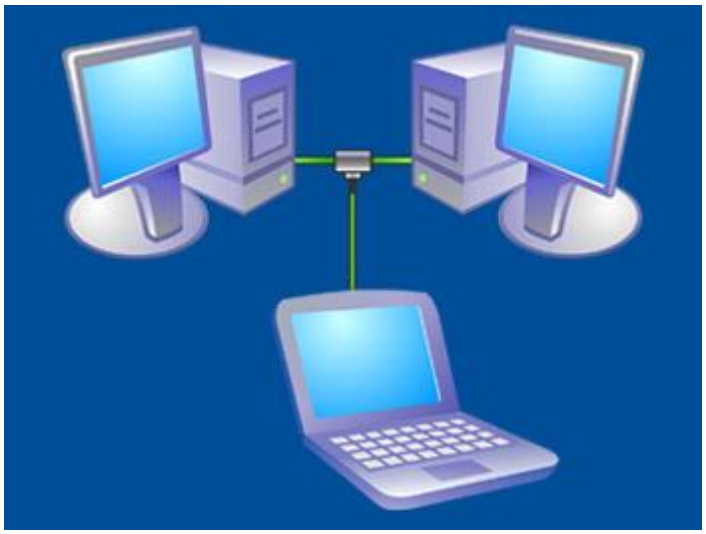
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Брянский государственный аграрный университет»

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ



Никулин В.В.

Создание и администрирование сети на основе Windows Server 2003

Методические указания

по курсу «Вычислительные системы, сети и телекоммуникации»

Часть 2

Брянск – 2015

УДК 681.3 (07)
ББК 32.973-018.2

Никулин Валерий Владимирович

Создание и администрирование сети на основе Windows Server 2003: методические указания по курсу «Вычислительные системы, сети и телекоммуникации» В. В. Никулин. – Брянск : Изд-во БГАУ, 2015. – Часть.2. – 45 с.

Настоящее издание является руководством к лабораторно-практическим занятиям по курсу «Вычислительные системы, сети и телекоммуникации», посвященному изучению методам построения и администрирования сетей в современных сетях ЭВМ. Во второй части данного практикума исследуются методы создания и администрирования сети под управлением ОС windows 2003 server, изучаются протоколы сетевого и транспортного уровней и прикладные протоколы стека TCP/IP с помощью Сетевого анализатора Network Monitor.

Лабораторный практикум подготовлен на кафедре «Информационных систем и технологий» и предназначен для студентов, обучающихся по направлению 09.03.03 «Прикладная информатика» профиль «Прикладная информатика в экономике».

Рецензенты:
ассистент кафедры
информационных систем и технологий БГСХА Н.Н. Чемисов

к.э.н., доцент кафедры
Информатики БГСХА Н.А. Верезубова

Рекомендовано к изданию решением методической комиссии экономического факультета от 12.11.2015 г. протокол № 2

Содержание

Введение

Предлагаемые методические указания дополняет лекционный курс по дисциплине «Вычислительные системы, сети и телекоммуникации».

Практикум построен на решениие конкретных практических задач. Все предлагаемые задачи посвящены разработке и администрированию сети экономического факультета. Такой подход стимулирует интерес студентов к дисциплине, позволяет им легче осваивать новые знания и умения в ходе практической деятельности.

Выполнять лабораторные работы можно самостоятельно или под руководством преподавателя, используя домашний компьютер или компьютер в аудитории.

Основной средой для выполнения лабораторных работ является виртуальная машина VMWare Workstation, на которой установлена ОС Microsoft Windows Server 2003. Данная среда позволяет выполнять сложные эксперименты с ОС и сетевыми настройками независимо от реальных машин и сетей. Кроме того, студенты обладают на виртуальной машине правами администратора, что в аудиторных условиях на компьютерах академиии обеспечить крайне сложно.

