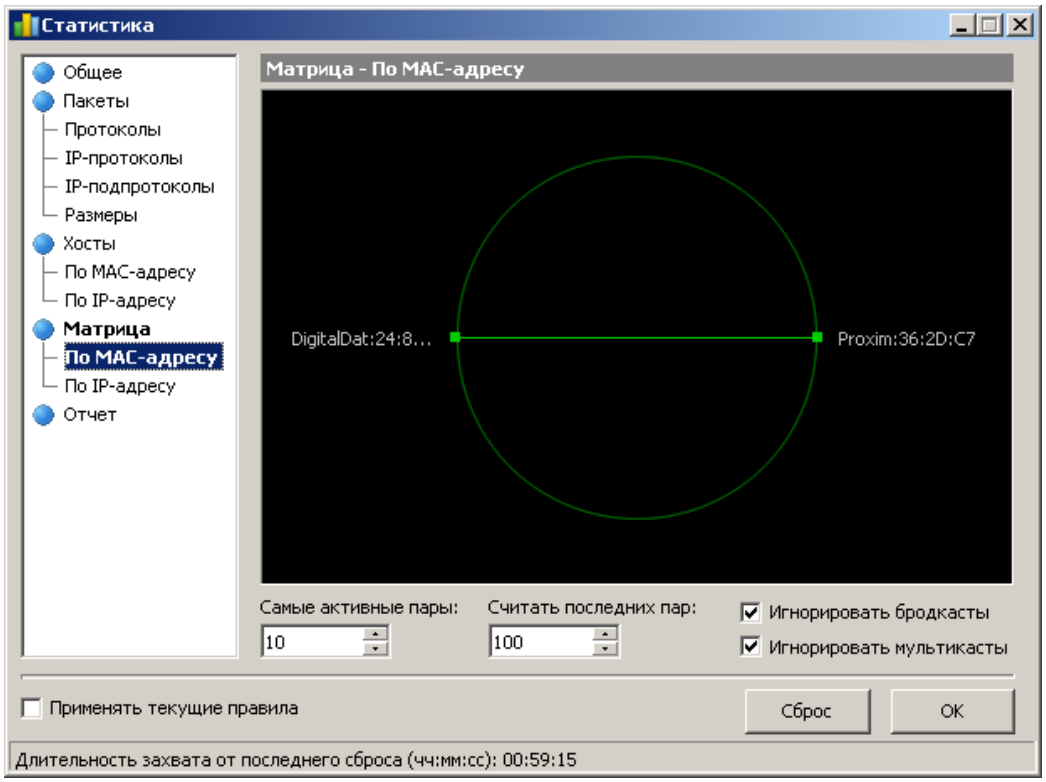


Рис. 25 Вкладка “Матрица по MAC адресу” в окне просмотра статистики

В этом окне показано общение узлов сети в графической форме, опираясь на значения MAC-адресов. Компьютеры, представленные их MAC-адресами, расположены по кругу, а сессии между ними показаны линиями, соединяющими соответствующие узлы. Подведя мышку к узлу, можно просмотреть все сессии, имевшиеся у данного компьютера с остальными. Меняя значение поля **Самые активные пары**, можно управлять количеством отображаемых связей в матрице. Меняя значение поля **Считать последних пар**, можно управлять числом пар адресов, отслеживаемых программой для построения матрицы. Если в сегменте локальной сети наблюдается слишком много широковещательных или групповых пакетов, переполняющих матрицу, можно игнорировать такие пакеты, установив соответствующий флажок: **Игнорировать бродкасты** или **Игнорировать мультикасты**.

Матрица по IP-адресу

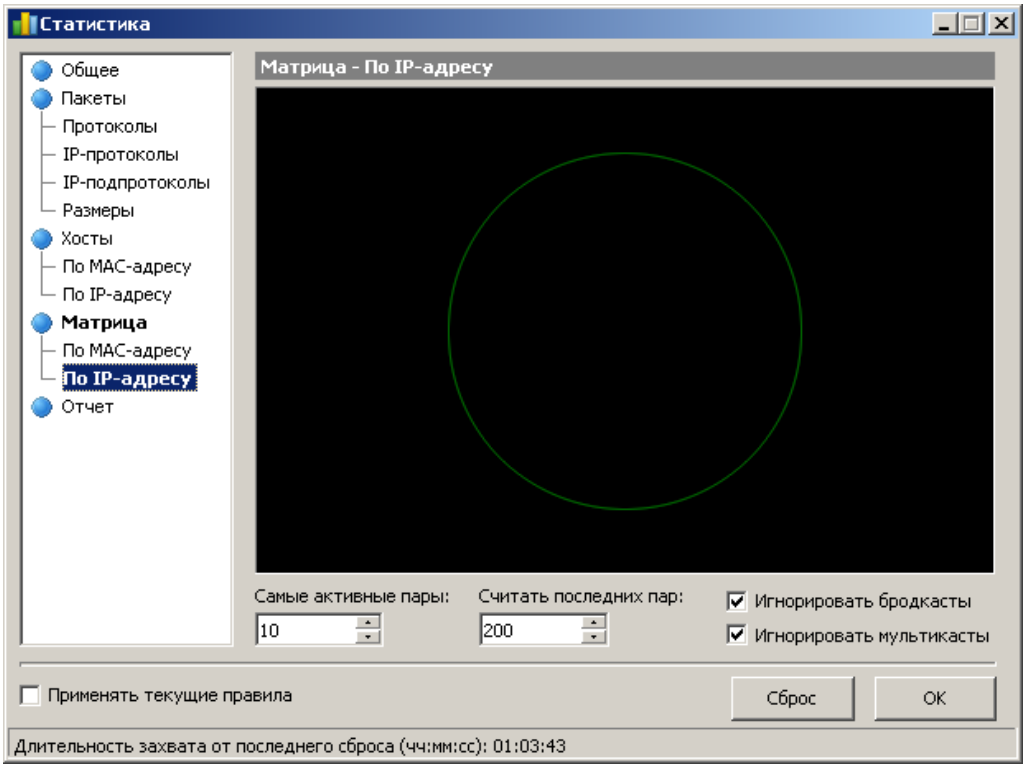


Рис. 26 Вкладка “Матрица по IP адресу” в окне просмотра статистики

В этом окне показана графическая матрица обмена данных между узлами сети с определенными IP-адресами. Узлы сети (их IP-адреса) расположены по кругу, а сессии между ними показаны линиями, соединяющими соответствующие узлы. Подведя курсор мыши к какому-либо узлу, можно увидеть все сессии, происходившие между данным узлом и остальными. Меняя значение поля **Самые активные пары**, можно управлять количеством отображаемых связей в матрице. Меняя значение поля **Считать последних пар**, можно управлять числом пар адресов, отслеживаемых программой для построения матрицы. Если в сегменте локальной сети наблюдается слишком много широковещательных или групповых пакетов, излишне перегружающих матрицу, можно игнорировать такие пакеты, установив соответствующий флажок: **Игнорировать бродкасты** или **Игнорировать мультикасты**.

Вкладка “Отчет”

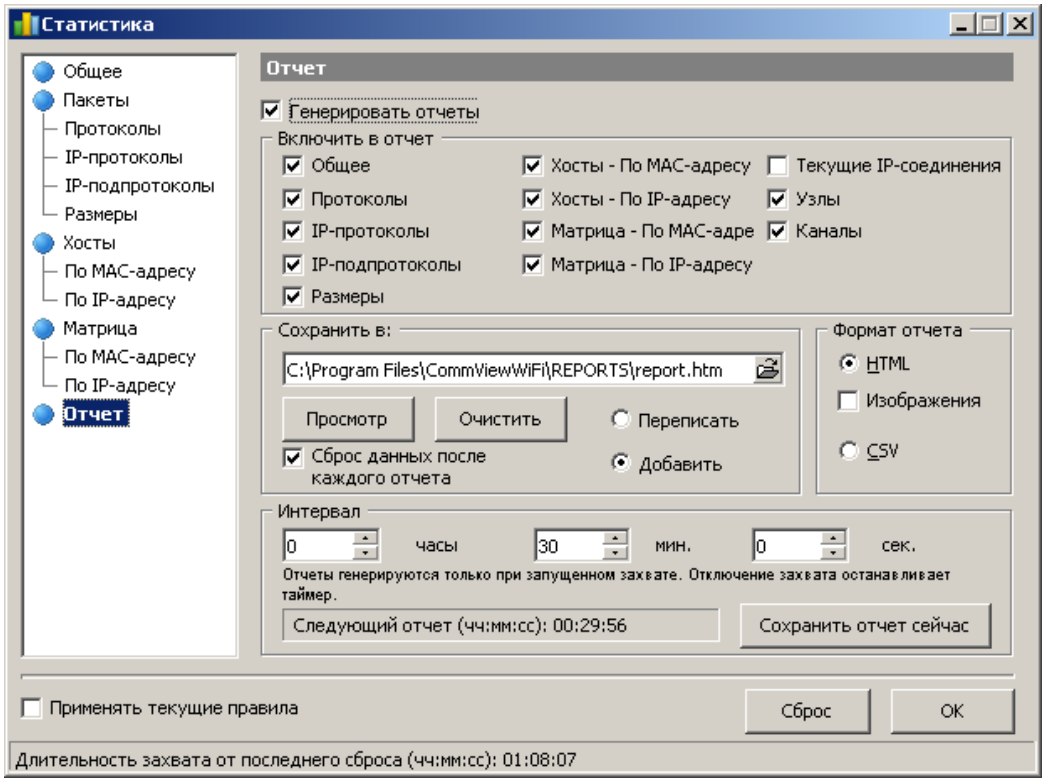


Рис. 27 Вкладка “Отчет” в окне просмотра статистики

Данная вкладка позволяет настроить автоматическое создание отчетов в форматах HTML (с графическим представлением гистограмм) или CSV.

