Министерство образования и науки РФ

ФГБОУ ВО «Томский государственный университет
систем управления и радиоэлектроники»
Кафедра комплексной информационной безопасности
электронно-вычислительных систем (КИБЭВС)

А.К. Новохрестов, А.И. Гуляев

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ

Часть 1

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность
телекоммуникационных систем»,
10.05.03 – «Информационная безопасность
автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

В-Спектр
Томск, 2017

УДК 004.056
ББК 32.973.26-018.2
Н 76

Н 76 **Новохрестов А.К., Гуляев А.И.** Безопасность сетей ЭВМ. Ч. 1: лабораторный практикум. – Томск: В-Спектр, 2017. – 92 с.
ISBN 978-5-91191-367-0

Практикум содержит описания лабораторных работ по дисциплине «Безопасность сетей ЭВМ» для специальностей 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность», а также дисциплины «Администрирование сетей ЭВМ» для специальности 10.05.02 – «Информационная безопасность телекоммуникационных систем» задания, методические указания по выполнению, вопросы для самоконтроля.

УДК 004.056
ББК 32.973.26-018.2

Работа выполнена при финансовой поддержке Министерства образования и науки РФ в рамках базовой части государственного задания ТУСУР на 2017–2019 годы (проект № 2.8172.2017/8.9)

ISBN 978-5-91191-367-0

СОДЕРЖАНИЕ

Введение

Лабораторный практикум подготовлен с целью обучения студентов специальностей 10.05.02 – «Информационная безопасность телекоммуникационных систем», 10.05.03 – «Информационная безопасность автоматизированных систем», 10.05.04 – «Информационно-аналитические системы безопасности» и направления 10.03.01 – «Информационная безопасность» работе с базовыми механизмами администрирования компьютерных сетей.

В процессе выполнения лабораторных работ студенты используют виртуальные операционные системы, созданные для каждого из занятий. За счет использования технологии виртуализации достигается интерактивность проведения занятий. Данная технология позволяет предоставить студентам полнофункциональную тестовую учебную среду, содержащую локальную операционную систему с установленным программным обеспечением. Использование виртуализации дает ряд преимуществ, например, студент может работать с операционной системой, имея права администратора системы. Гибкость применения технологии виртуализации заключается в возможности простой интеграции учебной среды в любую компьютеризированную аудиторию. Дополнительная возможность – использование полнофункционального учебного стенда при самостоятельной работе вне вуза.

Практикум содержит в себе работы, которые позволят студентам на примере операционной системы Windows освоить основные принципы по управлению компьютерными сетями. Данная среда была выбрана ввиду высокой популярности среди пользователей и удобства в плане наглядного представления настройки систем. В лабораторных работах данной части руководства используется Windows 7 и Windows Server 2012.

Помимо средств Windows в лабораторных работах применяются программные продукты Cisco Packet Tracer и SUMo.

В процессе выполнения комплекса лабораторных работ студенты в интерактивной форме освоят профессиональные компетенции, обозначенные в основной образовательной программе по данной дисциплине.

Так студенты специальности 10.03.01 – «Информационная безопасность» смогут освоить навыки организации технологического процесса защиты информации ограниченного доступа в компьютерных сетях, которые входят в компетенцию ПК-15, а также освоят базовые навыки управления компьютерными сетями и механизмами их защиты, что составляет компетенцию ПК-2.

Обучающиеся по направлению 10.05.02 – «Информационная безопасность телекоммуникационных систем», выполнив лабораторные

работы 1 и 2 освоят навыки настройки и обслуживания телекоммуникационного оборудования, что соответствует профессиональной компетенции ПК-14.

Студенты специальности 10.05.03 – «Информационная безопасность автоматизированных систем» получат должные навыки по компетенции ПК-26 «Способность администрировать подсистему информационной безопасности автоматизированной системы».

В свою очередь, студенты направления 10.05.04 – «Информационно-аналитические системы безопасности», рассмотрев процесс настройки параметров безопасности групповых политик домена, приобретут навыки применения основных защитных механизмов и средств обеспечения безопасности компьютерных сетей, составляющие компетенции ПК-9 и ПК-10.

ЛАБОРАТОРНАЯ РАБОТА №1
Cisco Packet Tracer

1. Цель работы

Целью лабораторной работы является освоение пакета «Cisco Packet Tracer», изучение его интерфейса и основных элементов, а также получение навыка создания сетей с дальнейшим их тестированием. В заключительной части работы необходимо собрать сеть, изображенную на рисунке, и проверить её работу.

2. Краткие теоретические сведения

Сетевые технологии лучше всего изучать на практике, посредством подключения устройств к сетям и наблюдения соответствующих процессы. Инновационное средство визуализации и моделирования сетей Cisco Packet Tracer поможет надежно закрепить навыки конфигурирования – результаты вашей работы отображаются непосредственно на экране настольного или мобильного устройства. Packet Tracer поможет вам:

– закрепить свои навыки при подготовке к собеседованию;

– подготовиться к сертификационному экзамену;

– опробовать на практике знания, полученные в ходе учебных курсов;

– овладев необходимыми навыками, вы сможете приступить к построению карьеры в сфере Интернета вещей.

В данной лабораторной работе будут рассмотрены устройства, работающие на трех уровнях сетевой модели OSI: первый уровень OSI – физический, второй уровень – уровень передачи данных и третий уровень – сетевой.

Маршрутизатор или роутер (транслитерация английского слова) – специализированный сетевой компьютер, имеющий два или более сетевых интерфейса и пересылающий пакеты данных между различными сегментами сети. Маршрутизатор может связывать разнородные сети различных архитектур. Для принятия решений о пересылке пакетов используется информация о топологии сети и определённые правила, заданные администратором. Маршрутизаторы работают на сетевом (третьем) уровне сетевой модели OSI.

Сетевой мост или коммутатор (жарг. свич от англ. switch – переключатель) – устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети. Коммутатор работает на канальном (втором) уровне модели OSI.

Коммутаторы были разработаны с использованием мостовых технологий и часто рассматриваются как многопортовые мосты.

В отличие от концентратора или хаба (1 уровень OSI), который распространяет трафик от одного подключённого устройства ко всем остальным, коммутатор передаёт данные только получателю (исключение составляет широковещательный трафик всем узлам сети и трафик для устройств, для которых неизвестен исходящий порт коммутатора). Это повышает производительность и безопасность сети, избавляя остальные сегменты сети от необходимости (и возможности) обрабатывать данные, которые им не предназначались.

3. Ход работы

3.1. Изучение интерфейса

Для работы с пакетом «Tracer» необходим аккаунт. Создайте его или работайте без авторизации, нажав «Guest Login» (рис. 1).

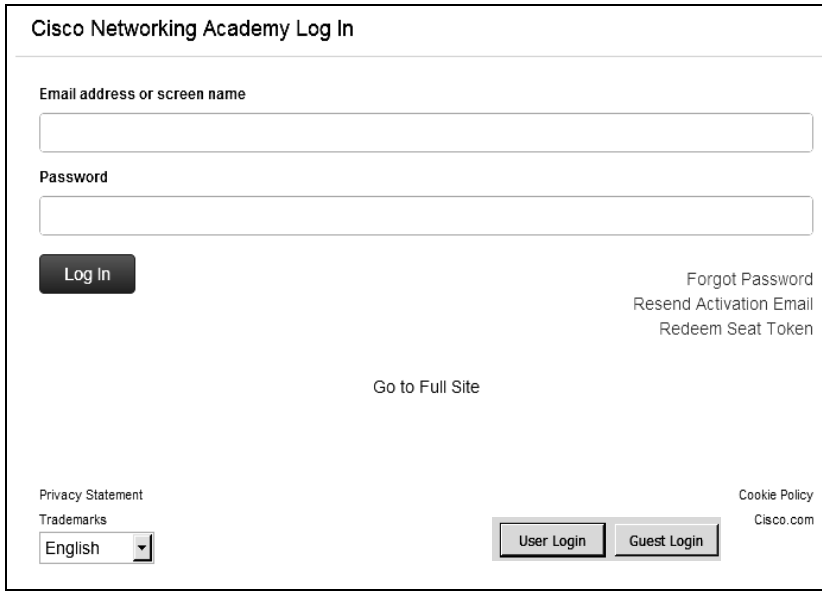

Рис. 1. Окно входа

При нажатии на кнопку «Guest Login» запустится таймер и откроется web-страница, которую можно закрыть. По истечению таймера нужно нажать «Confirm Guest», чтобы открылось основное окно программы «Tracer» (рис. 2).

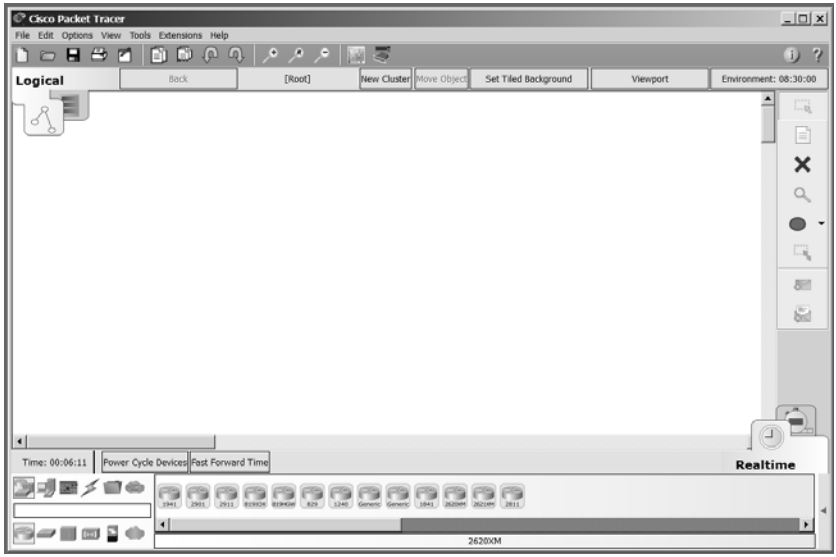

Рис. 2. Основное окно пакета «Tracer»

На основной панели располагаются иконки работа с файлом, работа с буфером и изменениями, работа с видом (отдаление или приближение), палитра и настройка шаблонов устройств. Главная панель приведена на рис. 3.

Рис. 3. Главная панель

Важным элементом интерфейса является панель управления рабочим пространством (рис. 4). Она позволяет переключаться между физическим и логическим пространствами. Здесь же расположены кнопки для навигации и для создания элементов, таких как кластеры, здания, шкафы оборудования и др.

Рис. 4. Панель управления рабочим пространством

Справа расположена панель инструментов для работы с рабочим пространством (рис. 5), где расположены инструменты «Выбрать», «Ус-

тановить заметку», «Удалить», «Осмотреть», «Нарисовать цветную фигуру», «Изменить размер», а также нужные для тестирования инструменты добавления PDU, обычного и пользовательского.

Примечание: Protocol Data Unit (PDU) – обобщённое название фрагмента данных на разных уровнях модели OSI: кадр Ethernet, IP-пакет, UDP-датаграмма, TCP-сегмент и т.д.

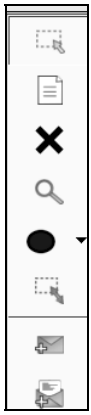

Рис. 5. Панель инструментов для работы с рабочим пространством

На панели управления временем в рабочем пространстве (рис. 6) расположен переключатель между режимом реального времени и симуляцией. В режиме реального времени можно сбросить настройки сети или промотать время вперед на 30 секунд. В режиме симуляции можно задать, пакеты каких протоколов нужно отображать, и регулировать скорость их прохождения по сети.

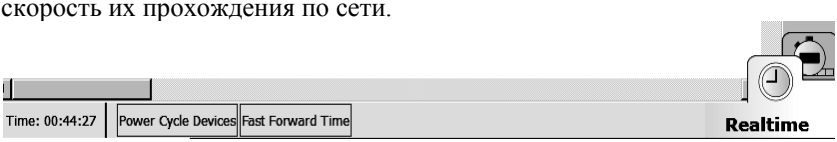

Рис. 6. Панель управления временем

Панель управления симуляциями представлена на рис. 7.

Ниже расположена панель с элементами сети, такими как маршрутизаторы, сетевые коммутаторы, компьютеры и др. На этой панели расположен список сценариев (открывается по клику на стрелочку справа), который отображает, успешно ли были отправлены PDU-пакеты. Панель элементов и сценариев приведена на рис. 8.

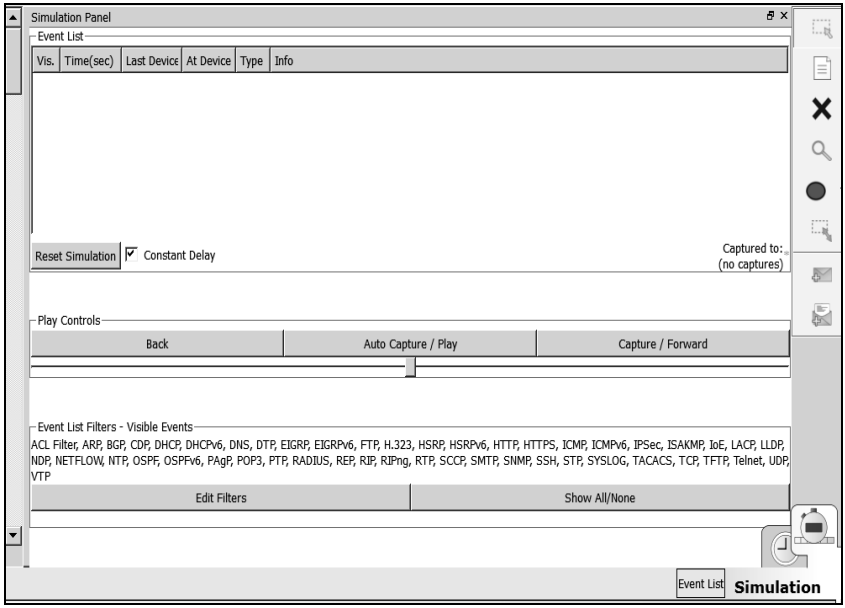

Рис. 7. Панель управления симуляциями

Рис. 8. Панель элементов и сценариев

3.2. Создание малой сети

Необходимо создать малую сеть, для этого понадобятся маршрутизаторы, сетевые коммутаторы и несколько компьютеров. В логической рабочей среде выберите маршрутизатор модели 1941 (рис. 9).

Создайте коммутатор модели 2960 и соедините его с маршрутизатором кабелем «Copper Cross-Over» (рис. 10). Все кабели находятся в группе со значком молнии. При соединении маршрутизатора и коммутатора необходимо выбирать гигабитный интерфейс (рис. 11).

Разместите точку доступа Wi-fi, один персональный компьютер и один ноутбук. Точки доступа Wi-fi находятся в разделе «Wireless Devices», компьютеры – во вкладке «End Devices». Выбирайте устройства модели «Generic» (рис. 12).

Соедините устройства кабелем «Copper Straight-Through», как показано на рис. 13 и 14. Необходимо подключать FastEthernet порты.

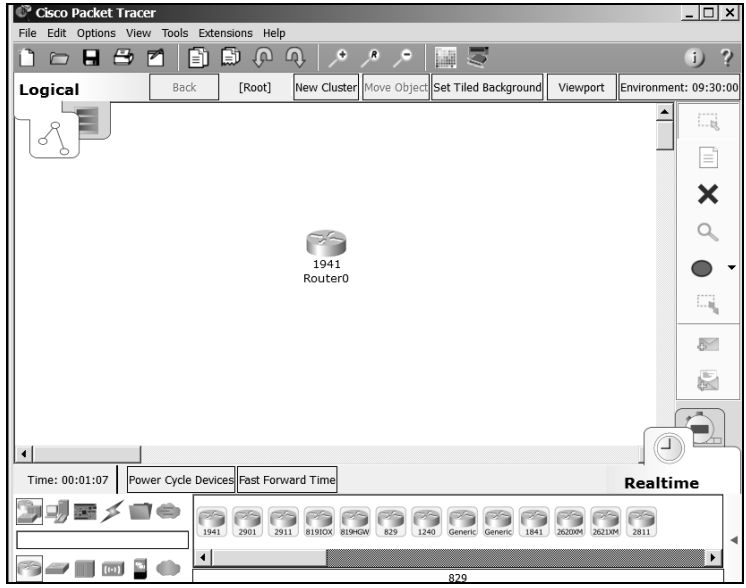

Рис. 9. Размещение маршрутизатора

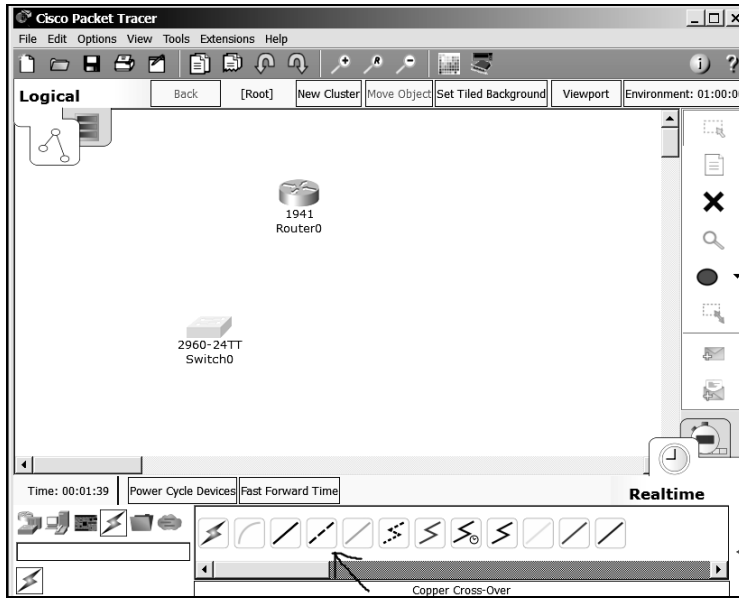

Рис. 10. Размещение коммутатора и выбор кабеля

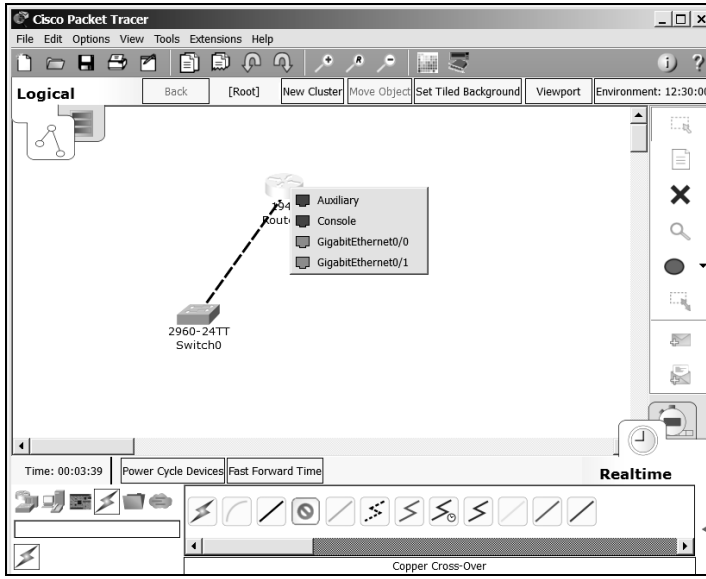

Рис. 11. Подключение кабеля к гигабитному интерфейсу

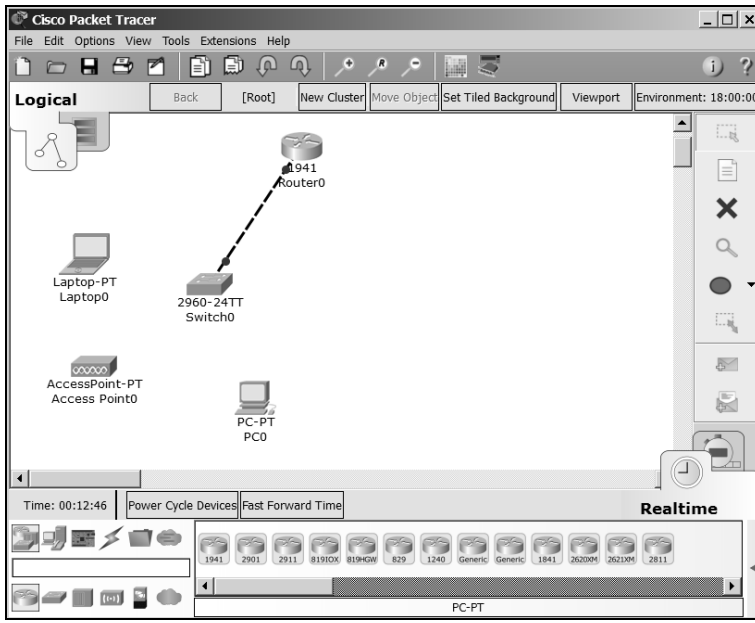

Рис. 12. Размещение компьютеров и точки доступа Wi-fi

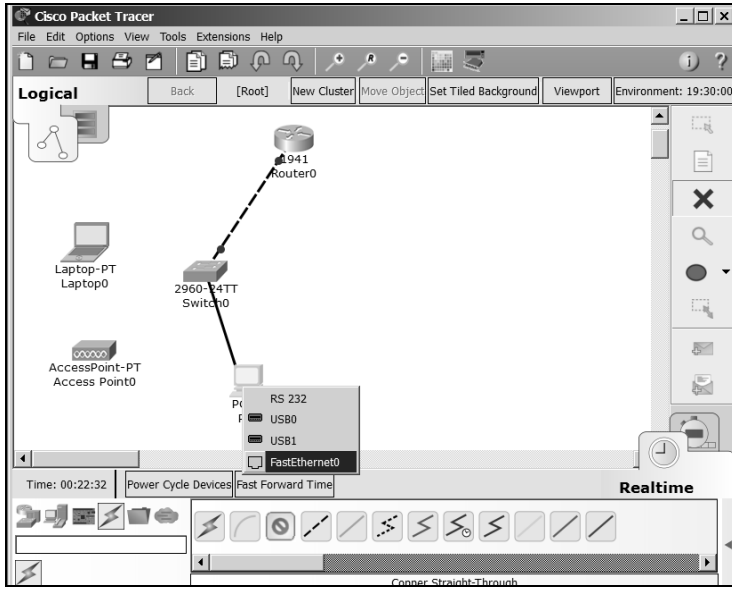

Рис. 13. Соединение коммутатора и компьютера

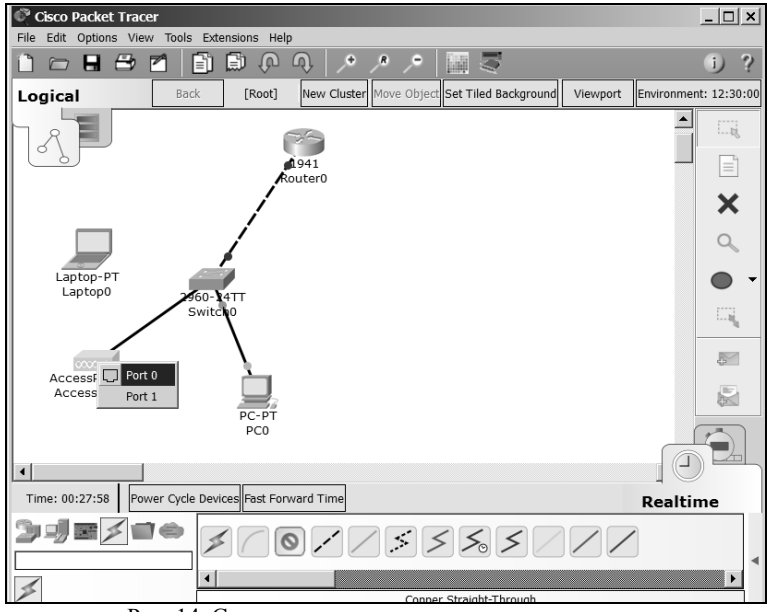

Рис. 14. Соединение коммутатора и точки доступа

3.3. Настройка малой сети

Чтобы компьютеры могли обмениваться пакетами внутри сети, необходимо настроить сеть. Начните с настройки маршрутизатора. При двойном щелчке на маршрутизаторе появится окно настроек (рис. 13).