Каждая лабораторная работа содержит цели работы, задания, указания к выполнению, требования к отчету и контрольные вопросы. Также указывается связь данной работы с проектом по созданию факультетской сети. Обычно работа строится на следующем принципе: сначала достаточно подробно описывается процесс решения задачи, затем студентам предлагается выполнить ряд самостоятельных заданий. По выполненным заданиям требуется составление отчета, который сдается преподавателю на проверку.

В каждом задании при описании лабораторных работ приведены требования к тому, что нужно поместить в отчет. Требования выделяются следующим маркером:

Представленные материалы имеют целью формирование компетенций и освоение обучающимися видов профессиональной деятельности в соответствии с ФГОС ВО и ОПОП ВО по направлению подготовки 09.03.03 Прикладная информатика (уровень бакалавриата).

1.Требования к аппаратному и программному обеспечению

Среда выполнения лабораторных работ представляет собой персональный компьютер, на котором установлена программа эмуляции виртуальных машин VMWare Workstation. В качестве операционной системы физического компьютера можно использовать Microsoft Windows XP, Microsoft Windows Server 2003.

Перед выполнением лабораторных работ необходимо создать две виртуальные машины со следующими установленными операционными системами:

Microsoft Windows Server 2003 (Standard Edition или Enterprise Edition);

Microsoft Windows XP Professional (Service Pack не имеет значения).

После того, как операционные системы будут установлены, нужно выбрать подходящий тип сетевого взаимодействия. Отметим, что возможность работы с сетью является ключевой для успешного выполнения лабораторного практикума, поэтому на проблему настройки сетевых параметров на физическом компьютере следует обратить повышенное внимание.

VMWare Workstation предоставляет несколько вариантов сетевого взаимодействия. В любом случае на виртуальную машину требуется установить хотя бы один сетевой адаптер. После этого в свойствах адаптера требуется выбрать подходящий вид сети:

Способы сетевого взаимодействия виртуальных машин:

Bridged networking (мост) – позволяет присоединить сетевой интерфейс виртуальной машины к локальной сети. Т.е. из локальной сети будет виден еще один Ethernet-интерфейс, со своим Ip-адресом, а данные будут передаваться через реальный интерфейс основной машины. По умолчанию, для этого используется интерфейс vmnet0

Host-only networking – служит для объединения основной и виртуальных машин в единую сеть. В данном случае, присоединение к реальной сети не происходит и данная сеть видна только на локальном компьютере.

NAT adapter (Network Address Translation adapter) – используется для подключения виртуальных машин к Интернету через основную машину. Похоже на соединение при помощи моста, но отличается тем, что в сети не появляются новые интерфейсы. Устройство NAT преобразует пакеты таким образом, что все устройства реальной сети считают, что они общаются с реальным сетевым адаптером. В свою очередь устройство NAT, на основе

созданной им специальной таблицы, различает какой сети принадлежат приходящие на реальный адаптер пакеты.

Microsoft Loopback Adapter - адаптер виртуальной машины подключается к особому виртуальному адаптеру физической машины, который называется Microsoft Loopback Adapter (Адаптер Microsoft замыкания на себя). В этом случае организуется внутренняя сеть между виртуальными машинами и физическим компьютером, причем виртуальные машины не имеют доступа в реальную сеть.

Адаптер замыкания на себя устанавливается (в Windows XP) с помощью запуска Мастера установки оборудования (Пуск - Панель управления - Установка оборудования). Затем следует выбирать следующие пункты: Да, устройство уже подсоединено - Добавление нового устройства - Установка оборудования, выбранного из списка вручную - Сетевые платы - Microsoft - Адаптер Microsoft замыкания на себя.

Сетевые параметры адаптера нужно настроить следующим образом:

- IP-адрес: 192.168.1.10;
- маска подсети: 255.255.255.0;
- шлюз по умолчанию: 192.168.1.1;
- адрес DNS-сервера: 192.168.1.1.

Среда выполнения лабораторного практикума может быть настроена с использованием всех перечисленных способов. В большинстве случаев предпочтительно использование варианта Microsoft Loopback Adapter. В этом случае не требуется наличие реальной сети, а для связи физического компьютера и виртуальной машины не нужен реальный сетевой адаптер. Именно этот вариант считается основным при описании лабораторных работ.

