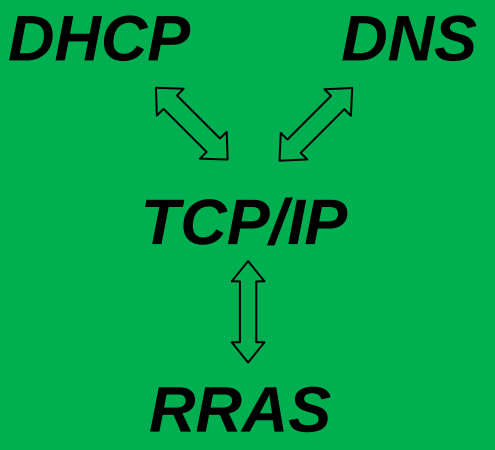
Д.В. Дюгуров

Сетевая адресация, разрешение имен, маршрутизация

Упражнения и задачи



Ижевск
2014

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИИ
ФГБОУ ВПО «УДМУРТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

Д.В. Дюгуров

Сетевая адресация, разрешение имен, маршрутизация
Упражнения и задачи

Учебное пособие

Ижевск 2014

УДК 004.732
Д 95

Рекомендовано к изданию Учебно-методическим советом УдГУ

Рецензенты: к.т.н., доцент В.Н. Пишков
к.ф.-м.н., доцент М.А. Клочков

Дюгуров Д.В.
Д 95 Сетевая адресация, разрешение имен, маршрутизация. Упражнения и задачи: учебное пособие. – Ижевск: Изд-во «Удмуртский университет», 2014. – 94 с.
ISBN

Пособие посвящено управлению различными серверными ролями, требующимися для организации связности и доступности сетевых сегментов. На примерах показана настройка служб DNS, DHCP, Маршрутизации и удаленного доступа.

Предназначено для использования студентами и преподавателями в рамках курсов по системному администрированию крупных вычислительных или корпоративных сетей, а также для инженеров, занимающихся организацией и масштабированием корпоративных сетей.

Может применяться при изучении студентами бакалавриата, специалитета и магистратуры курсов «Компьютерные сети», «Системное администрирование», «Административное обеспечение управления» и других смежных дисциплин по профилям подготовки Прикладная информатика, Фундаментальная информатика и информационные технологии, Информатика и вычислительная техника, Информационные системы и технологии.

ISBN
УДК 004.732

Содержание

Предисловие

Данное учебное пособие является третьей частью комплекса пособий автора по управлению корпоративными вычислительными сетями. Ранее издательством «Удмуртский университет» были выпущены первые две части: «Системное администрирование» и «Управление контроллером домена. Упражнения и задачи».

Настоящее пособие содержит девятнадцать лабораторных работ, отражающих основные технические аспекты по управлению важнейшими элементами сетевой инфраструктуры: DNS-сервером, DHCP-сервером, а также сервером маршрутизации и удаленного доступа. Отдельное внимание уделено базовым принципам управления адресным пространством в вычислительных сетях.

Каждая работа состоит из нескольких упражнений – инструкций. Большинство предлагаемых к выполнению работ связаны друг с другом – результат начальных работ является необходимым условием для выполнения последующих упражнений.

В результате выполнения всех работ учащиеся будут иметь основанный на виртуальных машинах работоспособный сетевой сегмент, пригодный к дальнейшему масштабированию в реальных условиях. Если же учащиеся ранее выполняли упражнения по управлению контроллером домена, то в результате они значительно расширят возможности созданного ими ранее базового домена.

Пособие также будет полезно системным администраторам и инженерам при создании управлении действующими корпоративными сетями.

Лабораторная работа №1
Решение задач по устранению неполадок

Предложенное ниже упражнение поможет освоить решение задач, возникающих в реальных ситуациях, а также научиться быстро и эффективно устранять неполадки, при конфигурировании сетевых адаптеров.

Для выполнения работы необходимо:

1. Внимательно ознакомиться с постановкой задачи.
2. Ответить на предлагаемые вопросы.

Постановка задачи

После физического объединения 15 компьютеров в небольшую сеть вы выполняете на каждом компьютере команду *ipconfig /all*, которая на большинстве узлов показывает наличие APIPA-адреса на включенных сетевых интерфейсах, но есть исключения.

Узел CS-7 возвращает такую информацию:

C:\Documents and Settings\Administrator>ipconfig /all
Windows IP Configuration
Host Name:. ……. . CS-7
Primary Dns Suffix:
Node Type:…… Mixed
IP Routing Enabled……. No
WINS Proxy Enabled:….. No
Ethernet adapter Local Area Connection:
Media State: Media disconnected
Description: Intel(R) PRO/100 P Mobile Combo Adapter
Physical Address: 00-00-59-80-B7-F6

Узел CS-8 никак не реагирует на команду *ipconfig /all*. Вы убедились, что сетевой адаптер на узле установлен.

Узел CS-10 возвращает IP-адрес 0.0.0.0. После выполнения команды *ipconfig /renew* адрес не изменяется.

Вопросы

1. Что нужно предпринять в первую очередь на узле CS-7?
2. Что предпринять далее на узле CS-8?
3. Что делать, если узлу CS-10 надо присвоить APIPA-адрес?

Лабораторная работа №2
Октеты. Маски. Преобразование чисел

В рамках данной лабораторной работы необходимо переводить числа из десятичной в двоичную систему счисления и обратно, а также преобразовывать маски подсети.

Для выполнения работы необходимо:

1. Знания правил скалярного произведения векторов.
2. Ручка и бумага, калькулятор (необязательно).

Упражнение 1. Перевод числа из десятичной системы счисления в двоичную

Преобразуйте указанные ниже числа. Для преобразования сначала воспользуйтесь таблицей, а затем – инженерным калькулятором, и сравните результаты.

Представьте в двоичной системе числа 159 и 65.

Представьте в десятичной системе числа: 1001010 и 01110011.

Таблица преобразования.

ряд	128	64	32	16	8	4	2	1
результат								

NB! Необязательно перечерчивать таблицу вновь для преобразования каждого числа. Достаточно всякий раз добавлять к таблице еще одну строку с результатом.

Упражнение 2. Преобразование маски подсети из десятично-точечной формы в форму с префиксом сети и обратно

Преобразуйте нестандартную маску подсети из десятично-точечной формы в форму с префиксом сети и наоборот. При выполнении задания воспользуйтесь калькулятором или таблицей из предыдущего упражнения.

1. 255.255.255.192
2. 255.255.252.0
3. /27
4. /21

Лабораторная работа №3
Сети и подсети

В рамках данной лабораторной работы необходимо вычислить различные параметры сетей и подсетей в различных адресных пространствах.

Для выполнения работы необходимо:

1. Ручка и бумага, калькулятор (необязательно).

Упражнение 1. Вычисление масок подсети

Интернет-провайдер выделил вам адрес сети 206.73.118.0/24. Ответьте на вопросы, указав количество бит, необходимое для идентификаторов подсети или узла, число бит, оставшееся на идентификатор узла или подсети, маску подсети в различных формах записи.

При ответе учитывайте указанные требования.

Образец.

Требование 1: 6 подсетей.

Количество бит в идентификаторе подсети	3
Оставшееся на идентификатор узла количество бит	4
Маска подсети (в виде префикса сети)	/27
Маска подсети (в десятично-точечном виде)	255.255.255.224

Требование 2: 9 подсетей.

Требование 3: 3 подсети.

Требование 4: 20 узлов на подсеть.

Упражнение 2. Вычисление различных параметров подсети

Определите класс сети и маску подсети по умолчанию для каждого приведенного в таблице идентификатора сети. Затем вычислите действительную маску подсети, назначенную адресу, доступное количество подсетей, количество узлов в каждой подсети.

Идентификатор сети	Класс сети	Маска подсети по умолчанию	Заданная маска подсети	Количество подсетей	Емкость подсети
207.209.68.0/27					
131.107.0.0/20					
10.0.0.0/13					
208.147.66.0/25					

Упражнение 3. Вычисление диапазонов адресов подсети

В этом упражнении нужно вычислить диапазоны адресов подсети, определив диапазоны первых трех подсетей сети, а также указать в вычисленных диапазонах адрес сети и широковещательный адрес. Для выполнения упражнения заполните таблицу, приведенную ниже. Первая строка таблицы уже заполнена в качестве примера.

Адрес сети и маска подсети	Диапазоны (первые три)
10.0.0.0 255.240.0.0	10.0.0.0 - 10.15.255.255 10.16.0.0 - 10.31.255.255 10.32.0.0 - 10.47.255.255
172.16.0.0 255.255.224.0	
172.18.0.0 255.255.248.0	
192.168.1.0 255.255.255.192	

NB! Обратите внимание, что идентификатор узла в начальном адресе диапазона всегда четный. Более того – он состоит из одних нулей. Это адрес сети для диапазона. Именно он используется для маршрутизации. Конечный адрес диапазона всегда нечетный. Идентификатор узла в нем состоит из одних единиц. Это широковещательный адрес диапазона. Оба эти адреса нельзя назначать физическим сетевым узлам.

Упражнение 4. Проверка адресов на принадлежность одной подсети с помощью конъюнкции («И»)

Заполните таблицу, приведенную ниже.

Маска подсети	Адрес №1	«И» №1	Адрес №2	«И» №2	Адреса в одной подсети (да/нет)?
255.255.255.192	192.168.1.116		192.168.1.124		
255.255.255.224	192.168.0.180		192.168.0.192		
255.255.252.0	172.16.100.234		172.16.98.234		
255.255.240.0	172.16.64.10		172.16.72.200		

Лабораторная работа №4
Создание виртуальных машин

Для выполнения дальнейших упражнений необходимы две виртуальные машины под управлением Windows Server 2003 Enterprise Edition. Обе машины будут находиться в одной подсети.

Для выполнения работы необходимо:

1. Персональный компьютер со следующими характеристиками:
    - 600 Mb свободной оперативной памяти;
    - 128 Mb свободной видео памяти;
    - 8 Gb свободного дискового пространства;
    - привод оптических дисков;
    - реальный сетевой адаптер с подключением в Интернет (рекомендуется).
2. Работоспособное приложение Oracle VM VirtualBox.
3. Загрузочный оптический диск Microsoft Windows Server 2003 Enterprise Edition 32 bit.

Упражнение 1. Настройка виртуальной машины под управлением Windows Server 2003

1. Запустить Oracle VM Virtual Box.
2. В меню *Машина* выбрать пункт *Создать*.
3. В окне *Мастера создания виртуальной машины* нажмите кнопку *Вперед*.
4. В поле *Имя виртуальной машины* вписать *Server1*. В выпадающем списке *Операционная система* выбрать *Microsoft Windows*. В выпадающем списке *Версия* выбрать *Windows 2003*. Нажмите кнопку *Вперед*.

5. В поле выбора размера оперативной памяти ввести число *300*. Нажмите кнопку *Вперед.*
6. На странице *Виртуальный жесткий диск* установить галочку напротив параметра *Загрузочный диск* и выбрать параметр *Создать новый жесткий диск*. Нажмите кнопку *Вперед*.
7. На странице *Мастер создания нового виртуального диска* выбрать параметр *VMDK*. Нажмите кнопку *Вперед.*
8. На странице *Дополнительные атрибуты виртуального диска* выбрать параметр *Фиксированный виртуальный диск*. Нажмите кнопку *Вперед*.
9. На странице *Размер и расположение виртуального диска* указать размер диска равный *3,0 Гб*. Нажмите кнопку *Вперед.*
10. Нажмите кнопку *Создать*.
11. Нажмите кнопку *Create*.
12. В окне *Oracle VM Virtual Box Менеджер* выбрать *Свойства* вновь созданной виртуальной машины *Server1*.
13. Перейти к пункту *Система.* Снять галочку с параметра *Дискета* в списке *Порядок загрузки*.
14. Перейти к пункту *Дисплей.* Установить размер видеопамяти равным *64 Мб.*
15. Перейти к пункту *Носители*. Нажмите на кнопку *Добавить жесткий диск*. Нажмите на кнопку *Создать новый диск.* Повторить шаги 7, 8, 9, 10 указав на 9-м шаге размер жесткого диска равным *1 Гб*. В списке *Носители информации* отметить значок оптического диска. В поле *Атрибуты* нажмите на кнопку *Настроить привод оптических дисков* и выбрать параметр *Привод*

хоста, установить галочку напротив параметра *Разрешить прямой доступ*.

16. Перейти к пункту *Сеть*. На вкладке *Адаптер 1* установить галочку напротив параметра *Включить сетевой адаптер*. Параметр *Тип подключения* установить равным *Внутренняя сеть*. Нажмите на кнопку *Ok*.
17. Установить диск с дистрибутивом Windows Server 2003 в дисковод оптических дисков хост-машины.
18. Запустить вновь созданную виртуальную машину *Server1*, нажав на кнопку *Старт* в меню окна *Oracle VM Virtual Box Менеджер*. Ознакомиться с информацией во всплывающих окнах. При необходимости нажимать кнопки *Ok, Захватить* и др.

NB !Для возврата фокуса ввода (указателя мыши) в хостовую ОС нажимать правую клавишу Ctrl!

19. После появления приглашения к установке системы нажмите клавишу *Ввод*.
20. Принять лицензионное соглашение, нажав клавишу F8.
21. Создать новый раздел на всем пространстве диска *ID0*, используя *быстрое форматирование NTFS*. Начать установку операционной системы на созданный раздел.
22. В окне *Язык и региональные стандарты* нажмите кнопку *Далее*.
23. В поле *Имя* ввести *user*. Нажмите кнопку *Далее*.
24. Ввести серийный номер Windows Server. Нажмите кнопку *Далее*.
25. Ознакомиться с информацией в окне Режимы лицензирования. Нажмите кнопку *Далее*.

26. В качестве имени компьютера указать *Server1*. В качестве пароля администратора использовать строку P@ssw0rd. Нажмите кнопку *Далее*.

NB! Везде в дальнейшем следует помнить данные учетной записи администратора логин: Администратор, пароль: P@ssw0rd. Реквизиты локального и доменного администратора в нашем случае совпадают.

27. В окне установка времени и даты нажмите кнопку *Далее*.
28. В окне *Сетевые параметры* нажмите кнопку *Далее.*
29. После установки войти в систему с учетными данными администратора.

NB! При использовании виртуальных машин под управлением Oracle VM Virtual Box вместо сочетания клавиш Ctrl+Alt+Delete Использовать сочетание Правый_Ctrl+Delete.