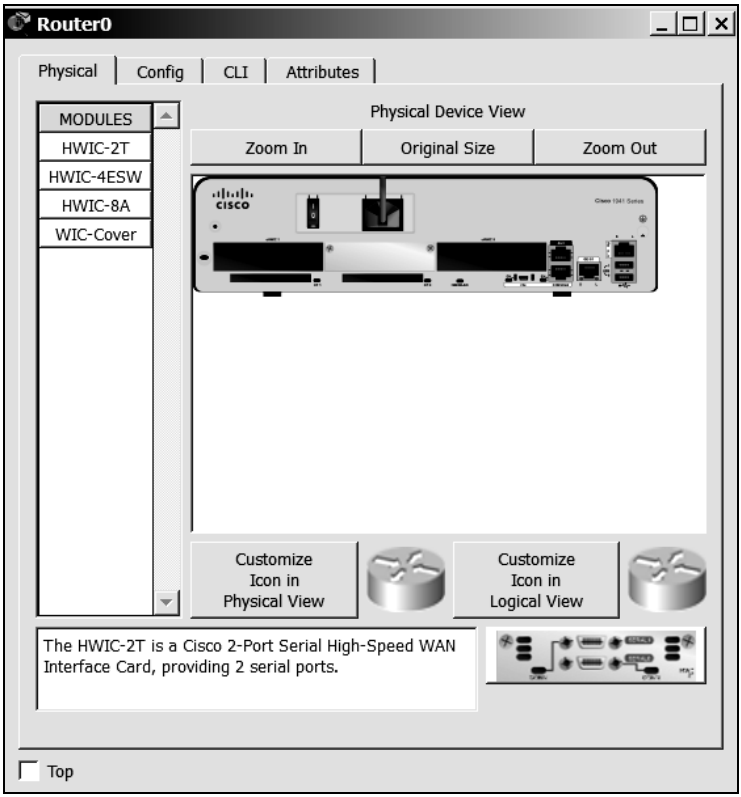

Рис. 15. Окно настроек маршрутизатора

В первой вкладке окна можно включить или выключить маршрутизатор, просмотреть подключенные к нему модули. Откройте вкладку Config. В ней необходимо переименовать маршрутизатор и присвоить IP-сети (рис. 16). При этом стоит учитывать, что устройство имеет два имени: одно – условное, другое – для обращения к устройству.

Откройте группу интерфейсов и нажмите на гигабитный порт, к которому подключен кабель. Чтобы узнать, к какому порту подключен кабель, наведите мышку на кабель (рис. 17).

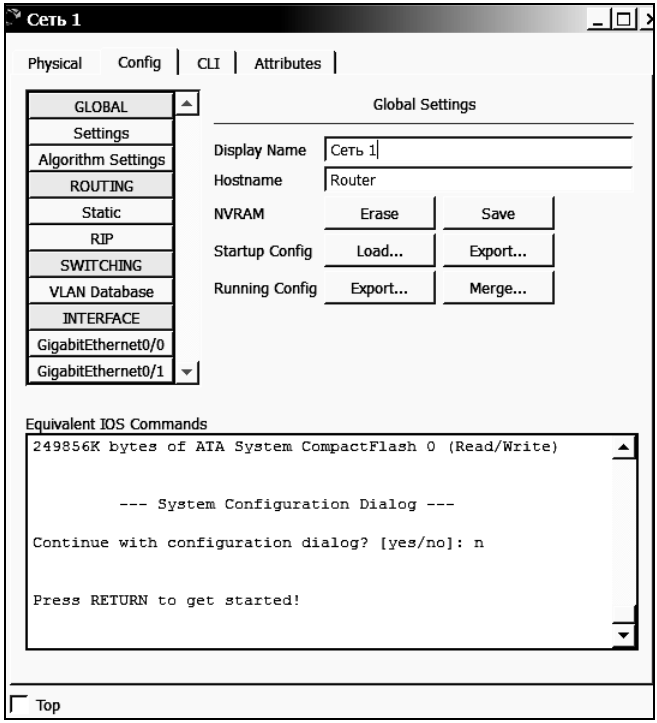

Рис. 16. Изменение названия маршрутизатора

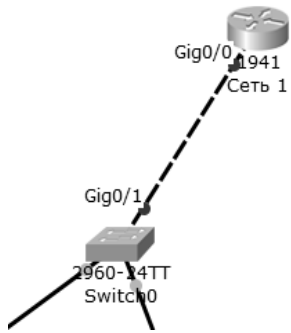

Рис. 17. Используемые порты

В данном случае у маршрутизатора используется нулевой гигабитный порт. Присвойте IP-адрес сетевому шлюзу. Настройте его, как показано на рис. 18.

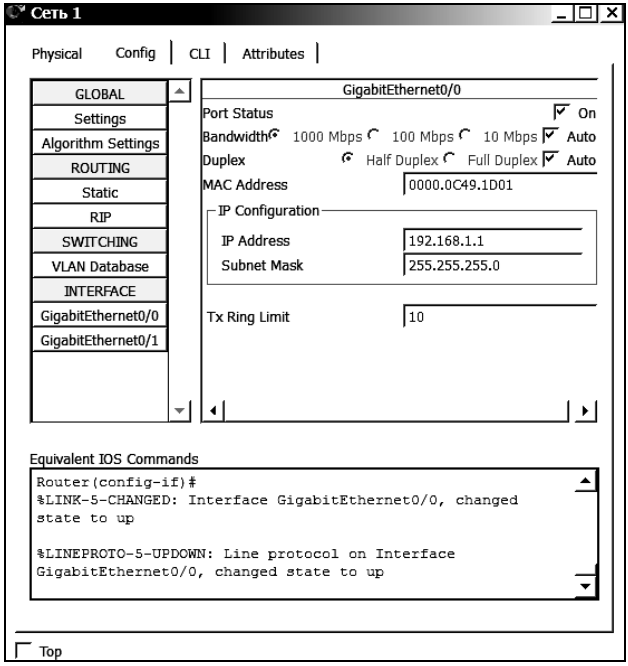

Рис. 18. Настройки сетевого шлюза

Необходимо убедиться, что напротив «Port Status» стоит галочка, иначе порт будет неактивным. Сделайте запись в настройках прокола RIP о настраиваемой сети, чтобы маршрутизатор мог перенаправлять пакеты в другие сети и получать пакеты из других сетей. Нужно добавить IP-адрес шлюза, т.е. 192.168.1.1, в записи (рис. 19).

Настройте IP-адреса компьютеров в сети для обмена данными. Можно начать с настольного ПК, по двойному щелчку по нему откроется окно настроек (рис. 20).

У компьютера тоже можно менять модули в зависимости от необходимого типа интерфейса. В данном случае ничего менять не нужно. Перейдите во вкладку Desktop и выберите IP Configuration. Здесь нужно задать компьютеру IP-адрес в локальной сети и адрес сетевого шлюза по умолчанию (рис. 21).

Аналогично настраивается IP-адрес ноутбука. Учитывайте, что адрес должен быть уникальным, поэтому нужно изменить последний байт адреса (увеличить последнее число на 1). Чтобы подключить ноутбук к Wi-fi, сначала нужно установить на него модуль Wi-fi. Для установки модулей на какое-либо устройство нужно сперва отключить устройство кнопкой на нем (рис. 22).

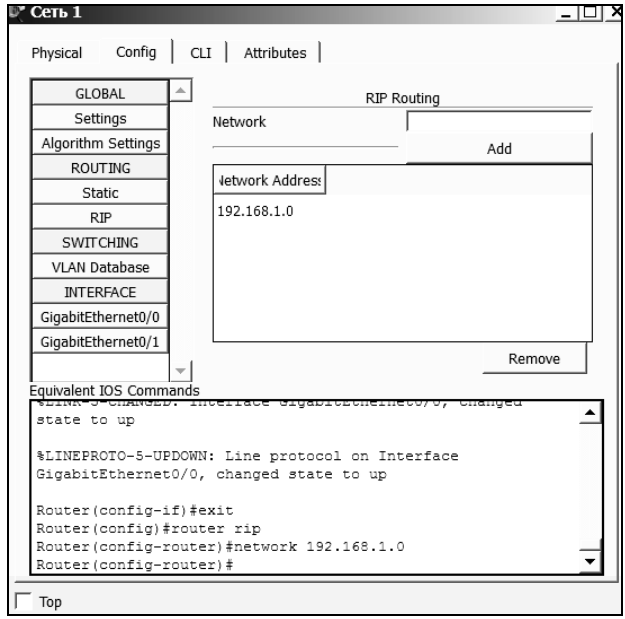

Рис. 19. Настройка протокола RIP

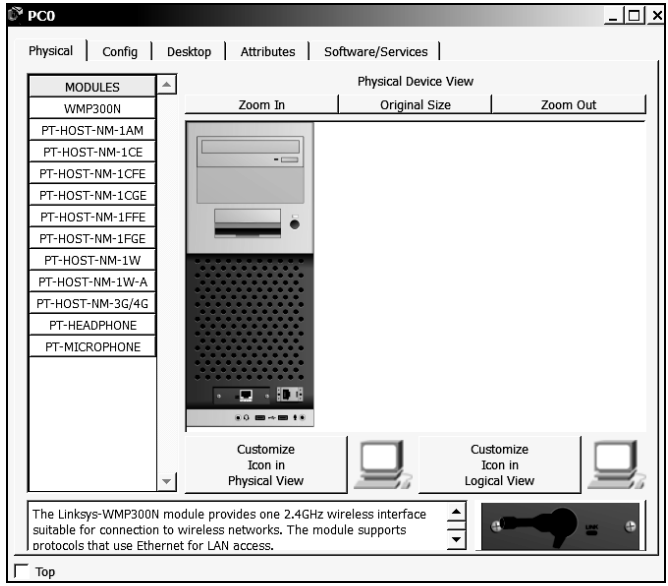

Рис. 20. Окно настроек компьютера

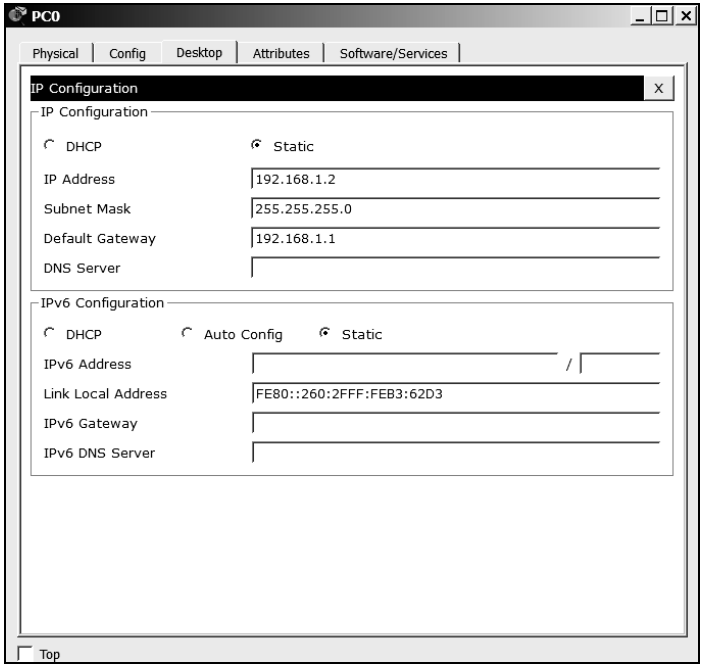

Рис. 21. Настройка адреса компьютера

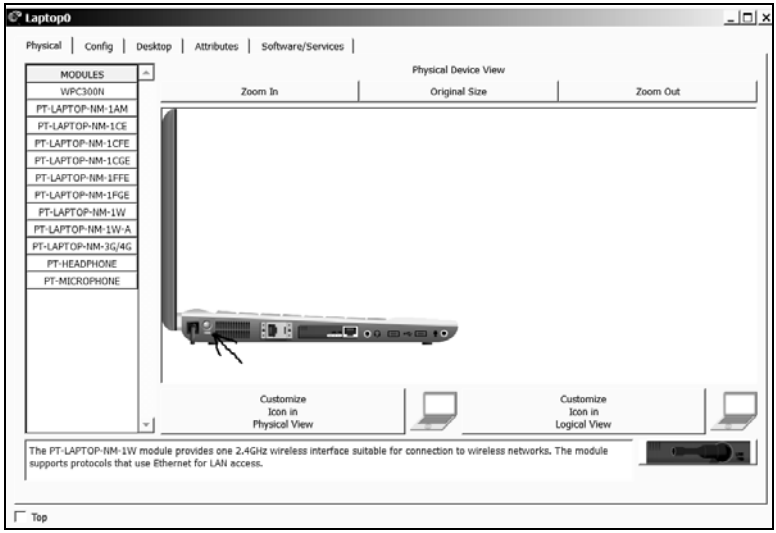

Рис. 22. Выключение ноутбука

Затем нужно удалить подключенный в текущий момент модуль, перетащив его в раздел модулей, как показано на рис. 23.

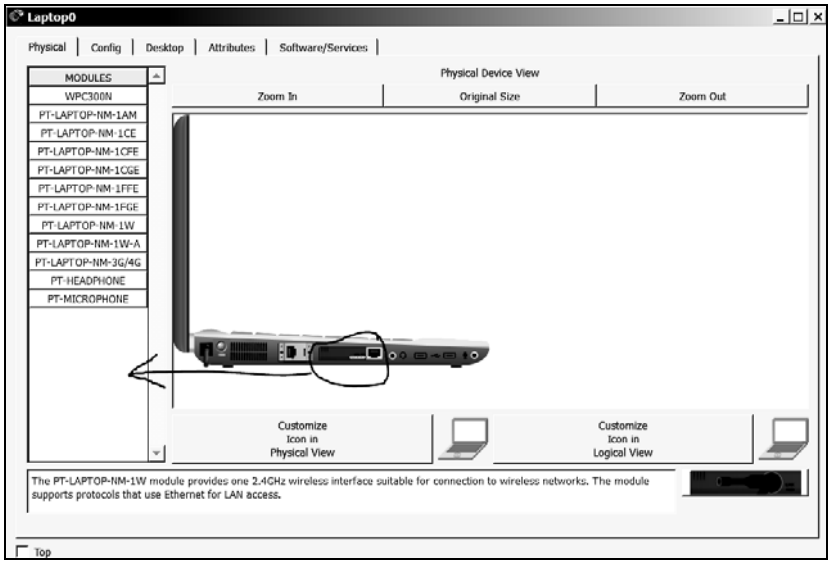

Рис. 23. Удаление модуля

Установите в ноутбук модуль Wi-fi WPC300N, после чего включите ноутбук кнопкой на нем (рис. 24).

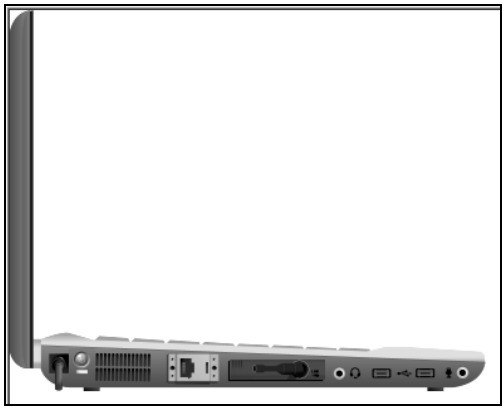

Рис. 24. Установленный Wi-fi модуль

Перейдите во вкладку Desktop и там выберите PC Wireless. Через вкладку Connect подключитесь к сети (рис. 25).

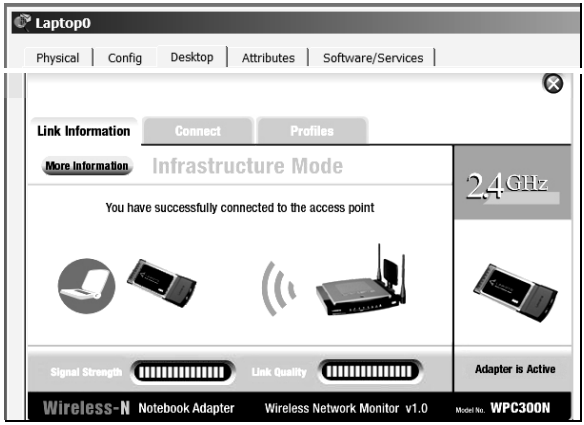

Рис. 25. Установленное с точкой доступа соединение

В результате должна получиться сеть как на рис. 26. Для проверки работы сети отправьте PDU-пакеты от ноутбука к настольному компьютеру (иконка конверта на правой панели). Увидеть, что передача прошла успешно, можно в списке тестов, который откроется, если кликнуть на стрелочку справа на нижней панели. Если пакет не прошел (Failed), можно сделать повторную отправку, дважды кликнуть на значке Fire. Successful означает успешную отправку.

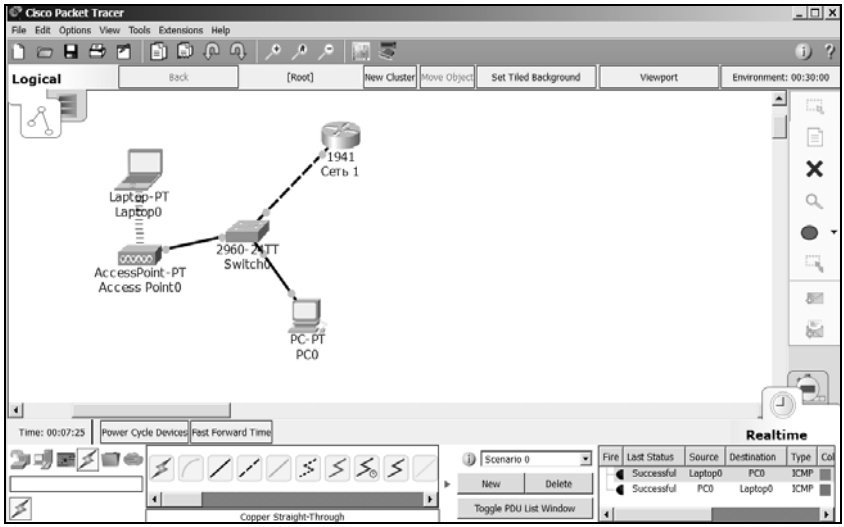

Рис. 26. Работающая сеть

3.4. Настройка нескольких маршрутизаторов

В реальных сетях используется больше устройств, поэтому нужно уметь настраивать обмен пакетами между маршрутизаторами. Добавьте в существующую сеть еще один маршрутизатор 1941 и подключите к нему модуль HWIC-2T (рис. 27). Не забудьте выключить маршрутизатор перед установкой модуля. При выключении устройств их настройки сбрасываются, так что сохраните настройки устройства или задайте их еще раз.

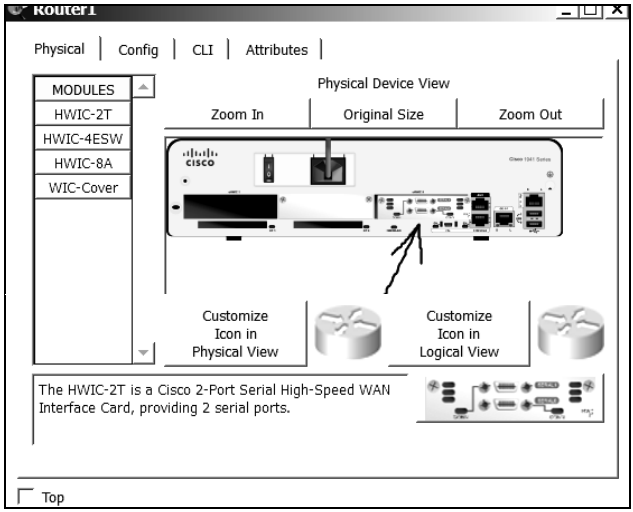

Рис. 27. Установленный модуль

Данный модуль нужен для подключения Serial DTE кабеля, так как маршрутизаторы, которые находятся на большом друг от друга расстоянии, не соединить обычным сетевым кабелем. Модули нужно установить на оба маршрутизатора, после чего соединить их Serial DTE кабелем (рис. 28).

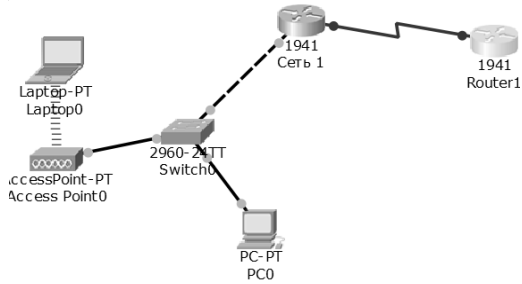

Рис. 28. Соединенные маршрутизаторы

Теперь маршрутизаторы нужно настроить для обмена пакетами. Откройте настройки маршрутизатора и в группе интерфейсов выберите порт, к которому подключен кабель Serial DTE. Задайте настройки для интерфейса (рис. 29).

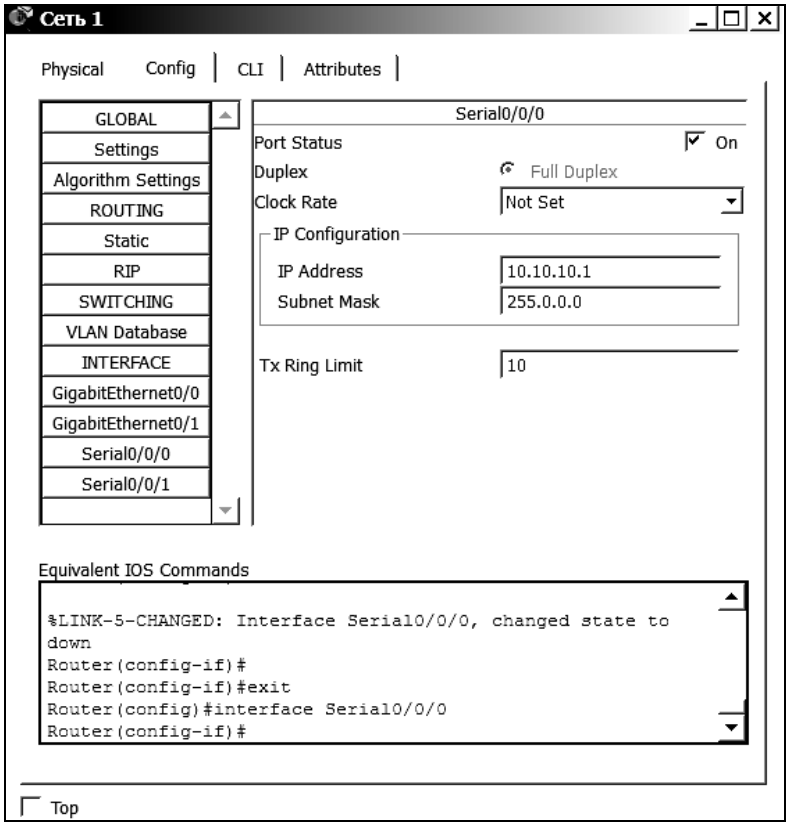

Рис. 29. Настройка интерфейса

Добавьте в список адресов RIP настраиваемую сеть (рис. 30).

Проделайте те же действия на втором маршрутизаторе (не забывайте про уникальность адресов). Когда закончите, отправьте PDU-пакеты от дальнего маршрутизатора к компьютерам (рис. 31).

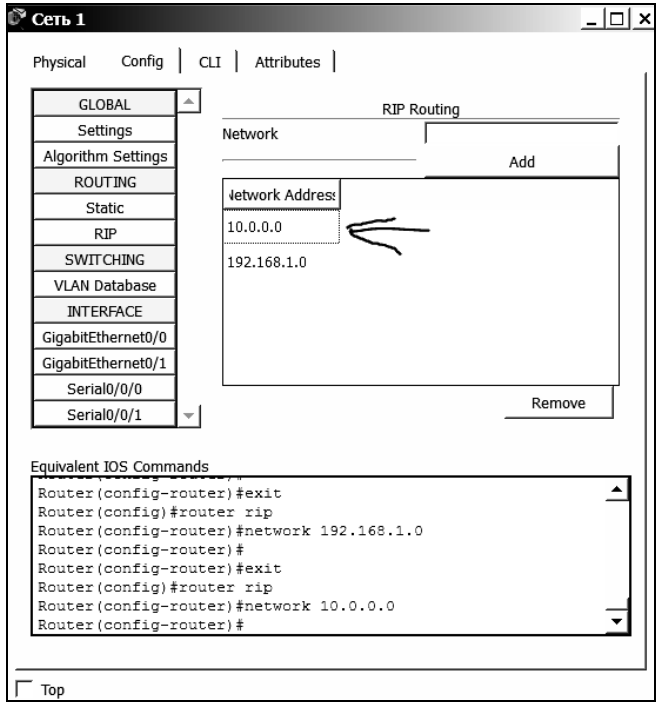

Рис. 30. Список адресов RIP

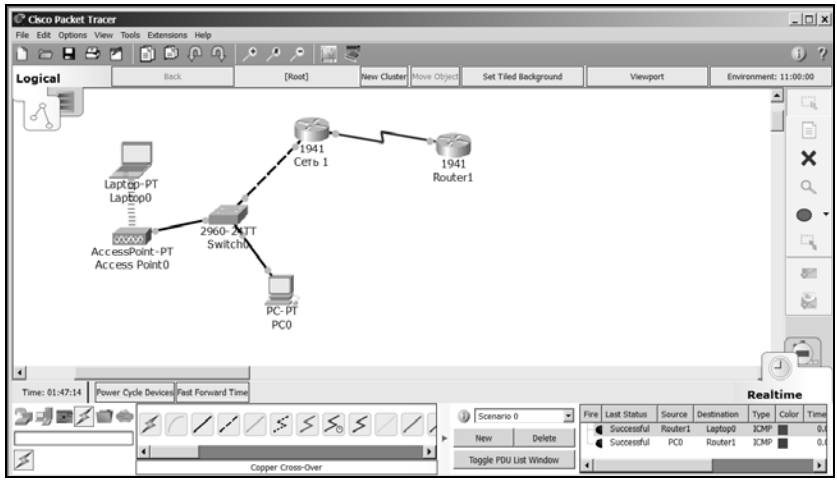

Рис. 31. Рабочий обмен пакетами между маршрутизаторами

3.5. Настройка сети в физической рабочей среде

Основное назначение физической среды – дать возможность посмотреть размах вашей сети в физическом мире. В физической среде есть несколько уровней, на каждом отображаются разные объекты. Основные уровни: межгород, город, офис и стойка оборудования. При переключении на физическую рабочую среду откроется город, в котором вы работаете – Home City. Можно переместить его или создать еще один город (рис. 32).