В случае присутствия на физическом компьютере брандмауэра (firewall), следует его настроить на разрешение пакетов от сетевого адаптера, подключенного к виртуальным машинам.

2. Описание проекта

Все предлагаемые лабораторные работы связаны с выполнением сквозного проекта по созданию и настройке локальной сети экономического факультета. Связь лабораторной работы с выполнением проекта отражена в соответствующем разделе работы.

Компьютерная сеть факультета состоит из трех частей: деканат, кафедра информационных систем и компьютерный класс (рис. 1).

Кроме того, в сеть входит сервер, на котором установлена ОС Windows Server 2003. Остальные ПК имеют клиентские ОС Windows XP. Части сети объединяются при помощи коммутаторов.

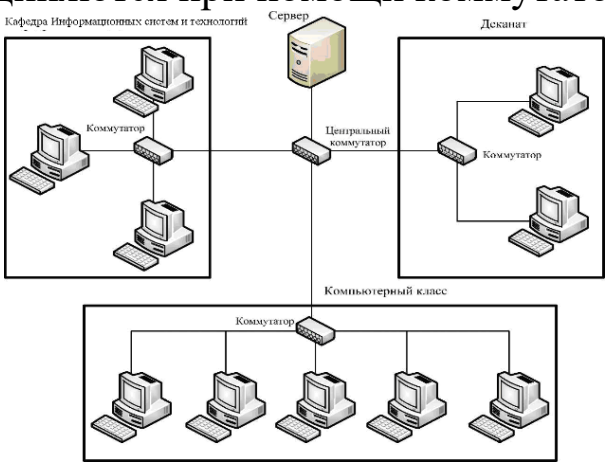


Рис. 1. Локальная сеть экономического факультета

Для пользователей локальной сети существуют следующие правила:

Администратор. Должен осуществлять управление всеми ресурсами сети. Может осуществлять вход на любой компьютер.

Декан. Имеет доступ ко всем ресурсам сети. Может осуществлять вход на любой компьютер.

Преподаватели. Могут осуществлять вход на любой компьютер сети, кроме сервера. Для каждого из преподавателей существует собственная учетная запись и настройки, которые конфигурируется лично преподавателем.

Лаборанты. Могут осуществлять вход на любой компьютер сети, кроме сервера. Для каждого из лаборантов существует собственная учетная запись и настройки, которые конфигурируется лично лаборантом.

Студенты. Могут осуществлять вход на компьютеры учебного класса под общей для всех студентов учетной записью. Время входа в систему ограничивается временным диапазоном 7.30 - 19.30. Пространство сетевого диска ограничивается 500 Мб. В воскресные дни вход в систему запрещен. Для студентов отсутствует возможность изменять свои настройки, пользоваться командой Выполнить, менять рисунок рабочего стола.

Все сетевые файловые ресурсы хранятся на сервере. Среди них обязательно должны существовать следующие папки:

Личные папки преподавателей. Каждый преподаватель должен обладать правом единоличного доступа к своей личной папке.

Документы. В папке хранится вся документация о работе факультета, нормативные документы. К ней разрешен доступ декану и лаборантам и отказано в доступе преподавателям.

Задания. В этой папке преподаватели могут размещать задания для лабораторных работ. Студенты должны иметь доступ только для чтения.

Отчеты. В этой папке студенты будут хранить отчеты о работе. Для преподавателей должна существовать возможность изменять эти файлы, но не удалять.

Студенты. Папка предназначена для хранения личной информации студентов. Лаборанты должны иметь возможность редактировать содержимое этой папки.

Для выполнения требований, а также для обеспечения надежной работы факультетской сети администратору требуется решить ряд задач:

- объединение компьютеров в сеть;
- определение структуры сети;
- планирование адресного пространства подсетей;
- настройка автоматического назначения сетевых параметров компьютерам сети;
- именование компьютеров;
- создание учетных записей пользователей и групп пользователей;
- задание разрешений для доступа к общим ресурсам сети.