В поле **Включить в отчет** можно указать, какие именно данные следует занести в файл отчета.

В поле **Сохранить в** можно указать путь и имя файла отчета, а также некоторые другие параметры, касающиеся данного файла.

В поле **Формат отчета** можно выбрать тот формат, в котором будет производиться сохранения файла отчета: HTML или CSV. Если вместе с отчетом необходимо сохранять и графики, то следует отметить флажком поле **Изображения**. Изображения возможно сохранять только в отчеты в формате HTML.

В поле **Интервал** можно задать интервал времени между сохранением отчетов. Если требуется сохранить отчет в текущий момент времени, то необходимо нажать на кнопку **Сохранить отчет сейчас**.

Время выполнения работы 90 мин;
Контрольные вопросы
Сделайте выводы.
Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 9 «Исследование сервера в Windows 2003 Server»

Цель работы: Познакомиться с основными характеристиками Windows Server 2003 и средствами администрирования программно-аппаратной части информационно вычислительной системы. Изучить задачи администратора и инструментарий, применяемый для их решения. Получение навыков по применению механизмов резервного копирования и восстановления..

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
2. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Введение в Windows Server 2003

Система Windows Server 2003 - это развитие системы Windows 2000. Для администраторов, работающих с сетями Windows 2000, развертывание этой новой версии Windows не станет сложной задачей, поскольку основы изменились не слишком сильно. Для администраторов, работающих с сетями Windows NT, эта превосходно настроенная версия корпоративной операционной системы Microsoftсодержит столько инструментов администрирования и средств управления, что у них не найдется причин для того, чтобы продолжать работать с NT.

Версии Windows Server 2003

Windows Server 2003 поставляется в виде следующих четырех версий (изданий):

- Windows Server 2003, Standard Edition, разработана для предоставления служб и ресурсов другим системам в сети. Она сменилаWindows NT 4.0 Server и Windows 2000 Server. Эта ОС обладает богатым набором функций и конфигурационных параметров.Windows Server 2003 поддерживает до двух центральных процессоров и до 4 Гбайт оперативной памяти.

- Windows Server 2003, Enterprise Edition, расширяет возможности Windows Server 2003, Standard Edition, обеспечивая поддержку служб кластеров, служб метакаталогов и служб для Macintosh. В ней также поддержи каются 64-разрядные процессоры Intel Itanium, оперативная память с возможностью ≪горячей≫ замены и неоднородный доступ к памяти (nonuniform memory access, NUMA). Эта версия поддерживает до 32 Гбайт оперативной памяти на процессорах x86, до 64 Гбайт оперативной памяти на процессорах Itanium и до 8 центральных процессоров.

- Windows Server 2003, Datacenter Edition, — самый надежный Windows-сервер. Эта версия поддерживает более сложную кластеризацию и способна работать с большими объемами оперативной памяти — до 64 Гбайт на процессорах x86 и до 128 Гбайт на процессорах Itanium. Минимальное количество процессоров для работы Datacenter Edition — 8, максимальное — 32.

- Windows Server 2003, Web Edition, предназначена для запуска служб Web при развертывании Web-узлов и Web-приложений. Для решения этих задач в данную вер-

сиювключены Microsoft .NET Framework, Microsoft Internet Information Sendees (IIS), AS P.NET и функции для равномерного распределения нагрузки на сеть, Многие другие функции, в частности Active Directory, в ней отсутствуют. Строго говоря, из стандартных компонентой Windows в этой версии предусмотрены лишь распределенная файловая система DFS, шифрованная файловая система EFS и удаленный рабочий стол. Версия Windows Server 2003, Web Edition, поддерживает до 2 Гбайт оперативной памяти и до двух центральных процессоров.

Все версии поддерживают одни и те же базовые функции и средства администрирования. Т. е. методики, описанные в этой книге, можно применять независимо от того, какой версией Windows Server 2003 вы пользуетесь. Помните, что в версии Web Edition нет Active Directory, поэтому сервер, работающий под управлением этой версии, нельзя сделать контроллером домена. Он, тем не менее, может быть частью домена Active Directory.

Различия в администрировании

Сети Microsoft Windows поддерживают две модели служб каталогов: рабочую группу (workgroup) и домен (domain).

- Рабочие группы — это свободные объединения компьютеров, в которых каждый компьютер управляется независимо.
- Домены — это объединения компьютеров, коллективно управляемых с помощью контроллеров домена, т. е. систем Windows Server 2003, регулирующих доступ к сети, базе данных каталога и общим ресурсам.

Для организаций, внедряющих Windows Server 2003, модель домена наиболее предпочтительна. Модель домена характеризуется единым каталогом ресурсов предприятия — Active Directory, — которому доверяют все системы безопасности, принадлежащие домену. Поэтому такие системы способны работать с субъектами безопасности (учетными записями пользователей, групп и компьютеров) в каталоге, чтобы обеспечить защиту ресурсов. Служба Active Directory, таким образом, играет роль идентификационного хранилища и сообщает «кто есть кто» в этом домене.

Впрочем, Active Directory — не просто база данных. Это коллекция файлов, включая журналы транзакций и системный том (Sysvol), содержащий сценарии входа в систему и сведения о групповой политике. Это службы, поддерживающие и использующие БД, включая протокол LDAP (Lightweight Directory Access Protocol), протокол безопасности Kerberos, процессы репликации и службу FRS (File Replication Service). БД и ее службы устанавливаются на один или несколько контроллеров домена. Контроллер домена назначается Мастером установки Active Directory, который можно запустить с помощью Мастера настройки сервера или командой DCPROMO из командной строки. После того как сервер становится контроллером домена, на нем хранится копия (реплика) Active Directory, и изменения БД на любом контроллере реплицируются на все остальные контроллеры домена.

Домены, деревья и леса

Active Directory не может существовать без домена и наоборот. Домен — это основная административная единица службы каталогов. Однако предприятие может включить в свой каталог Active Directory более одного домена. Когда несколько моделей доменов совместно используют непрерывное пространство имен DNS, они образуют логические структуры, называемые деревьями (tree). Например, домены contoso.com, us.contoso.com и europe.contoso.com совместно используют непрерывное пространство имен DNS и, следовательно, составляют дерево.

Домены Active Directory с разными корневыми доменами образуют несколько деревьев. Они объединяются в самую большую структуру Active Directory — лес (forest). Лес Active Directory содержит все домены в рамках службы каталогов. Лес может состоять из нескольких доменов в нескольких деревьях или только из одного домена. Когда доменов несколько, приобретает важность компонент Active Directory, называемый глобаль-

ным каталогом (global catalog): он предоставляет информацию об объектах, расположенных в других доменах леса.

Групповая политика

Организационные подразделения (ОП) также используются для объединения одинаково настроенных объектов — компьютеров и пользователей. Групповая политика Active Directory позволяет централизованно управлять практически любыми конфигурационными изменениями системы. С ее помощью можно указать настройки безопасности, развернуть ПО и настроить поведение ОС и приложений, даже не прикасаясь к компьютерам пользователей. Вы просто реализуете свою конфигурацию в рамках одного объекта групповой политики (ОГП).

ОГП состоят из сотен возможных конфигурационных параметров: от прав и привилегий пользователя до ПО, которое разрешено запускать на системе. ОГП подключается к контейнеру внутри Active Directory (обычно к ОП, но может и к доменам или даже сайтам), и после этого его настройки распространяются на всех пользователей и компьютеры внутри этого контейнера.

Любой сервер может поддерживать одну или более следующих ролей.

- Контроллер домена (Domain controller) — сервер, на котором работают службы каталогов и располагается хранилище данных каталога. Контроллеры домена также отвечают за вход в сеть и поиск в каталоге. При выборе этой роли на сервере будут установлены DNS и Active Directory. Почтовый сервер (POPS, SMTP) [Mail server (POP3, SMTP)] - сервер, на котором работают основные почтовые службы POP3 (Post Office Protocol 3) и SMTP (Simple Mail Transfer Protocol), благодаря чему почтовые POP3-клиенты домена могут отправлять и получать электронную почту. Выбрав эту роль, вы определяете домен по умолчанию для обмена почтой и создаете почтовые ящики. Эти службы удобны в небольших компаниях или при удаленном соединении, когда электронная почта необходима, но вполне может обойтись без функциональности Microsoft Exchange Server.
- Сервер печати (Print, server) — сервер, организующий доступ к сетевым принтерам и управляющий очередями печати и драйверами принтеров. Выбор этой роли позволит вам быстро настроить параметры принтеров и драйверов.
- Сервер потоков мультимедиа (Streaming media server) — сервер, предоставляющий мультимедийные потоки другим системам сети или Интернета. Выбор этой роли приводит к установке служб Windows Media. Эта роль поддерживается только в версиях Standard Edition и Enterprise Edition.
- Сервер приложений (Application server) — сервер, на котором выполняются Web-службы XML, Web-приложения и распределенные приложения. При назначении серверу этой роли на нем автоматически устанавливаются IIS, COM+ и Microsoft .NET Framework. При желании вы можете добавить к ним серверные расширения Microsoft FrontPage, а также включить или выключить ASP.NET.
- Сервер терминалов (Terminal Server) — сервер, выполняющий задачи для клиентских компьютеров, которые работают в режиме терминальной службы. Выбор этой роли приводит к установке Terminal Server. Для удаленного управления сервером устанавливать Terminal Server не нужно. Необходимый для этого удаленный рабочий стол (Remote Desktop) устанавливается автоматически вместе с ОС.
- Сервер удаленного доступа или VPN-сервер (Remote access/VPN server) — сервер, осуществляющий маршрутизацию сетевого трафика и управляющий телефонными соединениями и соединениями через виртуальные частные сети (virtual private network, VPN). Выбрав эту роль, вы запустите Мастер настройки сервера маршрутизации и удаленного доступа (Routing and Remote Access Server Setup Wizard). С помощью параметров маршрутизации и удаленного доступа вы можете разрешить только исходящие подключения, входящие и исходящие подключения или полностью запретить доступ извне.
- Узел кластера серверов (Server cluster node) — сервер, действующий в составе группы серверов, объединенных в кластер. Выбор этой роли приводит к запуску Мастера

создания кластера (New Server Cluster Wizard), позволяющего создать новую кластерную группу, или Мастера добавления узлов (Add Nodes Wizard), который поможет добавить сервер к существующему кластеру. Эта роль поддерживается только в версиях Enterprise Edition и Datacenter Edition.