30. Закройте страницу *Послеустановочные обновления Windows Server*.
31. Ознакомьтесь с информацией в консоли *Управление данным сервером*. Установите флажок напротив параметра *Не показывать эту страницу при входе в систему* и закройте консоль.
32. Настройте по желанию параметры рабочего стола.
33. Отключите *Автоматическое обновление системы*.
34. Включите *Удаленный доступ к рабочему столу* для *Администратора.*

35. Выберите параметры наилучшего быстродействия системы и отмените использование файла подкачки.
36. В виртуальной машине создайте папку C:\distr\Server2003. Скопируйте содержимое установочного диска с Windows Server 2003 в созданную папку.
37. Завершите работу созданной виртуальной машины. Для выключения сервера необходимо написать причину отключения в поле *Примечание* окна отключения системы, в нашем случае в этом поле можно поставить любой символ.
38. В свойствах виртуальной машины Server1 оставьте загрузку только с жесткого диска.

Упражнение 2. Создание второй виртуальной машины. Проверка связи виртуальных машин

1. Запустить Oracle VM Virtual Box.
2. Выбрать виртуальную машину *Server1*, созданную в упражнении 1.
3. В меню *Машина* выбрать пункт *Копировать.*
4. В окне *Мастер копирования виртуальной машины* задать имя копии *Server2* и установить галочку напротив параметра *Сгенерировать новые MAC адреса для всех сетевых адаптеров*. Нажмите кнопку *Вперед*.
5. В окне *Конфигурация копирования* выберите параметр *Полная копия*. Нажмите кнопку *Копировать*.
6. Запустите созданную виртуальную машину Server2 и войдите в систему под учетной записью *Администратора.*
7. Переименовать компьютер, использую имя *Server2*.

8. Перезагрузите виртуальную машину Server2.

NB! Серверные операционные системы не предназначены к частым отключениям. Поэтому все события, связанные с отключением или перезагрузкой журналируются. Для того чтобы перезагрузить сервер, укажите что-либо в поле *Комментарий*, тогда кнопка *Ok* станет активной.

9. Запустите виртуальную машину Server1.
10. Войдите в Server2 под учетной записью *Администратора*.
11. Завершите работу виртуальных машин Server1 и Server2.

Лабораторная работа №5
Настройка TCP/IP-адресов

Вы сконфигурируете статический IP-адрес на Server1 и альтернативный адрес для Server2. До этого момента вашим компьютерам были назначены APIPA-адреса.

Для выполнения работы необходимо:

Выполненная в полном объеме лабораторная работа №4.

Упражнение 1. Проверка существующего IP-адреса

1. Запустите виртуальную машину Server1 и войдите в систему как *Администратор*.
2. Из командной строки выполните команду *ipconfig*.
3. Убедитесь, что напротив строки *IP-адрес автонастройки* указывается текущий адрес в

форме 169.254.x.y, где *x* и *y* соответствуют текущему идентификатору узла Serverl, назначенному APIPA. Маска подсети – 255.255.0.0. APIPA назначила компьютеру Serverl адрес потому, что установка Windows Server 2003 с параметрами по умолчанию подразумевает автоматическое назначение IP-адреса. APIPA используется при недоступности DHCP-сервера.

Упражнение 2. Ручная настройка IP-адреса

1. На Server1 выберите меню *Сетевые подключения* в *Панели управления*.
2. Правой кнопкой мыши выделите *Подключение по локальной сети*. В выпадающем меню выберите пункт *Свойства*.
3. В появившемся окне на вкладке *Общие* в списке *Компоненты, используемые данным подключением* выберите пункт *Протокол Интернета (TCP/IP)*. Нажмите кнопку *Свойства*.
4. В появившемся окне выберите параметр *Использовать следующий IP-адрес*. Укажите следующие адреса 192.169.0.1 и 255.255.255.255.0 в качестве IP-адреса и маски подсети соответственно. Нажмите кнопку *Ok*.
5. Закройте окно свойств сетевого подключения.
6. Из командной строки выполните команду *ipconfig*. Проанализируйте результат.

Упражнение 3. Настройка альтернативного статического адреса и проверка сетевой связности

1. Запустите виртуальную машину Server2 и войдите в систему как *Администратор*.
2. Из командной строки выполните команду *ipconfig*.

3. Убедитесь, что сетевому подключению назначен APIPA-адрес.
4. Из командной строки выполните команду *ping Server1*. Объясните результат.
5. Выберите меню *Сетевые подключения* в *Панели управления.*
6. Правой кнопкой мыши выделите *Подключение по локальной сети.* В выпадающем меню выберите пункт *Свойства.*
7. В появившемся окне на вкладке *Общие* в списке *Компоненты, используемые данным подключением* выберите пункт *Протокол Интернета (TCP/IP).* Нажмите кнопку *Свойства*.
8. Убедитесь, что на вкладке *Общие* выбраны параметры *Получить IP-адрес автоматически* и *Получить адрес DNS-сервера автоматически.*
9. Перейдите на вкладку *Альтернативная конфигурация.*
10. Выберите параметр *Настраиваемый пользователем.*
11. В качестве IP-адреса и маски подсети укажите соответственно следующие адреса 192.168.0.2 и 255.255.255.0. Нажмите кнопку *Ok.*
12. Закройте окно свойств сетевого подключения.
13. Из командной строки выполните команду *ipconfig.* Проанализируйте результат.
14. Из командной строки выполните команду *ping Server1* и убедитесь, что компьютеры Server1 и Server2 осуществляют сетевое взаимодействие.
15. Завершите работу Server1 и Server2.

Лабораторная работа №6
Использование сетевого монитора

В рамках этой работы вы будете использовать утилиту *Сетевой монитор* для записи и анализа сетевого трафика.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 и №5.

Упражнение 1. Установка *Сетевого монитора*

1. Запустите виртуальную машину Server1 и войдите в систему как *Администратор*.
2. Выберите меню *Установка и удаление программ* в *Панели управления*.
3. В открывшемся окне выберите пункт *Установка компонентов Windows.*
4. В окне *Мастер компонентов Windows* в списке *Компоненты* установите галочку напротив параметра *Средства управления и наблюдения*. Нажмите кнопку *Состав.*
5. В открывшемся окне установите галочку напротив параметра *Средства сетевого монитора*. Нажмите кнопку *Ok.*
6. В окне *Мастер компонентов Windows* нажмите кнопку *Далее.*
7. Дождитесь завершения установки. При необходимости укажите расположение дистрибутивов Windows Server.
8. После завершения установки в появившемся окне нажмите кнопку *Готово*. Закройте окно *Установка и удаление программ.*

NB! Напомним, что при выполнении лабораторной работы №4 дистрибутивы Windows Server были записаны в папку *…\distr\Server2003* одного из жестких дисков виртуальных машин. При установке служб нужно указывать путь к папке *…\distr\Server2003\I386*, входящей в комплект дистрибутива. Для мониторинга сетевого трафика можно использовать утилиты сторонних разработчиков, например WireShark.

Упражнение 2. Запись данных средствами сетевого монитора

1. Запустите виртуальную машину Server2.
2. Вернитесь к уже запущенной виртуальной машине Server1.
3. С помощью меню *Сетевые подключения* в *Панели управления* откройте свойства *Подключения по локальной сети*. Убедитесь, что напротив параметра *Драйвер сетевого монитора* установлена галочка. Закройте все открытые окна.

NB! Помните, что *Сетевой монитор* будет перехватывать сетевой трафик только тех подключений, к которым непосредственно подключен его драйвер.

4. Запустите *Сетевой монитор*: *Пуск→Все программы→Администрирование→Сетевой монитор.*
5. В открывшемся окне нажмите кнопку *Ok.* Выберите для мониторинга *Подключение по локальной сети* в окне *Выбор сети.* Нажмите кнопку *Ok.*

6. В меню *Запись* выберите пункт *Запустить* или нажмите клавишу F10.
7. Из командной строки выполните команду *ping Server2*.
8. После окончания работы команды *ping* вернитесь к окну *Сетевого монитора* и в меню *Запись* выберите пункт *Остановить и просмотреть* или нажмите клавиши Shift+F11.
9. Выберите любой кадр из списка. Щелкните по нему дважды левой кнопкой мыши. Внимательно изучите всю информацию в открывшихся окнах.
10. Сохраните записанную информацию в файл. Для этого в меню *Файл* выберите пункт *Сохранить как*. В качестве имени сохраняемого файла укажите занчение *PingCapture*. Обратите внимание, с каким расширением, и в какой по умолчанию папке сохраняются данные записей *Сетевого монитора*.
11. Закройте окно записи трафика. Обратите внимание, какие теперь данные отображаются в окне *Сетевого монитора*.
12. Завершите работу Serever2.

Упражнение 3. Сохранение кадров в текстовое файле

1. В меню *Файл Сетевого монитора* на Server1 выберите пункт *Открыть* и откройте файл Ping Capture, созданный в предыдущем упражнении.
2. Поставьте курсор на любой кадр, в котором как протокол верхнего уровня отмечен ICMP. Нажмите клавиши Ctrl+C.
3. Откройте *Блокнот* и нажмите клавиши Ctrl+V. Перед вами подробное содержимое кадра. Изучите его.

NB! Помните, что клавиша правый_Ctrl является системной клавишей в VirtualBox. Для управления функциями копирования и выделения объектов используйте клавишу правый_Ctrl.

4. Сохраните данный файл под именем *ICMPFrame* в кодировке Юникод в той же папке, где сохранен файл PingCapture.cap.
5. Закройте все окна и завершите работу Server1.

Лабораторная работа №7
Использование средств диагностики сети

Во время данной работы будут использованы утилита *Диагностика сети*, команда Netdiag и протокол Telnet. .

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 и №5.

Упражнение 1. Использование утилиты *Диагностика сети*

1. Запустите виртуальную машину Server1 и войдите в систему как *Администратор*.
2. Войдите в меню *Пуск→Справка и поддержка.*
3. В открывшемся окне в списке *Задачи поддержки* перейдите по ссылке *Служебные программы*.
4. В появившемся списке *Средства* разверните узел *Средства центра справки и поддержки* и перейдите по ссылке *Диагностика сети*.
5. В рабочей области перейдите по ссылке *Собрать информацию*. Дождитесь окончания сбора данных. Подробно изучите представленную информацию.

6. В рабочей области перейдите по ссылке *Настроить параметры сбора информации*.
7. В списке *Действия* установите флажок напротив параметра *Подробно*.
8. В списке *Категории* снимите флажки напротив следующих параметров*: Почтовая служба, Служба новостей, Прокси-сервер, Информация о компьютере, Операционная система, Версия Windows, Модемы*.
9. В рабочей области перейдите по ссылке *Собрать информацию*. Дождитесь окончания сбора данных.
10. Нажмите на кнопку *Сохранить в файл*. Обратите внимание, где и в каком формате сохраняются собранные данные. Нажмите кнопку *Ok*.
11. В рабочей области перейдите по ссылке *Показать сохраненные файлы*.
12. Изучите содержимое файлов. При просмотре включайте заблокированное содержимое.
13. Файл результатов диагностики сети, сохраненный на рабочем столе, переместите в папку *Мои документы*.
14. Закройте все открытые окна.

Упражнение 2. Установка средств поддержки Windows

1. Откройте папку C:\distr\Server2003\SUPPORT\TOOLS.
2. Запустите установочный пакет SUPPORTTOOLS.MSI.
3. Следуйте инструкциям мастера установки, не изменяя параметров по умолчанию.
4. Завершите установку и закройте все ненужные окна.

Упражнение 3. Использование команды Netdiag по протоколу Telnet

1. Откройте консоль *Службы*: *Пуск→ Администрирование→ Службы*.
2. В списке выделите службу Telnet правой кнопкой мыши. В выпадающем меню выберите пункт *Свойства*. Измените тип запуска службы, выбрав параметр *Вручную*. Затем запустите службу.
3. Закройте консоль Службы.
4. Запустите виртуальную машину Server2 и войдите в систему как *Администратор*.
5. Из командной строки на Server2 выполните команду *telnet server1*.
6. Система предупредит об уязвимости передачи пароля на другой компьютер. В нашем случае это не важно. Согласитесь с передачей пароля.

NB! Наши виртуальные машины настроены так, что в них используются одинаковые учетные записи. Поэтому после подключения к Server1 по telnet сразу появляется доступ к командной строке. Если бы реквизиты учетных записей не совпадали, то для доступа к командной строке пришлось бы вводить логин и пароль администратора.

7. В командной строке telnet выполните команду *netdiag*. Ознакомьтесь с результатами.
8. В командной строке telnet выполните команду *cd мои документы*.
9. В командной строке telnet выполните команду *netdiag > NetdiagOutput.txt.*
10. На Server1 ознакомьтесь с содержимым файла, созданного на предыдущем шаге.

11. Вернитесь к Server2. В командной строке telnet выполните команду *netdiag /v > VerboseNetdiagOutput.txt*.

NB! Помните, что любая команда командной строки в среде Windows Server снабжена справкой. Для вызова справки нужно вызвать команду с ключом *help* или *?* Команды принимают ключи через / или -.

12. На Server1 будет создан файл с подробным отчетом о работе сети. Изучите вновь созданный файл.
13. Сравните информацию в изученных файлах с информацией, полученной в первом упражнении с помощью утилиты *Диагностика сети*. После этого завершите работу Server1 и Server2.

Лабораторная работа №8
Разрешение имен. Установка DNS-сервера

В рамках данной лабораторной работы вы запишите трафик разрешения имен. Установите роль DNS-сервера, используете зоны и записи ресурсов разных типов, а также создадите подключение к Интернету.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6. Подключение хост-машины к Интернету.

Упражнение 1. Запись трафика разрешения имен

1. Запустите виртуальную машину Server2.
2. Запустите виртуальную машину Server1 и войдите в систему как *Администратор*.
3. Из командной строки выполните последовательно команды *ipconfig /flushdns* и *nbtstat –R*.

4. Запустите *Сетевой монитор*.
5. В окне *Сетевого монитора* выберите меню *Запись* и в нем пункт *Сети*.

NB! Нажав на кнопку *Пуск* можно увидеть список ранее запускавшихся утилит. Используйте его для быстрого запуска нужных приложений.

6. В качестве сети для записи выберите *Подключение по локальной сети*.
7. Включите запись трафика.
8. Из командной строки выполните команду *ping server2*.
9. Остановите запись трафика и отобразите записанные данные после завершения выполнения команды *ping*.
10. Определите по типу протокола, как имя Server2 было преобразовано в адрес 192.168.0.2. Объясните, почему использовано именно такой механизм?
11. Сохраните результаты записи сетевого трафика в файле *NameResoluton1.cap*.
12. Закройте на Server1 все открытые окна.

Упражнение 2. Установка компонентов DNS

1. Войдите в меню *Пуск→ Панель управления→ Установка и удаление программ*.
2. В рабочей области открывшегося окна *Установка и удаление программ* выберите пункт *Установка компонентов Windows*.
3. В коне *Мастер компонентов Windows* в списке *Компоненты* выделите параметр *Сетевые службы* и нажмите кнопку *Состав*.