Решение данных задач и составляет содержание лабораторного практикума.

Отметим, что виртуальная машина с ОС Windows Server 2003 будет исполнять роль сервера, виртуальная машина с Windows XP и физический компьютер являются в лабораторных работах клиентскими компьютерами.

Лабораторная работа № 1. Работа в виртуальной машине VMWare Workstation

Цели работы:

- научиться работать с виртуальными машинами VMWare Workstation;
- научиться настраивать сетевые параметры компьютера;
- изучить утилиты диагностики TCP/IP.

Связь с проектом

Первой задачей, с которой сталкивается администратор новой сети, является обеспечение физической связи ПК. Для этого ему требуется обладать знаниями по настройке сетевых параметров и диагностике сетевых протоколов для выявления причин неисправностей.

Примечание. Результатом выполнения лабораторной работы является отчет. В каждом задании указывается, что нужно поместить в отчет.

Задания к лабораторной работе

Задание 1. Запустить программу VMWare Workstation и виртуальную машину с установленной ОС Windows Server 2003.

Указания к выполнению

Запустите программу VMWare Workstation. Откроется VMWare Workstation. Выбрать виртуальную машину с установленной ОС Windows Server 2003 и открыть её настройки (Settings).

Выберите виртуальную машину с Windows Server 2003, затем пункт Settings.

Просмотрите настройки виртуальной машины:

Имя файла виртуальной машины.

Память - объем используемой памяти. Рекомендуется распределять имеющуюся физическую память поровну между всеми запущенными виртуальными машинами, а также физическим компьютером.

Жесткий диск - местонахождение файла жесткого диска виртуальной машины.

Сетевые настройки. Выберите один сетевой адаптер. В появившемся списке выберите адаптер Microsoft замыкания на себя. Таким образом, создается сетевое соединение физического компьютера и виртуальной машины, не влияющее на реальную сеть.

Остальные настройки оставьте неизменными.

Включите виртуальную машину. ОС должна стартовать. После запуска появится окно Welcome to Windows. Нажмите комбинацию клавиш Ctrl+ Alt + Insert, эта комбинация соответствует в виртуальной машине комбинации Ctrl+Alt+Delete. Введите пароль администратора (если есть) и войдите в систему.

Теперь вы находитесь в виртуальной машине. Чтобы выйти из её окна на физический компьютер нажмите Ctrl+Alt.

Выключите виртуальную машину. Выберите в меню окна виртуальной машины пункт ВМ , затем Питание.

Выберите Выключение питания.

Задание 2. Изучить утилиту диагностики TCP/IP IPconfig.

Указания к выполнению

Узнайте назначение утилит диагностики TCP/IP

На виртуальной машине запустите командную строку Пуск - Выполнить - Командная строка - cmd.

Выясните назначение параметров утилиты, пользуясь ключом /?: ipconfig /?

Выпишите назначение следующих ключей утилиты ipconfig: /all, /release, /renew.

4. Выполните утилиту IPconfig с ключом /all. Отметьте, что при наличии нескольких сетевых адаптеров информация о сетевых параметрах выводится отдельно для каждого из них.

Выпишите следующие данные (только для адаптера локальной сети):

имя компьютера;

IP-адрес;

маску подсети;

основной шлюз по умолчанию;

адреса DNS-серверов;

физический адрес.

Задание 3. Назначить своей виртуальной машине заданные сетевые параметры.

Указания к выполнению

Откройте окно Пуск - Панель управления - Сетевые соединения.

Щелкните два раза на значке Подключение по локальной сети. Отобразится информация о текущих сетевых параметрах и активности сети.

Нажмите на кнопку Свойства и два раза щелкните в окне установленных компонентов на Протокол TCP/IP.