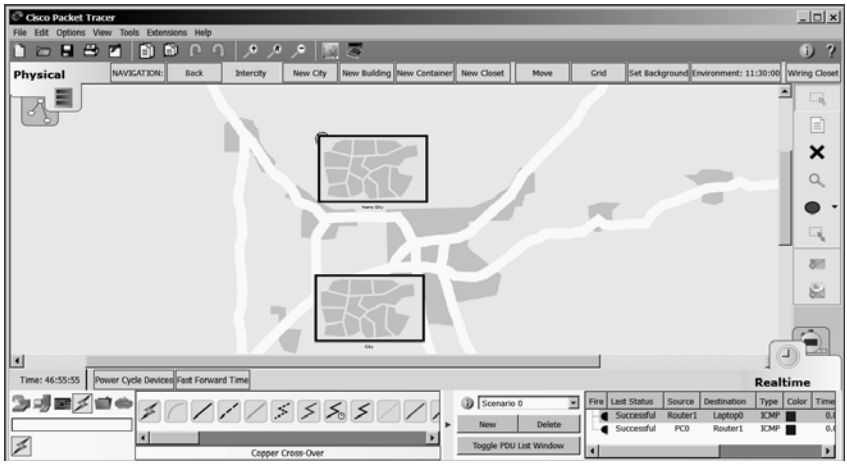

Рис. 32. Уровень межгорода

Кликните на Home City, чтобы перейти на уровень города (рис. 33). В этом уровне можно размещать и передвигать офисы.

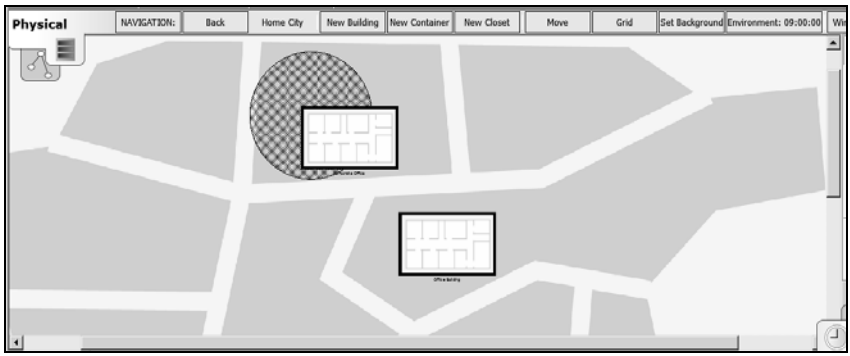

Рис. 33. Уровень города

Перейдите в Corporate Office. В офисе можно видеть оборудование, размещенное хаотично, как на рис. 34.

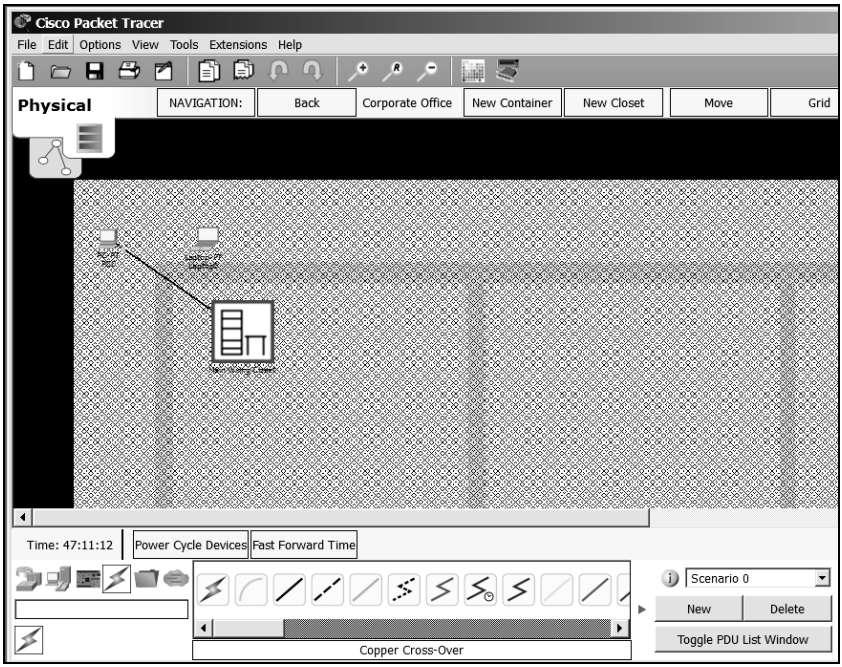

Рис. 34. Уровень офиса

Чтобы навести порядок, переместите все оборудование в стойку оборудования. Для этого выберите сверху инструмент «Move». и выберите оборудование (рис. 35).

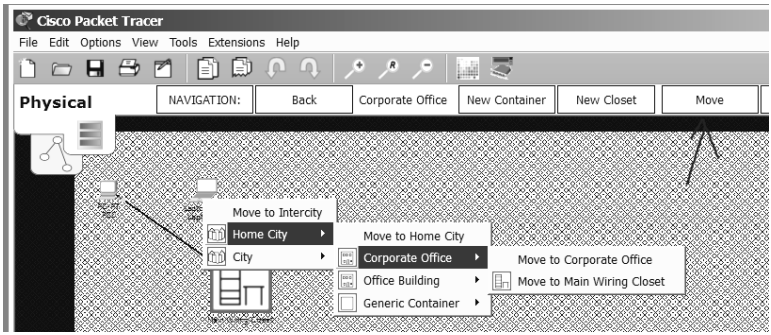

Рис. 35. Перемещение оборудования

В итоге должна получиться стойка оборудования как на рис. 36. Можно видеть, какое оборудование включено, какие порты заняты и какие устройства к чему подключены.

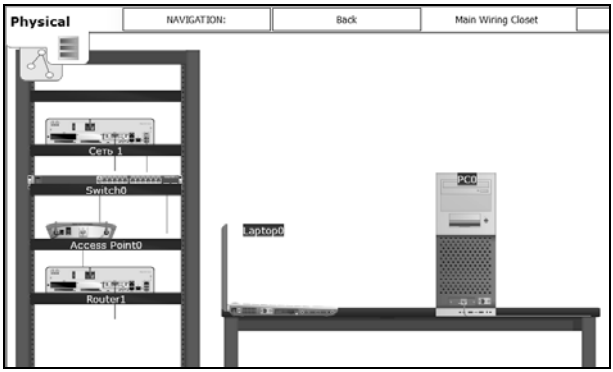

Рис. 36. Стойка оборудования

4. Задание на лабораторную работу

1. Ознакомиться с теорией.
2. Выполнить представленные задания.
3. Настроить сеть, представленную на рис. 37. В верхнем участке сети реализовать любую из следующих топологий:

– физическая «шина» (bus);
– физическая «звезда» (star);
– физическое «кольцо» (ring);
– физическая «звезда» и логическое «кольцо» (Token Ring).

4. Показать успешную отправку PDU-пакета по сети.
5. Составить по проделанной работе отчет.

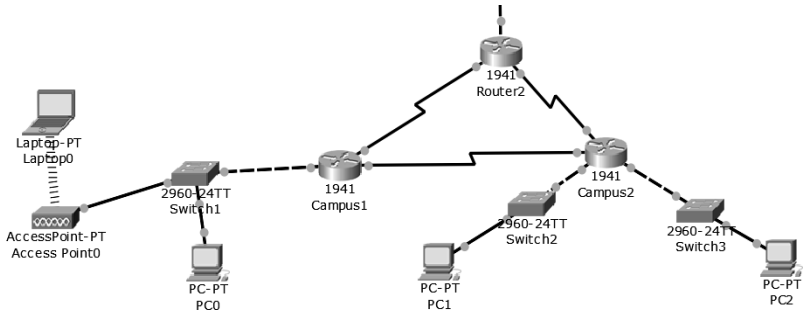

Рис. 37. Сеть для самостоятельной сборки и настройки

5. Контрольные вопросы

1. Что представляет собой пакет «Tracer»?
2. Что такое маршрутизатор?
3. Чем маршрутизатор отличается от сетевого коммутатора?
4. Как настроить обмен пакетами между маршрутизаторами?
5. Что означает цвет кружков на линии связи между двумя устройствами?
6. Какие есть способы настройки маршрутизации в пакете «Tracer»?
7. Для чего используется инструмент Inspect?
8. Какие рабочие среды (workspace) есть в пакете «Tracer» и для чего они нужны?
9. Как подключить ПК к сети в пакете «Tracer»?
10. Для чего нужен Serial DTE кабель?

ЛАБОРАТОРНАЯ РАБОТА №2
Cisco Packet Tracer. Виртуальные локальные сети

1. Цель работы

Целью данной работы является изучение работы с VLAN в пакете «Tracer» от Cisco, создание и тестирование собственной VLAN. Будет рассмотрена настройка оборудования CISCO при помощи CLI (англ. Command Line Interface).

2. Краткие теоретические сведения

Сетевые технологии лучше всего изучать на практике, посредством подключения устройств к сетям и наблюдения соответствующих процессы. Инновационное средство визуализации и моделирования сетей Cisco Packet Tracer поможет надежно закрепить навыки конфигурирования – результаты вашей работы отображаются непосредственно на экране настольного или мобильного устройства. Packet Tracer поможет вам:

– закрепить свои навыки при подготовке к собеседованию;

– подготовиться к сертификационному экзамену;

– опробовать на практике знания, полученные в ходе учебных курсов;

– овладев необходимыми навыками, вы сможете приступить к построению карьеры в сфере Интернета вещей.

VLAN (аббр. от англ. Virtual Local Area Network) – логическая («виртуальная») локальная компьютерная сеть, представляет собой группу хостов с общим набором требований, которые взаимодействуют так, как если бы они были подключены к широковещательному домену, независимо от их физического местонахождения. VLAN имеет те же свойства, что и физическая локальная сеть, но позволяет конечным станциям группироваться вместе, даже если они не находятся в одной физической сети. Такая реорганизация может быть сделана на основе программного обеспечения вместо физического перемещения устройств

Широковещательный домен – область сети, в которой происходит обмен широковещательными сообщениями и устройства могут отправлять друг другу сообщения непосредственно, без участия маршрутизатора.

3. Ход работы

3.1. Создание сети

Для выполнения работы необходимо создать два маршрутизатора 1941, два коммутатора 2960 и шесть компьютеров или ноутбуков. Для более удобной настройки переименуйте их как на рис. 1.

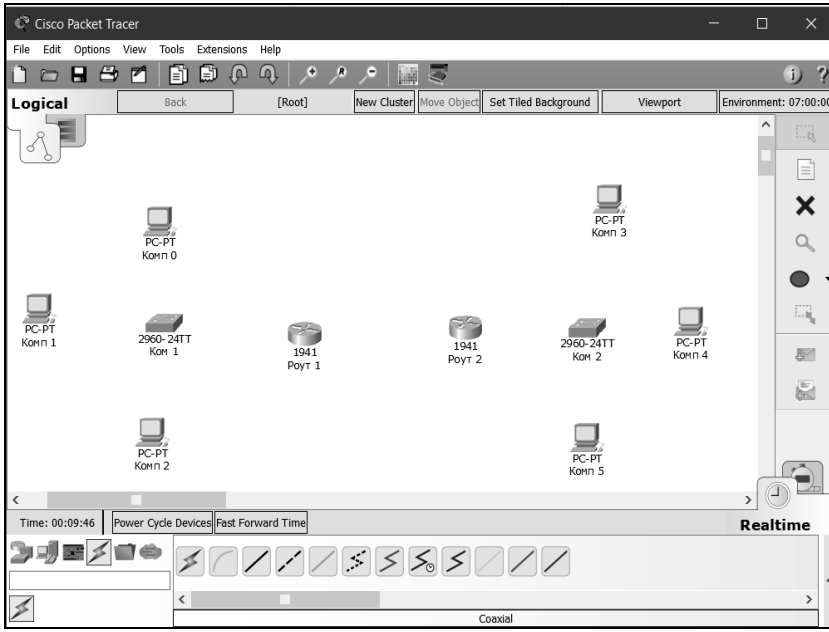

Рис. 1. Создание оборудования

Соедините устройства согласно данным табл. 1.

Таблица 1

Соединение устройств

Устройство 1	Устройство 2	Тип кабеля	Интерфейс устройства 1	Интерфейс устройства 2
Комп 0	Ком 1	Copper Straight-Through	Fa0	Fa0/1
Комп 1	Ком 1			Fa0/2
Комп 2	Ком 1			Fa0/3
Комп 3	Ком 2			Fa0/1
Комп 4	Ком 2			Fa0/2
Комп 5	Ком 2			Fa0/3
Ком 1	Роут 1	Copper Cross-Over	Gig0/1	Gig0/1
Ком 2	Роут 2			
Роут 1	Роут 2	Serial DTE	Se0/0/0	

Не забывайте, что для соединения роутеров, в них должен быть установлен модуль HWIC-2T. В итоге получится сеть, как на рис. 2.

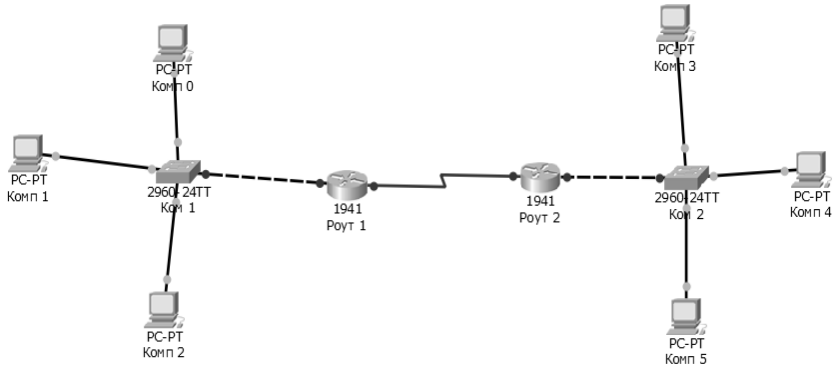

Рис. 2. Соединенные устройства

3.2. Настройка устройств

Нужно создать внутри одной сети три виртуальные (VLAN). Виртуальные сети позволяют разделять на группы устройства, подключенные к одному коммутатору, уменьшить широковещательный трафик в сети, увеличить безопасность сети или уменьшить количество сетевого оборудования и так далее. Так как реальное оборудование Cisco настраивается в основном с помощью интерфейса командной строки, то большую часть настройки будем выполнять с её помощью.

Используемые команды:

ena – включить устройство;

conf t – войти в режим настройки устройства;

vlan * – создать виртуальную сеть *;

exit – выйти из текущего режима настройки;

int * – режим настройки интерфейса *;

switchport mode access – переключить режим порта на статичный доступ;

switchport mode trunk – переключить режим порта на магистральный;

switchport access vlan * – переключить порт на виртуальную сеть *;

ip address * # – задать текущему интерфейсу адрес * с маской #;

no shut – включить интерфейс;

encapsulation dot1Q * – включение инкапсуляции dot1Q для виртуальной сети *.

Настройте коммутатор Ком 1 для работы с виртуальными сетями. Перейдите во вкладку CLI и введите команды, приведенные на рис. 3.

Таким образом в коммутаторе будут созданы три виртуальные сети. Далее нужно указать, какой интерфейс должен работать с каждой сетью, для этого выполните команды, представленные на рис. 4.

```
Switch>ena
Switch#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config)#vlan 2
Switch(config-vlan)#vlan 3
Switch(config-vlan)#vlan 4
Switch(config-vlan)#exit
Switch(config)#
```

Рис. 3. Создание виртуальных сетей

```
Switch(config)#int Fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 2
Switch(config-if)#exit
Switch(config)#int Fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 3
Switch(config-if)#exit
Switch(config)#int Fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 4
Switch(config-if)#exit
Switch(config)#
```

Рис. 4. Настройка интерфейсов

Теперь, когда настроены порты, идущие к ПК, нужно разрешить трафик виртуальных сетей между коммутатором и маршрутизатором (рис. 5).

```
Switch(config)#int Gig0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#
```

Рис. 5. Переключение режима порта

Если навести мышку на коммутатор, отобразится состояние портов. Состояние портов после проделанных действий представлено на рис. 6.

Настроим маршрутизатор. Для настройки IP-адреса виртуальных интерфейсов для сетей выполните команды, показанные на рис. 7.

Порт для обмена данными с коммутатором настроен, также нужно, чтобы роутер мог обмениваться данными со вторым роутером. Для этого введите команды с рис. 8.

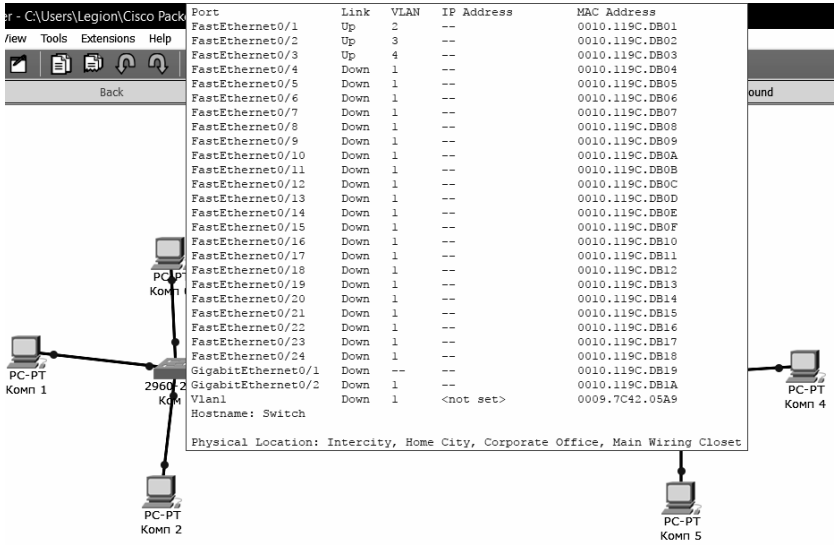

Рис. 6. Состояние портов

```
Router>ena
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#int gig0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.248
Router(config-if)#no shut

Router(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up

Router(config-if)#exit
Router(config)#int gig0/0.2
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.2, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.2, changed state to up

Router(config-subif)#encapsulation dot1Q 2
Router(config-subif)#ip address 192.168.1.9 255.255.255.248
Router(config-subif)#exit
Router(config)#int gig0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to
up
```

Рис. 7 (начало)

```
Router(config)#int gig0/0.3
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.3, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.3, changed state to up

Router(config-subif)#encapsulation dot1Q 3
Router(config-subif)#ip address 192.168.1.17 255.255.255.248
Router(config-subif)#exit
Router(config)#int gig0/0.4
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.4, changed state to
up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.4, changed state to up

Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 192.168.1.25 255.255.255.248
Router(config-subif)#exit
Router(config)#
```

Рис. 7 (окончание). Настройка маршрутизатора

```
Router#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
Router(config)#router rip
Router(config-router)#version 2
Router(config-router)#network 10.10.10.0
Router(config-router)#network 192.168.1.0
Router(config-router)#exit
Router(config)#int se0/0/0
Router(config-if)#ip address 10.10.10.1 255.0.0.0
Router(config-if)#no shut

%LINK-5-CHANGED: Interface Serial0/0/0, changed state to
down
Router(config-if)#exit
```

Рис. 8. Настройка обмена данными между роутерами

Задайте IP-адреса компьютерам Комп 0, Комп 1, Комп2 в соответствии с табл. 2.

Таблица 2

Адреса компьютеров

Компьютер	IP адрес	Mask	Gateway IP
Комп 0	192.168.1.10	255.255.255.248	192.168.1.9
Комп 1	192.168.1.18		192.168.1.17
Комп 2	192.168.1.26		192.168.1.25

Получится сеть как на рис. 9.

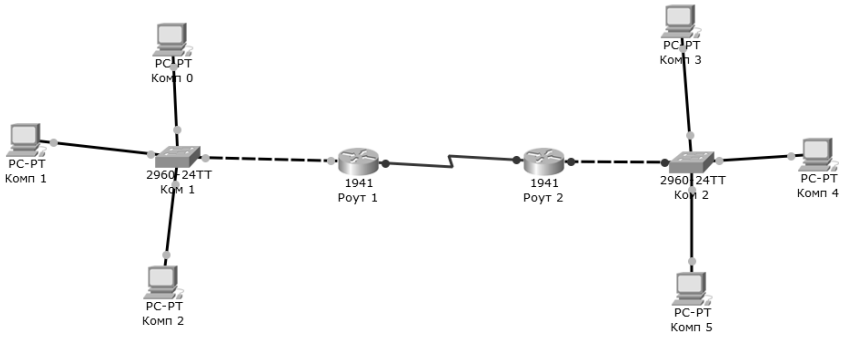

Рис. 9. Рабочая левая часть сети

Чтобы убедиться, что виртуальные сети работают, попробуйте отправить UDP-пакет с Комп 0 на Комп 1 в режиме симуляции. Вы должны увидеть, что пакет идет не напрямую через коммутатор к Комп 1, а через маршрутизатор, т.е. через маршрутизатор идет пересылка данных в другую сеть. Если бы компьютеры были в одной виртуальной сети, то пакет прошел бы через коммутатор напрямую к цели.

4. Задание на лабораторную работу

1. Ознакомиться с теорией.
2. Настроить правую часть сети самостоятельно, чтобы обе части могли через маршрутизаторы обмениваться данными, например, Комп 0 мог успешно отправить данные Комп 5.
3. После настройки подтвердить успешную отправку PDU пакета по сети.

5. Контрольные вопросы

1. Что такое VLAN?
2. Зачем используются VLAN?
3. Может ли компьютер, подключенный к VLAN 1, увидеть компьютер, подключенный к VLAN 2, без маршрутизатора?
4. Что такое CLI?
5. Как с помощью CLI можно задать адрес интерфейсу?
6. Зачем настраивают протокол RIP на маршрутизаторе?
7. Для чего используют режим интерфейса «access»?
8. Для чего используют режим интерфейса «trunk»?
9. За счет чего реализуется VLAN в Packet «Tracer»?
10. Как с помощью CLI сделать виртуальный интерфейс?

ЛАБОРАТОРНАЯ РАБОТА №3
Одноранговые сети

1. Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows.

2. Краткие теоретические сведения

Одноранговая сеть – это сеть равноправных компьютеров, каждый из которых имеет уникальное имя и может иметь пароль для входа во время загрузки ОС. Имя компьютера и пароль входа назначаются владельцем компьютера средствами ОС. Каждый компьютер такой сети может одновременно являться и сервером, и клиентом сети, хотя допустимо назначение одного компьютера только сервером, а другого только клиентом.

Достоинством одноранговых сетей является их высокая гибкость: в зависимости от конкретной задачи сеть может использоваться очень активно, либо совсем не использоваться. Из-за большой самостоятельности компьютеров в таких сетях редко бывает ситуация перегрузки, тем более, что количество компьютеров в таких сетях обычно невелико. Установка одноранговых сетей довольно проста, для них не требуются дополнительные дорогостоящие серверы. Кроме того, нет необходимости в системном администрировании, пользователи могут сами управлять своими ресурсами.

В одноранговых сетях допускается определение различных прав пользователей на доступ к сетевым ресурсам, но система разграничения прав не слишком развита. Если каждый ресурс защищен своим паролем, то пользователю приходится запоминать большое число паролей.

К недостаткам одноранговых сетей относятся также слабая система контроля и протоколирования работы сети, трудности с резервным копированием распределенной информации. Выход из строя любого компьютера-сервера приводит к потере части общей информации, по возможности все компьютеры должны быть высоконадежными. Эффективная скорость передачи информации по одноранговой сети часто оказывается недостаточной, поскольку трудно обеспечить быстродействие процессоров, большой объем оперативной памяти и высокие скорости обмена с жестким диском для всех компьютеров сети. К тому же компьютеры сети работают не только на сеть, но и решают другие задачи.

3. Ход работы

3.1. Рабочие группы

Данная лабораторная работа выполняется на двух виртуальных машинах под управлением операционной системы Windows 7.

Для работы с рабочими группами на виртуальных машинах необходимо проверить, что в параметрах сетевого адаптера установлен пункт «Внутренняя сеть».