4. В открывшемся окне поставьте галочку напротив параметра *DNS* и нажмите кнопку *Ok.*
5. В коне *Мастер компонентов Windows* нажмите кнопку *Далее.*
6. Дождитесь завершения работы мастера установки и закройте окно *Установка и удаление программ*.
7. Завершите работу Server1.

Упражнение 3. Создание подключения к Интернету

1. Убедитесь что хост-машина подключена к Интернету и подключение работоспособно.
2. Запустите *VirtualBox Менеджер*.
3. В списке виртуальных машин выделите Server1 и нажмите кнопку *Свойства.*
4. В рабочей области окна свойств Server1 выберите пункт *Сеть* и перейдите на вкладку *Адаптер 2*.
5. Установите галочку напротив параметра *Включить сетевой адаптер*.
6. В выпадающем списке *Тип подключения* выберите *Сетевой мост*, а в качестве *Имени* укажите устройство хост-машины, через которое осуществляется доступ в Интернет. Нажмите кнопку *Ok.*
7. Запустите виртуальную машину Server1 и войдите в систему как *Администратор*.
8. Запустите *Internet Explorer* и убедитесь, что теперь Server1 имеет выход в Интернет, посетив какой-нибудь сайт.
9. Закройте *Internet Explorer.*
10. Перейдите к папке сетевых подключений: *Пуск→ Панель управления→ Сетевые подключения.*
11. Переименуйте *Подключение по локальной сети №3* в *MyISP.*

Упражнение 4. Базовая настройка DNS-сервера

1. Запустите консоль *DNS*: *Пуск→ Администрирование→ DNS.*
2. В дереве консоли правой кнопкой мыши выделите *SERVER1* и в выпадающем меню выберите параметр *Настроить DNS-сервер…*
3. В окне *Мастер настройки DNS-сервера* нажмите кнопку *Далее.*
4. Выберите параметр *Создать зоны прямого и обратного просмотра (рекомендуется для большинства сетей)* и нажмите кнопку *Далее.*
5. Ответьте *Да* на вопрос *Создать зону прямого просмотра сейчас?* Нажмите кнопку *Далее.*
6. Выберите параметр *Основная зона*. Нажмите кнопку *Далее.*
7. В качестве имени зоны укажите *contoso.com*. Нажмите кнопку *Далее*.
8. Выберите параметр *Создать новый файл*. Не изменяйте имя файла. Нажмите кнопку *Далее.*
9. Выберите параметр *Запретить динамические обновления*. Нажмите кнопку *Далее.*
10. Ответьте *Да* на вопрос *Создать зону обратного просмотра сейчас?* Нажмите кнопку *Далее.*
11. Выберите параметр *Основная зона*. Нажмите кнопку *Далее.*
12. В качестве *Кода сети* укажите *192.168.0*. Обратите внимание, какое имя присваивается создаваемой зоне. Нажмите кнопку *Далее*.
13. Повторите шаги 8 и 9.
14. Ответьте *Нет* на вопрос *Должен ли этот DNS-сервер пересылать запросы?* Нажмите кнопку *Далее.*
15. Нажмите кнопку *Готово* и завершите работу *Мастера настройки DNS-сервера.*
16. В консоли *DNS* изучите созданные роны прямого и обратного просмотра.

Упражнение 5. Тестирование DNS-сервера

1. В дереве консоли правой кнопкой мыши выделите *SERVER1* и в выпадающем меню выберите параметр *Свойства.*
2. В окне *SERVER1 – свойства* перейдите на вкладку *Корневые ссылки.*
3. Если в Списке Серверы имен FQDN всех указанных серверов сопоставлены IP-адреса, то перейдите к шагу 7, иначе перейдите к шагу 4.
4. Выделите имя первого корневого DNS-сервера и нажмите на кнопку *Изменить*.
5. В открывшемся окне нажмите на кнопку *Сопоставить*. Дождитесь получения IP-адреса и нажмите кнопку *Ok*.
6. Повторите шаги 4 и 5 для всех остальных имен корневых DNS-серверов. После этого закройте окно *SERVER1 – свойства.*
7. На вкладке *Наблюдение* окна *SERVER1 – свойства* установите галочки напротив параметров *Простой запрос к этому DNS-серверу* и *Рекурсивный запрос к другим DNS-серверам*. Нажмите кнопку *Тест* и убедитесь, что оба теста пройдены успешно.
8. Закройте все открытые окна на Server1.

NB! Запомните, что простой тест DNS-сервера основан на обратном просмотре адреса замыкания на себя 127.0.0.1. Если происходит отказ при прохождении этого теста, нужно убедиться, что запись с именем *1* находится в зоне обратного просмотра *0.0.127.in-addr.arpa* (видима в консоли *DNS* в режиме *Расширенный*). Рекурсивный тест поверяет способность взаимодействия с другимиDNS-серверами и правильность настроек корневых ссылок.

Упражнение 6. Настройка основного DNS-суффикса

1. Из командной строки выполните команду *ping server1*. Обратите внимание на имя компьютера, от которого приходит ответ.
2. На рабочем столе выделите значок *Мой компьютер* правой кнопкой мыши и в выпадающем меню выберите параметр *Свойства.*
3. В открывшемся окне *Свойства системы* перейдите на вкладку *Имя компьютера* и нажмите кнопку *Изменить*.
4. В окне *Изменение имени компьютера* нажмите кнопку *Дополнительно…*
5. В поле *Основной DNS-суффикс этого компьютера* укажите *contoso.com*. Нажмите кнопку *Ok* несколько раз. Согласитесь с перезагрузкой компьютера и выполните ее.
6. После перезагрузки войдите на Server1 как *Администратор* и из командной строки еще раз выполните команду *ping server1*. Обратите внимание, как изменилось имя компьютера, от которого приходит ответ.
7. Повторите шаги 2 – 5 на Server2.

Упражнение 7. Включение ICS

1. На Server2 из командной строки исполните команду *ipconfig /all.* Изучите результат.
2. На Server1 перейдите к папке сетевых подключений: *Пуск→ Панель управления→ Сетевые подключения.*
3. Выделите правой кнопкой мыши подключение *MyISP* и в выпадающем меню выберите *Свойства.*
4. В окне *MyISP – свойства* перейдите на вкладку *Дополнительно*.

5. Установите галочку напротив параметра *Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера* и нажмите кнопку *Ok*.
6. Дождитесь, пока служба *ICS* будет включена.
7. Перезагрузите Server2.
8. Войдите в Server2 как *Администратор* и из командной строки вновь исполните команду *ipconfig /all*. Объясните результат.

NB! Помните, что служба ICS назначает локальному подключению компьютера, на котором она запущена, адрес 192.168.0.1, что означает, что в локально сегменте ICS можно использовать только один раз. Эта служба определенным образом реализует протокол DHCP (назначает узлам локального сегмента адреса из диапазона 192.168.0.2 – 192.168.0.254, в качестве основного шлюза и DNS-сервера назначает адрес 192.168.0.1), рекурсивные запросы DNS и добавляет статический маршрут во внешнее подключение. Чтобы узлы локального сегмента могли взаимодействовать с ICP их сетевые подключения должны быть настроены на автоматическое получение сетевых адресов.

Упражнение 8. Выполнение рекурсивных запросов

1. На Server2 из командной строки исполните команду *ipconfig /flushdns.*
2. На Server1 запустите *Сетевой монитор* и начните запись трафика.
3. На Server2 запустите *Internet* Explorer и перейдите по адресу *http://www.ya.ru*.
4. На Server1 в окне *Сетевого монитора* нажмите на кнопку *Остановить запись и отобразить данные.*

5. В окне *Запись данных* разверните первый DNS-кадр. Обратите внимание на FQDN искомого узла.
6. В центральной панели раскройте узел DNS Flags. Какой из флагов имеет значение 1? Что это значит?
7. Закройте окно *Сетевой монитор*. Не сохраняйте результаты записей трафика.
8. Откройте консоль *DNS* и разверните узел SERVER1.
9. В меню *Вид* консоли *DNS* установите галочку напротив параметра *Расширенный*.
10. Изучите содержание узла *Кэшированные просмотры*.
11. Закройте все отрытые окна и завершите работу Server1 и Server2.

Лабораторная работа №9
Сравнение трафика разрешения имен в NetBIOS и DNS. Создание нового домена

В рамках данной лабораторной работы вы запишите трафик разрешения имен и сравните результаты с полученными ранее при выполнении упражнения 1 предыдущей лабораторной работы. Также вы сделаете Server1 контроллером домена, а Server2 – членом домена.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4, №5, №6 и №8.

Упражнение 1. Запись трафика разрешения имен

1. Запустите виртуальную машину Server1.
2. Запустите виртуальную машину Server2 и войдите в систему как *Администратор*.

3. Установите *Сетевой монитор* как описано в упражнении №1 лабораторной работы №6.
4. Запустите *Сетевой монитор,* и настройте его на запись трафика *Подключения по локальной сети*.
5. Из командной строки выполните последовательно команды *ipconfig /flushdns* и *nbtstat –R*.
6. Включите запись трафика.
7. Из командной строки выполните команду *ping server1*.
8. Остановите запись трафика и отобразите записанные данные после завершения выполнения команды *ping*.
9. Сохраните результаты записи сетевого трафика в файле NameResoluton2.cap.
10. Сравните трафик, записанный только что с тем, который записан в файле NameResoluton1.cap и сохранен ранее на Server1. Каково основное различие между записями и чем оно объясняется?
11. Закройте на Server1 и Server2 все открытые окна, ничего не сохраняйте.

Упражнение 2. Установка ролей контроллера домена и DNS-сервера на Server1

1. На Server1 в папке *Сетевые подключения Панели управления* выделите правой кнопкой мыши подключения *MyISP* и в выпадающем меню выберите пункт *Свойства*.
2. Перейдите на вкладку *Дополнительно* и снимите галочку напротив параметра *Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера*.
3. В папке *Сетевые подключения Панели управления* выделите правой кнопкой мыши подключения

MyISP и в выпадающем меню выберите пункт *Запретить*.

4. Запустите консоль *Службы* из меню *Администрирование Панели управления*.
5. Двойным щелчком левой кнопки мыши откройте свойства службы *Брандмауэр Windows/Общий доступ к Интернету (ICS)*.
6. В открывшемся окне нажмите кнопку *Стоп*. В выпадающем списке *Тип запуска* установите значение *Отключено* и нажмите кнопку *Ok*.
7. Запустите консоль *Управление данным сервером* из меню *Администрирование Панели управления*.
8. В консоли *Управление данным сервером* выберите команду *Добавить или удалить роль*.
9. Ознакомьтесь с информацией в появившемся окне мастера и нажмите кнопку *Далее*.
10. В окне *Параметры настройки* выберите параметр *Особая конфигурация* и нажмите кнопку *Далее*.
11. В окне *Роль сервера* выберите параметр *DNS-сервер* , нажмите кнопку *Далее*. Поставьте галочку напротив параметра *Удалить роль,* нажмите кнопку *Готово* и дождитесь завершения работы мастера.
12. В окне *Роль сервера* выберите параметр *Контроллер домена (Active Directory)* и нажмите кнопку *Далее* четыре раза, изучая информацию в появляющихся окнах мастера.
13. В окне *Тип контроллера домена* выберите параметр *Контроллер домена в новом домене*. Нажмите кнопку *Далее*.
14. В окне *Создать новый домен* выберите параметр *Новый домен в новом лесу*. Нажмите кнопку *Далее*.
15. В окне *Новое имя домена* введите *contoso.com*. Нажмите кнопку *Далее*.

16. В окне *NetBIOS-имя домена* нажмите кнопку *Далее.*
17. В окне *Папки баз данных и журналов* нажмите кнопку *Далее.*
18. В окне *Общий доступ к системному тому* нажмите кнопку *Далее.*
19. В окне *Диагностика регистрации DNS* выберите параметр *Установить и настроить DNS-сервер на этом компьютере и выбрать этот DNS-сервер в качестве предпочитаемого DNS-сервера*. Нажмите кнопку *Далее*.
20. В окне *Разрешения* выберите параметр *Разрешения, совместимые только с Windows 2000 и Windows Server 2003*. Нажмите кнопку *Далее.*
21. В качестве пароля администратора укажите P@ssw0rd. Нажмите кнопку *Далее* три раза, изучая информацию в окнах мастера.
22. После завершения работы мастера нажмите кнопку *Готово* и перезагрузите Server1.
23. После перезагрузки войдите в домен CONTOSO под учетной записью *Администратора*.
24. В окне *Этот сервер теперь является контроллером домена* нажмите кнопку *Готово.*
25. Закройте консоль *Управление данным сервером*.
26. В меню *Администрирование* выберите консоль *Active Directory – пользователи и компьютеры*.
27. Разверните содержимое контейнера *contoso.com* и найдите учетную запись *Server1* в организационном подразделении (ОП) *Domain Controllers.*
28. Выделите узел contoso.com правой кнопкой мыши и выберите пункт меню *Свойства*. Прейдите на вкладку *Групповая политика.*
29. Выделите объект *Default Domain Group Policy* и нажмите кнопку *Изменить.*

30. Последовательно выберите узлы *Конфигурация компьютера→Конфигурация Windows→Параметры безопасности→Локальные политики→Параметры безопасности→Интерактивный вход в систему: количество предыдущих подключений кэшу* и установите значение параметра равным 0.
31. Закройте консоль *Active Directory – пользователи и компьютеры.*
32. В меню *Администрирование* выберите консоль *DNS.*
33. Последовательно разверните контейнеры *Server1*, *Зоны прямого просмотра*, *_tcp* и найдите запись локатора службы (SRV) протокола *_ldap* с именем *server1.contoso.com*.
34. В папке *Сетевые подключения Панели управления* выделите правой кнопкой мыши подключения *MyISP* и в выпадающем меню выберите пункт *Включить*. Обратите внимание, что теперь нельзя активировать технологию ICS на этом подключении. Почему?
35. Вновь перейдите к консоли DNS. Повторно выполните упражнение №5 лабораторной работы №8.
36. Заново создайте на сервере зону обратного просмотра (упражнение №4 лабораторной работы №8).
37. Закройте консоль *DNS.*

Упражнение 3. Присоединение компьютера Server2 к домену contoso.com

1. На Server1 запустите консоль *Active Directory – пользователи и компьютеры.*
2. Выделите домен *contoso.com* правой кнопкой мыши.
3. В выпадающем меню выберите пункт *Создать→ Подразделение*.