Отобразится окно свойств протокола. Введите следующие данные:

IP-адрес: 172.16.1.10;

маска подсети: 255.255.0.0;

шлюз по умолчанию: 172.16.1.1;

адрес DNS-сервера: 172.16.1.1.

Поместите в отчет скриншот, в котором отражены установленные настройки IP-протокола на виртуальной машине. Нажмите Alt + C, выделенная часть экрана скопируется в буфер обмена. Теперь его можно вставить в графический редактор или в Microsoft Word.

Закройте оба окна свойств кнопкой ОК.

Проверьте сетевые настройки с помощью утилиты IPconfig.

Задание 4. Объединить в сеть виртуальную машину и физический компьютер.

Указания к выполнению

Проверьте в настройках виртуальной машины раздел Настрока виртуальной сети, что у неё имеется один сетевой адаптер, подключенный к сетевому адаптеру Microsoft замыкания на себя. Это означает, что виртуальная машина подключена по сети к физическому компьютеру, но для возможности передачи сообщений между ними требуется настроить сетевые параметры виртуальной машины, в частности, объединить их в одну подсеть.

Выясните с помощью утилиты IPconfig сетевые параметры физического компьютера (если имеется несколько сетевых адаптеров, выберите те параметры, которые относятся к адаптеру с описанием Адаптер Microsoft замыкания на себя. Параметры должны быть следующими:

IP-адрес: 192.168.1.10;

маска подсети: 255.255.255.0;

шлюз по умолчанию: 192.168.1.1;

адрес DNS-сервера: 192.168.1.1.

Если это не так, исправьте сетевые параметры на указанные.

Назначьте своей виртуальной машине следующие сетевые параметры:

IP-адрес: 192.168.1.20;

маска подсети: 255.255.255.0;

шлюз по умолчанию: 192.168.1.1;

адрес DNS-сервера: 192.168.1.1.

Таким образом, получилась следующая конфигурация компьютерной

Так как физический компьютер и виртуальная машина находятся в одной подсети 192.168.1.0/24, между ними возможна передача сообщений.

сети:

Рис. 2. Конфигурация виртуальной сети

Задание 5. Проверить возможность связи между физическим компьютером и виртуальной машиной.

Указания к выполнению

Узнайте назначение утилиты ping.

На виртуальной машине запустите командную строку Пуск - Выполнить - cmd.

Выясните назначение параметров утилиты ping, пользуясь ключом /?.

Проверьте возможность связи виртуальной машины с физическим компьютером при помощи утилиты ping:

ping 192.168.1.20

Таким же способом проверьте способность соединения физического компьютера с виртуальной машиной (запустите утилиту ping на физическом компьютере).

Выпишите назначение следующих ключей утилиты ping:

-t, -a, -1, — w.

Поместите в отчет скриншот, в котором отражено подтверждение возможности установления связи между физическим компьютером и виртуальной машиной.

Задание 6. Узнать имя физического компьютера и название рабочей группы.

Указания к выполнению

Существует два способа узнать имя и рабочую группу компьютера. Первый способ: откройте окно системных свойств (щелкните правой кнопкой мыши по значку Мой компьютер - Свойства. На вкладке Имя компьютера определите имя компьютера и название рабочей группы.

Второй способ (с помощью командной строки): для определения имени компьютера воспользуйтесь утилитой hostname.

Чтобы узнать название рабочей группы, примените утилиту nbtstat (утилита отображает информацию о протоколе NBT - NetBIOS через TCP/IP). В командной строке введите: nbtstat -a <имя компьютера>

Выпишите имя физического компьютера и название рабочей группы.

Экспериментальным путем выясните максимальную длину имен NetBIOS.

Задание 7. Изменить имя виртуальной машины и ввести её в рабочую группу физического компьютера.

Указания к выполнению

Откройте окно системных свойств. На вкладке Имя компьютера нажмите кнопку Изменить... Введите имя виртуальной машины (например, server) и название рабочей группы, совпадающее с названием рабочей группы физического компьютера.

Проверьте новое имя виртуальной машины с помощью утилиты hostname.