При настройке сети Windows автоматически создает рабочую группу и присваивает ей имя. Существует возможность присоединиться к уже существующей рабочей группе в сети и создать новую.

На виртуальных машинах, используемых в данной лабораторной работе, используются учетные записи admin Admin505 (win7) и Администратор Qwerty_123.

Для проверки принадлежности компьютера к рабочей группе откройте свойства компьютера, перейдите на вкладку «Имя компьютера» (Пуск – Компьютер – Свойства – Дополнительные параметры системы – Имя копьютера). Чтобы компьютеры могли взаимодействовать они должны принадлежать одной рабочей группе (рис. 1).

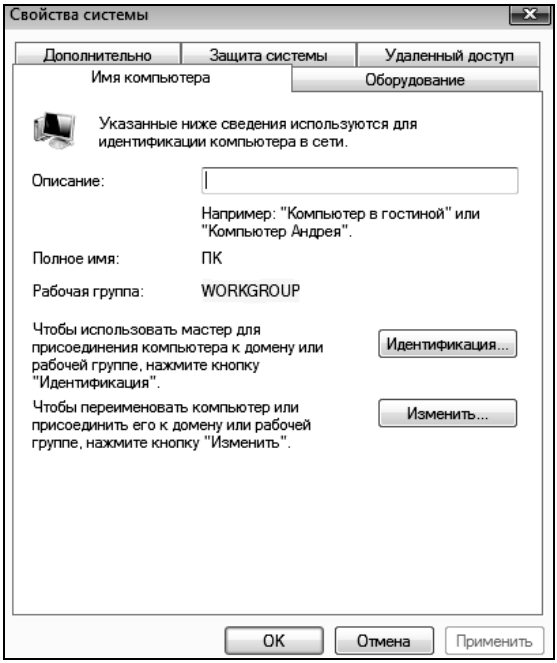

Рис. 1. Проверка принадлежности компьютера к рабочей группе

Чтобы переименовать компьютер или присоединить его к рабочей группе, нажмите кнопку «Изменить».

Чтобы присоединиться к существующей рабочей группе, необходимо ввести имя новой рабочей группы и нажать «ОК».

Для создания новой рабочей группы, также нужно ввести имя новой рабочей группы и нажать «ОК».

Присоедините гостевые ОС к одной рабочей группе: пользователей:

– в свойствах системы на вкладке «Имя компьютера» нажмите кнопку «Изменить»;

– выберите параметр «Является членом рабочей группы», введите имя рабочей группы (рис. 2) и нажмите «ОК»;

– в появившемся окне с сообщением о вступлении в рабочую группу нажмите «ОК» и перезагрузите гостевую ОС.

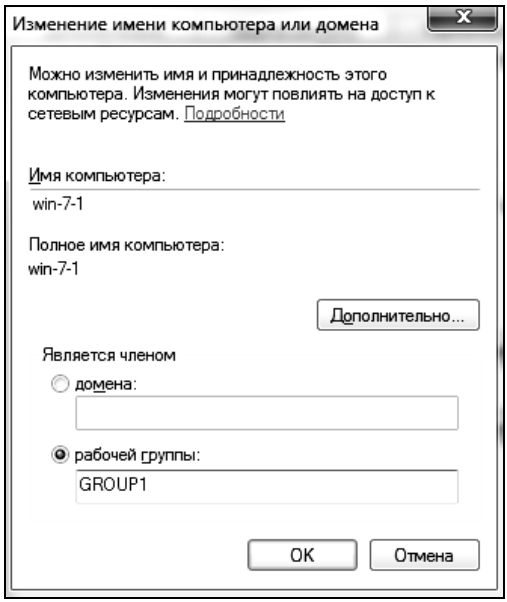

Рис. 2. Изменение рабочей группы компьютера

Для просмотра компьютеров рабочей группы в графическом интерфейсе нужно открыть Сетевое окружение и нажать «Отобразить компьютеры рабочей группы».

Для просмотра компьютеров рабочей группы в командной строке запустите командную строку и выполните команду: net view (рис. 5).

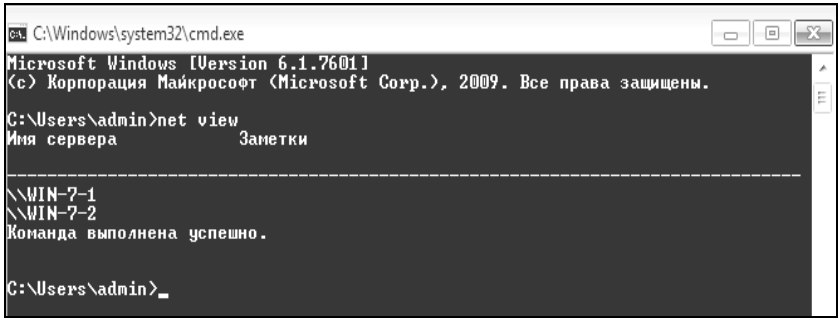

Рис. 3. Просмотр компьютеров рабочей группы

3.2. Настройка общего доступа к каталогам

Настройте общий доступ к папке, находящейся на сервере. Для этого выберите папку (можете создать папку на рабочем столе), нажмите на неё правой кнопкой мыши и выберете Свойства. Перейдите на вкладку Доступ и откройте «Общий доступ…», в выпадающем списке выберите пункт «Все» (рис. 4).

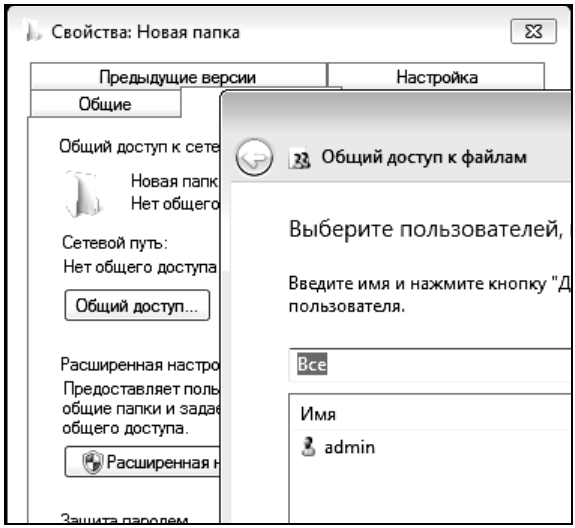

Рис. 4. Настройка общей папки

После настройки общего доступа к папке найдите ее в Сетевом окружении на второй машине и проверьте возможность добавления и изменения файлов.

Для подключения сетевой папки (т.е. для подключения общей папки как сетевого диска) на второй машине, вызовите контекстное меню Компьютера и выберите «Подключить сетевой диск». В появившемся окне (рис. 5) задайте букву сетевого диска и установите параметр «Восстанавливать при входе в систему», нажмите «Готово». Теперь общая папка будет отображаться в папке «Компьютер» как сетевой диск.

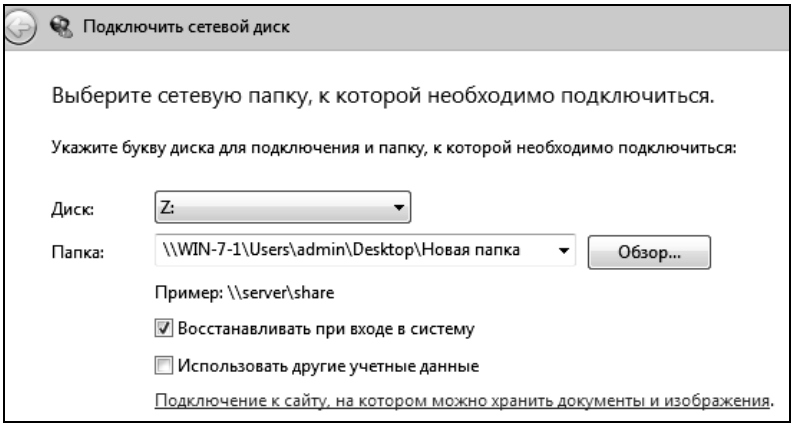

Рис. 5. Подключение сетевого диска

3.2. Настройка удаленного доступа

Для настройки удаленного доступа к компьютеру можно воспользоваться стандартными средствами Windows. Для этого удаленный компьютер должен быть включен и подключен к сети, удаленный доступ должен быть включен.

Настройте удаленный доступ:

– откройте свойства компьютера (win-7-1), выберите «Дополнительные параметры системы» и перейдите на вкладку «Удаленный доступ»;

– в группе «Удаленный помощник» установите параметр «Разрешить отправку приглашений удаленному помощнику» (рис. 6), нажмите кнопку «Дополнительно», установите параметр «Разрешить удаленное управление этим компьютером», задайте предельный срок 8 часов и нажмите «ОК»;

– в группе «Удаленный рабочий стол» выберите третий параметр и нажмите кнопку «Выбрать пользователей»;

– в появившемся окне нажмите кнопку «Добавить», введите имя пользователя, нажмите кнопку «Проверить имена» и нажмите ОК (рис. 7).

Если учетные записи на машинах совпадают, как в данном случае, то этот пункт проделывать нет необходимости;

– нажмите кнопку «Применить» на вкладке «Удаленные сеансы» для вступления изменений в силу.

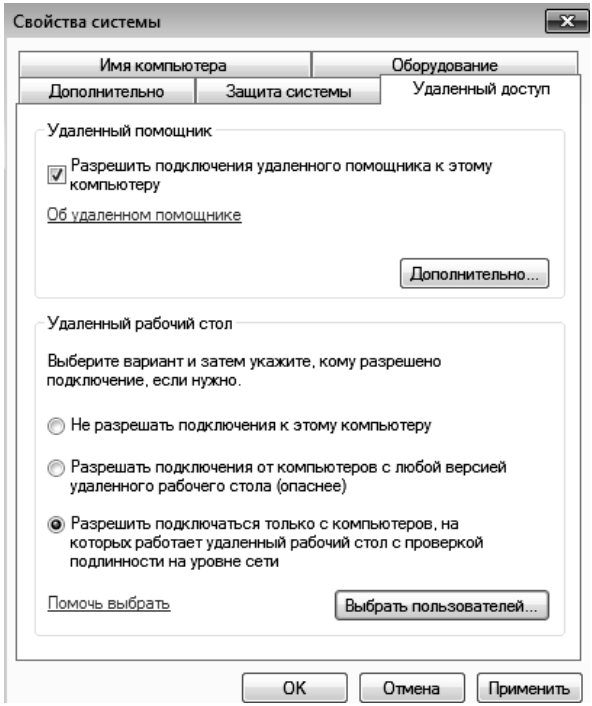

Рис. 6. Настройка параметров удаленного использования компьютера

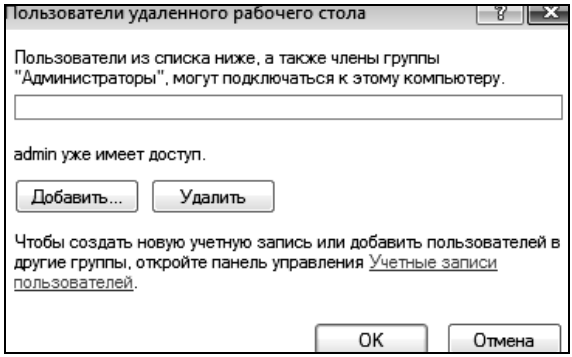

Рис. 7. Добавление пользователей удаленного доступа

Для того, чтобы подключиться к компьютеру с использованием удаленного доступа, войдите в компьютер-клиент (win-7-2), перейдите в меню Пуск – Все программы – Стандартные – Подключение к удаленному рабочему столу (рис. 8). Введите имя компьютера или его ip-адрес. Далее нажмите кнопку «Подключить». Необходимо выполнить вход в систему, после чего можно работать с компьютером с помощью удаленного доступа.

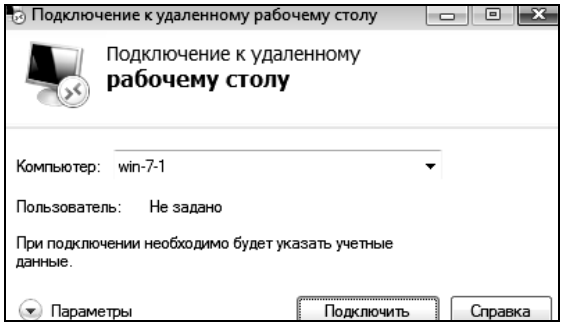

Рис. 8. Подключение к удаленному рабочему столу

4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Создать рабочую группу из двух компьютеров.
3. Настроить общий доступ и проверить его работу.
4. Написать отчет по проделанной работе и защитить его у преподавателя.

5. Контрольные вопросы

1. Что такое одноранговая сеть?
2. Каковы достоинства и недостатки одноранговых сетей?
3. Что нужно сделать, чтобы создать рабочую группу?
4. Какое условие должно выполняться, чтобы компьютеры могли взаимодействовать?
5. Какую команду необходимо ввести в командной строке для просмотра компьютеров рабочей группы?
6. Что такое удаленный доступ?
7. Как настроить удаленный доступ?
8. Существуют ли альтернативные способы создания рабочей группы в операционных системах Windows? Если да, то какие?
9. Как просмотреть компьютеры рабочей группы в графическом интерфейсе?
10. Как присоединить гостевую ОС к рабочей группе?

ЛАБОРАТОРНАЯ РАБОТА №4
Настройка домена. Групповые политики

1. Цель работы

Целью данной работы является получение навыков работы в локальных компьютерных сетях с ОС Windows с доменной структурой и управления пользователями и компьютерами домена с помощью групповых политик безопасности домена.

2. Краткие теоретические сведения

Доменом называется отдельная область безопасности в компьютерной сети Microsoft Windows.

В домене один или несколько компьютеров являются серверами. Администраторы сети используют серверы для контроля безопасности и разрешений для всех компьютеров домена. Это позволяет легко изменять настройки, так как изменения автоматически производятся для всех компьютеров.

Пользователи домена должны указывать пароль или другие учетные данные при каждом доступе к домену. Если пользователь имеет учетную запись в домене, он может войти в систему на любом компьютере. Для этого не требуется иметь учетную запись на самом компьютере.

В домене могут быть тысячи компьютеров. Компьютеры могут принадлежать к различным локальным сетям. В каждом домене действует своя политика безопасности и свои отношения безопасности с другими доменами. Если несколько доменов связаны доверительными отношениями и имеют одни и те же схему, конфигурацию и глобальный каталог, их называют деревом доменов. Несколько деревьев доменов могут быть объединены в лес.

Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя. Администратор может использовать механизм групповых политик для централизованного управления средой пользователей. Политика безопасности позволяет единообразно конфигурировать большое количество субъектов безопасности. Например, определить уровень доступа к системному реестру или задать порядок осуществления аудита событий.

Папка Мои документы традиционно рассматривается как место хранения пользовательских документов. Посредством механизма групповой политики администратор может задать перенаправление всех обращений пользователей к этой папке на некоторый сетевой ресурс.

Параметры групповой политики хранятся в виде объектов групповой политики (Group Policy Object, GPO). Эти объекты хранятся в ка-

талоге подобно другим объектам. Различают два вида объектов групповой политики – объекты групповой политики, создаваемые в контексте службы каталога, и локальные объекты групповой политики.

Локальные объекты групповой политики (Local Group Policy Object, LGPO) создаются в процессе установки операционной системы Windows и используются, если компьютер не включен в состав домена. Как только компьютер подключается к домену, компьютер и пользователь, работающий на нем, подпадают под действие объектов GPO, определенных в контексте данного домена.

Любой объект групповой политики может быть привязан к некоторому сайту, домену или подразделению, тогда параметры данного объекта групповой политики будут распространяться на все объекты службы каталога, зарегистрированные в данном контейнере. Один объект групповой политики может быть привязан к множеству контейнеров. Так же несколько объектов групповой политики могут быть привязаны к одному контейнеру.

Множество параметров, определяемых в рамках объекта групповой политики, разделено на две части: конфигурирование компьютера и конфигурирование среды пользователя. Конфигурирование компьютера предполагает определение значений для параметров, влияющих на формирование окружения любых пользователей, регистрирующихся на данном компьютере. Конфигурирование среды пользователя дает возможность управлять процессом формирования окружения конкретного пользователя, независимо от того, на каком компьютере он регистрируется в сети. Категории параметров групповой политики организованы в три контейнера в соответствии со своим назначением:

– Конфигурация программ. В контейнере размещаются категории параметров групповой политики, посредством которых можно управлять перечнем приложений, доступных пользователям.

– Конфигурация Windows. В контейнере размешаются категории параметров групповой политики, определяющие настройки непосредственно самой операционной системы. Содержимое данного контейнера может быть различным, в зависимости от того, определяются параметры групповой политики для пользователя или для компьютера.

– Административные шаблоны. Этот контейнер содержит категории параметров групповой политики, применяемых для управления содержимым системного реестра компьютера.

3. Ход работы

3.1. Создание домена

Данная лабораторная работа выполняется на двух виртуальных машинах: под управлением операционных систем Windows 7 и Windows Server 2012. Проверьте, что в параметрах сетевого адаптера виртуальных машин установлен пункт «Внутренняя сеть». Перед началом работы не забудьте сконфигурировать сетевые соединения на обеих виртуальных машинах, а именно задать IP адреса и маски подсети.

Запустите виртуальную машину с ОС Windows Server, войдите в систему от имени администратора. Запустите Диспетчер серверов. Выберите «Добавить роли и компоненты», запустив тем самым «Мастер добавления ролей и компонентов».

1. На первой странице мастер напоминает, что необходимо сделать перед началом добавления роли на сервер. Нажмите «Далее».

2. На втором шаге нужно выбрать «Установка ролей и компонентов» и нажать «Далее».

3. Выберите сервер, на который необходимо установить роль AD и снова нажмите «Далее».

4. На этом шаге нужно выбрать роль, которую мы хотим добавить на компьютер, отметьте галочкой «Доменные службы Active Directory». Откроется окно, в котором будет предложено установить службы ролей или компоненты, необходимые для установки роли AD, нажмите кнопку «Добавить компоненты», после чего кликните «Далее».

5. На шаге выбора компонентов для установки нажмите «Далее».

6. Вы увидите описание роли Доменных служб Active Directory. Прочтите описание роли и пункт «На что обратить внимание», затем нажмите «Далее».

7. Перед установкой будут показаны компоненты, которые будут добавлены на сервер. Проверьте, всё ли верно, и нажмите «Установить».

8. После того, как установка будет завершена, нажмите «Закрыть» (рис. 1).

После того, как роль была добавлена на сервер, необходимо настроить доменную службу. Запустите «Мастер настройки доменных служб Active Directory», для чего нажмите на иконку «Уведомления» в диспетчере сервера, затем нажмите «Повысить роль этого сервера до уровня контроллера домена».

1. Выберите пункт «Добавить новый лес», после этого впишите имя домена в поле «Имя корневого домена». Полное имя домена задается в формате доменных имен сети Интернет, например, headquarters.example.microsoft.com или keva.int. Задайте имя своему домену (например, labs.keva.ru). Нажмите «Далее».

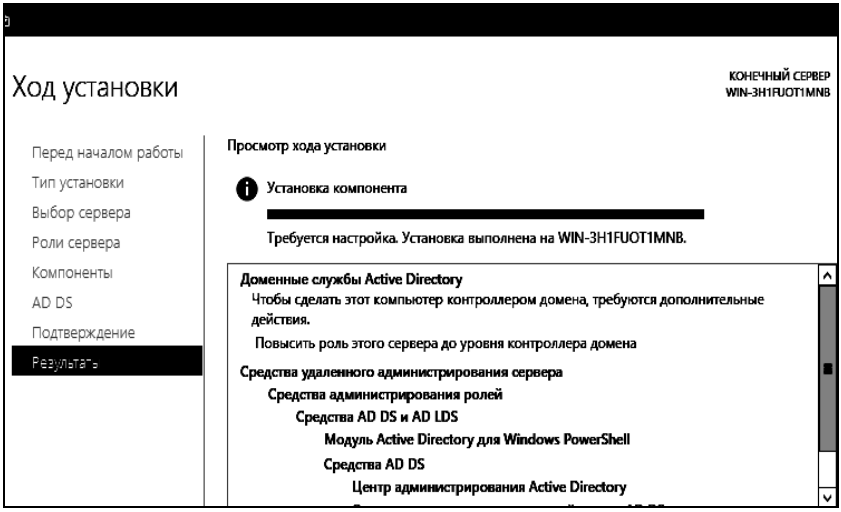

Рис. 1. Мастер добавления ролей и компонентов

2. На этом шаге можно изменить совместимость режима работы леса и корневого домена. Оставьте настройки по умолчанию. Задайте пароль для DSRM (Directory Service Restore Mode – режим восстановления службы каталога) и нажмите «Далее».

3. Мастер предупредит, что делегирование для этого DNS-сервера создано не было. Нажмите «Далее».

4. Будет предложено задать NetBIOS имя домена, которое используется младшими версиями операционных систем Microsoft Windows для идентификации домена, оставьте его по умолчанию.

5. Необходимо указать путь к файлу базы данных Active Directory, лог-файлу и путь к папке SYSVOL, которая содержит общие файлы и реплицируется другими контроллерами домена. Оставьте значения по умолчанию.

6. Проверьте, какие параметры были выбраны для установки (рис. 2). Можно просмотреть сценарий Windows PowerShell для развертывания AD DS. Нажмите «Далее».

7. Мастер проверит, соблюдены ли предварительные требования, после чего покажет отчёт. Одно из обязательных требований – это установленный пароль на профиль локального администратора. Внизу можно видеть предупреждение мастера о том, что после нажатия кнопки «Установить» уровень сервера будет повышен до контроллера домена и произойдёт автоматическая перезагрузка. Нажмите «Установить».

8. Когда установка будет закончена, компьютер перезагрузится, и вы сможете ввести первый компьютер в домен. Для этого введите логин и пароль администратора домена и нажмите «Войти».

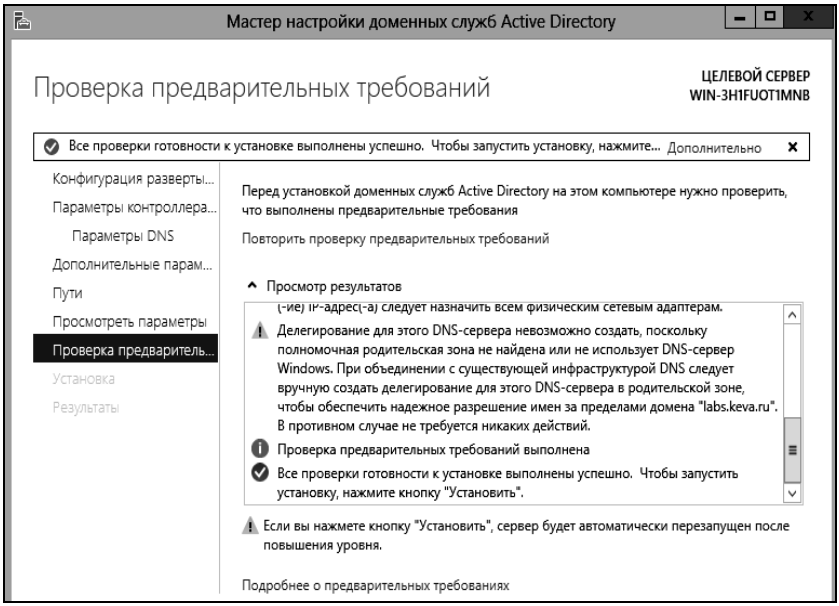

Рис. 2. Мастер настройки доменных служб AD

Нужно добавить новых пользователей в домен, после чего можно присоединить компьютер к домену и войти в домен под новым пользователем.

Запустите оснастку «Пользователи и компьютеры Active Directory» (рис. 3), для чего перейдите в Пуск – Панель управления – Система и безопасность – Администрирование – Пользователи и компьютеры Active Directory.

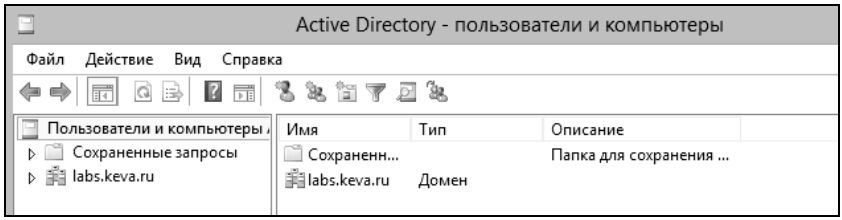

Рис. 3. Оснастка «Пользователи и компьютеры Active Directory»

Выделите название домена и вызовите контекстное меню, в котором выберите Создать – Подразделение. Введите имя для подразделения и нажмите «OK» (рис. 4).