4. В качестве имени ОП укажите *Servers*. Нажмите кнопку *Ok*.
5. Выделите ОП Servers правой кнопкой мыши.
6. В выпадающем меню выберите пункт *Создать→ Компьютер*.
7. В качестве имени компьютера укажите *Server2*. Нажмите кнопку *Далее* дважды. В конце нажмите кнопку *Готово*.
8. Войдите в Server2 под учетной записью *Администратора*.
9. Выберите *Свойства* системы, выделив значок *Мой компьютер* правой кнопкой мыши.
10. Выберите вкладку *Имя компьютера* и нажмите кнопку *Изменить*.
11. Нажмите кнопку *Дополнительно*. В поле *Основной DNS-суффикс этого компьютера* введите *contoso.com*. Нажмите кнопку *Ok*.
12. В окне *Изменение имени компьютера* выберите параметр *Является членом домена* и введите *contoso.com*. Нажмите кнопку *Ok*.
13. В появившемся окне авторизации введите реквизиты учетной записи администратора.
14. Нажмите кнопку *Ok* в окне-приглашении в домен и перезагрузите Server2.
15. Войдите на Server1 и убедитесь, что поля свойств учетной записи *Server2* в подразделении *Servers* стали заполненными.

NB! Теперь Server2 является членом домена contoso.com, значит, можно входить в Server2 локально, а можно входить в домен. В дальнейшем для входа в домен используйте имя учетной записи в формате имя_пользователя@имя_домена, в нашем случае *Администратор@contoso.com*.

Лабораторная работа №10
Создание дополнительного DNS-сервера

В рамках данной лабораторной работы вы создадите дополнительный DNS-сервер и опробуете зонную передачу.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8 и №9.

Упражнение 1. Создание дополнительной зоны

1. Запустите виртуальную машину Server1.
2. Запустите виртуальную машину Server2 и войдите в домен как *Администратор*.
3. Установите компонент *Средства поддержки Windows* (упражнение 2 лабораторной работы №7) и службу *DNS-сервер* (упражнение 2 лабораторной работы №8). При установке DNS-сервера не создавайте зоны, настройте только корневые ссылки. Проигнорируйте все предупреждения.
4. Войдите в домен с Server1 под учетной записью *Администратора*.
5. Запустите консоль *DNS*. В дереве консоли выделите правой кнопкой мыши зону *contoso.com* и в выпадающем меню выберите пункт *Свойства*.
6. Перейдите на вкладку *Серверы имен*. Нажмите кнопку *Добавить…*
7. В открывшемся окне в поле *Полное доменное имя сервера (FQDN)* введите *server2.contoso.com*. В поле *IP-адрес* введите *192.168.0.2*. Нажмите кнопку *Добавить*, затем дважды нажмите кнопку *Ok*.
8. Перейдите к системе Server2.

9. Откройте консоль *DNS* и с помощью мастера создайте на сервере дополнительную зону прямого просмотра с именем *contoso.com*. В качестве адреса основного сервера укажите *192.168.0.2*.
10. По окончании работы мастера выделите вновь созданную зону правой кнопкой мыши, и в выпадающем меню выберите пункт *Передать зону с основного сервера*.
11. Если при передаче зоны произойдет сбой, подождите минуту и повторите попытку. Также можете перезапустить службу *DNS-сервер* на Server2.
12. В дереве консоли выделите правой кнопкой мыши узел *DNS*, и в выпадающем меню выберите пункт *Подключиться к DNS-серверу...* Подключитесь к Server1.
13. После подключения изучите возможности управления зоной *contoso.com* на Server1 и Server2. Для этого выделяйте зоны и обращайтесь к меню *Действие*. Можно ли создавать и конфигурировать записи в зоне *contoso.com* с Server2? Почему?

Упражнение 2. Просмотр параметров

1. В консоли *DNS* на Server2 в дереве консоли разверните узел *Server1*, затем выделите павой кнопкой мыши зону прямого просмотра *contoso.com* и в выпадающем меню выберите параметр *Свойства*.
2. Перейдите на вкладку *Передачи зон* и нажмите кнопку *Уведомить…* Изучите представленные параметры и объясните их значение.
3. Перейдите на вкладку Начальная запись зоны и ответьте на следующие вопросы:

- как долго DNS-сервер на Server2 будет обслуживать DNS-запросы клиентов после потери связи с Server1?
- как часто Server2 запрашивает на Server1 изменения зоны?
- через какое время после потери связи с Server1 при запросе SOA Server2 повторит попытку?
- если другой основной DNS-сервер Server3 успешно получит с Server2 ответ на запрос об IP-адресе Server1, как долго соответствующая Server2 запись ресурса A сохранится в кэше Server3?

4. В консоли *DNS* выделите правой кнопкой узел *Server1* и в выпадающем меню выберите пункт *Удалить*.
5. Подтвердите удаление, в диалоговом окне нажмите кнопку *Да*.
6. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №11
Делегирование зон. Зоны-заглушки

В данной лабораторной работе вы создадите новую зону – поддомен домена contoso.com, настроите делегирование и проверите конфигурацию, а также создадите зону-заглушку.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8 – №10.

Упражнение 1. Создание хоны для делегирования

1. Запустите виртуальную машину Server1.
2. Запустите виртуальную машину Server2 и войдите в домен как *Администратор.*
3. Запустите консоль *DNS.* В дереве консоли разверните узел *SERVER2*. Выделите правой кнопкой мыши узел *Зоны прямого просмотра* и в выпадающем меню выберите параметр *Создать новую зону...*
4. В окне *Мастер создания новой зоны* нажмите кнопку *Далее.*
5. На странице *Тип зоны* выберите параметр *Основная зона*. Нажмите кнопку *Далее.*
6. На странице Имя зоны в поле ввода укажите *sub.contoso.com.* Нажмите кнопку *Далее.*
7. На странице *Файл зоны* выберите параметр *Создать новый файл*. Нажмите кнопку *Далее.*
8. На странице *Динамические обновления* выберите параметр *Разрешить любые динамические обновления*. Нажмите кнопку *Далее.*
9. На странице *Завершение мастера создания новой зоны* нажмите кнопку *Готово*.

Упражнение 2. Создание в зоне записи ресурса – узла (A)

1. В дереве консоли *DNS* выделите правой кнопкой мыши вновь созданную зону *sub.contoso.com* и в выпадающем меню выберите пункт *Создать узел (A)…*
2. В окне *Новый узел* в качестве имени компьютера укажите *Server1*, а в качестве IP-адреса – *192.168.0.1*. Нажмите на кнопку *Добавить узел*. В информационном окне нажмите кнопку *Ok.*
3. Окно *Новый узел* останется открытым. Теперь в качестве имени компьютера укажите *Server2*, а в

качестве IP-адреса – *192.168.0.2*. Нажмите на кнопку *Добавить узел*. В информационном окне нажмите кнопку *Ok*.

4. В окне *Новый узел* нажмите на кнопку *Готово*.
5. Закройте консоль *DNS*.

Упражнение 3. Создание делегирования

1. Войдите в домен с Server1 как *Администратор*.
2. Запустите консоль *DNS*. В дереве консоли выделите правой кнопкой мыши зону contoso.com и в выпадающем меню выберите пункт *Создать делегирование…*
3. В окне *Мастер делегирования* нажмите кнопку *Далее*.
4. В текстовое поле окна *Имя делегируемого домена* введите значение *sub* и нажмите кнопку *Далее*.
5. На странице *Серверы имен* нажмите кнопку *Добавить…*
6. В текстовое поле *Полное доменное имя сервера (FQDN):* введите значение *server2.sub.contoso.com*. В поле *IP-адрес* укажите значение *192.168.0.2* и нажмите кнопку *Ok*.
7. На странице *Серверы имен* нажмите кнопку *Далее*.
8. На странице *Завершение мастера делегирования* нажмите кнопку *Готово*.
9. Сколько записей ресурсов типа A хранится в зоне sub.contoso.com на Server1?

Упражнение 4. Проверка созданной конфигурации

1. Из командной строки выполните команды

   ping server2.sub.contoso.com и

   ping server1.sub.contoso.com.

   Вы должны получить эхо-ответы. Если этого не происходит, то перезапустите службы *DNS-сервер* и *DNS-клиент* из консоли *Службы* (*Пуск→ Панель*

управления→ Администрирование→ Службы) и повторите попытку.

2. Объясните, почему команды выполняются успешно, несмотря на то, что в базе DNS на Server1 нет данных о запрашиваемых FQDN узлов?

Упражнение 5. Сравнение трафика разрешения имен

1. Еще раз перезапустите службы *DNS-сервер* и *DNS-клиент*. Повторите упражнение 1 из лабораторной работы №9. При выполнении команд *ping* используйте команды из предыдущего упражнения.
2. Изучите DNS-пакеты с помощью *Сетевого монитора*. Вспомните механизм разрешения DNS-запросов. Сравните его с ARP-request и запросом NBT.

Упражнение 6. Создание зоны-заглушки

1. Из командной строки выполните команду

dnscmd server2 /recordadd sub.contoso.com @ ns server1.contoso.com

NB! Указанная выше команда делает Server1 полномочным сервером имен для зоны sub.contoso.com на Server2. Если она не выполняется, удостоверьтесь в том, что для указанной зоны включены динамические обновления. Помните, что если DNS-сервер установлен на Server2 с помощью *Мастера компонентов Windows*, то передачи зоны sub.contoso.com разрешены по умолчанию, но ограничены полномочными серверами имен. Если же установить DNS-сервер путем добавления соответствующей роли в окне *Управление данным сервером*, зонные передачи во всех локальных зонах по умолчанию запрещены. В этом случае до начала упражнения надо включить передачи зон на полномочные сервера.

2. Запустите консоль *DNS*. В дереве консоли выделите правой кнопкой мыши узел *Зоны прямого просмотра* и в выпадающем меню выберите пункт *Создать новую зону…*
3. В окне *Мастер создания новой зоны* нажмите кнопку *Далее.*
4. В окне *Тип зоны* выберите параметр *Зона-заглушка*. Снимите флажок напротив параметра *Хранить зону в Active Directory (только если DNS-сервер на контроллере домена)*. Нажмите кнопку *Далее*.
5. На странице Имя зоны в текстовое поле введите значение *sub.contoso.com*. Нажмите кнопку *Далее*.
6. На странице *Файл зоны* выберите параметр *Создать новый файл*. Нажмите кнопку *Далее.*
7. На странице *Основные DNS-серверы* укажите IP-адрес *192.168.0.2* и нажмите кнопку *Добавить*. Нажмите кнопку *Далее*.
8. На странице *Завершение мастера создания новой зоны* нажмите кнопку *Готово*.
9. В дереве консоли *DNS* выделите вновь созданную зону *sub.contoso.com* правой кнопкой мыши и в выпадающем меню выберите параметр *Передать зону с основного сервера*.
10. Убедитесь, что в рабочей области зоны отображаются только три записи ресурсов начальная запись зоны (SOA) и два сервера имен (NS).
11. Закройте все окна и завершите работу Server1 и Server2.

Лабораторная работа №12
Устранение неполадок DNS с помощью встроенных инструментов

Во время этой лабораторной работы вы воспользуетесь утилитой *nslookup* и настроите журнал DNS.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8 и №9.

Упражнение 1. Использование отдельных команд nslookup

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор*.
2. Из командной строки выполните команду
   netsh interface ip set dns MyISP static 192.168.0.1
   После выполнения указанной команды локальный DNS-сервер будет опрашиваться прежде удаленного.
3. Из командной строки выполните команду *nslookup www.ya.ru*. В результате вы должны увидеть примерно такой текст:
   Server: server1.contoso.com
   Address: 192.168.0.1
   Non-authoritative answer:
   Name: ya.ru
   Addresses: 213.180.183.3, 93.158.134.3, 213.180.204.3
   Aliases: www.ya.ru
4. Из командной строки выполните команду *nslookup 93.158.134.3*.

5. На экране вы должны увидеть примерно такой текст:
   Server: server1.contoso.com
   Address: 192.168.0.1
   Name: www.yandex.ru
   Address: 93.158.134.3

Упражнение 2. Nslookup в интерактивном режиме

1. Из командной строки выполните команду
dnscmd /zoneresetsecondaries contoso.com /nonsecure
   С помощью этой команды вы разрешаете зонную передачу на любой сервер для того, чтобы просматривать все содержимое зоны contoso.com.
2. Из командной строки выполните команду *nslookup*. На экране должно появиться приглашение >, свидетельствующее, что утилита работает в интерактивном режиме.
3. В командной строке nslookup выполните команду *set all*. В результате отобразится список всех параметров nslookup. Обратите внимание, что первый параметр – *nodebug*. В этом случае nslookup выводит информацию в сокращенном режиме.
4. В командной строке nslookup введите адрес *www.msnbc.com.* (точка после имени обязательна). Изучите результат. При появлении сообщения об истечении времени запроса повторите попытку.
5. В командной строке nslookup выполните команду *set d2*. Утилита перейдет в режим подробной отладки.
6. В командной строке nslookup выполните команду *set all.* Изучите результат. Укажите два отличи от результата, полученного на шаге 3 этого упражнения.

7. Повторите шаг 4. Вы получите детализированный ответ, состоящий из трех разделов SendRequest, Got answer, Non-authoritative answer. Что содержится в первых двух разделах? Почему они появились в результате выполнения команды? Почему раздел answer считается неполномочным?
8. В командной строке nslookup выполните команду *set nod2*. Повторите шаг 4. Сравните результаты с полученными на шаге 7 этого упражнения. В чем разница между режимами *d2* и *debug*?
9. В командной строке nslookup выполните команду *set nodebug.*
10. В командной строке nslookup выполните команду *ls contoso.com.* На экран будут выведены все записи ресурсов A и NS в зоне. Полная информация не отображается, так как на предыдущем шаге nslookup вышел из режима отладки.
11. В командной строке nslookup выполните команду *set q=srv.* В дальнейшем будут выводиться только записи ресурсов SRV.
12. В командной строке nslookup выполните команду *ls –t contoso.com.* Изучите результат.
13. В командной строке nslookup выполните команду *_ldap._tcp*. Изучите информацию о локаторе протокола LDAP в системе.
14. В командной строке nslookup выполните команду *exit.*
15. Из командной строки выполните команду

dnscmd /zoneresetsecondaries contoso.com /securens

для восстановления настроек зонной передачи (только на серверы имен).

16. Закройте окно командной строки.

NB! Шаги 11 и 12 в предыдущем упражнении можно объединить, выполнив одну команду *ls –t srv contoso.com*.

Упражнение 3. Отладка с применением журнала DNS

1. В дереве консоли *DNS* выделите узел *SERVER1* правой кнопкой мыши и в выпадающем меню выберите пункт *Свойства*.
2. В окне *SERVER1 – свойства* перейдите на вкладку *Ведение журнала отладки* и установите галочку напротив параметра *Записывать пакеты в журнал для отладки*.
3. Изучите, какие пакеты регистрируются по умолчанию и нажмите кнопку *Ok*.
4. Из командной строки выполните команду *nslookup www.rambler.ru*.
5. Остановите службу *DNS-сервер* (шаг 1 упражнения 4 лабораторной работы №11).
6. С помощью *WordPad* откройте файл *c:\windows\system32\dns\dns.log* и найдите в нем последовательность сообщений сгенерированных вопросов и ответов при разрешении имени www.rambler.ru.
7. Почему первое из найденных сообщений считается входящим (Rev – Receive) и осуществлено по протоколу UDP?
8. Запустите службу DNS-сервер. Отмените ведение журнала отладки DNS на Server1.
9. Закройте все открытые окна и завершите работу Server1.