- Файл-сервер (File server) — сервер, предоставляющий доступ к файлам и управляющий им. Выбор этой роли позволит вам быстро настроить параметры квотирования и индексирования. Вы также можете установить Web-приложен и для администрирования файлов. В этом случае будет установлен IIS и включены страницы ASP (Active Server Pages).

- DHCP-сервер (DHCP Server) — сервер, на котором запущен DHCP (Dynamic Hose Configuration Protocol), позволяющий автоматизировать назначение IP-адресов клиентам сети. При выборе этой роли на сервере будет установлен DHCP и запущен Мастер создания области (New Scope Wizard).

- DNS-сервер (DNS Server) — сервер, на котором запущена служба DNS, разрешающая имена компьютеров в IP-адреса и наоборот. При выборе этой роли на сервере будет установлена DNS и запущен Мастер настройки DNS-сервера (Configure DNS Server Wizard).

- WINS-сервер (WINS server) — сервер, на котором запущена служба WINS (Windows Internet Name Service), разрешающая имена NetBIOS в IP-адреса и наоборот. Выбор этой роли приводит к установкеWINS.

Управление выбранными ролями сервера осуществляется с помощью программы Управление данным сервером (Manage Your Server), в окне которой сосредоточены все основные инструменты для управления Windows Server 2003. В частности, здесь перечислены текущие роли сервера (рис.1). Чтобы открыть это окно, воспользуйтесь меню Администрирование (Administrative Tools).

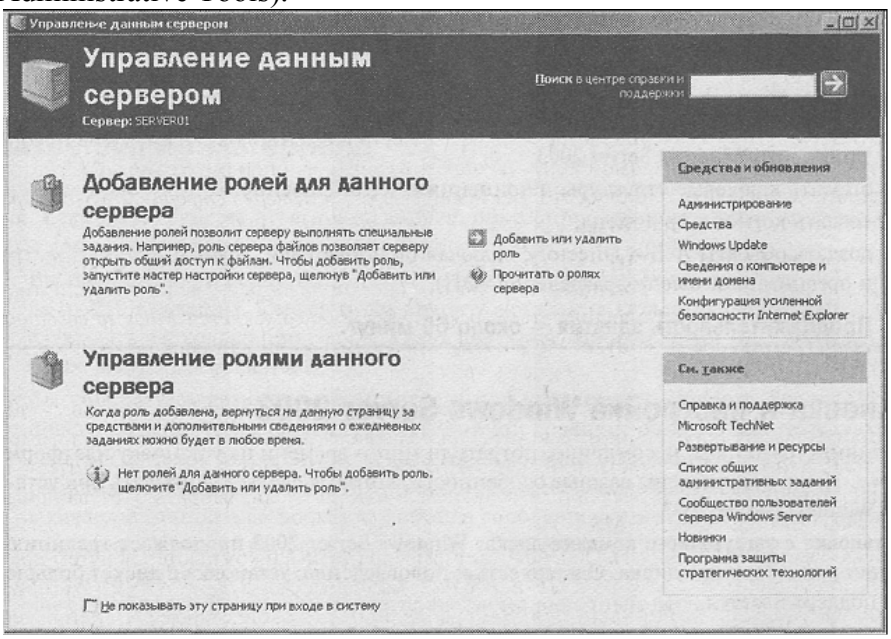


Рисунок 1. Страница Управление данным сервером

Таблица 1. Краткий справочник основных средств администрирования Windows Server 2003

Средство администрирования	Назначение
Active Directory — домены и доверие (Active Directory Domains and Trusts)	Управление доверительными отношениями между доменами
Active Directory — пользователи и компьютеры (Active Directory Users and Computers)	Управление пользователями, группами, компьютерами и другими объектами Active Directory

Active Directory — сайты и службы (Active Directory Sites and Service)	Создание сайтов для управления репликацией Active Directory
DHCP	Конфигурация и управление службой DHCP
DNS	Управление службой системы доменных имен (DNS)
WINS	Управление службой WINS, преобразующей имена NetBIOS в IP-адреса
Администратор кластеров (Cluster Administrator)	Управление службой Cluster
Администратор серверных расширений (Server Extensions Administrator)	Управление серверными расширениями, например FrontPage
Внешнее хранилище (Remote Storage)	Управление службой Remote Storage
Диспетчер служб Интернета (Internet Information Services Manager)	Управление Web-, FTP- и SMTP-серверами
Диспетчер служб терминалов (Terminal Services Manager)	Управление и МОЕНПЧЛШНГ пользователей, сеансов и процессов Terminal Service
Источники данных (ODBC) [Data Sources (ODBC)]	Добавление, удаление и настройка источников данных и драйверов ODBC (Open Database Connectivity)
Контроль допуска QpS (QoS Admission Control)	Управление службой Quality of Service(QpS) Admissions Control для регулировки пропускной способности сети
Лицензирование (Licensing)	Управление лицензированием доступа клиентов к серверным продуктам
Маршрутизация и удаленный доступ к сети (Routing and Remote Access)	Конфигурация и управление службой Routing and Remote Access, контролирующей интерфейсы маршрутизации, динамическую IP-маршрутизацию и удаленный доступ
Настройка сервера (Configure Your Server)	Добавление, удаление и конфигурация служб Windows для сети
Настройка служб терминалов (Terminal Services Configuration)	Управление настройкой протокола Terminal Service и параметрами сервера
Пакет администрирования диспетчера подключений (Connection Manager Administration Kit)	Конфигурирование и настройка диспетчера подключений
Политика безопасности домена (Domain Security Policy)	Просмотр и редактирование политики безопасности в домене
Политика безопасности контроллера домена (Domain Controller Security Policy)	Просмотр и редактирование политики безопасности для организационного полразделения контроллера домена
Производительность (Performance)	Отображение графиков производительности системы и настройка журналов и сигналов оповещения
Просмотр событий (Event Viewer)	Управление событиями и журналами
Распределенная файловая система DIFS (Distributed File System)	Создание и управление распределенными файловыми системами, объединяющими общие папки из разных компьютеров
Сетевой монитор (Microsoft Network	Мониторинг сетевого трафика и

Monitor)	устранение неисправностей в сети
Службы (Services)	Управление запуском и настройка служб Windows
Службы компонентов (Component Services)	Конфигурация и управление приложениями COM-, управление событиями и службами
Удаленные рабочие столы (Remote Desktop)	Настройка удаленных подключений и просмотр сеансов удаленных подключений
Управление компьютером(Computer Management)	Запуск и остановка служб, управление дисками и доступ к другим средствами управления системой
Центр сертификации (Certification Authority)	Управление сертификационными службами

Регистрация пользователя в системе

Защиту ресурсов реализуют несколько процессов на разных уровнях операционной системы. Первый из них — механизм регистрации — обеспечивает защиту доступа к домену или компьютеру.

Чтобы получить доступ к ресурсам, пользователям необходимо сначала зарегистрироваться — идентифицировать себя в домене или на компьютере.

При регистрации пользователя, в зависимости от выбранного способа регистрации в системе, появляется диалоговое окно «Операционная система Windows» с текстом «Нажмите Ctrl+Alt+Delete».

Рисунок 2. Диалоговое окно "Операционная система Windows"

Рисунок 3. Диалоговое окно "Вход в Windows"

Параметры диалогового окна «Вход в Windows» описаны в таблице 2.

Таблица 2. Параметры диалогового окна "Вход в Windows"

Параметры	Описание
User Name (Имя)	Введите уникальную учетную запись пользователя, присвоенную Вам администратором. Эта учетная запись должна присутствовать в базе данных каталогов на контроллерах домена, чтобы обеспечивать регистрацию в домене, и в базе данных каталогов локального компьютера — для регистрации на локальном компьютере
Password (Пароль)	Введите пароль, присвоенный указанному Вами имени пользователя, учитывая регистр символов. Чтобы пароль не стал достоянием посторонних, при его вводе символы на экране заменяются звездочками (*)
Domain (Домен)	Чтобы зарегистрироваться в домене, укажите его имя. При попытке регистрации пользователя в домене база данных контроллера домена проверяется на наличие соответствующего элемента. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя домена соответствуют данным в базе данных контроллера домена. Чтобы зарегистрироваться на локальном компьютере, укажите его имя. Локальный компьютер проверит наличие информации о Вас в локальной базе данных каталогов. Регистрация по указанной учетной записи разрешается, если введенное имя пользователя, пароль и имя компьютера соответствуют данным в локальной базе данных каталогов. Пользователь может зарегистрироваться на локальном компьютере, только указав имя пользователя, имеющееся в локальной базе данных каталогов. Серверы и компьютеры под управлением Windows 2003 содержат встроенные локальные учетные записи *Administrator* (Администратор) и *Guest* (Гость).

Проверка глобальной учетной записи

Когда пользователь щелкнет кнопку **ОК,** компьютер передает имя домена, имя пользователя и пароль контроллеру домена. Последний сначала проверяет имя домена, а затем ищет имя пользователя и пароль в базе данных домена. Далее события могут разворачиваться по одному из трех сценариев.