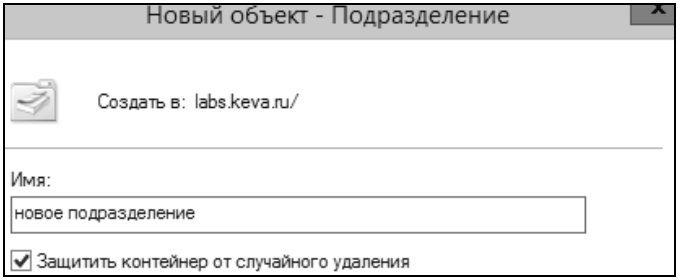

Рис. 4. Создание нового подразделения

Подразделения служат для управления группами компьютеров пользователей. Например, можно разбить пользователей по группам с именами подразделений, соответствующих названиям отделов компании, в которой они работают (бухгалтерия, отдел кадров, менеджеры и др.).

Создайте учетную запись пользователя в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт Создать – Пользователь (рис. 5).

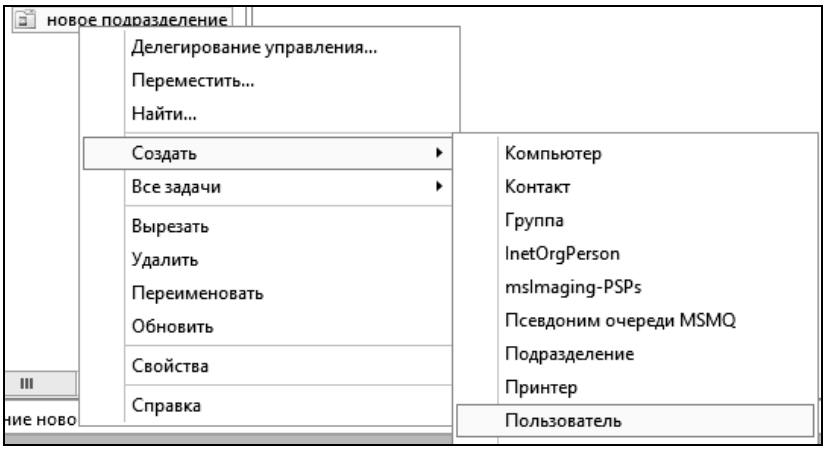

Рис. 5. Контекстное меню

Форма создания нового пользователя представлена на рис. 6.

На следующем шаге мастера создания нового объекта необходимо задать пароль учетной записи пользователя и дополнительные параметры. По умолчанию пароль должен соответствовать требованиям сложности, т.е. содержать три из четырех групп символов: заглавные буквы, строчные буквы, цифры, специальные знаки (. , + – = ? № $ и т.д.). Установите параметр «Требовать смену пароля при следующем входе в систему». Выясните назначение других параметров и установите нужные. Подтвердите создание новой учетной записи.

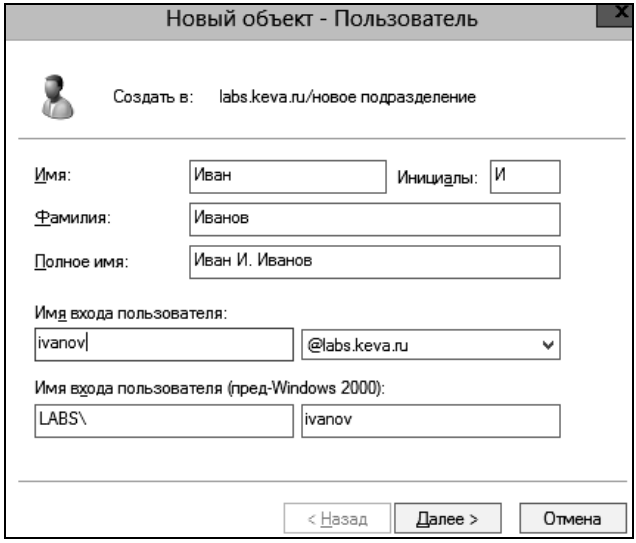

Рис. 6. Создание нового пользователя

Создайте учетную запись группы безопасности в новом подразделении. Для этого в контекстном меню нового подразделения выберите пункт Создать – Группа. Форма создания группы представлена на рис. 7.

При создании новой группы безопасности необходимо ввести имя, область действия и тип группы. Область действия определяет видимость данной группы в службе каталога. Глобальная группа видна в любом домене службы каталога и ей могут назначаться привилегии доступа к ресурсам других доменов. Локальная группа видна только в своем домене, т.е. ей будут доступны ресурсы только ее домена. Группы безопасности позволяют объединять пользователей и другие группы для назначения им одинаковых привилегий на различные объекты. Группы распространения используются для рассылки сообщений, они не участвуют в разграничении прав доступа.

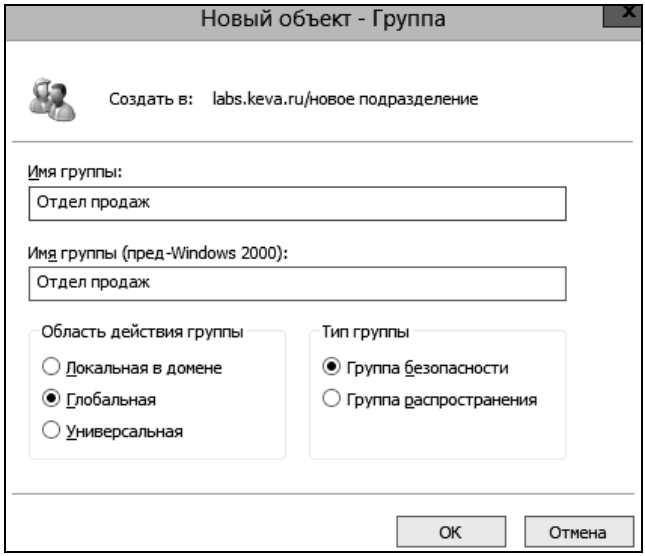

Рис. 7. Создание группы

Теперь нужно ввести компьютер в домен и зайти под новым пользователем. Укажите на клиентском компьютере DNS-адрес. Для этого откройте «Свойства сетевого подключения» (Пуск – Панель управления – Сеть и Интернет – Центр управления сетями и общим доступом – Изменение параметров адаптера), вызовите контекстное меню подключения и выберите «Свойства». Выделите «Протокол Интернета версии 4 (TCP/IPv4)», нажмите кнопку «Свойства», выберите «Использовать следующие адреса DNS-серверов» и в поле «Предпочитаемый DNS-сервер» укажите адрес вашего DNS-сервера (рис. 8). Проверьте, что задан IP-адрес и маска той же подсети, в которой находится сервер.

Присоедините компьютер к домену. Откройте свойства системы (Пуск – Панель управления – Система и безопасность – Система – Дополнительные параметры системы). Выберите вкладку «Имя компьютера» и нажмите «Изменить». Выберите «Компьютер является членом домена» и введите имя домена (рис. 9). После этого необходимо ввести логин и пароль пользователя с правами присоединения к домену (обычно администратора домена). Если вы всё указали правильно, то появиться приветственное сообщение «Добро пожаловать в домен ...» (рис. 10). Для того чтобы завершить присоединение, необходима перезагрузка.

После перезагрузки войдите в систему под доменной учётной записью пользователя, которая была создана ранее.

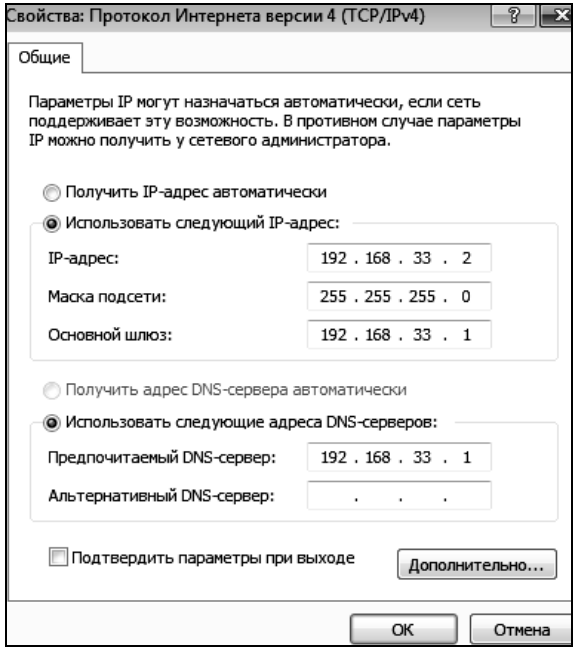

Рис. 8. Настройка подключения к сети

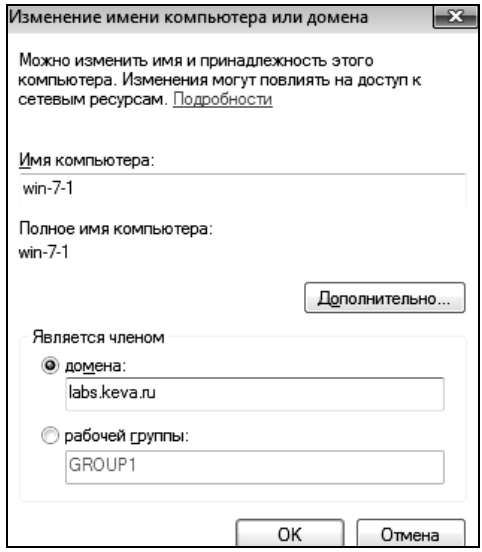

Рис. 9. Присоединение компьютера к домену

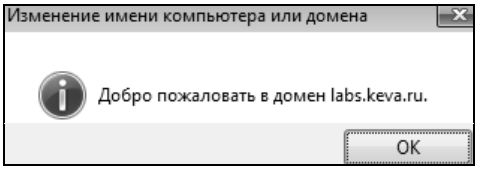

Рис. 10. Присоединение к домену

Войдите в систему Windows Server под учетной записью Администратора. Нажмите «Пуск» и перейдите в окно Управления групповой политикой (рис. 11).

Для создания нового объекта групповой политикой нажмите правой кнопкой на «Объекты групповой политики», выберите «Создать» и укажите имя объекта (рис. 12).

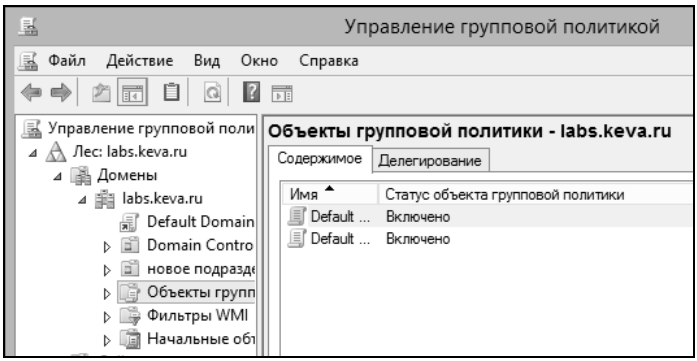

Рис. 11. Вид окна управления групповой политикой

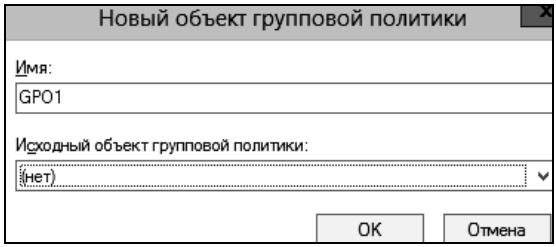

Рис. 12. Создание объекта групповой политики

Теперь необходимо привязать данный объект групповой политики к созданному контейнеру. Для этого нажмите правой кнопкой на созданное подразделение и выберите «Связать существующий объект групповой политики…» (рис. 13), затем выберите созданный ранее объект в списке (рис. 14) и нажмите «ОК».

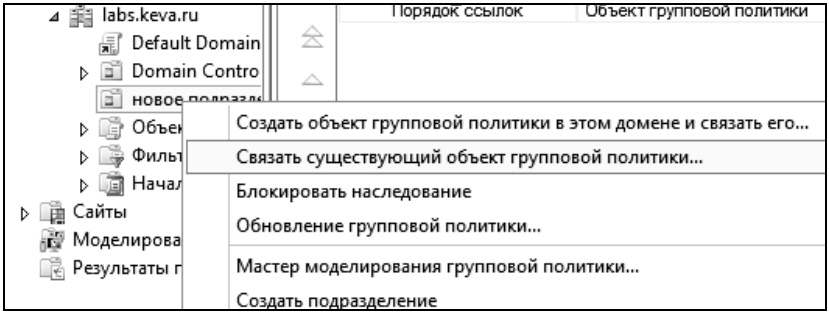

Рис. 13. Привязка объекта групповой политики

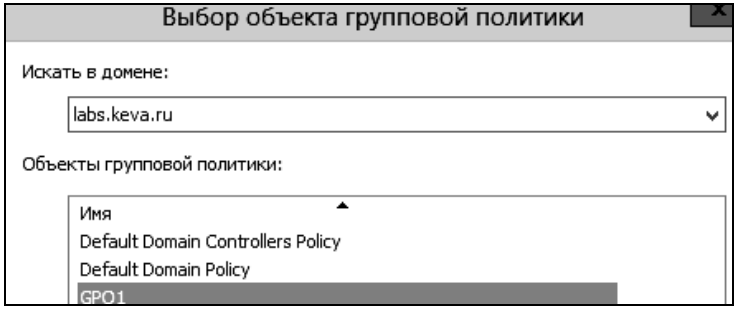

Рис. 14. Выбор объекта групповой политики

Выбранный объект должен появиться в списке связанных объектов групповой политики. Для редактирования параметров, определяемых данным объектом, нажмите на него правой кнопкой и выберите «Изменить» (рис. 15).

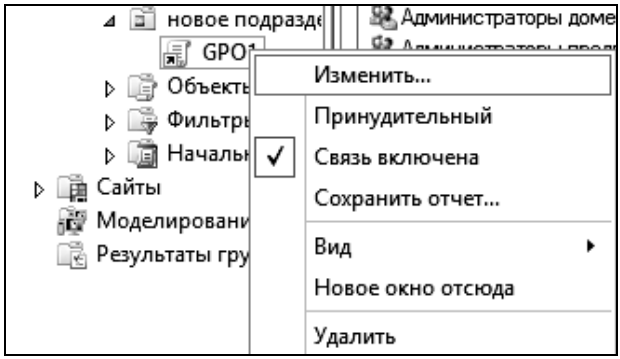

Рис. 15. Контекстное меню объекта

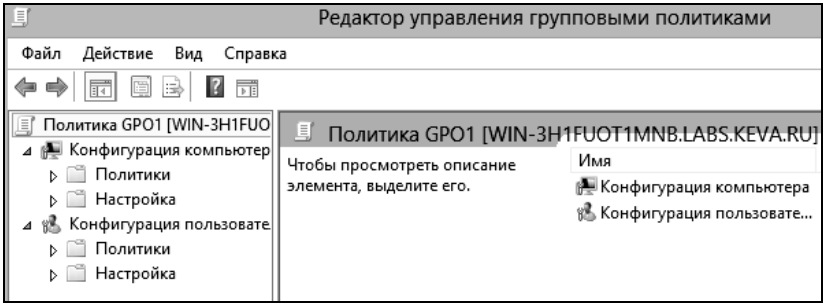

Рис. 16. Окно редактора управления групповыми политиками

3.2. Установка параметров безопасности

Ограничение на параметры парольной системы защиты задаются в контексте «Конфигурация компьютера». Выберите Конфигурация Windows – Параметры безопасности – Политики учетных записей – Политика паролей (рис. 17).

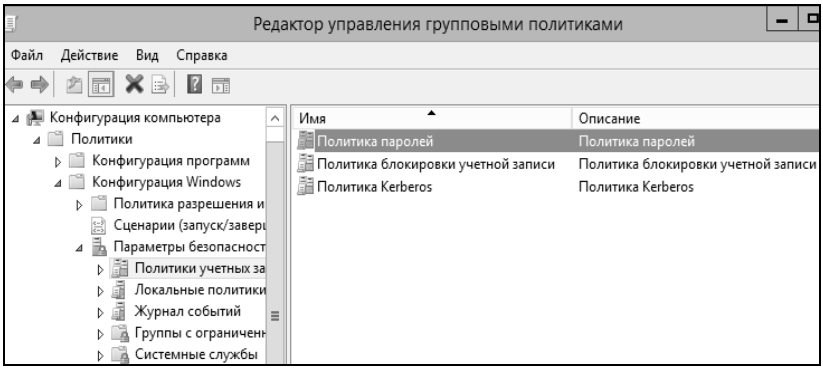

Рис. 17. Политики учетных записей

В данном разделе объекта групповой политики определяются следующие параметры:

– «Минимальный срок действия пароля» задает периодичность смены пароля;

– «Минимальная длина пароля» определяет минимальное количество знаков пароля;

– «Максимальный срок действия пароля» определяет интервал времени, через который разрешается менять пароль;

– «Пароль должен отвечать требованиям сложности» определяет требования к составу групп знаков, которые должен включать пароль;

– «Хранить пароли, используя обратимое шифрование» задает способ хранения пароля в базе данных учетных записей;

– «Вести журнал паролей» определяет количество хранимых устаревших паролей пользователя.

Укажите необходимые значения данных параметров. Ознакомьтесь с параметрами из группы Параметры безопасности.

3.3. Политика ограниченного использования программ

Объекты групповой политики позволяют запретить запуск определенных программ на всех компьютерах, на которые распространяется действие политики. Для этого необходимо в объекте групповой политики создать политику ограниченного использования программ и создать необходимые правила.

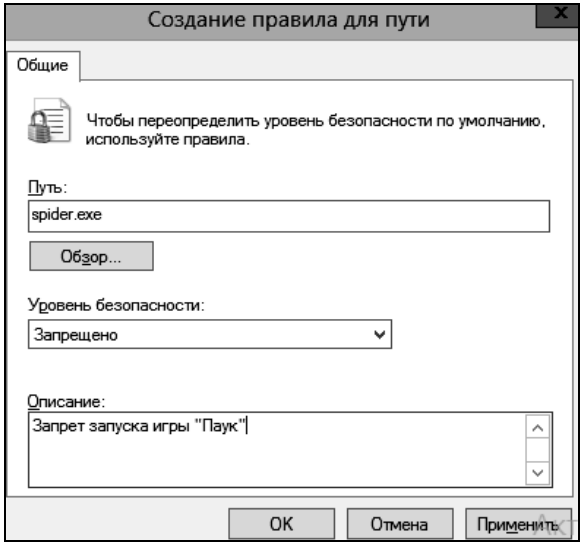

Рис. 18. Окно создания правила для пути политики ограниченного использования программ

Выберите раздел Конфигурация компьютера – Конфигурация Windows – Параметры безопасности – Политики ограниченного использования программ. Нажмите правой кнопкой на «Политики ограниченного использования программ» и выберите команду «Создать политику ограниченного использования программ». В контекстном меню раздела «Дополнительные правила» выберите необходимый способ создания правила выбора программы (рис. 18).

После обновления объекта групповой политики на рабочей станции, политика ограниченного использования программ вступит в действие и запуск программ, соответствующих правилам, будет невозможен.

3.4. Перенаправление пользовательских папок

Перенаправление пользовательских папок задается в контексте Конфигурация пользователя. Откройте раздел Конфигурация Windows – Перенаправление папки. В контекстном меню соответствующей папки выберите команду «Свойства». Пример окна свойств перенаправления папки «Документы» показан на рис. 19.

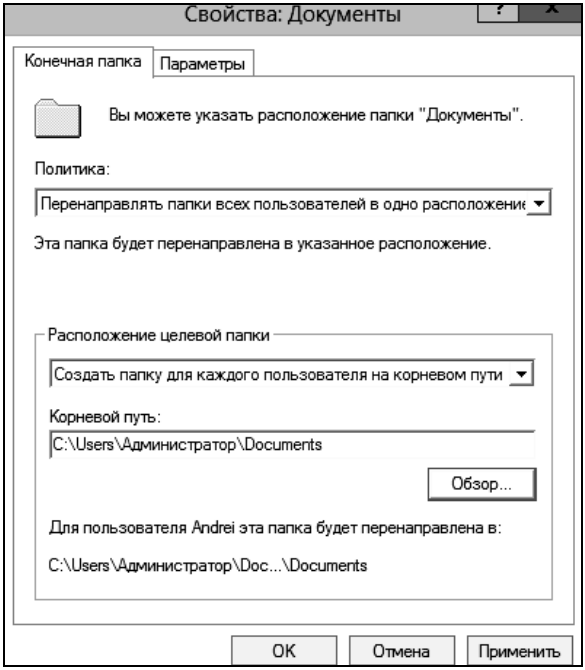

Рис. 19. Настройка перенаправления папки «Документы»

На закладке «Размещение» можно указать политику перенаправления:

– перенаправлять папки всех пользователей в одно место – документы всех пользователей размещаются в одной папке на сервере;

– указать различные места для разных групп пользователей – документы разных групп пользователей размешаются в разных сетевых папках, возможно на разных серверах;

– не задано – перенаправление пользовательских папок выключено.

Первый и второй варианты политики предполагают указание пути для размещения документов пользователей. На закладке Параметры задается необходимость переноса данных из существующих пользовательских папок при включении или отключении политики перенаправления.

4. Задание на лабораторную работу

1) Изучить теоретические сведения.
2) Задать серверу роль контроллера домена.
3) Присоединить рабочую станцию к домену.
4) Создать новый объект групповой политики и привязать его к созданному подразделению.
5) С помощью нового объекта групповой политики выполнить следующие действия:

– установить на рабочей станции приложение;

– задать ограничения на параметры парольной системы защиты;

– запретить запуск определенных программ на компьютере пользователя;

– настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;

– установить несколько административных шаблонов, запрещающих пользователю какие-либо действия

6) На рабочей станции проверить работу настроек, которые заданы в групповой политике.
7) Написать отчет и защитить его у преподавателя.

5. Контрольные вопросы

1. Что такое домен?
2. Сколько компьютеров может находиться в домене?
3. Что понимается под групповой политикой?
4. В чем различие между локальными политиками безопасности и групповыми политиками домена?
5. Какова структура объекта групповой политики, в какой последовательности применяются разделы объекта групповой политики?
6. Каково назначение административных шаблонов в групповой политике, как создать новый административный шаблон?
7. Для кого чего можно применять режимы планирования и ведения журналов?
8. Для чего нужен журнал паролей?
9. Что содержится в контейнере Конфигурация программ?
10. Что содержится в контейнере Конфигурация Windows?

ЛАБОРАТОРНАЯ РАБОТА №5
Установка программного обеспечения через домен

1. Цель работы

Целью лабораторной работы является ознакомление с основными способами автоматизации установки программного обеспечения в локальной вычислительной сети при помощи Active Directory.

2. Краткие теоретические сведения

Для централизованного управления средой пользователей используется механизм групповых политик. Под групповой политикой понимается совокупность параметров и настроек системы, определяющая конкретное окружение пользователя.

Групповые политики позволяют управлять настройками операционной системы. Все параметры операционной системы, определяющие ее функциональность, а также режимы работы ее служб и их настройки, хранятся в системном реестре. Посредством механизма групповой политики администратор может контролировать содержимое отдельных, наиболее важных ключей реестра.

С помощью групповой политики администратор может определить сценарии, которые будут выполняться при запуске и выключении компьютера, а также при входе пользователя в систему и выходе из нее.

Групповые политики могут применятся при определении параметров системы безопасности. С каждым пользователем или компьютером ассоциирован определенный набор настроек системы безопасности. Политика безопасности позволяет единообразно конфигурировать большое количество субъектов безопасности.

Управление приложениями также может осуществляться при помощи групповых политик. Используя механизм групповой политики, администратор может назначать и публиковать приложения, выполнять их централизованное обновление и восстановление

3. Ход работы

3.1. Подготовка к установке установка программного обеспечения

Данная лабораторная работа выполняется на двух виртуальных машинах: под управлением операционных систем Windows 7 и Windows Server 2012.

Запустите операционную систему Windows Server 2012. Создайте каталог для хранения установочных файлов (например, C:\install). Установочные файлы должны быть в формате установочных пакетов

Microsoft (msi). Скопируйте в созданный каталог предоставленные установочные файлы программного обеспечения Opera (рис. 1).

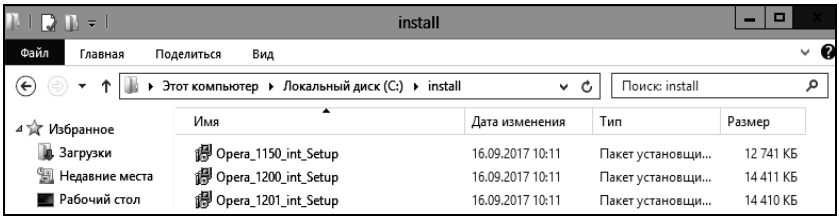

Рис. 1. Установочные файлы

Откройте общий доступ к созданному каталогу при помощи вкладки «Доступ» свойств каталога (рис. 2). Запустите оснастку «Active Directory – пользователи и компьютеры» (Пуск – Администрирование – Active Directory – пользователи и компьютеры, рис. 3).