Лабораторная работа №13
Установка и настройка DHCP-сервера

В настоящей лабораторной работе вы установите и настроите новый DHCP-сервер.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8 и №9.

Упражнение 1. Добавление роли DHCP-сервера

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор*.
2. Откройте окно *Управление данным сервером* (*Пуск→ Управление данным сервером*).
3. Перейдите по ссылке *Добавить или удалить роль*. Запустится *Мастер настройки сервера*.
4. В окне *Предварительные шаги* нажмите кнопку *Далее*.
5. В окне роль сервера выделите параметр *DHCP-сервер* и нажмите кнопку *Далее.*
6. В окне *Сводка выбранных параметров* нажмите кнопку *Далее.* При необходимости укажите расположение установочных файлов. Дождитесь запуска *Мастера создания области* и в первом открывшемся окне нажмите кнопку *Далее.*
7. В окне *Имя области* в текстовое поле *Имя* введите значение *TestScope* и нажмите кнопку *Далее*.
8. В окне *Диапазон адресов* укажите значения *192.168.0.11* и *192.168.0.254* в качестве начального и конечного значения диапазона соответственно. Проследите, чтобы длина маски подсети была равна 24.

9. В окне *Добавление исключений* в поле *Начальный адрес* введите значение *192.168.0.100* и нажмите кнопку *Добавить*. Затем в поле *Начальный адрес* введите значение *192.168.0.200*, а в поле *Конечный адрес* – значение *192.168.0.205* и нажмите кнопку *Добавить*. Нажмите кнопку *Далее*.
10. На странице *Срок действия аренды* примите значение по умолчанию и нажмите кнопку *Далее*.
11. На странице *Настройка параметров DHCP* выделите параметр *Да, настроить эти параметры сейча*с и нажмите кнопку *Далее*.
12. На странице *Маршрутизатор (основной шлюз)* в поле *IP-адрес* укажите значение *192.168.0.1*, нажмите кнопку *Добавить*, а затем – кнопку *Далее.*
13. На странице *Имя домена и DNS-серверы* в текстовое поле *Родительский домен* укажите значение *contoso.com*. В поле *Имя сервера* укажите значение *server1.contoso.com*, нажмите кнопку *Сопоставить*, затем – кнопку *Добавить*, затем – кнопку *Далее.*
14. На странице *WINS-серверы* ничего не вводите и нажмите кнопку *Далее.*
15. На странице *Активация области* выберите параметр *Да, я хочу активировать эту область сейчас* и нажмите кнопку *Далее*.
16. На странице *Завершение мастера создания области* нажмите кнопку *Готово*.
17. Прочитайте сообщение о добавлении роли DHCP-сервера и нажмите кнопку *Готово*.
18. В окне *Управление данным сервером* перейдите по ссылке *Управление этим DHCP-сервером*. Откроется консоль *DHCP*.

19. В дереве консоли выделите правой кнопкой узел *server1.contoso.com* и в выпадающем меню выберите пункт *Авторизовать*.
20. Закройте консоль *DHCP*.

NB! Клиенты доменных сетей принимают настройки только от авторизованных в домене DHCP-серверов. В консоли DHCP авторизованные сервера помечаются зеленой стрелкой, направленной вверх, неавторизованные сервера – красной стрелкой, направленной вниз. При авторизации первого сервера в домене все неавторизованные сервера автоматически прекращают вещание. Если в сетевом сегменте физически существует трафик других DHCP-серверов (не членов вашего домена), вполне возможно, что сетевые узлы домена будут получать настройки от них. В этом случае необходимо исключать наличие такого трафика в сети.

Упражнение 2. Настройка DHCP-клиента

1. Запустите виртуальную машину Server2 и войдите в домен как *Администратор*.
2. Из командной строки выполните команду *ipconfig /all*. Изучите результат. Убедитесь, что установленный в прошлом упражнение DHCP-сервер действительно назначил параметры сетевому подключению. Какой адрес из диапазона назначен Server2?

NB! Иногда клиенты не сразу получают сетевые настройки от DHCP-сервера. Чаще всего это связано с использованием в сегменте технологии ICS. В таком случае необходимо назначить клиентам сначала

произвольные статические адреса, например, командами

netsh interface ip set address "Подключение по локальной сети" static 192.168.0.2 255.255.255.0

netsh interface ip set dns "Подключение по локальной сети" static 192.168.0.1.

Затем перезагрузить компьютер, и только после этого настроить сетевой интерфейс на автоматическое получение параметров настройки.

3. Перейдите к Server1 и запустите консоль *DNS*.
4. Разверните все зоны прямого и обратного просмотра, найдите записи, связанные с Server2 и убедитесь, что в базе данных внесены новые корректные данные об адресах. Если все верно – перейдите к шагу 8. Если есть неверные данные – перейдите к шагу 5. (не обращайте внимания на записи ресурсов A в зоне sub.contoso.com).
5. Удалите все записи о Server2 из консоли *DNS*.
6. Перейдите к Server2 и из командной строки исполните команду *ipconfig /registerdns*.
7. Повторите шаги 3 и 4.

Упражнение 3. Сохранение базы данных DHCP

1. На Server1 запустите консоль *DHCP*.
2. В дереве консоли выделите правой кнопкой мыши узел *server1.contoso.com* и в выпадающем меню выберите пункт *Архивировать*.
3. В окне *Обзор папок* обратите внимание на место хранения архивов DHCP по умолчанию и нажмите кнопку *Ok*.
4. В проводнике найдите папку *c:\windows\system32\dhcp\backup*, а вней – файл

DhcpCfg. Это и есть архивная копия базы данных DHCP.

5. Изучите данные о времени изменения этого файла. Если время изменения отличается от текущего на несколько минут или секунд – архивирование произошло успешно.
6. Закройте все открытые окна.

Упражнение 4. Создание суперобласти и ее дочерних областей

1. На Server1 запустите консоль *DHCP*.
2. В дереве консоли выделите правой кнопкой мыши узел *server1.contoso.com* и в выпадающем меню выберите пункт *Создать супероблась*.
3. В окне *Мастер создания суперобласти* нажмите кнопку *Далее.*
4. В окне *Имя суперобласти* в текстовое поле *Имя* введите значение *Super1*. Нажмите кнопку *Далее.*
5. В окне *Выберите области* выделите одну имеющуюся в списке область левой кнопкой мыши. Нажмите кнопку *Далее.*
6. В окне *Завершение работы мастера создания суперобласти* нажмите кнопку *Готово*.
7. В дереве коусоли *DHCP* выделите узел *Суперобласть Super1* правой кнопкой мыши и в выпадающем меню выберите пункт *Создать область*.
8. Для работы мастера создания области используйте параметры из таблицы, приведенной ниже. Для всех остальных параметров используйте значения по умолчанию.

Имя	TestScope2
Начальный IP-адрес	192.168.1.11
Конечный IP-адрес	192.168.1.254
Маска подсети	255.255.255.0
Длина	24

9. Изучите полученную конфигурацию. Для связи имеющихся областей нужен маршрутизатор. Пока его у нас нет. Поэтому вновь созданную область и суперобласть нужно удалить.

NB! Сначала удаляют суперобласть, а потом – входящие в нее области.

10. В дереве консоли выделите правой кнопкой мыши узел *Суперобласть Super1* и в выпадающем меню выберите пункт *Удалить*. В открывшемся окне подтвердите удаление.
11. Повторите шаг 10 для узла *Область TestScope2*.
12. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №14
Анализ DHCP-сообщений

В этой лабораторной работе вы проанализируете трафик как первичной, так и обновленной DHCP-аренды.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8, №9 и №13.

Упражнение 1. Запись трафика первичной аренды

1. Запустите виртуальные машины Server1 и Server2 и войдите в обе системы как *Администратор*.
2. На Server1 запустите утилиту *Сетевой монитор* и включите запись трафика.
3. Перейдите к Server2 и в командной строке исполните команд *ipconfig /release*.
4. После появления сообщения о том, что Server2 имеет адрес 0.0.0.0 и не подключен к сети в командной строке выполните команду *ipconfig /renew*.
5. После получения Server2 нового адреса перейдите к Server1 и в окне *Сетевого монитора* нажмите на кнопку *Остановить запись и отобразить данные*.
6. В меню *Отображение* выберите пункт *Фильтр*.
7. В окне *Фильтр отображения* дважды щелкните левой кнопкой мыши по строке *Protocol == Any*.
8. В окне *Выражение* перейдите на вкладку *Протокол* и нажмите на кнопку *Отключить все*.
9. В списке *Отключенные протоколы* найдите и выделите левой кнопкой мыши протокол *DHCP* и нажмите кнопку *Включить*. Затем нажмите кнопку *Ok*.
10. В окне *Фильтр отображения* нажмите кнопку *Ok*.
11. Сохраните запись в файле *DHCPLeaseInitialization.cap*. Не забудьте при сохранении установить флажок напротив параметра *Фильтр* в диалоге сохранения.

Упражнение 2. Анализ записи первичной аренды

1. Откройте созданный в пердыдущем упражнении файл *DHCPLeaseInitialization.cap*.
2. Ответьте на следующие вопросы. Как называются пять DHCP-сообщений? Какое сообщение и почему не является широковещательным? Из каких сообщений состоит получение первичной

аренды? Изучите узел DHCP Option Field в сообщениях. Какие два сообщения включают параметры Domain Name, Router и Domain Name Server? Какое единственное сообщение содержит параметр Dynamics DNS Updates? Какой UDP-порт указывается как порт источника при отправке информации от DHCP-сервера и как порт назначения при получении информации DHCP-сервером?

3. Выделите в одном из сообщений раздел Dynamics DNS Updates. Какая информация содержится в этом разделе? Какую запись ресурса обновит в DNS DHCP-сервер на основе этой информации?

Упражнение 3. Запись трафика обновления аренды DHCP

1. В окне *Сетевого монитора* включите запись трафика.
2. Перейдите к Server2 и в командной строке исполните команд *ipconfig /renew.*
3. После получения Server2 нового адреса перейдите к Server1 и в окне *Сетевого монитора* нажмите на кнопку *Остановить запись и отобразить данные*.
4. Отфильтруйте и сохраните данные как в упражнении 1 настоящей лабораторной работы. В качестве имени файла укажите значение *DHCPLeaseRenewal.cap.*

Упражнение 4. Анализ записей обновления аренды

1. Откройте созданный в предыдущем упражнении файл *DHCPLeaseRenewal.cap.*
2. Ответьте на следующие вопросы. Из скольких сообщений состоит процесс обновления аренды? Как называются записанные DHCP-сообщения?

Чем отличается набор этих сообщений от набора сообщений при первичной аренде адреса?

3. В обоих записанных кадрах найдите поля *Client IP Address* и *Your IP Address* и ответьте на следующие вопросы. При обновлении аренды запрашивает ли DHCP-клиент обновление конкретного IP-адреса? Какое конкретно поле какого DHCP-сообщения обновляет параметры конфигурации клиента?
4. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №14
Настройка маршрутизации

В рамках данной лабораторной работы вы настроите маршрутизацию в локальном сетевом сегменте.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8, №9 и №13.

Упражнение 1. Настройка службы *Маршрутизация и удаленный доступ*

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор*.
2. Запустите консоль *Маршрутизация и удаленный доступ* (*Пуск→ Администрирование→ Маршрутизация и удаленный доступ*).
3. В дереве консоли выделите правой кнопкой мыши узел *SERVER1 (локально)* и в выпадающем меню выберите пункт *Настроить и включить маршрутизацию и удаленный доступ*.

4. В окне *Мастер настройки сервера маршрутизации и удаленного доступа* нажмите кнопку *Далее.*
5. В окне *Конфигурация* выберите параметр *Особая конфигурация* и нажмите кнопку *Далее.*
6. На странице *Особая конфигурация* ознакомьтесь со списком возможных вариантов настройки. Сколько базовых функций маршрутизации позволяет сконфигурировать мастер? Установить галочку напротив параметра *Маршрутизация ЛВС* и нажмите кнопку *Далее.*
7. На странице завершение мастера маршрутизации и удаленного доступа нажмите кнопку *Готово.* Согласитесь с запуском службы и дождитесь ее запуска.
8. В дереве консоли разверните узел *IP-маршрутизация*. Правой кнопкой мыши выделите узел *Статические маршруты* и в выпадающем меню выберите параметр *Отобразить таблицу IP-маршрутизации…*
9. Изучите таблицу маршрутизации. В каком случае для работоспособности сети на сервере маршрутизации достаточно лишь предпринять действия, ранее проделанные вами в этом упражнении?
10. Запустите виртуальную машину Server2 и войдите в домен как *Администратор.*
11. В командной строке Server2 выполните команду *tracert www.ya.ru*. Объясните результат. Учитывайте адрес искомого узла и фактическую сетевую топологию. При необходимости проверьте командами *ping* доступность всех интерфейсов и шлюзов.

12. Повторите шаг 11 на Server1. Объясните результат.

NB! Недоступность внешних узлов с Server2 объясняется специфической реализацией сетевого моста в VirtualBox. Если бы подключение *MyISP* существовало на реальном сетевом адаптере, внешние узлы были бы доступны. Желающие убедиться в работоспособности сервера маршрутизации могут использовать третью виртуальную машину, настроив на ней и на Server1 дополнительное подключение по внутренней сети в адресном пространстве, отличающемся от используемого ранее. Затем можно проверить доступность по сети, например, третьей машины и Server2 при выключенной и включенной службе маршрутизации на Server1.

Упражнение 2. Включение NAT

1. В консоли *Маршрутизация и удаленный доступ* на Server1 выделите правой кнопкой мыши узел *SERVER1 (локально)* и в выпадающем меню выберите пункт *Отключить маршрутизацию и удаленный доступ*. Согласитесь с предупреждением.
2. Повторите шаги 3 и 4 предыдущего упражнения.
3. В окне *Конфигурация* выберите параметр *NAT и основной брандмауэр* и нажмите кнопку *Далее*.
4. На странице завершение мастера маршрутизации и удаленного доступа нажмите кнопку *Готово*. Согласитесь с запуском службы и дождитесь ее запуска.
5. В дереве консоли разверните узел *IP-маршрутизация*. Правой кнопкой мыши выделите узел *Статические маршруты* и в

выпадающем меню выберите параметр *Отобразить таблицу IP-маршрутизации…* Изучите таблицу.