1. Если имя домена указано верно, а имя пользователя и пароль соответствуют имеющейся учетной записи, сервер уведомляет компьютер, что регистрация разрешен.
2. Если пользователь указал имя домена, не совпадающее с именем домена контроллера, но контроллер распознает его как имя доверяемого домена, то он передает информацию контроллеру этого домена. Последний выполняет аутентификацию и возвращает соответствующую информацию
3. Если имя домена не совпадает с именем контроллера домена и тот не распознает указанный домен, то контроллер запрещает доступ к домену.

Проверка локальной учетной записи

Когда пользователь щелкает кнопку **ОК,** компьютер сначала проверяет указанное имя компьютера, а затем ищет имя пользователя и пароль в локальной базе данных каталогов. Если имена совпадают, регистрация разрешается и пользователь получает доступ к локальным ресурсам. Если же нет, пользователь не получает доступ к компьютеру.

Функции администратора Windows 2003

Администрирование Windows NT подразумевает выполнение как специальных операций после установки системы, так и рутинных каждодневных действий.

Функции администратора можно разделить на пять категорий.

Таблица 3. Функции администратора

Категория	Характерные задачи
Администрирование учетных записей пользователей и групп	Планирование, создание и ведение учетных записей пользователей и групп для обеспечения каждому пользователю возможности регистрации в сети и доступа к необходимым ресурсам
Администрирование защиты	Планирование и реализация стратегии безопасности для защиты данных и общих сетевых ресурсов, в том числе папок, файлов и принтеров
Администрирование принтеров	Настройка локальных и сетевых принтеров для обеспечения пользователям доступа к ресурсам печати. Устранение обычных проблем печати
Мониторинг событий и ресурсов сети	Планирование и реализация стратегии аудита событий в сети с целью обнаружения нарушений защиты. Управление ресурсами и контроль их использования
Резервное копирование и восстановление данных	Планирование и выполнение регулярных операций резервного копирования для обеспечения быстрого восстановления важных данных

Средства администратора Windows 2003

Средства администрирования входят в состав Windows 2003 и могут применяться или для администрирования любого компьютера домена, или для администрирования локального компьютера.

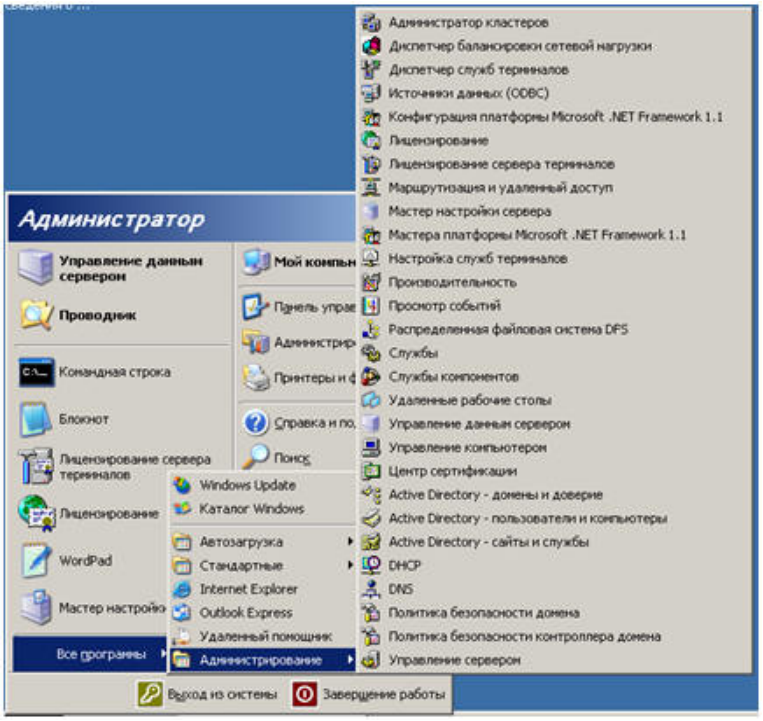


Рисунок 4. Средства администрирования

Таблица 4. Средства администрирования

Средство	Назначение
Администратор кластеров	Администратор кластеров - это основное средство администрирования и конфигурирования объектов кластера серверов, таких как узлы, группы и другие ресурсы. Это позволяет вам управлять кластером серверов без необходимости физического присутствия в одном из узлов.
Диспетчер балансировки сетевой нагрузки	Обеспечивает балансирование IP-трафика между несколькими серверами. Не обеспечивает переход по отказу (failover) для приложений и данных.
Диспетчер служб терминалов	Позволяет управлять конфигурацией сервера служб терминалов
Конфигурация платформы Microsoft.NET Framework 1.1	Позволяет настраивать среду .NET Framework
Лицензирование	Утилита, позволяющая управлять клиентскими лицензиями в масштабах предприятия
Лицензирование сервера терминалов	Утилита, позволяющая управлять клиентскими лицензиями для служб терминалов (Terminal Services), работающих в режиме выполнения приложений
Маршрутизация и удалённый доступ	Служит для управления маршрутизацией и удаленным доступом
Мастер настройки сервера	Мастер, позволяющий администратору настроить сервер в соответствии с выбранными ролями (файловый сервер, сервер служб Интернета и т. д.)
Производительность	Каждый компьютер с Windows Server 2003 содержит компоненты, мониторинг которых можно выполнять с помощью оснастки Performance (Производительность). Это могут быть аппаратные или программные компоненты, которые выполняют задачи или поддерживают рабочую нагрузку. Многие из этих компонентов имеют показатели, отражающие определенные аспекты их функционирования, которые можно точно измерить как скорость выполнения задач.
Просмотр событий	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Распределенная файловая системаDFS	Создает и управляет распределенными файловыми системами, объединяющими совместно используемые папки на различных компьютерах
Службы	Запускает, останавливает и конфигурирует службы (сервисы) Windows
Службы компо-	Конфигурирует и управляет службами компонентов

нентов	COM+
Удалённые рабочие столы	Позволяет управлять многочисленными сессиями терминального доступа к удаленным компьютерам
Управление данным сервером	Мастер, представляющий собой информационный центр для управления различными ролями сервера, обращения к службам поддержки и вспомогательным инструментам, а также позволяющий быстро находить информацию об обновлениях, способах решения проблем и т. п.
Управление компьютером	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Центр сертификации	Позволяет работать с центрами сертификации, развернутыми в корпоративной сети
Active Directory - домены и доверие	Служит для управления доменами и доверительными отношениями
Active Directory — сайты и службы	Определяет топологию и расписание репликации Active Directory. Обеспечивает изменение служб корпоративного уровня
Политика безопасности домена	Служит для управления параметрами безопасности (представленными в узле **Security Settings** объекта групповой политики, привязанного к объекту домена) для всего домена
Политика безопасности контроллера домена	Служит для управления параметрами безопасности (представленными в узле **Security Settings**объекта групповой политики, привязанного к подразделению Domain Controllers) на контроллерах домена

Мониторинг ресурсов

Сведения о системе

Утилита System Information (Сведения о системе) (Winmsd.exe) представляет исчерпывающую информацию об аппаратном обеспечении компьютера, системных компонентах и программной среде. Системная информация разделена на категории, которым в окне структуры соответствуют следующие узлы (Рисунок 5): **System Summary** (Сведения о системе),**Hardware Resources** (Ресурсы аппаратуры),**Components** (Компоненты), **Software Environment** (Программная среда) и **Internet Settings** (Параметры Интернета).

- Узел **System Summary** отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ, версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.

- Узел **Hardware Resources** отображает информацию об аппаратных установках, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел **Conflicts/Sharing** (Конфликты/ Совместное использование) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.

- Узел **Components** отображает информацию о конфигурации Windows и используется для определения статуса драйверов устройств, сетевых устройств и программного

обеспечения мультимедийных устройств. Кроме того, данный узел содержит обширную информацию об истории драйверов с записью всех изменений, которые производились с компонентами.

- Узел **Software Environment** отображает "снимок" программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра списка выполняющихся задач или для выяснения номера версии продукта.

- Узел **Internet Settings** содержит, в частности, информацию о настройках программы Internet Explorer.

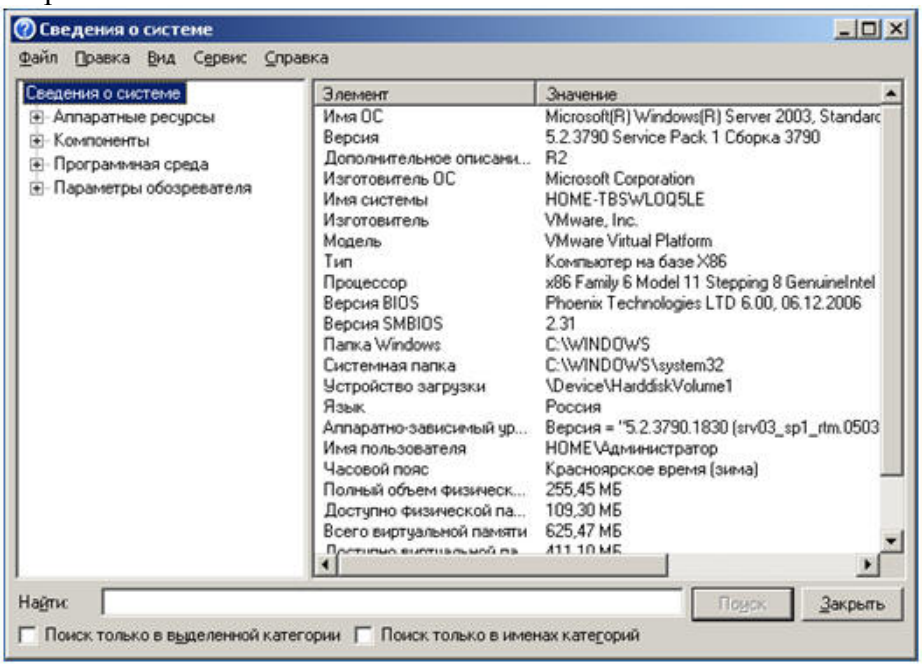


Рисунок 5. Внешний вид утилиты "Сведения о системе"

Составление и печать сводки

- Информация, предоставляемая программой System Information (Сведения о системе), нужна не только организации, осуществляющей поддержку, — напечатанная сводка может пригодиться службе инвентаризации. Из сводки можно быстро узнать объем оперативной памяти и дискового пространства на конкретном компьютере, а также, какие устройства на нем установлены.