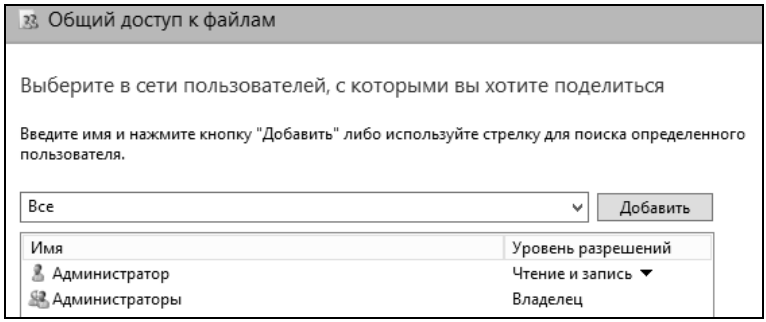

Рис. 2. Открытие общего доступа к каталогу

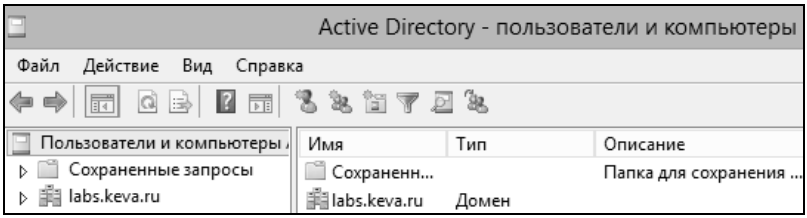

Рис. 3. Оснастка «Active Directory – пользователи и компьютеры»

В домене создайте новое подразделение, для объектов которого будет происходить установка программного обеспечения (например, «test»). Переместите в созданное подразделение доступный компьютер из подразделения «Computers» (рис. 4).

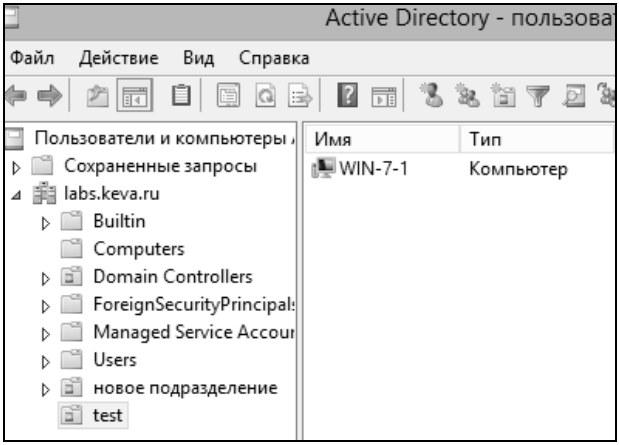

Рис. 4. Созданное подразделение

Создайте новую групповую политику для созданного подразделения (рис. 5).

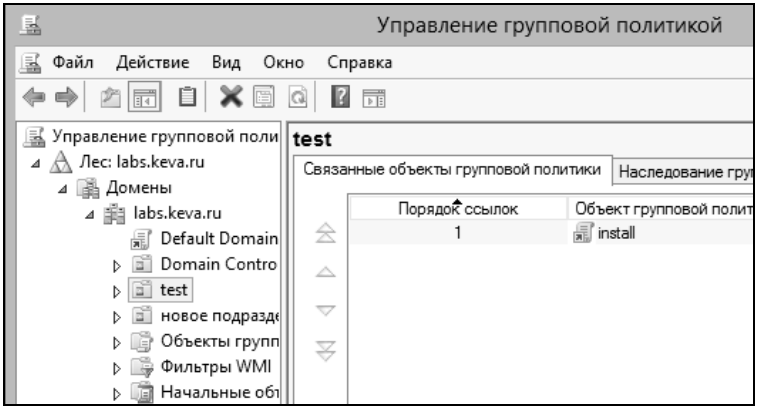

Рис. 5. Создание групповой политики

3.2. Установка программного обеспечения при помощи групповых политик

Откройте созданную групповую политику. Создание заданий на установку программного обеспечения на компьютерах, входящих в домен, осуществляется в разделе Конфигурация компьютера – Конфигурация программ – Установка программ. В контекстном меню раздела Установка программ выберите «Создать» и укажите полный сетевой путь к

месту расположения установочного файла – \\WIN\install\Opera_1150_int_Setup.msi (рис. 6). В появившемся окне выберите «Назначенный» метод развёртывания.

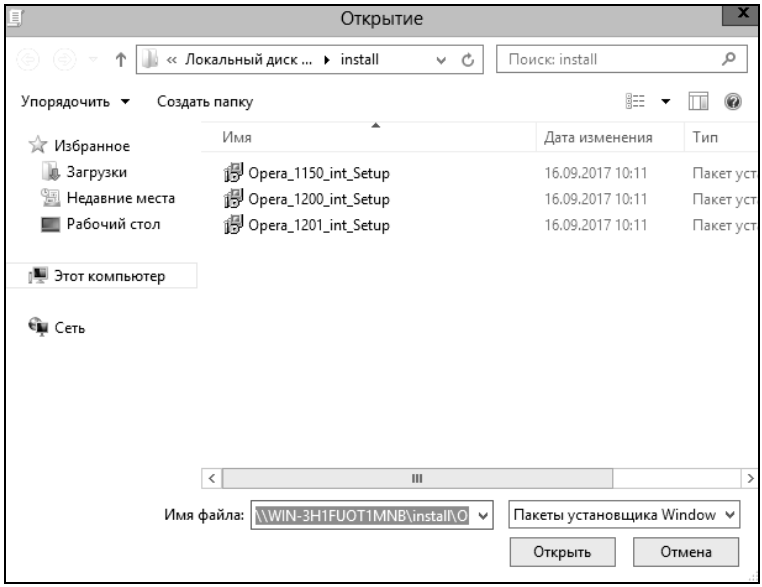

Рис. 6. Выбор установочного пакета

Аналогично создайте задание на установку для файла Opera_1200_int_Setup.msi (рис. 7).

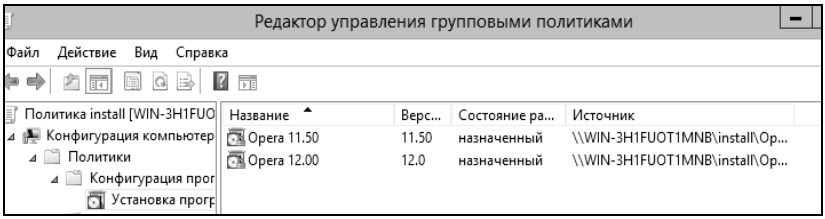

Рис. 7. Список заданий на установку ПО

Запустите операционную систему Windows 7. При первом запуске операционная система считает с домена текущие параметры групповой политики (параметры групповой политики можно обновить, используя команду gpupdate /force). Перезагрузите Windows 7. При загрузке долж-

но появиться окно информирования об установке программного обеспечения. Войдите в операционную систему и проверьте наличие установленного программного обеспечения.

3.3. Обновление программного обеспечения при помощи групповых политик

В операционной системе Windows Server 2012 откройте групповые политики подразделения «test». В разделе Установка программ создайте новый установочный пакет – \\WIN\install\Opera_1201_int_Setup.msi. Выберите особый метод развертывания (рис. 8). В появившемся окне свойств пакета выберите вкладку «Обновления» (рис. 9). Данный пакет является обновляющим для указанного программного обеспечения. В списке заданий на установку (рис. 10) программное обеспечение, являющееся обновляющим, имеет собственное обозначение.

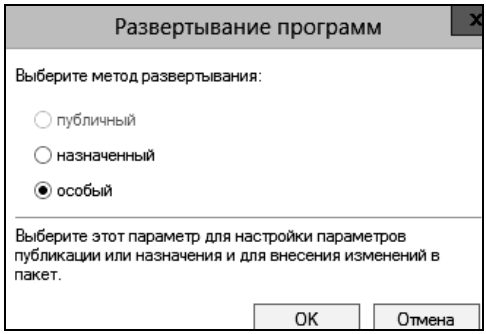

Рис. 8. Выбор метода развертывания

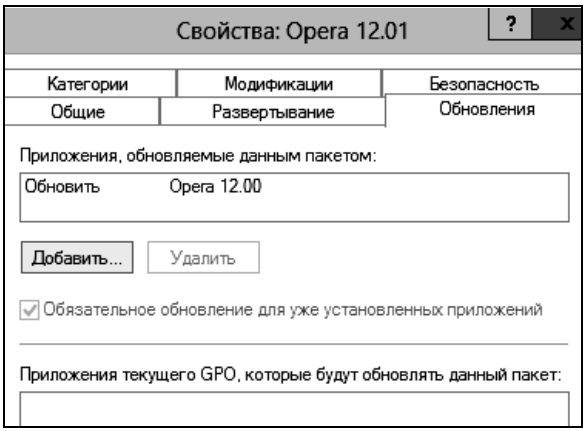

Рис. 9. Вкладка «Обновления» установочного пакета

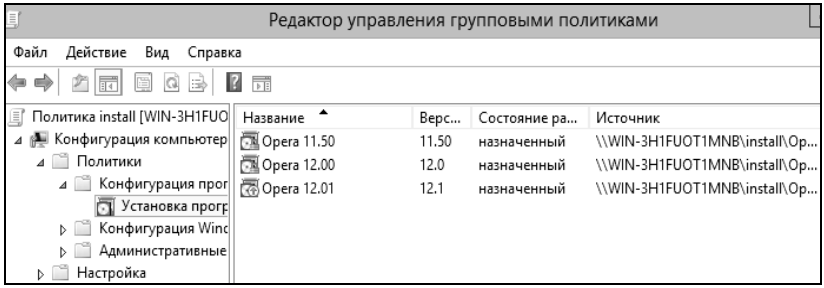

Рис. 10. Список заданий на установку ПО

Для применения изменённых параметров групповой политики Windows 7 перезагрузиться дважды. При загрузке должно появиться окно информирования об установке нового программного обеспечения. Войдите в операционную систему и проверьте наличие установленного программного обеспечения.

3.4. Удаление программного обеспечения при помощи групповых политик

Существует два варианта удаления заданий на установку программного обеспечения. Первый вариант позволяет удалить не только задание, но и программу, установленную на рабочие станции. Другой вариант удаляет только задание. Удалите задания на установку и обновление Opera, разрешив дальнейшее использование приложения (рис. 11, 12, второй вариант). Удалите первую версию Opera с рабочей станции (см. рис. 12, первый вариант).

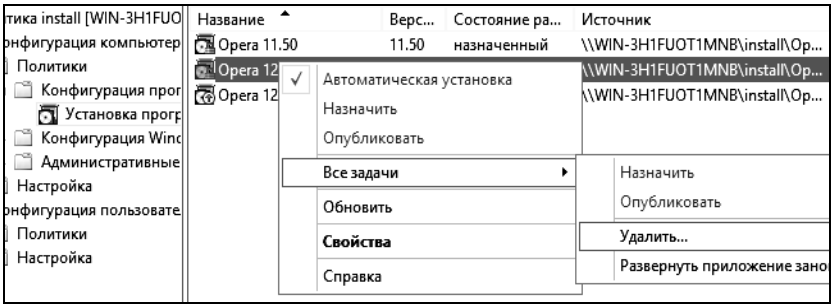

Рис. 11. Удаление приложения

Для применения изменённых параметров групповой политики Windows 7 перезагрузиться дважды. При загрузке должно появиться окно информирования об удалении программного обеспечения. Войдите

в операционную систему и проверьте отсутствие удаленного программного обеспечения.

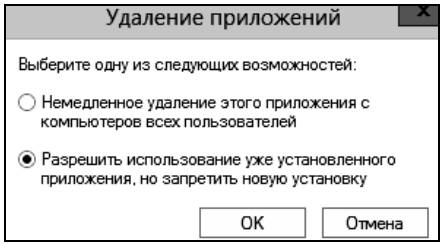

Рис. 12. Разрешение на дальнейшее использование и запрет на новую установку

4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. С помощью групповых политик установить программное обеспечение на рабочую станцию, обновить его и проверить правильность работы.
3. Написать отчет и защитить его у преподавателя.

5. Контрольные вопросы

1. Какие недостатки имеет способ установки программного обеспечения при помощи групповой политики на компьютеры в организации?
2. Как вы думаете, для чего может понадобиться установка программ при помощи групповой политики?
3. Объясните, что из себя представляют публичный, назначенный и особый методы развертывания программ?
4. Как проходит установка программ с помощью групповой политики?
5. Как проходит удаление программ с помощью групповой политики?
6. Существуют ли другие методы установки ПО в организации? Если да, то какие?
7. Есть ли какие-то особенности назначенного способа развертывания программ? Если да, то какие?
8. Какие есть варианты удаления приложений?
9. Почему нужно указывать полный путь к месту расположения загрузочного файла?
10. Зачем нужно открывать общий доступ к папке с загрузочными файлами?

ЛАБОРАТОРНАЯ РАБОТА №6
Обновление программного обеспечения и операционной системы

1. Цель работы

Целью данной работы является овладение основными способами обновления программного обеспечения при помощи программного продукта SUMo, предназначенного для обновления всего программного обеспечения на компьютере пользователя. Будут получены навыки обновления ОС Windows посредством службы Windows Server Update Services (WSUS), предназначенной для централизованного управления обновлениями и исправлениями корпоративных продуктов Microsoft.

2. Краткие теоретические сведения

SUMo (Software Update Monitor) – это бесплатная утилита, работающая под управлением операционной системы Windows, которая позволяет пользователям производить мониторинг обновлений для программного обеспечения, установленного на компьютере.

SUMo предоставляет простой и интуитивно понятный графический интерфейс, оснащённый многоязычной поддержкой для отслеживания в сети наличия новых версий для установленного программного обеспечения.

Утилита детально сканирует систему и выводит список всех программ, а также номера их версий и сведения о разработчиках.

SUMo может проверять наличие обновлений сразу для всех, или только для выборочных программ, без их предварительного запуска, и в случае обнаружения в сети более новой версии выводит окно с предложением обновить программу, предоставляя ссылку для её загрузки.

Возможности SUMo:

– автоматическое определение установленного программного обеспечения;

– обнаружение необходимых обновлений/патчей/бета-версий;

– чёрный список (отслеживает только необходимые конкретные релизы программного обеспечения);

– интернациональная поддержка;

– по заявлению пользователей имеет хорошую совместимость и выдаёт ложные обновления реже, чем другие утилиты для мониторинга обновлений.

Windows Server Update Services (WSUS) – сервер обновлений операционных систем и продуктов Microsoft. Программа бесплатно мо-

жет быть скачана с сайта Microsoft и установлена на серверную ОС семейства Windows Server. Сервер обновлений синхронизируется с сайтом Microsoft, скачивая обновления, которые могут быть распространены внутри корпоративной локальной сети. Это экономит внешний трафик компании и позволяет быстрее устанавливать исправления ошибок и уязвимостей в операционных системах Windows на рабочих местах, а также позволяет централизованно управлять обновлениями серверов и рабочих станций.

3. Ход работы

3.1. Работа с программой SUMo

До начала работы с программой SUMo необходимо войти в систему с правами администратора. Для запуска программы на рабочем столе найдите папку sumo и запустите приложение.

При первом запуске SUMo проверяет весь компьютер и собирает сведения обо всех установленных программах и их версиях, затем сравнивает номера версий с данными из базы данных, находящейся на сервере разработчиков. Если номер версии программы, установленной на компьютере пользователя, меньше максимальной в базе данных на сервере, то SUMo предложит обновить эту программу.

Нажмите на кнопку «Сканировать». Программа SUMo проверит компьютер и соберет сведения обо всех установленных программах, их версиях и возможных обновлениях (рис. 1).

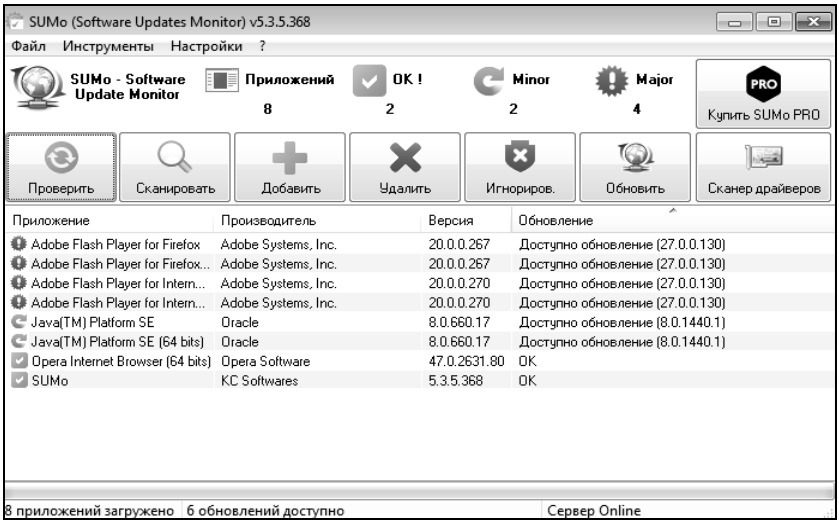

Рис. 1. Результат сканирования

Можно создать отчёт (рис. 2) в виде текстового файла, в котором будет отображен список программ, которых нет базе данных, с указанием пути файла. Для этого нажмите на кнопку «Экспорт» (Инструменты – Экспорт – Текстовый файл).

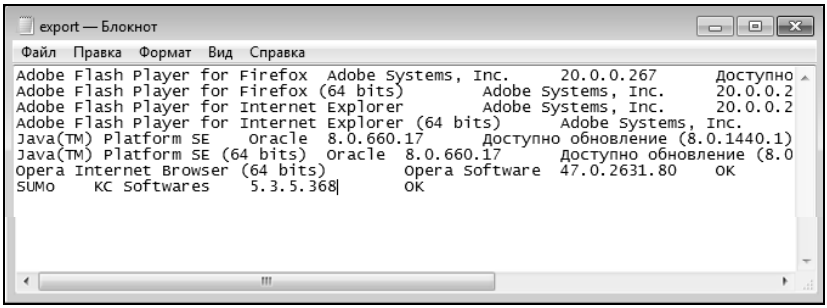

Рис. 2. Отчет о сканировании

Существует возможность добавить программу к списку вручную (рис. 3). Для этого нажмите кнопку «Добавить» и выберите путь, по которому установлено необходимое программное обеспечение (например, C:\7Zip\7zG.exe).

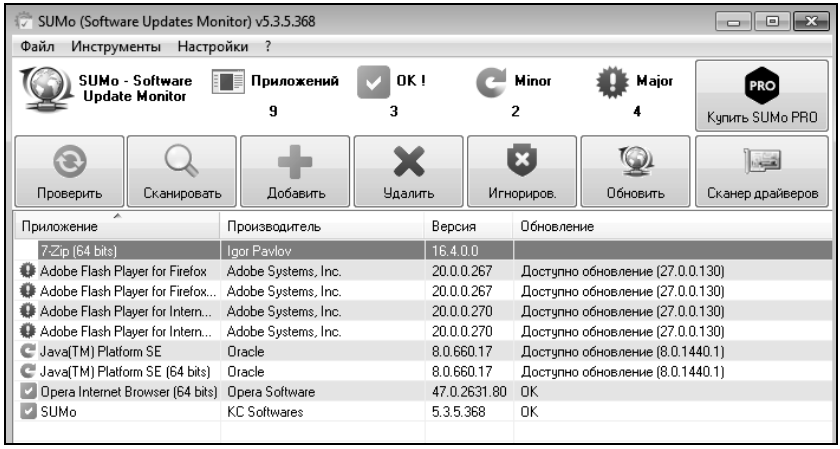

Рис. 3. Добавление программы вручную

В данном программном продукте после сканирования компьютера и сбора сведений обо всех установленных программах и их версиях при необходимости возможно удаление необходимой программы из

списка установленных. Для этого нажмите на кнопку «Удалить» в главном окне программы.

Для того что бы обновить нужное программное обеспечение, выделите его в списке и нажмите на кнопку «Обновить» на главном окне программы. Откроется web-страница, на которой можно будет увидеть, какая версия программы установлена, и какую версию необходимо искать. Для удобства разработчики поместили сразу несколько вариантов поиска, у некоторых программ есть прямые ссылки на сайт разработчика. Попробуйте обновить Adobe Flash Player.

3.2. Windows Server Update Services

На сервере, где планируется установить WSUS, необходимо войти в систему под учетной записью, входящей в локальную группу «Администраторы».

Откройте диспетчер серверов и создайте новую роль. Выберите в списке «Службы Windows Server Update Services» (рис. 4).

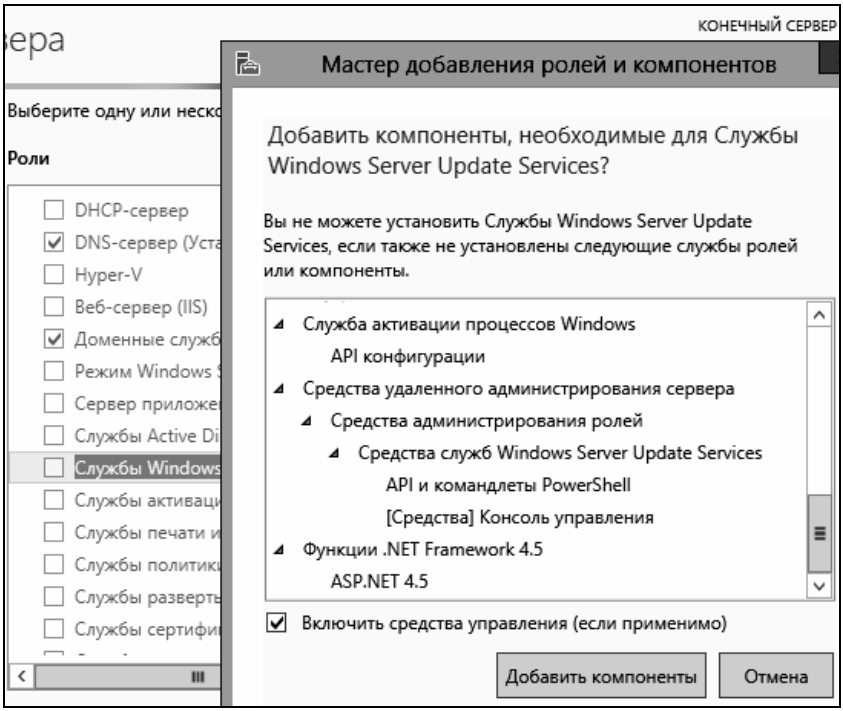

Рис. 4. Добавление службы WSUS

Далее необходимо выбрать тип базы данных, которую будет использовать WSUS. Выберите в списке пункт «Внутренняя база данных Windows». Далее выбираем базу данных WSUS (рис. 5).

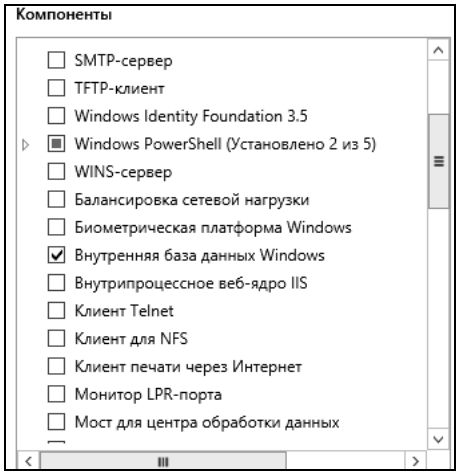

Рис. 5. Выбор базы данных

При выборе источника обновления по умолчанию установлен флажок «Хранить обновления в следующем расположении». Укажите путь, где будут храниться обновления: C:\WSUS (рис. 6).

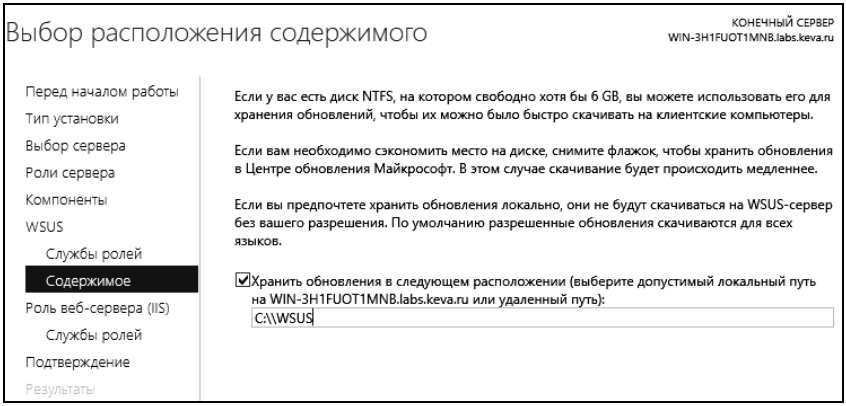

Рис. 6. Назначение пути для хранения обновлений

На завершающем этапе установки проверьте список компонентов, которые будут устанавливаться (рис. 7). Нажмите «Установить».