6. Выделите правой кнопкой мыши узел *NAT/Простой брандмауэр* и в выпадающем меню выберите пункт *Новый интерфейс…*
7. В списке интерфейсов выберите пункт *MyISP* и нажмите кнопку *Ok.*
8. В открывшемся окне выберите параметр *Общий интерфейс подключен к Интернету*. Установите галочку напротив параметра *Включить NAT на данном интерфейсе* и нажмите кнопку *Ok.*
9. Выделите правой кнопкой мыши узел *NAT/Простой брандмауэр* и в выпадающем меню выберите пункт *Новый интерфейс…*
10. В списке интерфейсов выберите пункт *Подключение по локальной сети* и нажмите кнопку *Ok.*
11. В открывшемся окне выберите параметр *Частный интерфейс подключен к частной сети* и нажмите кнопку *Ok.*
12. Выполните шаг 11 из предыдущего упражнения. Объясните результат.

Упражнение 3. Просмотр и настройка параметров NAT

1. В консоли *Маршрутизация и удаленный доступ* на Server1 последовательно разверните узлы *SERVER1 (локально)* и *IP-маршрутизация.*
2. Правой кнопкой мыши выделите узел *Статические маршруты* и в выпадающем меню выберите пункт *Отобразить таблицу IP-маршрутизации...*
3. Найдите в таблице маршрут по умолчанию. Его надо создавать вручную, если конфигурировать NAT не в режиме Мастера.

4. Перейдите к Server2.
5. В командной строке выполните команду *ipconfig /all*. Запомните адрес, назначенный сетевому подключению на Server2.
6. Запустите *Internet Explorer* и зайдите на сайт www.ya.ru.
7. Вернитесь к Server1.
8. В дереве консоли *Маршрутизация и удаленный доступ* разверните узел *NAT/простой брандмауэр*.
9. В рабочей области консоли выделите правой кнопкой мыши подключение *MyISP* и в выпадающем меню выберите пункт *Отображение сопоставлений…*
10. В открывшемся окне найдите записи с частным адресом Server2 и с портом Web-трафика (80). Изучите общий адрес этого сопоставления. Какому физическому интерфейсу принадлежит этот адрес?
11. Закройте окно сопоставлений.
12. В рабочей области консоли выделите правой кнопкой мыши подключение *MyISP* и в выпадающем меню выберите пункт *Свойства.*
13. Изучите информацию на всех вкладках открывшегося окна. Ответьте на следующие вопросы. Должен ли пул адресов, назначаемый внешнему интерфейсу, составлять непрерывное адресное пространство? Какую маску подсети надо назначить пулу 207.46.200.0 – 207.46.207.255? Какое максимальное число адресов возможно в пуле с маской 255.255.255.248? В каких ситуациях используется резервирование? Что такое *настройка специальных портов*? Блокирует ли маршрутизатор по умолчанию ping-запросы

внешнего интерфейса внешними клиентами? Внутренними клиентами?

14. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №15
Развертывание системы удаленного доступа по VPN

В этой лабораторной работе вы создадите необходимые элементы для использования VPN. В нашем случае результат будет лишь эмуляцией возможности соединения корпоративных сетевых сегментов через внешние сети. Предположим, что Server1 – граничная точка первого сегмента, Server2 – второго. Отличие от реальной ситуации лишь в том, что вместо внешних адресов Интернета на граничных точках будем использовать локальные адреса.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8, №9 и №13.

Упражнение 1. Изменение настроек системы

1. Запустите *VirtualBox Менеджер*.
2. В списке виртуальных машин выделите Server2 и нажмите кнопку *Свойства*.
3. В рабочей области окна свойств Server2 выберите пункт *Сеть* и перейдите на вкладку *Адаптер 2*.
4. Установите галочку напротив параметра *Включить сетевой адаптер*.
5. В выпадающем списке *Тип подключения* выберите *Сетевой мост*. Нажмите кнопку *Ok*.

6. Запустите виртуальные машины Server1 и Server2 и войдите в домен с Server2 как *Администратор.*
7. В командной строке выполните команду *ipconfig /all.* Изучите адреса, назначенные подключениям. Одному подключению адрес назначает DHCP-сервер нашего домена, другому – служба Сетевой мост VirtualBox.
8. Перейдите к Server1.
9. Повторите на Server1 шаг 7 этого упражнения.
10. Подключению *MyISP* скорее всего назначен адрес из той же подсети, что и *Подключению по локальной сети 2* на Server2.
11. С помощью команды *ping* с Server1 проверьте доступность *Подключения по локальной сети 2* Server2. Не перепутайте адреса. Объясните результат.
12. Выполните команду *ping server2.contoso.com.* Объясните результат.
13. Является ли с точки зрения маршрутизации реализация сетевого моста в VirtualBox прямым аналогом подключения к Интернету по выделенной линии?

Упражнение 2. Изменение режима работы домена и создание учетных записей группы и пользователя для удаленного подключения

1. На Server1 запустите консоль *Active Directory – пользователи и компьютеры* из группы *Администрирование Панели управления*.
2. В дереве консоли выделите правой кнопкой мыши контейнер *Users* и в выпадающем меню выберите пункт *Создать→ Пользователь*.
3. В открывшемся окне *Новый объект – пользователь* в текстовые поля *Имя* и *Имя входа*

пользователя введите значение *user1*. Нажмите кнопку *Далее.*

4. В следующем окне укажите пароль и подтверждение пароля (P@ssw0rd). Снимите галочку напротив параметра *Требовать смену пароля при следующем входе в систему* и установите галочки напротив параметров *Запретить смену пароля пользователем* и *Срок действия пароля не истекает*. Нажмите кнопку *Далее*. Затем нажмите кнопку *Готово*.
5. Из командной строки исполните две команды
   net group vpn_users /add /domain, и
   net group vpn_users user1 /add /domain.
6. В консоли *Active Directory – пользователи и компьютеры* найдите вновь созданную глобальную группу безопасности vpn_users и убедитесь, что учетная запись пользователя user1 теперь является членом этой группы.
7. В рабочей области консоли выделите правой кнопкой мыши учетную запись user1 и в выпадающем меню выберите пункт *Свойства*.
8. В открывшемся окне перейдите на вкладку *Входящие звонки*. Заметьте, что в группе *Разрешение на удаленный доступ (VPN или модем)* удаленный доступ по умолчанию запрещен, а параметр *Управление на основе политики удаленного доступа* недоступен. Нажмите кнопку *Ok*.
9. В дереве консоли выделите правой кнопкой мыши узел *contoso.com* и в выпадающем меню выберите параметр *Изменение режима работы домена…*
10. В открывшемся окне в качестве режима работы домена выберите параметр *Windows Server 2003* и нажмите кнопку *Изменить*.

11. Согласитесь с невозможностью отмены изменений. Дважды последовательно нажмите кнопку *Ok*.
12. Перезагрузите Server1 и после перезагрузки войдите в домен как *Администратор*.
13. Запустите консоль *Active Directory – пользователи и компьютеры*.
14. Откройте свойства учетной записи user1 и убедитесь, что на вкладке Входящие звонки в группе *Разрешение на удаленный доступ (VPN или модем)* параметр *Управление на основе политики удаленного доступа* теперь доступен и выбран по умолчанию.
15. Закройте все открытые окна и завершите работу Server1.

Упражнение 3. Создание сервера удаленного доступа по VPN

1. На Server1 запустите консоль *Маршрутизация и удаленный доступ* из группы *Администрирование Панели управления*.
2. В дереве консоли выделите правой кнопкой мыши узел *SERVER1 (локально)* и в выпадающем меню выберите параметр *Отключить маршрутизацию и удаленный доступ*.
3. Повторите шаг 2, но сейчас в выпадающем меню выберите параметр *Настроить и включить маршрутизацию и удаленный доступ*.
4. В открывшемся окне *Мастер установки сервера маршрутизации и удаленного доступа* нажмите кнопку *Далее.*
5. В окне *Конфигурация* выберите параметр *Удаленный доступ (VPN или модем)* и нажмите кнопку *Далее.*

6. На странице *Удаленный доступ* поставьте галочку напротив параметра *Доступ к виртуальной частной сети (VPN)* и нажмите кнопку *Далее.*
7. На странице *Соединение по VPN* в качестве интерфейса подключенного к Интернету укажите *MyISP* и нажмите кнопку *Далее.*

NB! Обратите внимание, что в реальной ситуации в качестве внешних интерфейсов надо указывать прямые подключений к провайдеру.

8. На странице *Назначение IP-адресов* выберите параметр *Из заданного диапазона адресов* и нажмите кнопку *Далее.*

NB! В нашей системе уже есть DHCP-сервер, но мы упростим себе задачу настройки VPN – не будем настраивать ретранслятор DHCP, а возложим назначение адресов удаленным клиентам на саму службу маршрутизации. Помните, что в реальной ситуации консоль *Маршрутизация и удаленный доступ* вполне может использоваться для настройки DHCP Relay Agent.

9. В коне *Назначение диапазона адресов* нажмите кнопку *Создать…* В окне *Новый диапазон адресов* в укажите значения *192.168.0.200* и *192.168.0.205* в качестве начального и конечного значений диапазона соответственно. Нажмите кнопку *Ok.* Нажмите кнопку *Далее*.
10. В окне *Управление несколькими серверами удаленного доступа* откажитесь от использования RADIUS-сервера. Нажмите кнопку *Далее*.

11. В окне *Завершение мастера сервера маршрутизации и удаленного доступа* нажмите кнопку *Готово*.
12. В открывшемся окне *Маршрутизация и удаленный доступ* прочитайте напоминание об автоматических системах адресации и нажмите кнопку *Ok*.

Упражнение 4. Создание политики удаленного доступа

1. На Server1 в дереве консоли *Маршрутизация и удаленный доступ* выделите правой кнопкой мыши узел *Политика удаленного доступа* и в выпадающем меню выберите параметр *Создать политику удаленного доступа*.
2. В окне *Мастер создания политики удаленного доступа* нажмите кнопку *Далее*.
3. В окне *Метод настройки политики* в текстовое поле *Имя политики* укажите значение *VPN_users*. Остальные параметры оставьте со значениями по умолчанию и нажмите кнопку *Далее*.
4. В окне *Способ доступа* выберите параметр *Доступ к виртуальной частной сети (VPN)* и нажмите кнопку *Далее*.
5. В окне *Пользователь или группа доступа* выберите параметр *разрешениях группы, которые могут переопределяться индивидуальными разрешениями пользователя*. Нажмите кнопку *Добавить…*
6. В открывшемся окне *Выбор группы* в текстовое поле *Введите имена выбранных объектов* введите значение *VPN* и нажмите кнопку *Проверить имена*. После появления в текстовое поле значения *vpn_users* последовательно нажмите кнопки *Ok* и *Далее*.

7. В окне *Методы проверки подлинности* поставьте галочку напротив параметра *Шифрованная проверка подлинности Microsoft версии 2 (MS-CHAPv2)* и нажмите кнопку *Далее.*

NB! В реальных сетях разумнее использовать протокол проверки подлинности EAP. В нашем случае для его функционирования нет внешних сертификатов, поэтому мы выбираем идентификацию на основе пароле по протоколу MS-CHAPv2.

8. На странице *Уровень шифрования, указанный в политике* выберите все возможные уровни шифрования и нажмите кнопку *Далее.*
9. В окне *Завершение мастера создания политики удаленного доступа* нажмите кнопку *Готово.*
10. В рабочей области консоли *Маршрутизация и удаленный доступ* выделите правой кнопкой мыши вновь созданную политику *VPN_users* и в выпадающем меню выберите пункт *Свойства.*
11. Обратите внимание, что первое условие политики соответствует всем VPN, а второе – глобальной группе безопасности contoso\vpn_users. Заметьте, что выбран параметр *Предоставить право удаленного доступа*.
12. Нажмите на кнопку *Изменить профиль…* и изучите информацию на всех шести вкладках открывшегося окна.
13. Закройте все открытые окна.

Упражнение 5. Создание VPN-подключение типа PPTP

1. Запустите виртуальную машину Server2 и войдите в домен как *Администратор.*

2. Запустите *Мастер новых подключений* (*Пуск→ Панель управления→ Сетевые подключения→ Мастер новых подключений*).
3. В окне запуска мастера нажмите кнопку *Далее.*
4. В окне *Тип сетевого подключения* выберите параметр *Подключить к сети на рабочем месте* и нажмите кнопку *Далее.*
5. В окне *Сетевое подключение* выберите параметр *Подключение к виртуальной частной сети* и нажмите кнопку *Далее.*
6. В окне *Имя подключения* в текстовое поле укажите значение *MyVPN* и нажмите кнопку *Далее*.
7. В окне *Выбор VPN-сервера* в текстовое поле укажите IP-адрес подключения *MyISP* Server1.
8. В окне *Доступность подключения* выберите параметр *для всех пользователей* и нажмите кнопку *Далее.*
9. В окне завершения работы мастера поставьте галочку напротив параметра *Добавить ярлык подключения на рабочий стол* и нажмите кнопку *Готово*.
10. В открывшемся окне *Подключение: MyVPN* нажмите кнопку *Свойства.*
11. Перейдите на вкладку *Параметры* и установите галочку напротив параметра *Включать домен входа в Windows.*
12. Перейдите на вкладку *Сеть*. Обратите внимание, что в списке *Тип VPN* установлен параметр *Автоматически.* В данном случае сначала выполняется попытка установить подключение на основе сертификатов L2TP/IPSec, но так как они отсутствуют, то устанавливается PPTP-подключение. Нажмите кнопку *Ok.*

13. В окне *Подключение: MyVPN* в текстовое поле *Пользователь* укажите значение *user1*, в поле *Пароль* – значение *P@ssw0rd*, в поле Домен – значение *CONTOSO*. Нажмите кнопку *Подключить*.
14. После того как подключение установится в командной строке выполните команду *ping server1*. Обратите внимание на адрес.
15. Повторите шаги 7 – 12 упражнения 1 данной лабораторной работы.
16. На Server2 запретите *Подключение по локальной сети*.
17. Откройте окно Мой компьютер и в поле *Адрес* введите значение \\server1. Вы должны получить доступ к общим ресурсам Server1.

NB! Если вам удалось получить доступ к общим ресурсам Server1 на предыдущем шаге, значит работают и VPN-сервер и политика удаленного доступа и подключение.

18. Выполните команду ping 192.168.0.1. Объясните результат.
19. Выйдите из системы Server2.
20. В окне *Вход в систему* на Server2 введите пароль Администратора в соответствующее поле, поставьте галочку напротив параметра *С использованием удаленного доступа* и нажмите кнопку *Ok*.
21. В открывшемся окне нажмите кнопку *Подключить*. Для подключения используйте реквизиты учетной записи user1.