- Распечатать постранично или всё целиком можно из меню **Файл->Печать.** Сохранить общий отчёт можно из меню **Файл->Экспорт.**

Управление компьютером

Инструмент (и одноименная оснастка) **Computer Management** (**Управление компьютером**) (Рисунок 6) является одним из основных средств системного администратора для конфигурирования компьютера. Данную оснастку можно использовать для администрирования, как локальной системы, так и удаленных компьютеров (в том числе систем Windows 2000 и — с некоторыми ограничениями — компьютеров с Windows NT 4.0). Это позволяет администратору со своего рабочего места устранять проблемы и конфигурировать любой компьютер в сети, на котором установлена Windows Server 2003.

Для запуска оснастки **Computer Management** можно пользоваться двумя способами: выбрать соответствующую команду в меню **Start | Administrative Tools** или щелкнуть правой кнопкой мыши на команде **My Computer**(Мой компьютер) в меню **Start**и выбрать в контекстном меню пункт **Manage**(Управление).

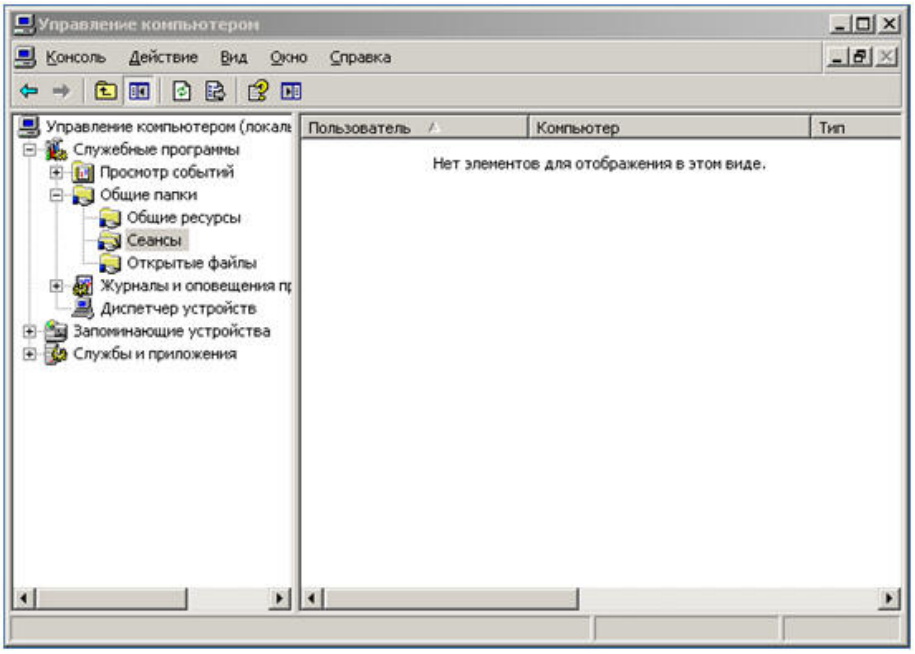


Рисунок 6. Оснастка "Управление компьютером"

Просмотр пользовательских сеансов

Оснастка **Shared Folders**(Общие папки) позволяет просматривать информацию о соединениях и использовании ресурсов локального или удаленного компьютеров. Данная оснастка используется вместо программы Server в Control Panel системы Windows NT 4.0. Оснастка **Shared Folders** содержит три узла: **Shares** (Ресурсы), **Sessions** (Сеансы) и **Open Files** (Открытые файлы). При выборе данных узлов в панели результатов отображается содержание соответствующего узла.

С помощью оснастки можно выполнять следующие задачи:

- создавать, просматривать, изменять свойства и удалять общие ресурсы на локальном или удаленном компьютерах (Windows NT 4.0/2000/XP и Windows Server 2003) и устанавливать разрешения на доступ к ним. Кроме того, можно управлять режимом кэширования общих папок (в случае их использования в качестве изолированных папок). В системах Windows XP и Windows Server 2003 появилась очень удобная новая возможность управления процессом публикации общей папки в каталоге Active Directory (рис. 6.12) — можно сразу после создания общей папки опубликовать ее в каталоге, не прибегая к помощи оснастки Active Directory Users and Computers. Все необходимые действия достаточно очевидны из содержания приведенного примера: в данном случае публикуется общая папка службы факсов, содержащая клиентское программное обеспечение для систем, не имеющих его (например, Windows 9x);
- просматривать список удаленных пользователей, подключенных к компьютеру, и отключать их;
- просматривать список файлов, открытых удаленными пользователями, и закрывать открытые файлы.

Windows 2003 Backup

Регулярное резервное копирование информации с серверов и локальных жестких дисков предотвращает утрату и повреждение данных из-за поломки жесткого диска, отключения питания, воздействия вирусов и т.д. Резервное копирование при грамотном планировании и наличии надежного оборудования позволяет безболезненно справиться с последствиями катастрофы.

Графическое инструментальное средство Windows 2003 Backup предназначено для автоматического и ручного резервного копирования и восстановления файлов, расположенных на разделах файловых систем FAT и NTFS.

Выбор стратегии резервного копирования

Перед тем как приступать к резервному копированию файлов, нужно разработать стратегию, отвечающую потребностям Вашей организации и гарантирующую восстановление утраченных данных. Эффективное архивирование и восстановление информации — одна из самых важных задач администратора.

Отбор файлов для резервного копирования

По степени важности (а следовательно, и по частоте создания резервных копий) папки и файлы можно разделить на три категории:

- важные — их резервные копии создаются всегда;
- полезные — их резервные копии создаются изредка;
- малозначимые — их резервные копии не создаются никогда.

Отбирая файлы для резервного копирования, учитывайте следующие правила:

- всегда создавайте резервные копии
- o файлов, жизненно важных для работы Вашей организации;
- o реестров всех главных и резервных контроллеров домена (каждый контроллер домена имеет свою копию базы данных каталогов; резервное копирование реестра контроллера домена предотвращает потерю информации об учетных записях пользователей и защите).
- резервные копии файлов, изменяемых редко или не представляющих особой ценности, следует создавать лишь время от времени.
- не сохраняйте временные файлы, так как они постоянно изменяются, и вряд ли могут быть использованы для восстановления данных.

Выбор типа резервного копирования

Windows 2003 Программа архивации (Backup Utility) предлагает пять вариантов резервного
копирования: *обычное* (normal),*копирующее* (copy), *инкрементальное* (incremental), *разностное* (differential) и *ежедневное* (daily). Выбор стратегии резервного копирования определяется тем, сколько времени отводится на сохранение данных и каковы требования к скоростям поиска резервных копий и восстановления файлов.

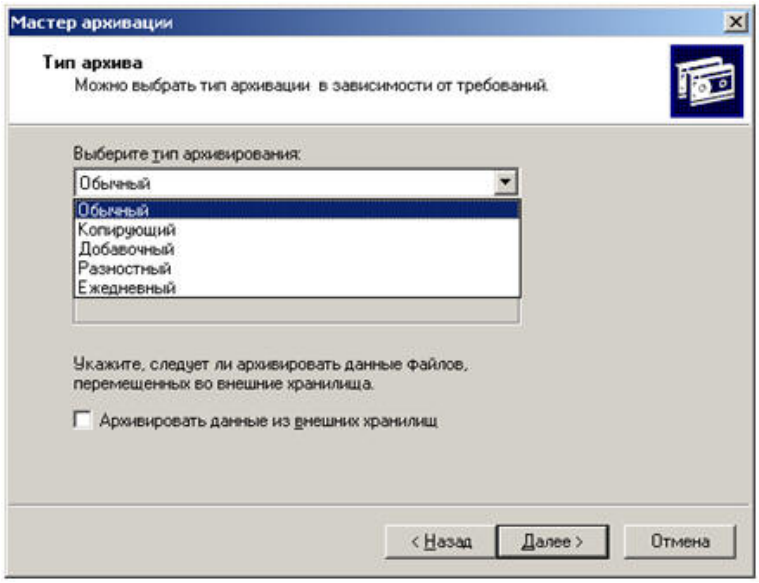


Рисунок 7. Выбор типа архивации

Краткая характеристика перечисленных выше типов резервного копирования приведена в таблице.

Таблица 5. Варианты резервного копирования

Варианты резервного копирования	Характеристика
Обычное или полное	Архивирует выбранные файлы и помечает их как сохраненные. Обычное резервное копирование позволяет быстро восстанавливать файлы, так как наиболее свежие файлы находятся на последней ленте. Для создания первой резервной копии всегда следует применять обычное резервное копирование всех файлов
Инкрементальное или добавочное	Архивирует только файлы, созданные или измененные с момента выполнения последнего обычного или инкрементального резервного копирования. Эти файлы помечаются флажком архивации. Если Вы сочетаете обычное и инкрементальное резервное копирование, то воссоздание информации начинается с восстановления последней обычной резервной копии, а затем последовательно восстанавливаются файлы инкрементальных копий
Разностное	Архивирует файлы, созданные или измененные со времени последнего обычного (или инкрементального) резервного копирования. Файлы при этом не помечаются флажком архивации. При комбинации обычного и разностного резервного копирования для восстановления данных требуются лишь 2 ленты: с последней обычной и с последней разностной копиями
Копирующее	Архивирует выбранные файлы, не помечая их флажком архивации. Тем самым не оказывает влияния на операции обычного и инкрементального резервного копирования и может применяться для промежуточного сохранения данных
Ежедневное копирование	Архивирует выбранные, файлы, которые были изменены во время ежедневного копирования. Файлы не помечаются флажком архивации. Эта операция полезна, например, когда Вы берете работу на дом и хотите быстро выбрать файлы, над которыми сегодня работали

Журналы резервного копирования

Журнал резервного копирования (backup log) — это текстовый файл, в котором регистрируются операции резервного копирования (рис. 8). Он полезен при восстановлении данных. Его можно либо распечатать, либо посмотреть в любом текстовом редакторе. Журнал хранится на диске, поэтому в случае повреждения каталога архива на ленте обратитесь к нему, чтобы найти нужный файл.