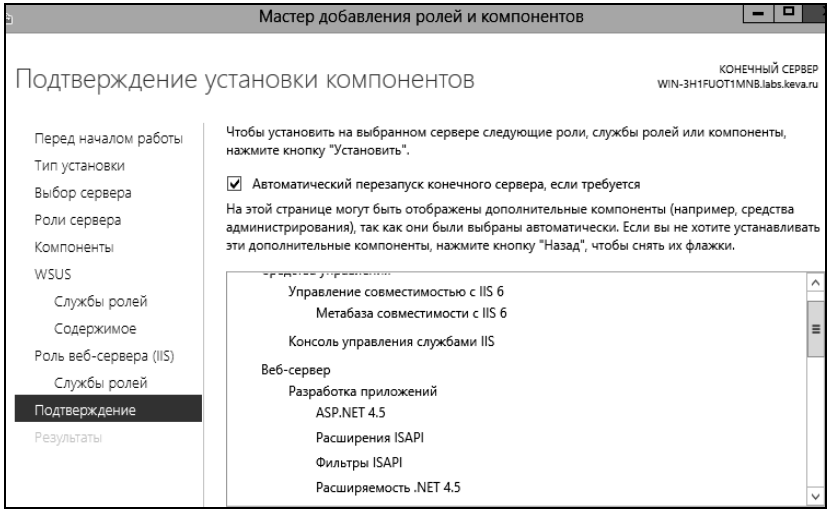

Рис. 7. Подтверждение установки

При первом запуске программы автоматически запустится мастер настройки сервера обновлений (рис. 8).

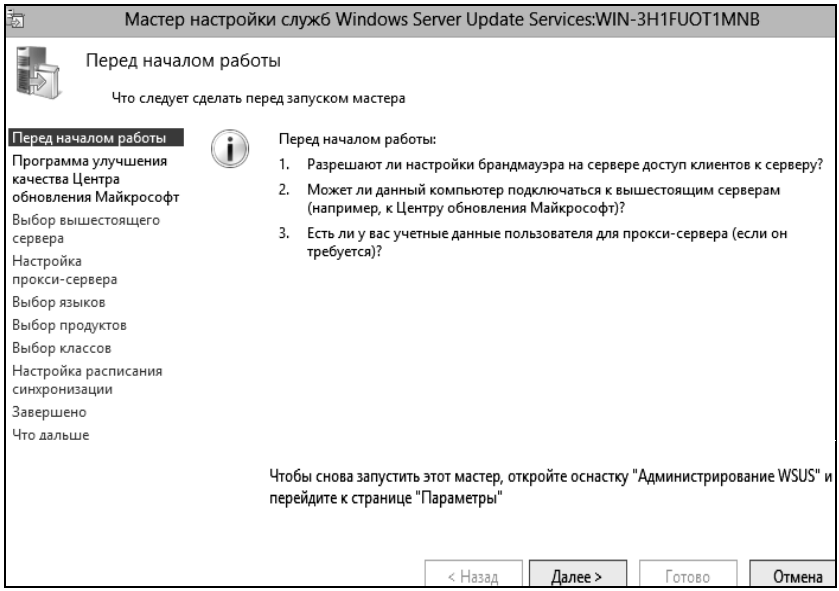

Рис. 8. Мастер настройки служб WSUS

В пункте «Выбор вышестоящего сервера» укажите, что сервер будет синхронизировать обновления с Центром обновления Майкрософт.

На следующем этапе ничего указывать не нужно, нажмите «Далее», а затем кнопку «Начать подключение», чтобы подключиться к вышестоящему серверу.

Затем необходимо выбрать языки, для которых WSUS будет скачивать обновления. Укажите английский и русский языки.

Далее указывается список продуктов, для которых WSUS должен скачивать обновления. Выберите все продукты Microsoft.

На странице «Классы» нужно указать типы обновлений, которые будут распространяться через WSUS (рис. 9).

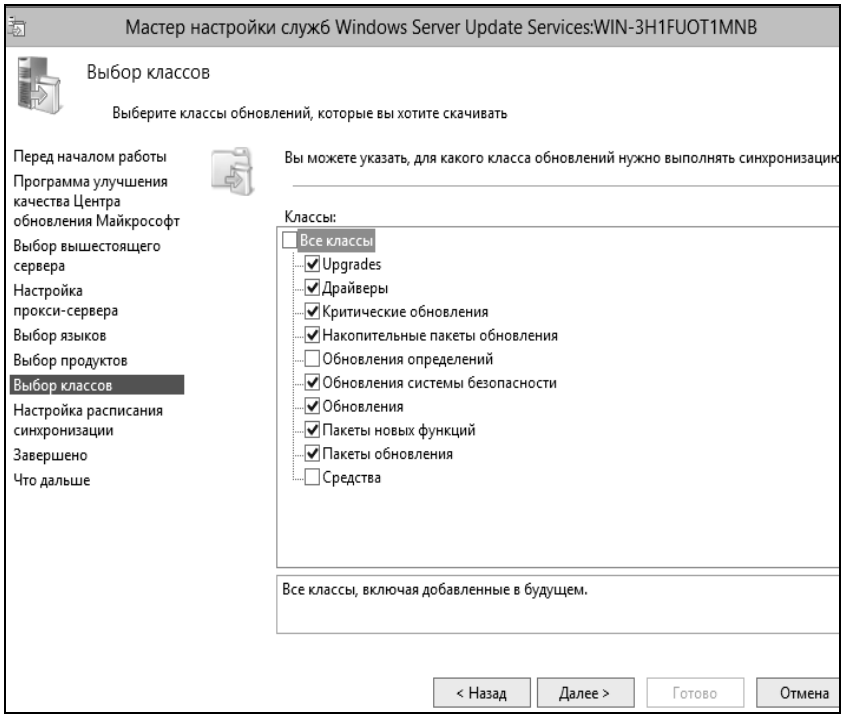

Рис. 9. Выбор классов

Далее необходимо указать расписание синхронизации обновлений. Выберите автоматическую синхронизацию (рис. 10).

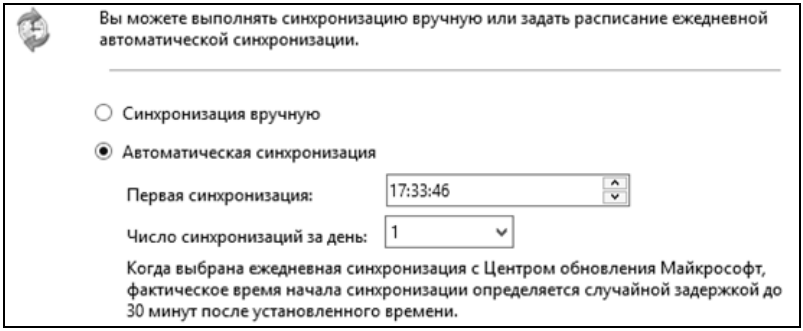

Рис. 10. Настройка расписания синхронизации

На странице завершения оставьте все по умолчанию и завершите установку. По окончанию работы мастера запустится консоль WSUS.

В редакторе объектов групповой политики откройте узел Конфигурация компьютера – Административные шаблоны – Компоненты Windows – Центр обновления Windows. Выберите пункт «Указать размещение службы обновлений Майкрософт в интрасети» (рис. 11).

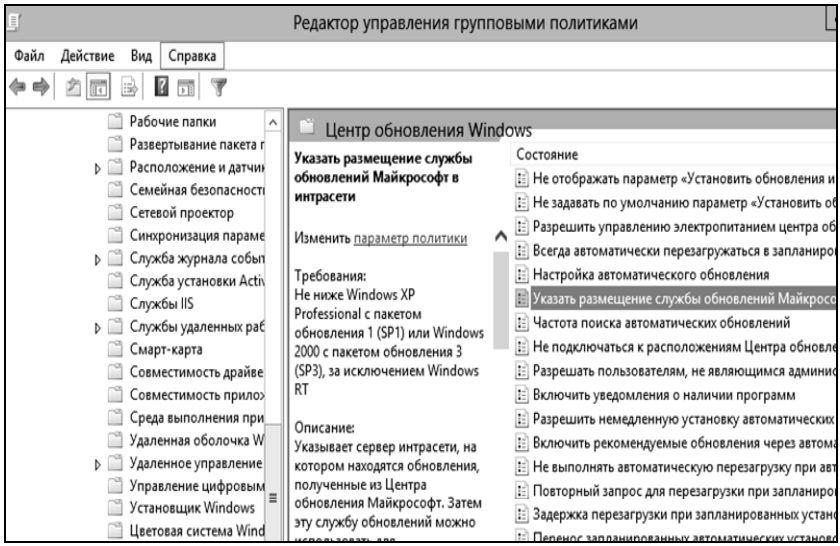

Рис. 11. Редактор управления групповыми политиками

Включите параметр и введите путь к серверу WSUS: http://(имя компьютера).labs.kibevs.ru (рис. 12).

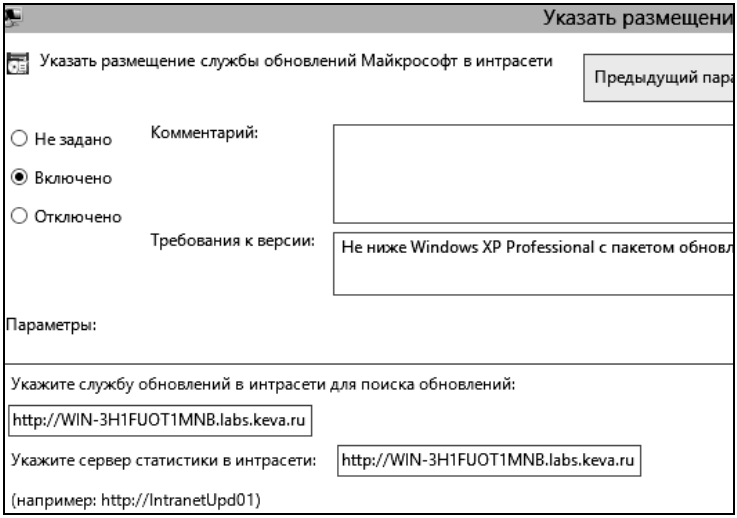

Рис. 12. Свойства параметра «Указать размещение службы обновлений Microsoft в интрасети»

Откройте свойства параметра «Настройка автоматического обновления» (рис. 13).

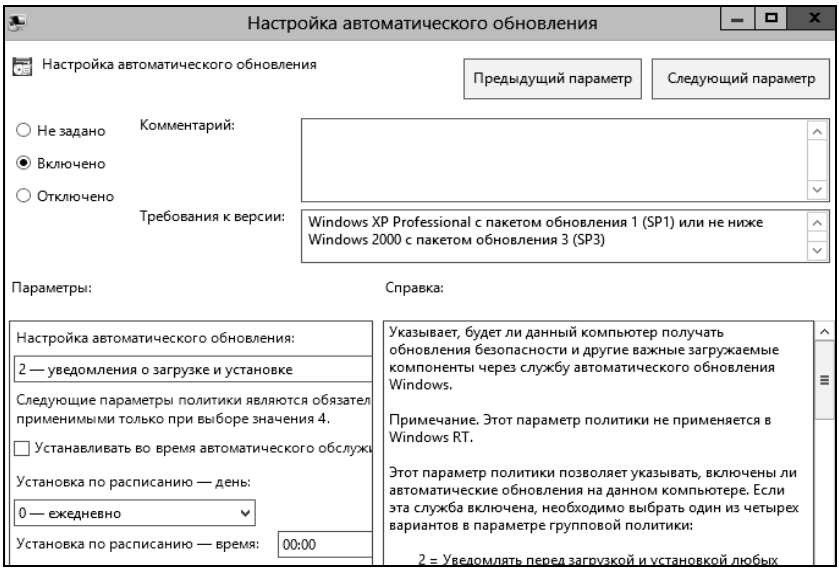

Рис. 13. Свойства параметра «Настройка автоматического обновления»

Во включенном состоянии этот параметр может принимать одно из четырех значений:

– уведомлять перед загрузкой обновлений и уведомлять повторно перед их установкой. При выборе этого варианта зарегистрированный в системе пользователь с правами администратора будет видеть уведомления перед началом загрузки и установки обновлений на компьютер;

– загружать автоматически и уведомлять перед установкой. Если установить это значение параметра, обновления начинают загружаться автоматически, а зарегистрированный в системе пользователь с правами администратора оповещается об установке перед ее началом;

– загружать автоматически и устанавливать по заданному расписанию. В этом случае нужно указать дни и время принудительной установки обновлений на клиентские компьютеры. Выберите это значение параметра и назначьте время, к примеру, на начало обеденного перерыва (12:00);

– разрешить локальному администратору указывать настройки. В этом случае локальные администраторы сами настраивают параметры автоматического обновления.

Выполните Пуск – Администрирование – Службы. Приостановите службу Sqlservr. Теперь скопируйте папку C:\WSUS1\UpdateServicesDbFiles в папку C:\WSUS\UpdateServicesDbFiles, нажмите «Заменить». Возобновите службу Sqlservr. Затем откройте страницу Компьютеры консоли WSUS. Через некоторое время, после применения рабочими станциями групповых политик, на этой странице начнут появляться имена компьютеров.

3.3. Настройка групп компьютеров

Группы компьютеров являются важной частью среды Windows Server Update Services. Такие группы позволяют проверять обновления и направлять их на конкретные компьютеры. По умолчанию заданы две группы компьютеров: «Все компьютеры» и «Неназначенные компьютеры». При первом подключении каждого клиентского компьютера к серверу WSUS он по умолчанию включается в обе эти группы. С целью управления обновлениями в организации можно создавать неограниченное количество произвольных групп компьютеров. Рекомендуется создать хотя бы одну группу компьютеров, чтобы проверять обновления перед тем, как устанавливать их на компьютеры организации.

Для создания тестовой группы в консоли администрирования WSUS раскройте ветвь «Компьютеры» и выберите пункт «Все компьютеры». Откройте контекстное меню пункта «Все компьютеры» и выберите «Добавить группу компьютеров» (рис. 14). В диалоговом окне

«Добавление группы компьютеров» укажите имя новой тестовой группы (test) и нажмите кнопку «Добавить».

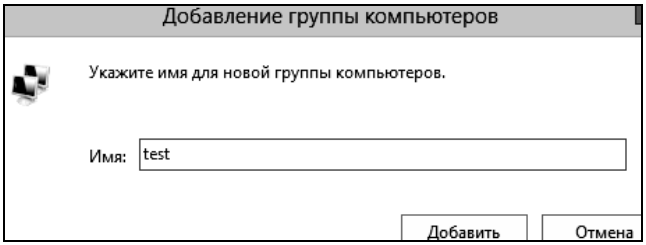

Рис. 14. Добавление группы компьютеров

Назначьте компьютер в тестовую группу. Для этого в консоли администрирования WSUS выберите ветвь «Компьютеры». Выберите группу компьютера, который необходимо назначить в тестовую группу. Вызовите контекстное меню компьютера и выберите «Изменить членство». В диалоговом окне «Настройка членства в группах компьютеров» выберите ранее созданную тестовую группу.

Для одобрения и развертывания обновлений WSUS в консоли администрирования WSUS необходимо выбрать ветвь «Обновления». Сводный отчет о состоянии обновлений отображается для узлов «Все обновления», «Критические обновления», «Обновления безопасности» и «Обновления WSUS».

В списке обновлений выберите обновления, установку которых необходимо одобрить для тестовой группы компьютеров. Сведения о выбранном обновлении выводятся в самой нижней части панели «Обновления». Вызовите контекстное меню выделенного обновления и выберите «Одобрить».

В диалоговом окне «Одобрить обновления» выберите тестовую группу. Выберите вариант «Одобрено для установки».

В появившемся окне «Ход одобрения», отображается ход выполнения заданий, влияющих на одобрение обновлений. По завершении одобрения нажмите «Закрыть».

Можно проверить состояние обновлений. При выборе обновления в списке в нижней части страницы (вкладка «Подробности») появится соответствующая дополнительная информация: название, описание, дата, класс, оценка критичности, и др.

На вкладке «Состояние» приводится информация о текущем состоянии установки данного исправления на клиентские компьютеры. На вкладке «Редакции» выводится список всех версий данного обновления. В разделе «Представление страницы обновления» можно задать условия

для фильтра отображения списка обновлений. По щелку по ссылке «Отчеты» откроется страница со списком доступных для генерации отчетов. С их помощью можно получить информацию о состоянии обновлений, компьютеров, результатах синхронизации, а также параметрах настройки сервера WSUS. В панели навигации консоли администрирования WSUS нажмите кнопку «Отчеты».

На странице «Отчеты» выберите «Сводный отчет о состоянии обновлений». Откроется окно «Отчет об обновлениях». Если необходимо выполнить фильтрацию списка обновлений, задайте необходимые критерии, например, «Учитывать обновления в следующих классах», затем нажмите кнопку «Выполнить отчет» на панели инструментов окна. Откроется окно «Отчет об обновлениях». Чтобы проверить состояние отдельного обновления, выберите его в левой части панели. В последней секции панели отчета отображается сводная информация о состоянии обновления.

4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Задать серверу роль контроллера домена.
3. Присоединить рабочую станцию к домену.
4. Создать новый объект групповой политики и привязать его к созданному подразделению.
5. С помощью нового объекта групповой политики выполнить следующие действия:

– установить на рабочей станции приложение;

– задать ограничения на параметры парольной системы защиты;

– запретить запуск определенных программ на компьютере пользователя;

– настроить перенаправление папки «Мои документы» на одну из сетевых папок сервера;

– установить несколько административных шаблонов, запрещающих пользователю какие-либо действия

6. На рабочей станции проверить работу настроек, которые заданы в групповой политике.
7. Написать отчет и защитить его у преподавателя.

5. Контрольные вопросы

1. Для чего предназначена программа SUMo?
2. Каковы функции программы SUMo?
3. Что такое WSUS?

4. Какие есть значения у параметра «Настройка автоматического обновления»?

5. Зачем нужно было приостанавливать службу Sqlservr?

6. Какие группы компьютеров имеются по умолчанию в среде WSUS?

7. Как создать тестовую группу?

8. Как назначить компьютер в тестовую группу?

9. Для каких узлов отображается сводный отчет о состоянии обновлений?

10. Для чего нужны отчеты об обновлениях?

ЛАБОРАТОРНАЯ РАБОТА №7
Высокоуровневые службы

1. Цель работы

Целью данной работы является изучение теоретических сведения о высокоуровневых службах и получение практических навыков в их установке и настройке.

2. Краткие теоретические сведения

Веб-сервер – это сервер, принимающий HTTP-запросы от клиентов и выдающий им HTTP-ответы, обычно вместе с запрошенными ресурсами. Веб-сервером называют как программное обеспечение, выполняющее функции веб-сервера, так и непосредственно компьютер на котором это программное обеспечение работает. Клиент, которым обычно является веб-браузер, передаёт веб-серверу запросы на получение ресурсов, обозначенных URL-адресами. Ресурсы – это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту. В ответ веб-сервер передаёт клиенту запрошенные данные. Этот обмен происходит по протоколу HTTP.

Веб-серверы могут иметь различные дополнительные функции, например:

– автоматизация работы веб страниц;

– ведение журнала обращений пользователей к ресурсам;

– аутентификация и авторизация пользователей;

– поддержка динамически генерируемых страниц;

– поддержка HTTPS для защищённых соединений с клиентами.

В качестве HTTP сервера могут использоваться такие программные продукты, как Apache, IIS, ngnix.

FTP-сервер – это удаленный компьютер, с файловой системой которого можно работать через специальный одноименный протокол. Протокол FTP – один из стандартных протоколов передачи данных через Интернет, он позволяет переносить файлы с одного компьютера на другой. Чтобы установить соединение и обменяться файлами в Интернете, согласно протоколу FTP, необходимо запустить специальную прикладную программу, называемую клиентской частью FTP. Клиентское программное обеспечение устанавливается вместе с коммуникационными утилитами TCP/IP. FTP-клиент – программа, позволяющая подключаться к удаленному FTP-серверу и получать/передавать файлы по протоколу FTP. Получить доступ к другому компьютеру для обмена файлами можно, указав пользовательское имя и пароль.

При работе с FTP широко используются два понятия: скачивание и закачивание. Скачивание (download) означает процесс сохранения папок и файлов с FTP-сервера на ваш компьютер. Закачивание (upload) – это передача папок и файлов с вашего компьютера на FTP-сервер. Обычно каждой папке (реже – файлу) на FTP-сервере назначают права доступа: чтение, запись и выполнение. Право на чтение означает, что вы можете просматривать файл или содержимое папки. Право на запись позволяет изменять содержимое файлов. Право на выполнение даёт возможность запускать исполняемые файлы и скрипты на сервере. С управлением правами доступа вы можете столкнуться, например, при разработке веб-сайта, когда посетителям нужно запретить доступ в одни каталоги сайта и разрешить выполнение скриптов из других каталогов. Для FTP-сервера наиболее распространенным программным продуктом является FileZilla.

Почтовым сервером (сервером электронной почты) в системе пересылки электронной почты называют агент пересылки сообщений (mail transfer agent, MTA). Это компьютерная программа, которая передаёт сообщения от одного компьютера к другому. Обычно почтовый сервер работает «за кулисами», а пользователи имеют дело с другой программой – клиентом электронной почты (англ. mail user agent, MUA).

Когда пользователь набрал сообщение и отправляет его получателю, почтовый клиент взаимодействует с почтовым сервером, используя протокол SMTP. Почтовый сервер отправителя взаимодействует с почтовым сервером получателя (напрямую или через промежуточный сервер – релей). На почтовом сервере получателя сообщение попадает в почтовый ящик, откуда при помощи агента доставки сообщений (mail delivery agent, MDA) доставляется клиенту получателя. Часто последние два агента совмещены в одной программе (к примеру, sendmail), хотя есть специализированные MDA, которые в том числе занимаются фильтрацией спама. Для финальной доставки полученных сообщений используется не SMTP, а другой протокол – POP3 или IMAP, который также поддерживается большинством почтовых серверов. Хотя в простейшей реализации MTA достаточно положить полученные сообщения в личный каталог пользователя в файловой системе центрального сервера («почтовый ящик»).

В качестве почтового сервера используются такие программные продукты, как Exchange Server, Courier Mail Server или Office mail Server (для ОС семейства Windows); для Unix-подобных ОС – sendmail или сочетание exim (MTA) и dovecot (MDA). В данной лабораторной работе рассматривается IIS (Internet Information Services) – проприетарный набор серверов для нескольких служб Интернета от компании Майкро-

софт. IIS распространяется с операционными системами семейства Windows NT. Основным компонентом IIS является веб-сервер, который позволяет размещать в Интернете сайты. IIS поддерживает протоколы HTTP, HTTPS, FTP, POP3, SMTP, NNTP

3. Ход работы

3.1. Веб-сервер

Войдите в операционную систему WinServer2012 под учётной записью администратора.

В первую очередь, необходимо установить IIS. Для этого в меню «Пуск» выберите пункт «Панель управления» запустите компонент «Установка и удаление программ». Откройте вкладку «Включение и отключение компонентов Windows». В пункте «Роли сервера» выберите компонент «Сервер приложений» и «Веб-сервер IIS». При выборе компонентов добавьте «SMTP-сервер». При выборе службы ролей для роли веб-сервера «IIS» установите флажки как на рисунке 1.

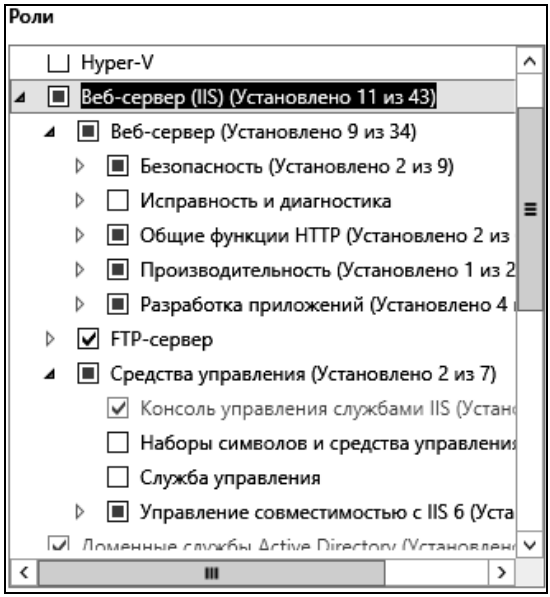

Рис. 1. Установка веб-сервера

Теперь необходимо подготовить тестовую страницу, вызываемую по умолчанию. Для этого, в приложении «Блокнот» напишите любой текст и сохраните файл как «Default.html» в каталоге C:\Inetpub\wwwroot.

Для настройки Web-сервера откройте «Диспетчер служб IIS» (Пуск – Администрирование – Диспетчер служб IIS) и перейдите к Веб-узлу по умолчанию (рис. 2).