NB! Обратите внимание, что входить в систему и использовать подключение удаленного доступа можно от имени разных учетных записей.

22. Перейдите к Server1 и откройте консоль *Маршрутизация и удаленный доступ*.
23. В дереве консоли разверните узел *Порты*. Убедитесь, что в рабочей области активен только один минипорт WAN, подключенный по PPTP.
24. Перейдите к Server2 и выйдите из системы.

Упражнение 6. Создание VPN-подключение типа L2TP/IPSec

1. Войдите в домен с Server2 как *Администратор*.
2. Откройте окно *Сетевые подключение* в *Панели управления*.
3. Правой кнопкой мыши выделите подключение *MyVPN* и в выпадающем меню выдерите пункт *Свойства*.
4. В открывшемся окне перейдите на вкладку *Безопасность* и нажмите кнопку *Параметры IPSec…*
5. В окне *Параметры IPSec* установите флажок напротив параметра *Для проверки подлинности использовать предварительный ключ* и в текстовое поле *Ключ* введите значение *test*. Нажмите кнопку *Ok*.

NB! Предварительные ключи никак не защищены, они передаются по сети в виде текста. Нам они подходят для иллюстрации использования IPSec. В реальных ситуациях для IPSec нужно использовать сертификаты.

6. Перейдите на вкладку *Сеть* и в поле *Тип VPN* выберите параметр *L2TP IPSec VPN*. Нажмите кнопку *Ok*.
7. Перейдите к Server1.
8. В дереве консоли *Маршрутизация и удаленный доступ* правой кнопкой мыши выделите узел *SERVER1 (локально)* и в выпадающем меню выберите пункт *Свойства*.
9. В открывшемся окне перейдите на вкладку *Безопасность*.
10. Установите галочку напротив параметра *Разрешать пользовательские IPSEC-политики для L2TP-подключения*. В текстовое поле *Предварительный ключ* введите значение *test* и нажмите кнопку *Ok*.
11. Повторите шаги 20 – 23 из предыдущего упражнения. Изучите результаты.
12. Разрешите *Подключение по локальной сети* на Server2.
13. Закройте все открытые окна и выйдите из систем Server2 и Server1.

Лабораторная работа №16
Развертывание RADIUS-сервера

В рамках данной работы вы настроите IAS для поддержки аутентификации и авторизации удаленного доступа по запросам, поступающим в службу *Маршрутизация и удаленный доступ*.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, №8, №9, №13 и №15.

Упражнение 1. Настройка RADIUS-сервера

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор*.
2. С помощью компонента *Установка и удаление программ* установите компонент Windows *Служба проверки подлинности в Интернете*, находящийся в составе *Сетевых служб* (пример, упражнение 1 лабораторной работы №6).
3. Запустите консоль *Маршрутизация и удаленный доступ*.
4. В дереве консоли выделите правой кнопкой мыши узел *SERVER1 (локально)* и в выпадающем меню выберите пункт *Свойства*.
5. В открывшемся окне перейдите на вкладку *Безопасность* и в списке *Служба проверки подлинности* выберите параметр *RADIUS – проверка подлинности*. Нажмите кнопку *Настроить…*
6. В открывшемся окне *RADIUS – проверка подлинности* нажмите кнопку *Добавить…*
7. В открывшемся окне *Добавление RADIUS-сервера* в текстовое поле *Имя сервера* введите значение *192.168.0.1*. Нажмите кнопку *Изменить...* В открывшемся окне введите и подтвердите пароль для шифрования данных (*P@ssw0rd*). Дважды последовательно нажмите кнопку *Ok* в открытых окнах.

NB! В реальных ситуациях секрет должен представлять собой случайную последовательность из различных символов не менее 22 знаков.

8. На вкладке *Безопасность* перейдите к списку *Служба учета*. Повторите пункты 5 – 7 этого упражнения для настройки сервера учета.
9. Из командной строки выполните команду *net stop RemoteAccess*.
10. После остановки службы из командной строки выполните команду *net start RemoteAccess*.

Упражнение 2. Добавление RADIUS-клиента и проверка конфигурации

1. Запустите Server2 и попробуйте войти в домен в использованием удаленного доступа. После получения отказа вернитесь к Server1.
2. Запустите консоль *Проверка подлинности в Интернете* (*Пуск→ Администрирование→ Проверка подлинности в Интернете*).
3. В дереве консоли выделите правой кнопкой мыши пункт Служба проверки подлинности в Интернете (локально). Обратите внимание, что в выпадающем меню есть пункт зарегистрировать сервер в Active Directory.

NB! RADIUS-серверы, выполняющие аутентификацию для домена, нужно регистрировать в AD. Server1 уже является контроллером домена, поэтому установленный нами RADIUS-сервер автоматически зарегистрирован в домене.

4. В дереве консоли выберите узел *Политика удаленного доступа*. Обратите внимание, что в рабочей области отображаются такие же политики, как в консоли *Маршрутизация и удаленный доступ*.

5. В дереве консоли выделите правой кнопкой мыши узел *RADIUS-клиенты* и в выпадающем меню выберите пункт *Новый RAS-клиент*.
6. В открывшемся окне *Новый клиент RADIUS* в текстовое поле *Понятное имя* введите значение *Local NAS*, в следующее текстовое поле введите значение *192.168.0.1* и нажмите кнопку *Далее*.
7. В окне *Дополнительные сведения* в текстовые поля *Общий секрет* и *Подтверждение* введите значение *P@ssw0rd*. Остальные параметры оставьте по умолчанию и нажмите кнопку *Готово*.
8. Перезапустите службу *Маршрутизация и удаленный доступ* из одноименной консоли.
9. Закройте все открытые окна.
10. Вновь попытайтесь войти в домен с Server2 с использованием удаленного доступа.
11. Убедитесь, что RADIUS-сервер и клиент работают исправно.
12. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №17
Анализ и настройка шаблонов безопасности

В рамках данной работы вы познакомитесь с возможностями консоли Анализ и настройка безопасности, а также создадите шаблоны безопасности.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6.

Упражнение 1. Создание консоли. Шаблоны по умолчанию

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор.*
2. Из командной строки выполните команду *mmc*.
3. В открывшемся окне *Консоль1* в меню *Консоль* выберите пункт *Добавить или удалить оснастку…*
4. В открывшемся окне *Добавить или удалить оснастку* нажмите кнопку *Добавить…*
5. В списке доступных изолированных оснасток выберите пункт *Шаблоны безопасности* и нажмите кнопку *Добавить*. Затем выберите оснастку *Анализ и настройка безопасности* и вновь нажмите кнопку *Добавить*.
6. Последовательно нажмите кнопку *Закрыть* и *Ok*.
7. В окне *Консоль1* в меню *Консоль* выберите пункт *Сохранить как* и сохраните консоль, назвав ее *Управление настройками безопасности*.
8. Создайте на рабочем столе ярлык для вновь созданной консоли.
9. Создайте на папку C:\Custom Templates.
10. В дереве консоли *Управление настройками безопасности* выделите правой кнопкой мыши узел *Шаблоны безопасности* и в выпадающем меню выберите пункт *Новый путь для поиска шаблонов…*
11. В качестве пути укажите путь к папке Custom Templates.

NB! Шаблоны по умолчанию изменять не рекомендуется. Новые шаблоны лучше всего хранить в специальной папке.

Упражнение 2. Создание собственных шаблонов

1. В дереве консоли *Управление настройками безопасности* последовательно разверните узлы *Шаблоны безопасности* и *C:\WINDOWS\security\templates*.
2. В дереве консоли выделите правой кнопкой мыши файл *securews.inf* и в выпадающем меню выберите пункт *Сохранить как…*
3. Сохраните выбранный файл под именем test1 в папке Custom Templates.
4. Перезапустите консоль *Управление настройками безопасности*.
5. В дереве консоли последовательно разверните узлы *Шаблоны безопасности, C:\Custom Templates, test1, Локальные политики, Параметры безопасности*.
6. В рабочей области консоли найдите разделы *Сетевой доступ* и *Сетевая безопасность*. Изучите их значения.
7. В рабочей области консоли найдите раздел *Завершение работы: разрешить завершение работы без выполнения входа в систем*у. Дважды кликните по нему левой кнопкой мыши.
8. В открывшемся окне поставьте галочку напротив параметра *Определить указанный ниже параметр политики в шаблоне*, выберите параметр *Отключить* и нажмите кнопку *Ok*.
9. В рабочей области консоли найдите раздел *Интерактивный вход в систему: количество предыдущих подключений кэшу* и установите значение параметра равным 0.
10. В дереве консоли выделите узел *test1* и в выпадающем меню выберите пункт *Сохранить*.

11. Запустите виртуальную машину Server1 и войдите в домен как *Администратор.*
12. Откройте с помощью *Блокнота* файл *c:\custom templates\test1.inf.* Изучите раздел *Registry Values*. Закройте *Блокнот*.
13. Создайте шаблон отката, выполнив из командной строки команду \

secedit /generaterollback /cfg "c:\custom templates\test1.inf"
/rbk "c:\custom templates\test1rollback.inf"
/log "c:\custom templatestest1rollback.log"

NB! Помните, что откат значений невозможен для параметров безопасности файлов и реестра, т.е. в случае применения «обратного» шаблона любые изменения, внесенные шаблоном в разрешения, не отменяются.

14. В дереве консоли *Управление настройками безопасности* выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Открыть базу данных…*
15. В открывшемся окне в поле *Имя файла* введите значение *test1* и нажмите кнопку *Открыть*.
16. В открывшемся окне *Импорт шаблона* выберите созданный ранее шаблон *test1* и нажмите кнопку *Открыть*.
17. В дереве консоли *Управление настройками безопасности* выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Настроить компьютер*. В окне *Настойка системы* нажмите кнопку *Ok.*
18. Перезагрузите Server1.
19. Убедись, что теперь кнопка *Завершение работы…* в окне входа в систему недоступна. Шаблон применен успешно.

Упражнение 3. Откат после применения шаблона

1. Войдите в домен с Server1 как *Администратор*.
2. Запустите консоль *Управление настройками безопасности.*
3. В дереве консоли выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Открыть базу данных…*
4. В диалоге открытия файлов выберите базу *test1.sdb* и нажмите кнопку *Открыть*.
5. В дереве консоли выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Импорт шаблона…*
6. В диалоге импорта выберите файл *test1rollback.inf, установите флажок напротив параметра Очистить эту базу перед импортом* и нажмите кнопку *Открыть*.
7. В дереве консоли *Управление настройками безопасности* выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Настроить компьютер*. В окне *Настойка системы* нажмите кнопку *Ok.*
8. Перезагрузите Server1.
9. Убедись, что теперь кнопка *Завершение работы…* в окне входа в систему снова доступна. Откат после применения шаблона произведен успешно.

Упражнение 4. Анализ соответствия действующей политике

1. Войдите в домен с Server1 как *Администратор*.
2. Запустите консоль *Управление настройками безопасности.*
3. В дереве консоли выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Импорт шаблона.*

4. В диалоге открытия файлов выберите файл *test1.inf* и нажмите кнопку *Открыть*.
5. В дереве консоли выделите узел *Анализ и настройка безопасности* и в выпадающем меню выберите пункт *Анализ компьютера.*
6. Согласитесь с местоположением файла журнала ошибок.
7. В рабочей области изучите параметры, отличные от текущих (помеченные белым крестом в красном круге) и совпадающие с текущими (помеченные зеленой галочкой).
8. Закройте все открытые окна и завершите работу Server1.

Лабораторная работа №18
Использование протоколов сетевой безопасности

В настоящей работе рассматриваются различные инструменты управления политикой IPSec.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6, и №16.

Упражнение 1. Создание запрещающей политики

1. Запустите виртуальную машину Server1 и войдите в домен как *Администратор.*
2. Запустите консоль *Управление настройками безопасности* и добавьте в нее оснастку *Управление политикой безопасности IP* (аналогично упражнению 1 лабораторной работы №16).
3. В дереве консоли правой кнопкой мыши выделите узел *Политики безопасности IP на «Локальный*

компьютер» и в выпадающем меню выберите пункт *Создать новую политику безопасности IP…*

4. В окне *Мастер политики IP-безопасности* нажмите кнопку *Далее.*
5. В окне *Имя политики безопасности IP* в текстовое поле *Имя* укажите значение *block web server access*. Нажмите кнопку *Далее.*
6. В окне *Запросов безопасного соединения* снимите галочку напротив параметра *Использовать правило по умолчанию*. Нажмите кнопку *Далее.*
7. В окне *Завершение работы мастера* нажмите кнопку *Готово.*
8. В открывшемся окне свойств новой политики снимите галочку напротив параметра *Использовать мастер*. Нажмите кнопку *Добавить…*
9. В окне *Свойства: Новое правило* на вкладке *Список фильтров* нажмите кнопку *Добавить...*
10. В окне *Список фильтров IP* в текстовое поле *Имя* введите значение *blocking*, а в текстовое поле *Описание* – значение *blocking protocols*. Снимите галочку напротив параметра *Использовать мастер*. Нажмите кнопку *Добавить…*
11. В окне *Свойства: IP-фильтр* в списке *Адрес назначения пакетов* выберите параметр *Любой IP-адрес*, а в списке *Адрес источника пакетов* – параметр *Мой IP-адрес*.
12. Перейдите на вкладку *Протокол* и в списке *Выберите тип протокола* выберите параметр *TCP*. В области *Установка порта для протокола IP* выберите параметр *Пакеты на этот порт*. В ставшем доступном текстовое поле введите значение *80* и дважды последовательно нажмите кнопку *Ok.*

13. В окне *Свойства: Новое правило* в области *Списки фильтров IP* выберите фильтр *blocking* и перейдите на вкладку *Действие фильтра*.
14. Снимите галочку напротив параметра *Использовать мастер* и нажмите кнопку *Добавить…*
15. В окне *Свойства: Создание действия фильтра* выберите параметр *Блокировать*.
16. Перейдите на вкладку *Общие*. В текстовое поле *Имя* введите значение *block* и нажмите кнопку *Ok*.
17. В окне *Свойства: Новое правило* в области *Действие фильтра* выберите параметр *block* и нажмите кнопку *Закрыть*. Затем нажмите кнопку *Ok*.

NB! Создание политики само по себе не изменяет свойств системы. Для того, чтобы политика начала работать ее нужно назначить.

Упражнение 2. Создание политики согласования

1. Повторите шаги 2 – 7 предыдущего упражнения, назвав новую политику *encrypt telnet traffic*.
2. В окне свойств вновь созданной политики перейдите на вкладку *Общие* и нажмите кнопку *Параметры…*
3. В окне *Параметры обмена ключами* нажмите на кнопку *Методы…*
4. В списке *Методы безопасности в порядке их предпочтения* удалите третью и четвертую строки.
5. Выберите второй из оставшихся методов и нажмите кнопку *Изменить…*
6. В открывшемся окне в списке *Группа Диффи – Хеллмана* выберите параметр *Высокая (2048)*. Нажмите кнопку *Ok*.