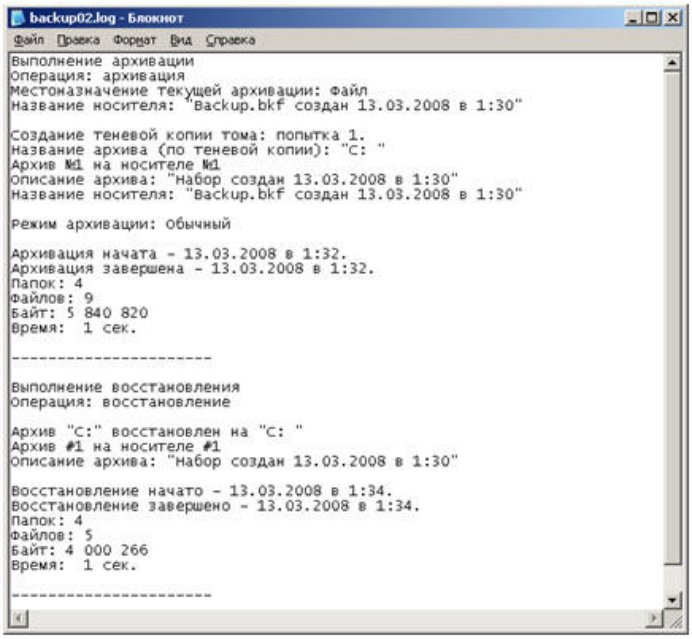


Рисунок 8. Журнал резервного копирования

Журнал резервного копирования содержит следующую информацию:

- дату создания архива;
- название варианта резервного копирования;

местонахождение накопителя.

Шаблон плана резервного копирования

Местонахождение накопителя __ Местонахождение лент_____

Путь к архивируемым файлам и папкам	**Ежедневное резервное копирование**	**Еженедельное резервное копирование (укажите день)**

Недельное расписание резервного копирования

Понедельник	**Вторник**	**Среда**	**Четверг**	**Пятница**
Тип копирования	**Тип копирования**	**Тип копирования**	**Тип копирования**	**Тип копирования**
Лента	**Лента**	**Лента**	**Лента**	**Лента**
Архив: Да Нет	**Архив: Да Нет**	**Архив: Да Нет**	**Архив: Да Нет**	**Архив: Да Нет**

Типы резервного копирования:

О = Обычное, Д = Инкрементальное, Р = Разностное, К = Копирующее, ЕК = Ежедневное копирование

Резервное копирование файлов

Программа резервного копирования Windows 2003 выглядит следующим образом. (рис. 9)

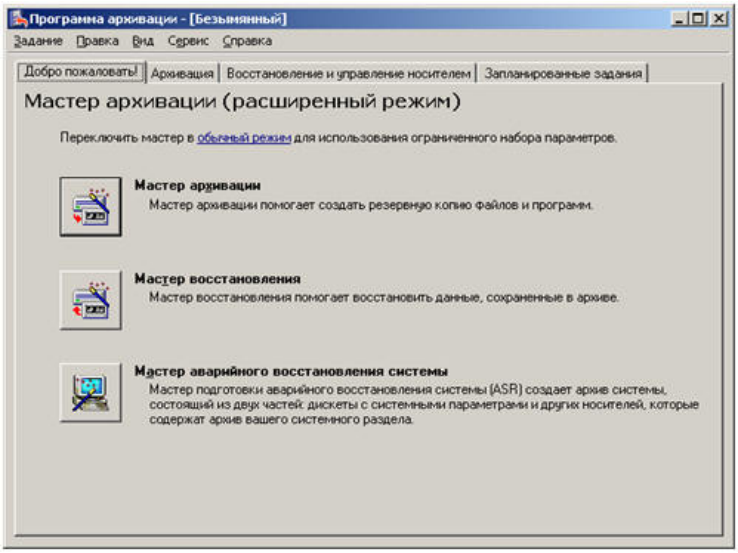


Рисунок 9. Окно мастеров архивации

Чтобы запустить программу, в меню **Start** (Пуск) выберите пункты **Programs** (Программы), **Accessories** (Стандартные), **System Tools**(Служебные), **Backup** (Архивация данных).

На рис. 10 представлены мастера архивации. Здесь можно выбрать 3 мастера: мастер архивации, мастер восстановления и мастер аварийного восстановления системы.

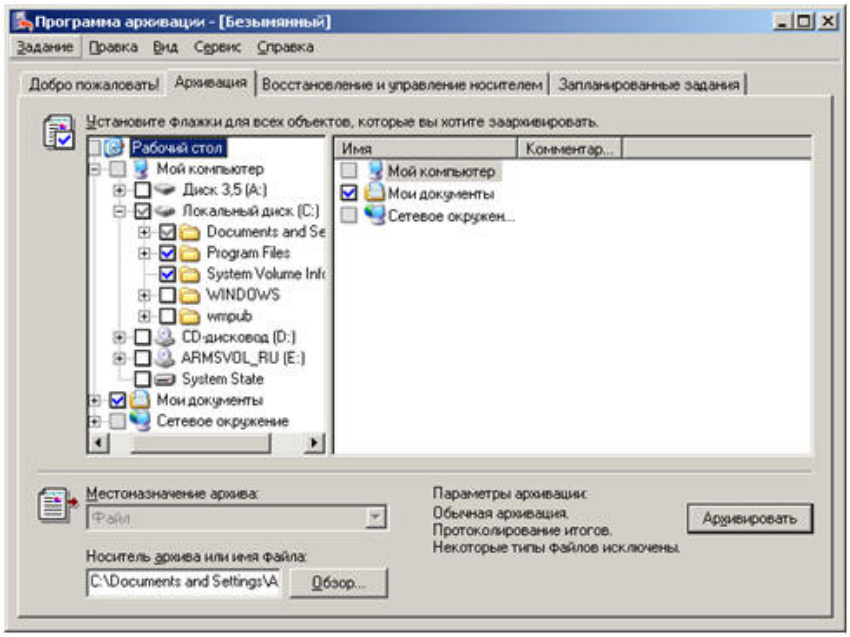


Рисунок 10. Окно "Архивация"

На рисунке 10 представлено окно архивации. Здесь можно выбрать параметры архивации: объекты архивации и назначение архивации. Можно также выбрать дополнительные параметры архивации (рисунок 11).

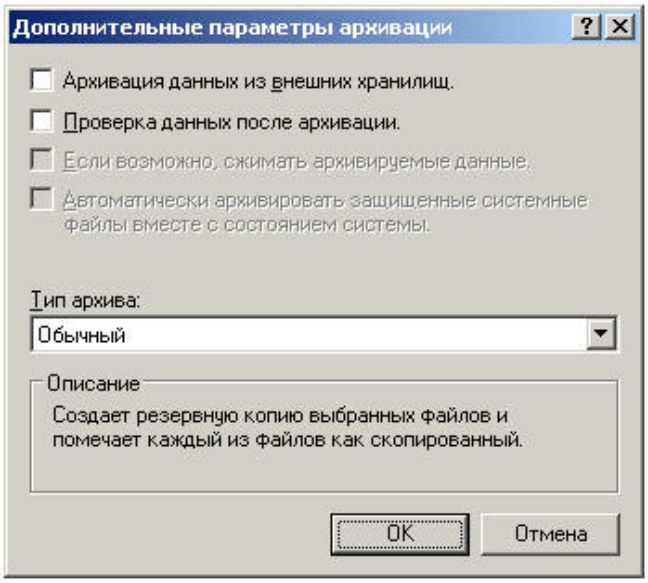


Рисунок 11. Окно "Дополнительные параметры архивации"

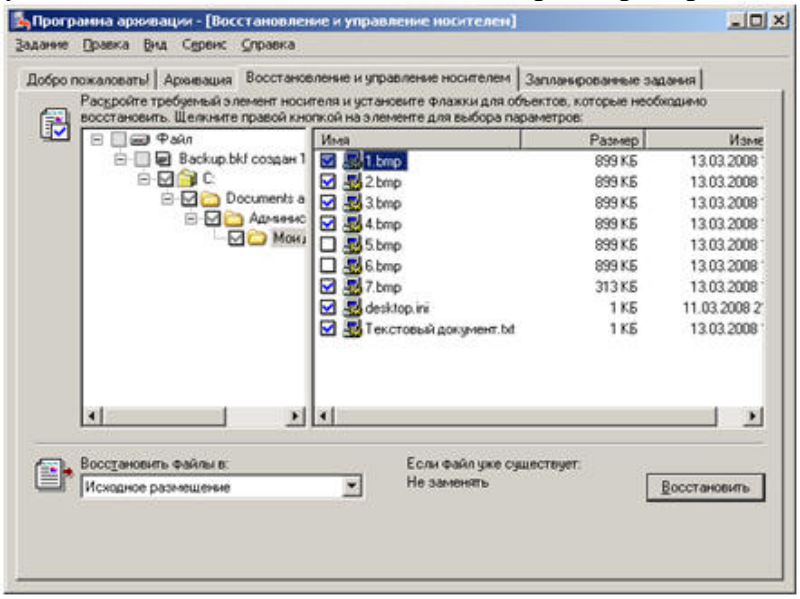


Рисунок 12. Окно "Восстановление и удаление носителем"

На рисунок 12 представлено окно восстановления управления носителем. Здесь можно выбрать необходимые для восстановления объекты.