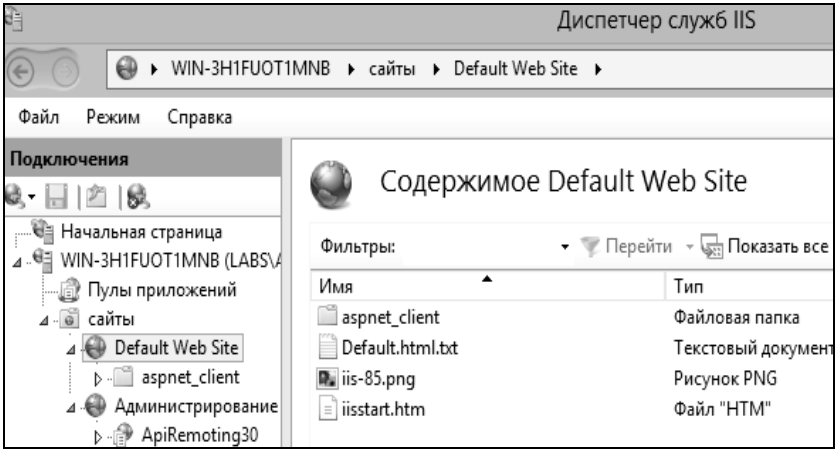

Рис. 2. Диспетчер служб IIS

Чтобы добавить страницу по умолчанию, перейдите на вкладку «Просмотр возможностей» и выберите «Документ по умолчанию». Оставьте в списке только тот документ, который был создан ранее (рис. 3).

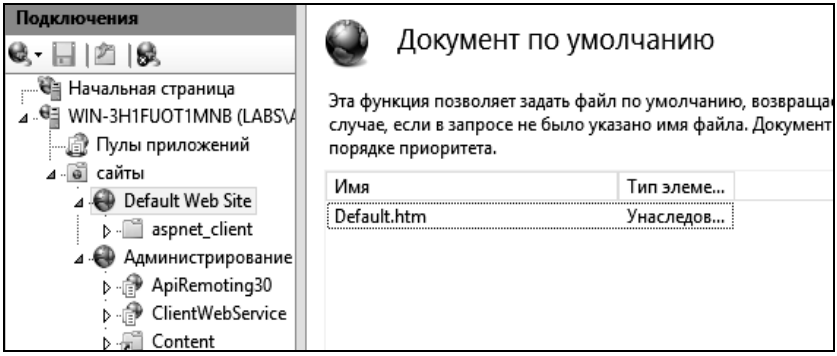

Рис. 3. Документ по умолчанию

Следующим шагом необходимо проверить настройку Web-сервера. Сначала уточните IP-адрес (Пуск – Выполнить – cmd – ipconfig /all). Затем, откройте браузер и в адресной строке наберите уточненный Вами IP-адрес (рис. 4).

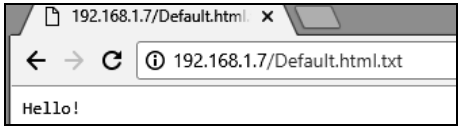

Рис. 4. Проверка настройки

Попробуйте открыть эту же страницу с другого рабочего места. Для этого войдите в операционную систему win7 под учётной записью администратора. Убедитесь, что на обеих виртуальных машинах установлена внутренняя сеть (Устройства – Настроить сеть – Тип подключения – Внутренняя сеть). Откройте браузер и в адресной строке наберите снова тот же адрес. На странице должен отобразиться текст созданного Вами документа «Default.html» в каталоге C:\Inetpub\wwwroot.

Создайте самостоятельно другой Web-узел. Для этого создайте новую папку на диске C для хранения образца содержимого web-узла, отключите веб-узел по умолчанию (правая кнопка мыши – Отключить). Щелкните правой кнопкой мыши на узле «сайты», выберите «Создать\Веб-сайт». Работа с мастером веб-сайтов (рис. 5) не вызовет у Вас сложностей, так как необходимо заполнить только пустые поля, стандартные же параметры можно не изменять.

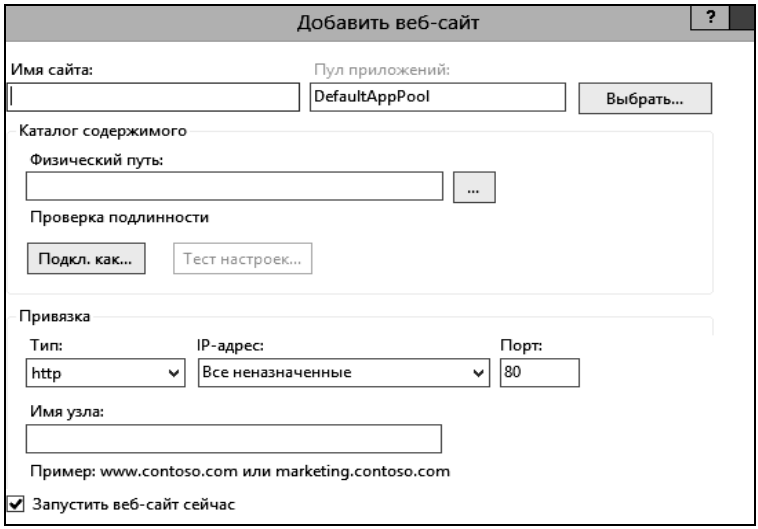

Рис. 5. Создание нового веб-сайта

Проверьте настройку вашего Web-сервера с виртуальной машины win7.

3.2. FTP-сервер

Для настройки папки службы FTP и виртуального корневого каталога создайте новую папку для хранения файлов. Папке можно дать любое имя. Например, назовите новую папку «Example», тогда путь к ней будет таким: C:\inetpub\ftproot\Example.

В диспетчере служб IIS нажмите «Добавить FTP-сайт». Откроется окно добавления нового FTP-сайта.

В мастере укажите имя, которое пользователи могут использовать для получения доступа к папке FTP, созданной в начале. Можно задать любое имя. Удобнее всего в качестве имени псевдонима использовать имя каталога.

Для пути напечатайте путь или перейдите к каталогу, который Вы создали, например, Inetpub\ftproot\Example (рис. 6).

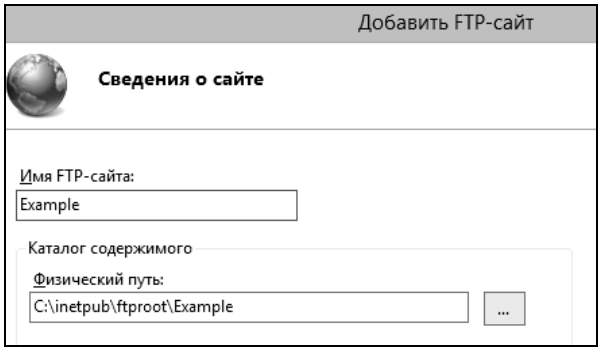

Рис. 6. Создание FTP-сайта

На следующем этапе в окне SSL отметьте пункт «Без SSL», нажмите «Далее».

Далее следует настройка разрешений. Предоставьте пользователям разрешения на чтение информации и на запись (рис. 7).

Чтобы установить разрешения для папки службы FTP, кликните правой кнопкой мыши на узел виртуального каталога для определенной папки службы FTP (например, Example) и нажмите «Редактировать разрешения». На вкладке «Безопасность» выберите или добавьте вашу учетную запись и присвойте разрешение на изменение (рис. 8).

Следующий шаг – это создание виртуального каталога веб-сервера. Чтобы веб-сервер мог получить доступ к корневому каталогу службы FTP, обычно создается виртуальный каталог для веб-сервера, соответствующий FTP-узлу. Имя виртуального каталога веб-сервера может быть таким же, как имя виртуального каталога FTP-сервера, однако это необязательно.

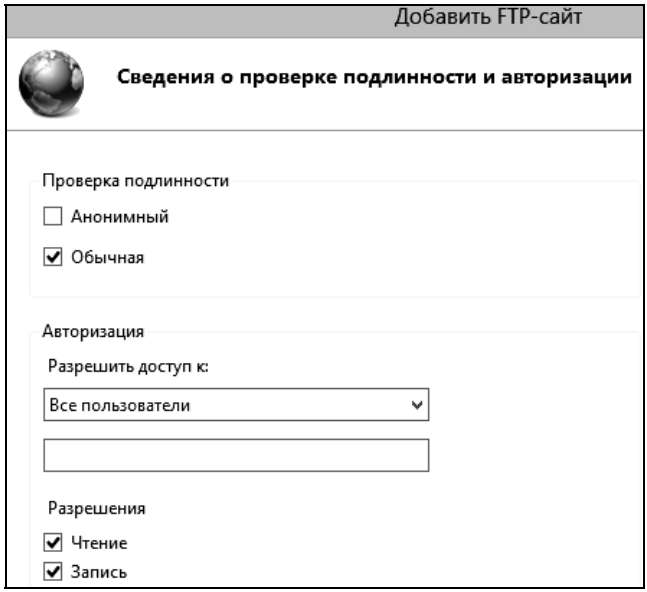

Рис. 7. Сведения о проверке подлинности и авторизации

Рис. 8. Разрешения

Чтобы создать виртуальный каталог веб-сервера, в диалоговом окне «Службы IIS» разверните узел «Веб-узлы». Кликните правой кнопкой мыши на узел «Веб-узел по умолчанию», нажмите «Добавить виртуальный каталог» (рис. 9).

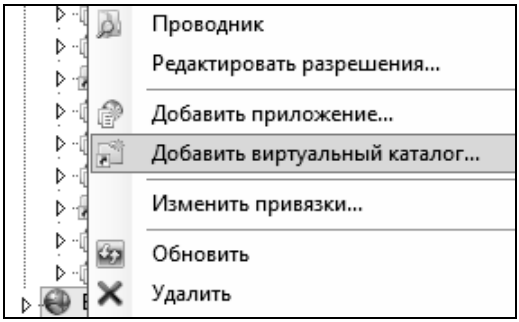

Рис. 9. Контекстное меню

В мастере задайте псевдоним, для пути напечатайте путь или перейдите к каталогу службы FTP, например, C:\inetpub\ftproot\Example (рис.10).

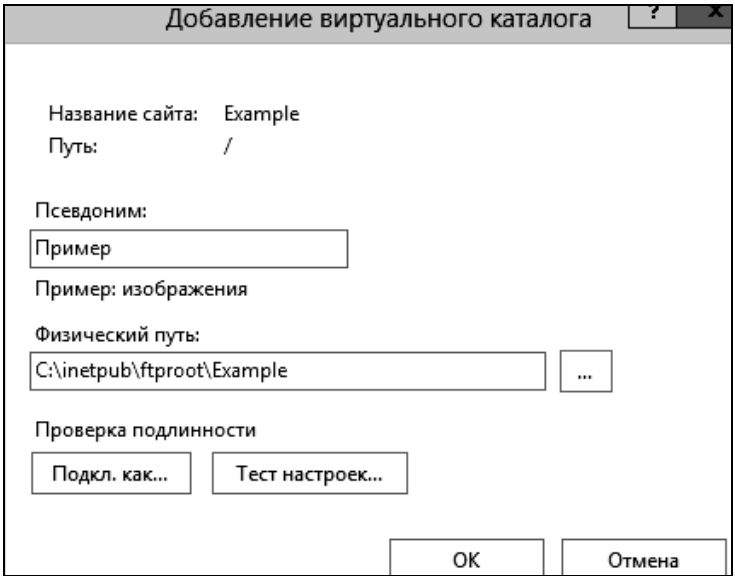

Рис. 10. Добавление виртуального каталога

Для разрешений доступа выберите чтение и выполнение.

Нажмите «Готово», чтобы создать виртуальный каталог и закрыть мастера. Проверьте настройку FTP-сервера с виртуальной машины win-7. Для этого откройте «Мой компьютер» и в адресной строке введите ftp://(ip-адрес сервера) (рис. 11).

Рис. 11. Ввод запроса

Создайте самостоятельно другой FTP-узел по аналогии с представленным примером и заданием для Web-узла. Установите разрешение на запись. Проверьте работоспособность с удаленного рабочего места.

3.3. Почтовый сервер

Необходимо настроить SMTP-сервер. Управляется SMTP сервер через консоль управления «Диспетчер служб IIS 6.0». Открыть эту консоль можно через Server Manager: Средства – Диспетчер служб IIS 6. В консоли разверните ветку с именем сервера, щёлкните правой кнопкой мыши по SMTP Virtual Server и откройте его свойства.

На вкладке «Общие», если необходимо, выберите IP адрес, на котором должен отвечать SMTP сервер и включите ведение журнала, чтобы сохранялась информация обо всех отправленных письмах (рис.12).

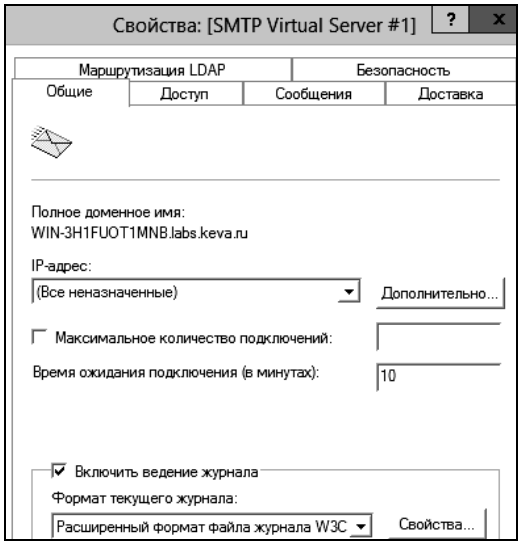

Рис. 12. Свойства SMTP

Перейдите на вкладку «Доступ». Нажмите на кнопку «Проверка подлинности» и убедитесь, что разрешен анонимный доступ (рис.13).

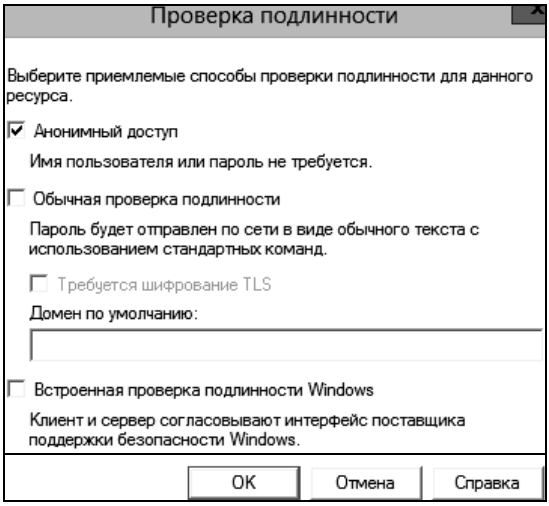

Рис. 13. Проверка подлинности

Вернитесь на вкладку «Доступ» и нажмите кнопку «Подключение». Здесь можно ограничить, с каких устройств могут отправлять почту через наш релей. Выберите опцию «Только компьютеры из списка ниже» и укажите список IP-адресов (рис. 14), не забыв себя (127.0.0.1).

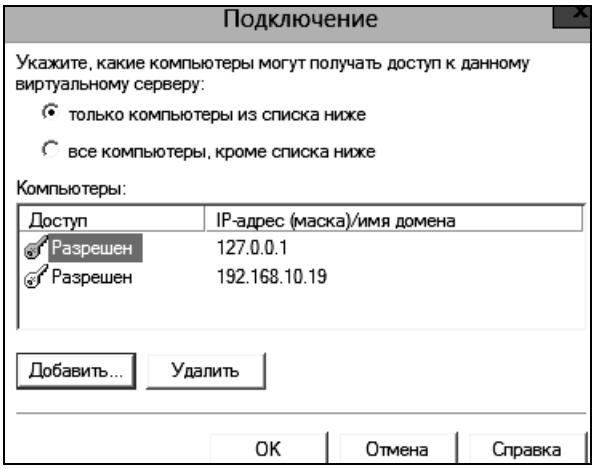

Рис. 14. Подключение

Перейдите на вкладку «Сообщения» (рис. 15). Здесь указывается административный email, куда будут приходить копии NDR сообщений, ограничения на максимальный размер писем, и количество получателей.

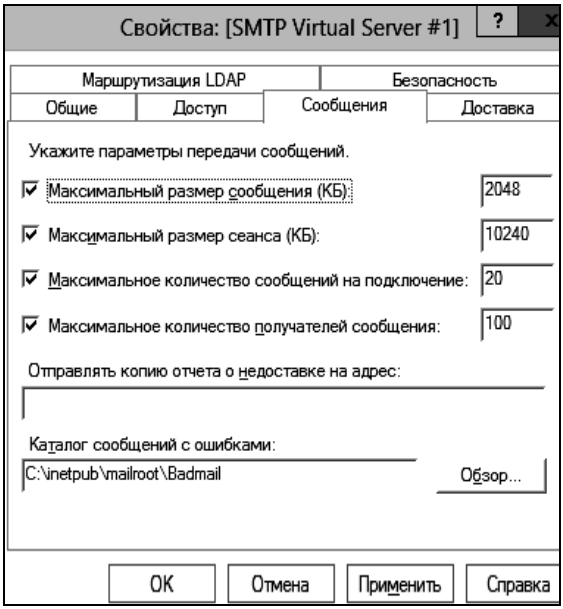

Рис. 15. Сообщения

Перейдите на вкладку «Доставка». Нажмите на кнопку «Безопасность исходящих подключений» (рис. 16). Здесь указывается, как нужно авторизоваться на сервере, куда будет пересылаться почта. К примеру, если вся почта будет отправляться на почтовый сервер Gmail и уже с него пересылаться адресатам, нужно выбрать «Обычная проверка подлинности», указав в качестве пользователя и пароля данные почтового ящика на сервисе Gmail (в настройках аккаунта Google нужно разрешить отправку через их smtp сервера).

Нажмите на кнопку «Дополнительно». Здесь указывается FQDN имя нашего SMTP-сервера (рис. 17). Нажмите на кнопку «Проверка DNS», чтобы проверить корректность записи в DNS.

Сохраните настройки SMTP-сервера.

Запустите службу из командной строки PoSh: start-service smtpsvc. Проверьте, что служба SMTPSVC запущена при помощи команды get-service smtpsvc (рис. 18).

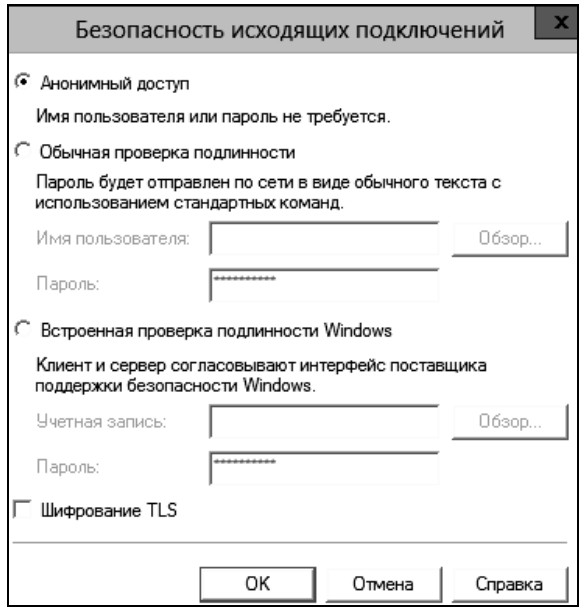

Рис. 16. Безопасность исходящих подключений

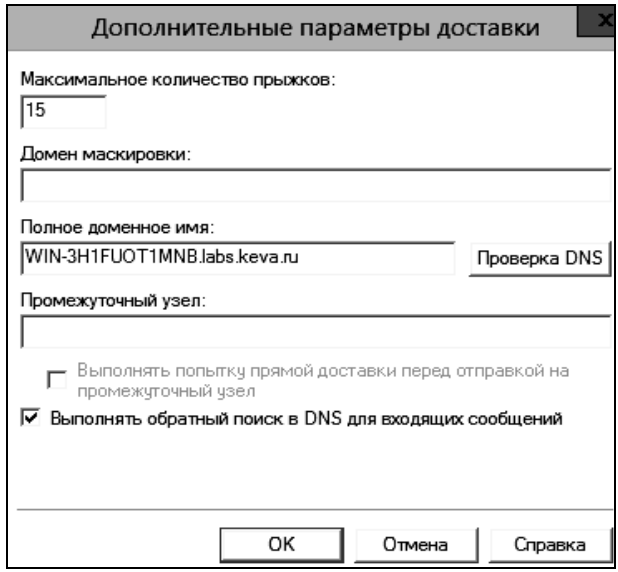

Рис. 17. Дополнительные параметры доставки

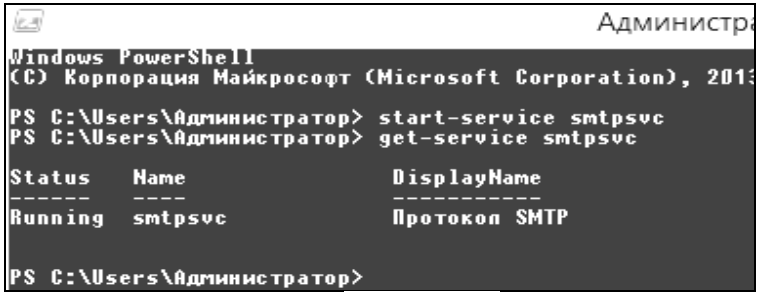

Рис. 18. Запуск службы

Необходимо проверить работу созданного SMTP сервера. Проще всего это сделать, создав на рабочем столе текстовый файл smtp-test-email.txt и, записать в него следующий текст, заменив имя отправителя и получателя на ваши (рис. 19).

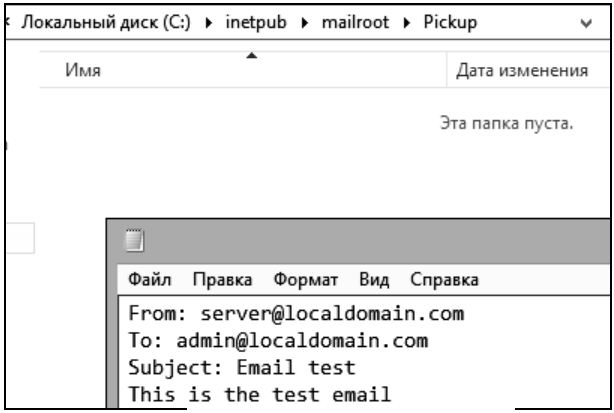

Рис. 19. Создание текстового документа

Скопируйте файл smtp-test-email.txt в каталог C:\inetpub\mailroot\Pickup. SMTP сервер следит за появлением файлов в этой каталоге и при обнаружении файла прочтет его содержимое и попытается отправить письмо с данной темой и текстом адресату, указанному в разделе To:.

Проверьте ящик получателя, в него должно упасть такое письмо.

4. Задание на лабораторную работу

1. Изучить теоретические сведения.
2. Создать Web-сервер. Проверить его работу.
3. Настроить FTP-сервер и проверить его работу.
4. Создать почтовый сервер. Изучить его работу.
5. Написать отчет и защитить его у преподавателя.

5. Контрольные вопросы

1. Что такое HTTP-сервер?
2. Что из себя представляет клиент для HTTP-сервера?
3. Приведите примеры программных продуктов, которые можно использовать в качестве HTTP-серверов?
4. Что такое FTP-сервер?
5. Что такое почтовый сервер?
6. Что такое MTA и MDA?
7. Что такое IIS? Каким образом устанавливается?
8. Какие протоколы поддерживает IIS?
9. Почему письма не отображаются во «Входящих», пока не пройдет синхронизация с сервером? В чем особенность протокола POP3?
10. Какой каталог предназначен для работы с Веб-сервером по умолчанию?

Литература

1. Станек У.Р. Microsoft Windows 8.1. Справочник администратора. СПб.: БХВ-Петербург, 2015. 400 с.

2. Руссинович М., Соломон Д., Ионеску А. Внутреннее устройство Microsoft Windows. Основные подсистемы ОС. 6-е изд. / Пер. Н. Вильчинский Ч. 1.: Питер. СПб., 2013. 800 с.

Учебное издание

Алексей Константинович Новохрестов,
Алексей Игоревич Гуляев

БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ
Часть 1

Лабораторный практикум
для студентов специальностей и направлений
10.03.01 – «Информационная безопасность»,
10.05.02 – «Информационная безопасность телекоммуникационных систем»,
10.05.03 – «Информационная безопасность автоматизированных систем»,
10.05.04 – «Информационно-аналитические системы безопасности»

Верстка – В.М. Бочкаревой
Текст дан в авторской редакции, без корректуры

Издательство «В-Спектр»
Подписано к печати 24.11.2017.
Формат $60\times84^{1}/_{16}$. Печать трафаретная.
Печ. л. 5,75. Тираж 150 экз. Заказ 32.

Тираж отпечатан ИП Бочкаревой В.М.
ИНН 701701817754
634055, г. Томск, пр. Академический, 13-24, тел. 49-09-91.
E-mail: bvm@sibmail.com