7. Повторите шаги 5 и 6 для оставшегося метода защиты.
8. Необходимое числе раз нажмите кнопку *Ok*. Перейдите к вкладке *Правила* окна *Свойства: encrypt telnet traffic*.
9. Установите галочку напротив параметра *Использовать мастер* и нажмите кнопку *Добавить…*
10. В окне *Мастер создания новых правил IP-безопасности* нажмите кнопку *Далее*.
11. На странице *Конечная точка туннеля* выберите параметр *Это правило не определяет туннель* и нажмите кнопку *Далее*.
12. На странице *Тип сети* выберите параметр *Все сетевые подключения* и нажмите кнопку *Далее*.
13. На странице *Список фильтров IP* нажмите кнопку *Добавить…*
14. В окне *Список фильтров IP* в поле *Имя* введите значение *negotiate*. Установите флажок напротив параметра *Использовать мастер* и нажмите кнопку *Добавить…*
15. В окне *Мастер IP-фильтра* нажмите кнопку *Далее*.
16. В окне *Описание IP-фильтра и свойство «Отраженный»* нажмите кнопку *Далее*.
17. В окне *Источник IP-трафика* в списке *Адрес источника пакетов* выберите параметр *Определенный IP-адрес*. В поле *IP-адрес* введите адрес *Подключения по локальной сети* Server1 (192.168.0.1). Обратите внимание на маску подсети и нажмите кнопку *Далее*.
18. В окне *Назначение IP-трафика* в списке *Адрес назначения* выберите параметр *Определенный IP-адрес*. В поле *IP-адрес* введите адрес *Подключения*

по локальной сети Server2 (скорее всего 192.168.0.11). Нажмите кнопку *Далее*.

19. В окне *Тип протокола IP* в списке *Выберите тип протокола* укажите параметр *TCP* и нажмите кнопку *Далее.*
20. В окне *Порт протокола IP* выберите параметр *Пакеты на этот порт*. В ставшем доступным текстовое поле введите значение *23* и нажмите кнопку *Далее.*
21. В окне *Завершение работы мастера IP-фильтра* нажмите кнопку *Готово*. Затем нажмите кнопку *Ok.*
22. В окне *Список фильтров IP* выберите фильтр *negotiate* и нажмите кнопку *Далее.*
23. В окне *Действие фильтра* в одноименном списке выберите параметр *Требуется безопасность* и нажмите кнопку *Далее.*
24. Нажмите необходимое число раз кнопки *Ok* и *Готово*, чтобы закончить процедуру.
25. Обратите внимание, что в качестве метода проверки подлинности по умолчанию выбран протокол Kerberos.
26. В дереве консоли выделите правой кнопкой мыши узел *Политики безопасности IP на «Локальный компьютер»* и в выпадающем меню выберите пункт *Экспортировать политики* из списка *Все задачи*.
27. Политики экспортируйте в файл *c:\123.ipsec*.
28. Запустите Server2 и войдите в домен как *Администратор.*
29. Скопируйте с Server1 файл *c:\123.ipsec* в корневой каталог Server2 (воспользуйтесь UNC-путем \\server2\c$).
30. Создайте на Server2 консоль с оснасткой *Управление политикой безопасности IP.*

Импортируйте политики из скопированного на предыдущем шаге файла. При успешном импорте в рабочей области консоли должны быть доступны пять политик, в том числе *block web server access* и *encrypt telnet traffic*.

Упражнение 3. Управление IPSec с помощью Netsh

1. На Server1 из командной строки выполните команду *netsh*.
2. Переведите утилиту в статический контекст: *netsh> static*.

NB! Далее все команды выполняйте в командной строке *netsh*. Учтите, в каждом пункте упражнения указана одна команда. Перед созданием правил надо знать список фильтров, сами фильтры и их действия. Если создать фильтр для несуществующего списка, то список фильтров будет создан автоматически.

3. Создайте новую политику:

add policy name="telnet" description="only allow negotiated telnet from server2 to server1" activatedefaultrule=no mmsecmethods="3DES-MD5-3"

В этой политике надо создать два правила. Первое правило блокирует весь telnet-трафик, второе – организует согласование telnet между Server1 и Server2.

4. Создайте фильтр для правила блокировки:

add filter filterlist="blocktelnet" srcaddr=Any dstaddr=Me description="all telnet to server1" protocol=TCP mirrored=yes srcmask=24 dstmask=24 srcport=0 dstport=23

5. Создайте действие фильтра:

add filteraction name="block all telnet" inpass=yes action=block

6. Создайте правило:

add rule name="telnet1" policy="telnet" filterlist="blocktelnet" filteraction="block all telnet" kerberos=yes description="this rule negotiates telnet if the source computer is server2"

7. Создайте список с одним фильтром, который реагирует на telnet, а в качестве IP-адреса источника укажите адрес Server2:

add filter filterlist="telnet server2" srcaddr=192.168.0.11 dstaddr=Me description="server2 telnet to server1" protocol=TCP mirrored=yes srcmask=32 dstmask=32 srcport=0 dstport=23

8. Определите действие фильтра, согласующего telnet между Server1 и Server2:

add filteraction name="negotiate server2 telnet" qmpfs=no inpass=no soft=no action=negotiate qmsecmethods="ESP[3DES,MD5]"

9. Добавьте правило, управляющее согласованием telnet:

add rule name="telnet2" policy="telnet" filterlist="telnet server2" filteraction="negotiate server2 telnet" kerberos=yes description="this rule negotiates telnet if then source computer is server2"

10. Назначьте политику:

set policy name=telnet assign=yes

11. Войдите в домен с Server2 как *Администратор*.
12. Из командной строки выполните команду *telnet server1*. Убедитесь, что подключение пока невозможно.
13. Повторите на Server2 первые три шага этого упражнения.

14. Создайте список фильтров:

add filter filterlist="telnet server1" srcaddr=Me dstaddr=192.168.0.11 description="server2 telnet to server1" protocol=TCP mirrored=yes srcmask=32 dstmask=32 srcport=0 dstport=23

15. Создайте действие фильтра:

add filteraction name="negotiate server2 telnet" qmpfs=no inpass=no soft=no action=negotiate

16. Добавьте правило, управляющее согласованием telnet:

add rule name="telnet1" policy="telnet" filterlist="telnet server1" filteraction="negotiate server2 telnet" kerberos=yes description="this rule negotiates telnet to server1"

17. Назначьте политику (шаг 10).
18. Повторите шаг 12. Убедитесь, что telnet-подключение успешно установлено. Не разрывайте это подключение до конца работы.

Упражнение 4. Применение Netsh для мониторинга IPSec

1. На Server2 в контексте выполните команду

   show policy name=telnet level=verbose

   Изучите результат.
2. Переведите Netsh в динамический режим:

   dynamic
3. Включите диагностику и запись всех событий:

   set config property=ipsecdiagnostics value=7
4. Установите интервал IPSec равным 60 секундам:

   set config property=ipseclogginterval value=60
5. Отобразите информацию об основном режиме сопоставления:

   show mmsas all
6. Отобразите информацию о быстром режиме сопоставления:

   show qmsas all
7. Закройте окно командной строки.

Упражнение 5. Применение Монитора IP-безопасности для мониторинга IPSec-подключений

1. На Server1 создайте консоль с оснасткой *Монитор IP-безопасности* (см. упражнение 1 лабораторной работы №16).
2. Развернув соответствующий узел убедитесь, что в качестве активной политики в рабочей области консоли отображается политика *telnet*. Ознакомьтесь с параметрами активной политики.
3. В дереве консоли разверните узел *Сопоставления безопасности*, затем последовательно – узлы *Основной режим* и *Быстрый режим*. Ознакомьтесь с содержимым рабочей области консоли. Сравните результаты с результатами, полученными в предыдущем упражнении.
4. Закройте все открытые окна и завершите работу Server1 и Server2.

Лабораторная работа №19
Измерение производительности и настройка служб

В рамках данной работы изучаются дополнительные возможности *Диспетчера задач*, а также консолей *Производительность* и *Службы*.

Для выполнения работы необходимо:

Выполненные в полном объеме лабораторные работы №4 – №6.

Упражнение1. Мониторинг сетевого трафика с помощью *Диспетчера задач*

1. Запустите виртуальные машины Server1 и Server2 и войдите с обеих в домен как *Администратор*.

2. На Server2 создайте папку *c:\temp* и сделайте ее общей для группы *Администраторы домена* с правами полного доступа.
3. Перейдите на Server1 и запустите *Диспетчер задач* (левый_Ctrl+Del→ кнопка *Диспетчер задач*).
4. В окне *Диспетчер задач Windows* перейдите на вкладку *Сеть* и в меню *Вид* выберите пункт *Выбрать столбцы…*
5. В окне *Выбор столбцов* отметьте галочками следующие параметры: *Использование сети, Скорость линии, Состояние, Всего одноадр. Пактов в интервале, Неодноадресных пакетов в интервале*. Нажмите кнопку *Ok.*
6. В командной строке выполните последовательно три команды:

net use T:\\server2\temp
copy "c:\windows\driver cache\i386\driver.cab" T: /y
net use T: /delete

7. На графике будет виден пик, соответствующий использованию сети. Следите за показаниями счетчиков в отображаемых столбцах. Заметьте, что показания счетчика *Всего одноадр. Пакетов в интервале* возросло, а счетчика *Неодноадресных пакетов в интервале* – не изменилось. Это указывает на корректную передачу данных.

Упражнение 2. Создание сетевого оповещения в консоли *Производительность*

1. На Server1 запустите консоль *Производительность* (*Пуск→ Администрирование→ Производительность*).
2. В дереве консоли разверните узел *Журналы и оповещения производительности*.

3. Правой кнопкой мыши выделите пункт *Оповещения* и в выпадающем меню выберите пункт *Новые параметры оповещений…*
4. В открывшемся окне в текстовое поле *Имя* введите значение *Packets Sent Alert*. Нажмите кнопку *Ok*.
5. В открывшемся окне *Packets Sent Alert* на вкладке *Общие* нажмите кнопку *Добавить…*
6. В открывшемся окне *Счетчики* в списке *Объект* выберите параметр *Сетевой интерфейс*, а в списке счетчиков – *Отправлено пакетов/сек*. Нажмите кнопку *Добавить*, а затем – *Закрыть*.
7. В окне *Packets Sent Alert* на вкладке *Общие* в текстовое поле *Порог* введите значение 5.
8. Перейдите на вкладку *Действие*. Установите галочку напротив параметра *Сделать запись в журнале событий приложений*. Нажмите кнопку *Ok*.
9. Убедитесь, что оповещение запущено – отмечено в рабочей области консоли зеленым значком.
10. Повторите шаг 6 предыдущего упражнения.
11. Просмотрите *Журнал событий* и найдите записи, сгенерированные только что созданным оповещением.
12. Закройте все открытые окна.

Упражнение 3. Настройка зависимости службы

1. На Server1 запустите консоль *Службы*.
2. В рабочей области консоли выделите правой кнопкой мыши службу *Сервер папки обмена* и в выпадающем меню выберите пункт *Свойства*.
3. В открывшемся окне в списке *Тип запуска* выберите параметр *Авто* и нажмите кнопку *Применить*.

4. Нажмите кнопку *Пуск*. Изучите сообщение об ошибке запуска. Нажмите кнопку *Ok*.
5. Перейдите на вкладку *Зависимости*. Изучите, от каких служб зависит запуск *Сервера папки обмена*.
6. Найдите в рабочей области консоли эти службы и запустите их. После этого попробуйте снова запустить службу *Сервер папки обмена*. Убедитесь в успешном запуске службы.

Упражнение 4. Настройка параметров восстановления службы

1. В рабочей области консоли *Службы* выделите правой кнопкой мыши службу *Telnet* и в выпадающем меню выберите пункт *Свойства*.
2. В открывшемся окне в списке *Тип запуска* выберите параметр *Авто* и нажмите кнопку *Применить*.
3. Перейдите на вкладку *Восстановление* и в списке *Первый сбой* выберите параметр *Перезапуск службы*. Нажмите кнопку *Применить*.
4. Запустите службу*Telnet* на вкладке *Общие*. Нажмите кнопку *Ok*.
5. Запустите *Диспетчер задач*.
6. В окне Диспетчер задач Windows перейдите на вкладку Процессы и завершите процесс *tlntsrv.exe*.
7. Подождите минуту, а затем убедитесь, что процесс *tlntsrv.exe* успешно запущен снова.
8. Закройте все открытые окна и завершите работу Server1 и Server2.

Литература

1. *Ватаманюк А.И.* Создание, обслуживание и администрирование сетей на 100%. –СПб.: Питер, 2010. 288 с.
2. *Дюгуров Д.В.* Системное администрирование. –Ижевск: УдГУ, 2008. 174 с.
3. *Дюгуров Д.В.* Управление контроллером домена. Упражнения и задачи. –Ижевск: Удмуртский университет, 2012, 102 с.
4. *Макин П., Маклин Й.* Внедрение, сопровождение и поддержка сетевой инфраструктуры Microsoft Windows Server 2003. –М.: Русская редакция, 2005. 586 с.
5. *Матвеев А., Яремчук С.* Системное администрирование Windows 7 и Windows Server 2008 R2 на 100% –СПб.: Питер, 2011. 384 с.
   URL.: http://ibooks.ru/reading.php?productid=22637.
6. *Орин Т., Холме Д.* Управление и поддержка Microsoft Windows Server 2003. –М.: Русская редакция, 2004. 420 с.
7. *Поляк-Брагинский А.* Администрирование сети на примерах. –СПб.: БХВ-Петербург, 2010. 432 с.
8. *Семенов А.Б.* Администрирование структурированных кабельных систем. –М.: ДМК Пресс, 2010. 192 с.
   URL: http://ibooks.ru/reading.php?productid=22461.
9. Информатика и системы управления // Ежемесячный журнал.
10. Промышленные АСУ и контроллеры // Ежемесячный журнал.

Учебное издание

Дюгуров Денис Владимирович

Сетевая адресация, разрешение имен, маршрутизация
Упражнения и задачи
Учебное пособие

Авторская редакция

Компьютерный набор и верстка Д.В. Дюгуров

Отпечатано с оргинал-макета заказчика

Подписано в печать . Формат 60x84 1/16.
Печать офсетная. Усл. печ. л. . Уч-изд. л. .
Тираж 30 экз. Заказ № .

Издательство «Удмуртский университет»
426034, Ижевск, ул. Университетская, 1 корп. 4
Тел./факс: +7(3412) 500-295 E-mail: editorial@udsu.ru