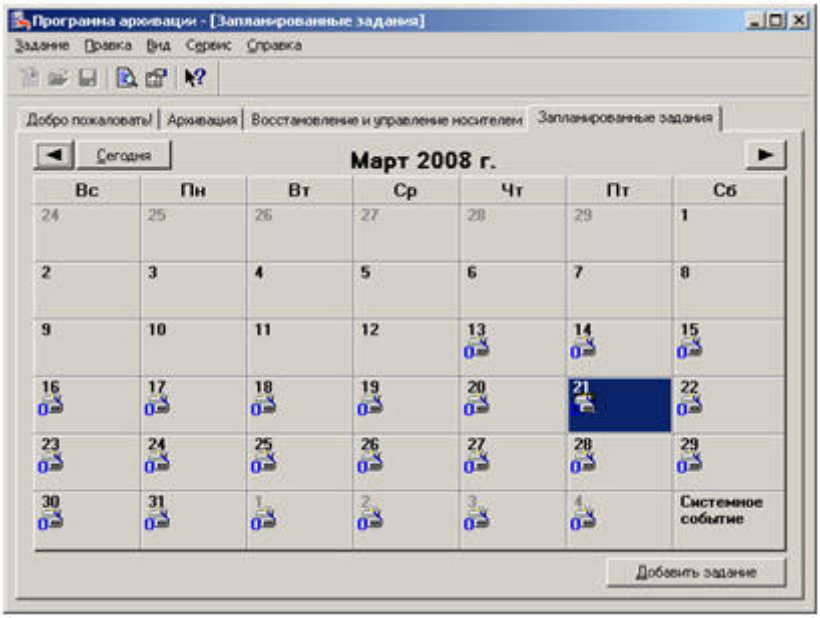


Рисунок 13. Окно "Запланированные задания"

На рисунок 13 представлено окно планировщика заданий. Здесь можно создать задание архивации, путем вызова мастера архивации (рисунок 14).

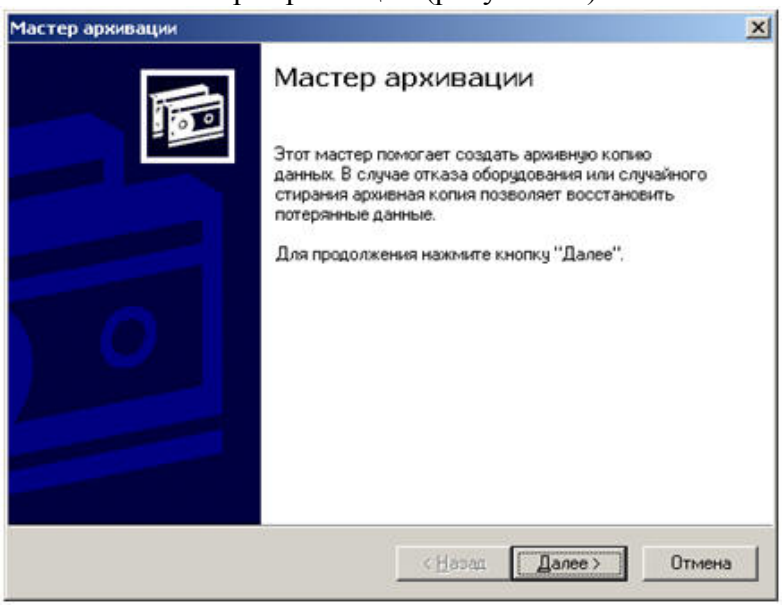


Рисунок 14. Мастер архивации

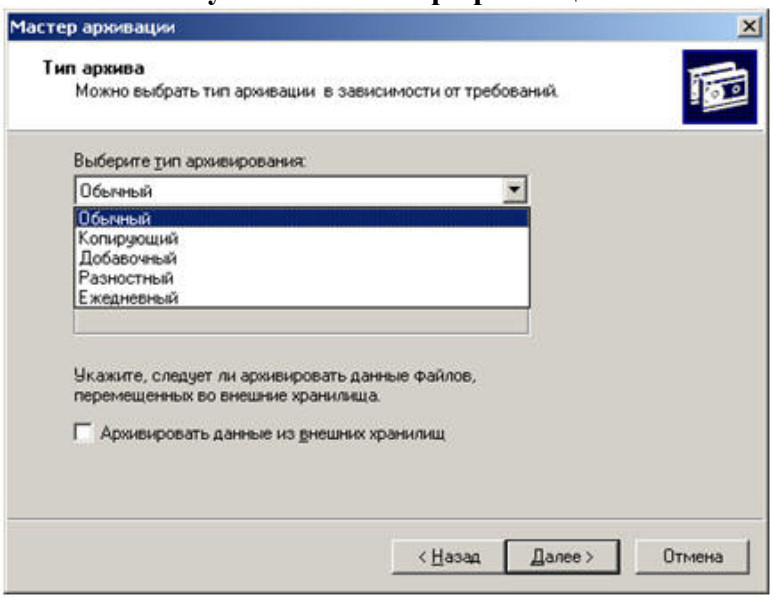


Рисунок 15. Окно "Мастер архивации". Выбор типа архивации.

На рисунок 15 представлены типы архивации: обычный, копирующий, добавочный, разностный, ежедневный. Далее предлагается выбрать время выполнения задания (рисунок 16) и параметры задания (рисунок 17).

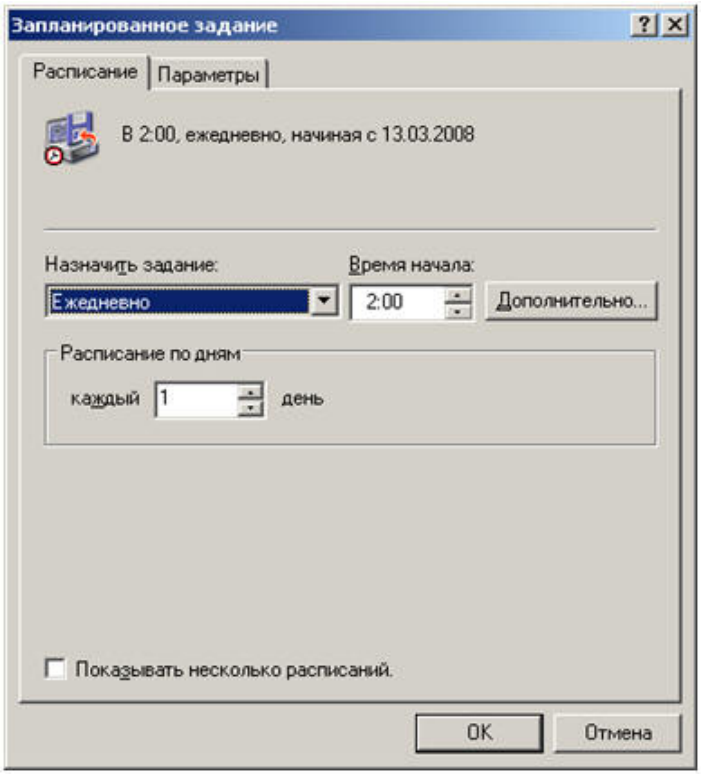


Рисунок 16. Окно "Расписание"

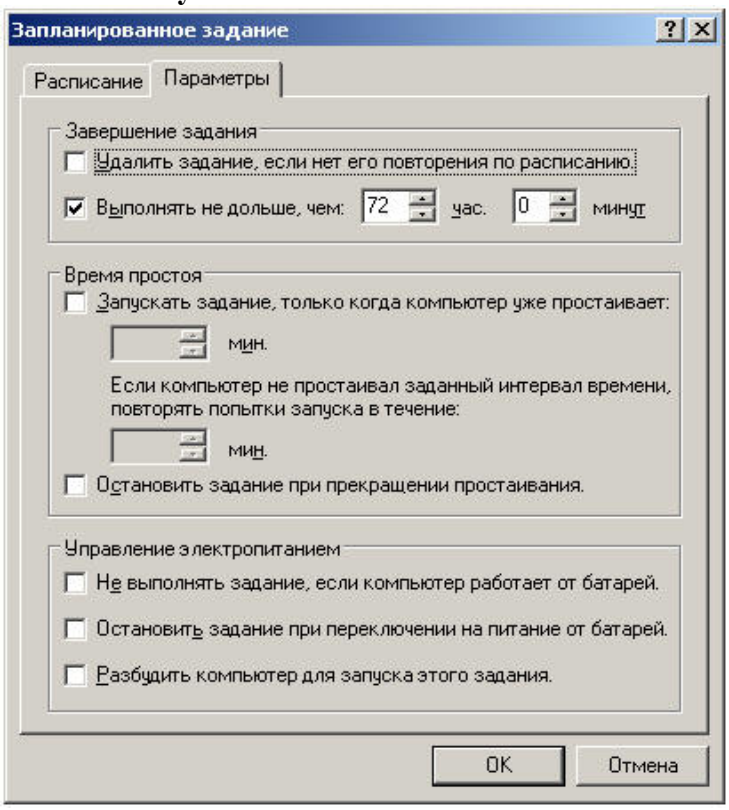


Рисунок 17. Окно "Параметры архивации"

Порядок работы

Лабораторная работа направлена на ознакомление с основными характеристиками Windows Server 2003 и администрированием программно-аппаратной части информационно вычислительной системы, получение навыков по применению механизмов резервного копирования и восстановления.

Требования к результатам выполнения лабораторного практикума:

1. при выполнении задания необходимо сопровождать все проделанные действия

скриншотами и описаниями к ним

2. также необходимо придерживаться строгой последовательности действий, при выполнении заданий

3. сделать общий вывод и выводы по каждому заданию.

o При выполнении задания связанного с получением информации о системе, определить объекты ИВС, которые необходимо администрировать.

o При составлении плана резервного копирования указать, какие файлы Вы хотите архивировать, периодичность архивации и время выполнения.

o Проанализировать журнал резервного копирования. Сделать вывод о возможностях журнала.

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

2. Получить следующую информацию с помощью утилиты System Information (Сведения о системе):

- свойства компьютера
- пользовательские сеансы
- список ресурсов, открытых на сервере

4. Построить отчет с максимальным объемом данных о компьютере (системе).

5. Создать план резервного копирования

6. Выполнить резервное копирование различного типа с помощью программы Backup Utility (**Start** (Пуск) - **Programs** (Программы) - **Accessories** (Стандартные) - **System Tools** (Служебные) - **Backup** (Архивация данных)):

- Полное
- Инкрементное
- Ежедневное

7. Проанализировать журнал резервного копирования. Сделать выводы на основании анализа.

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Лабораторная работа № 10 «Оформление технической документации, правила оформления документов»

Цель работы: целью лабораторной работы является приобретение практических навыков разработки и оформления технических документов.

В процессе занятия решаются следующие задачи:

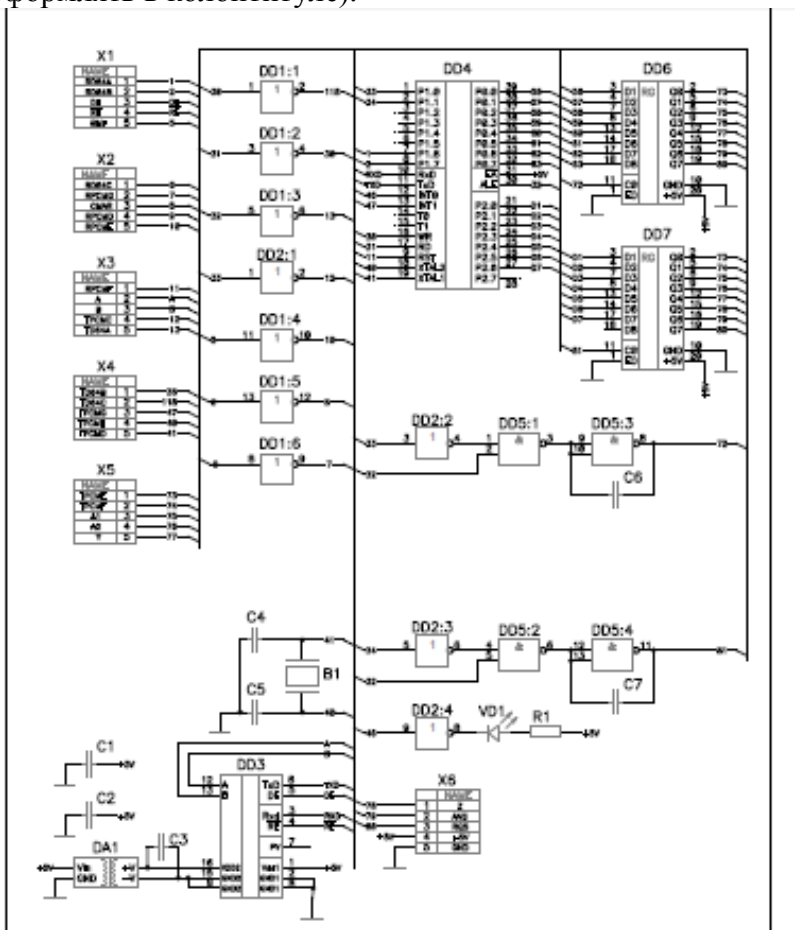
5. познакомить с основными настройками протокола TCP/ IP для работы с DHCP;
6. научить учащихся основным способам настройки TCP/IP;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Порядок работы

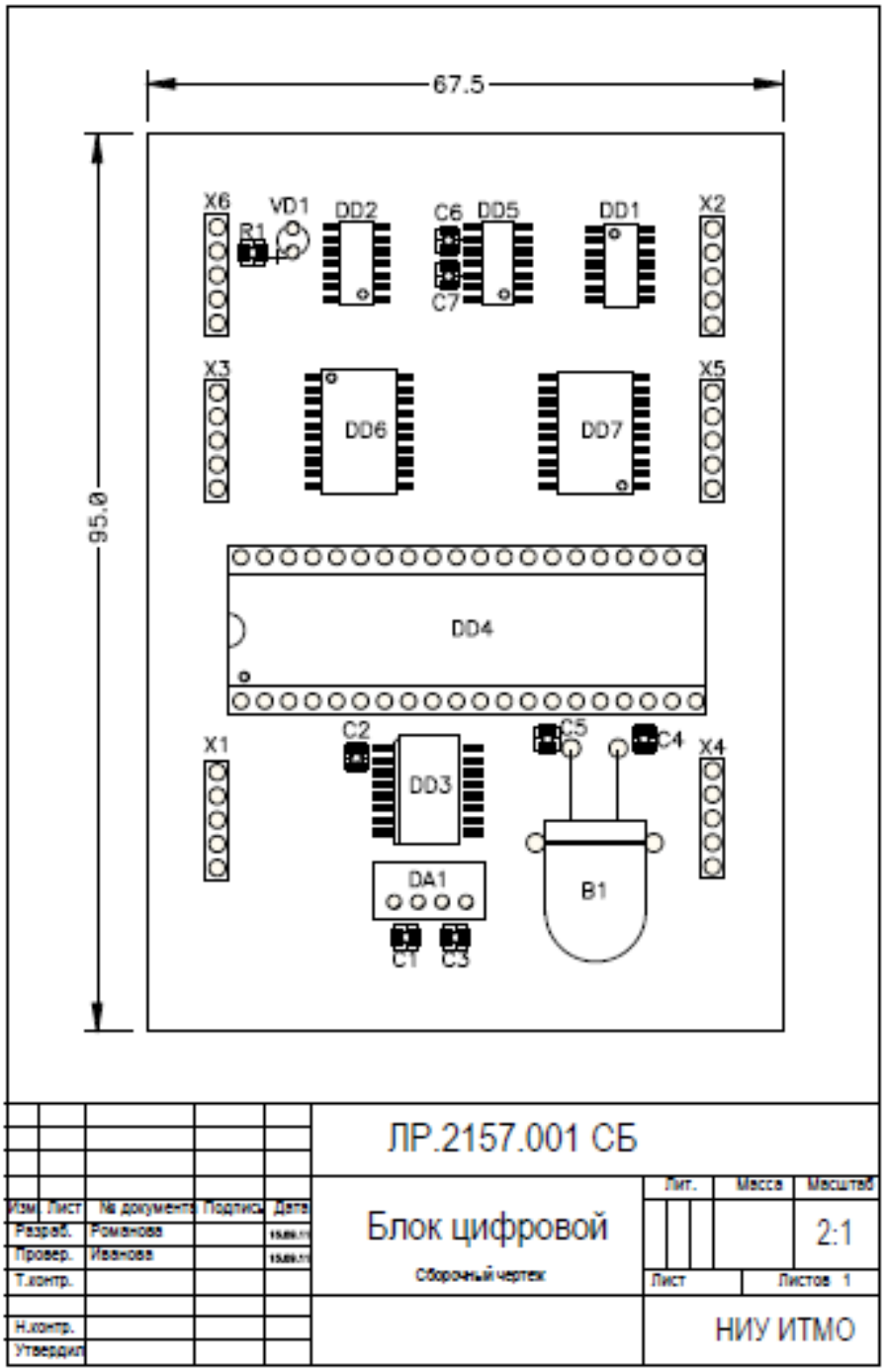
1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.

Задание: составить по ГОСТ ЕСКД в Microsoft Word комплект конструкторских документов (схему и чертеж вставлять в документ методом копирования из данного пособия, при этом изображение должно занимать не менее 75% пространства; основную надпись оформлять в колонтитуле).



Зона	Поз. обозна-чение	НАИМЕНОВАНИЕ	Кол.	Примечание
	B1	Резонатор кварцевый РК-379М	1	
		Конденсаторы		
	C4,C5	С-0805 33пФ	2	
	C1,C2, C3	С-0805 0,1мкФ	3	
	C6,C7	С-0805 1мкФ	2	
		Микросхемы		
	DA1	TME0505S	1	
	DD3	ADM2483BRW	1	
	DD4	AT89S52	1	
	DD6,DD7	ЭКФ1533ИР22	2	
	DD5	ЭКФ1533ЛА3	1	
	DD2	ЭКФ1533ЛН1	1	
	DD1	ЭКФ1533ЛП16	1	
	R1	Резистор RC-0805 750 Ом	1	
	VD1	Светодиод L934GT	1	
	X1… X6	Вилка PLS5	6	

					ЛР.2157.001 ПЭ3	
Изм.	Лист	№ докум.	Подпись	Дата		
Разраб.		Романова		10.06.11	Блок цифровой Перечень элементов	Лит. / Лист / Листов: 1
Пров.		Назимова		10.06.11		
Согл.						НИУ ИТМО
Н. контр.						
Утверд.						



6. Время выполнения работы 90 мин;

7. Контрольные вопросы

1) Какие документы включает конструкторская документация?

2) Какой документ является основным в технологической документации?

3) В каком случае оформляется титульный лист на комплект технологической документации?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

1. Работа оценивается на «пять баллов», если шаги выполнены верно, выводы сделаны правильно.

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

3. Работа оценивается на «три балла» если допущены 2 ошибки в выполнении работы, выводы сделаны правильно

Рекомендуемая литература

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