Проверьте, отображается ли физический компьютер в сетевом окружении виртуальной машины. Откройте окно Сетевое окружение из меню Пуск. Слева на панели Сетевых задач выберите пункт Отобразить компьютеры рабочей группы. Если все сделано правильно, в этом окне должно быть два компьютера - физический и виртуальная машина.

Поместите в отчет скриншоты, в которых отражены:

Окно Имя компьютера с названием рабочей группы виртуальной машины, результат выполнения утилиты hostname, окно Сетевое окружение.

Задание 8. Проверить способность связи по именам узлов.

Указания к выполнению

Допустим, физический компьютер называется host. На виртуальной машине в командной строке введите:

ping host.

Утилита ping, запущенная по IP-адресу, проверяет способность физического соединения двух узлов. Если использовать имя, то будет проверяться также способность разрешения имени.

Аналогично проверьте связь с сервером на физическом компьютере.

Поместите в отчет скриншот, в котором отражено подтверждение возможности установления связи между физическим компьютером и виртуальной машиной по именам узлов.

Самостоятельная работа

Для всех заданий поместите в отчете скриншоты, отражающие правильность выполнения заданий.

Подключите к сети третий компьютер (виртуальную машину с Windows XP). Нарисуйте схему полученной сети. Проверьте возможность связи по IP-адресам.

Добавьте виртуальную машину с Windows XP в рабочую группу. Проверьте возможность связи по именам узлов.

Организуйте постоянный опрос физического компьютера с одной из виртуальных машин при помощи утилиты ping.

Выясните с одной из виртуальных машин имя физического компьютера при помощи утилиты ping.

Изучите возможности утилиты tracert.

Исследуйте возможности утилиты netstat.

Контрольные вопросы

1. Как узнать физический адрес компьютера?
2. Нужно ли перезапускать компьютер, чтобы изменения вступили в силу, если изменяются следующие параметры:
3. настройки стека TCP/IP;
4. имя рабочей группы;
5. имя компьютера?
6. Какова максимальная длина имен NetBIOS?
7. Как с помощью утилиты ping определить достижимость узла? Какая информация, полученная при использовании утилиты ping, служит ответом о достижимости узла?
8. Как определить IP-адрес удаленного узла, зная только его символьное имя?
9. Как изменить размер пакета утилиты ping?
10. Параметры свойств протокола TCP/IP компьютера локальной сети были настроены вручную. После этого компьютер может устанавливать соединение с любым компьютером внутренней сети, но компьютеры удаленной подсети остаются недостижимыми. Объясните, в чем проблема и как ее устранить.
11. Какая утилита определяет имя узла?

Лабораторная работа № 2. IP-адресация

Цели работы:

научиться определять адрес подсети и адрес хоста по маске подсети;

научиться определять количество и диапазон адресов возможных узлов в подсетях;

научиться структурировать сети с использованием масок.

Связь с проектом

Для успешного решения задач администрирования необходимо хорошо разбираться в системе IP-адресации. Знание принципов использования масок и структуризации сетей поможет грамотно решать многие вопросы настройки локальной сети.

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях, если адреса компьютера А и компьютера В соответственно равны: 26.219.123.6 и 26.218.102.31, маска подсети 255.192.0.0.

Указания к выполнению

Переведите адреса компьютеров и маску в двоичный вид.

Для получения двоичного представления номеров подсетей обоих узлов выполните операцию логического умножения AND над IP-адресом и маской каждого компьютера.

Двоичный результат переведите в десятичный вид.

Сделайте вывод.

Процесс решения можно записать следующим образом:

Компьютер А:

IP-адрес: 26.219.123.6 = 00011010. 11011011. 01111011. 00000110

Маска подсети: 255.192.0.0 = 11111111. 11000000.00000000.00000000

Компьютер В:

IP-адрес: 26.218.102.31 = 00011010. 11011010. 01100110. 00011111

Маска подсети: 255.192.0.0= 11111111. 11000000.00000000.00000000

Получаем номер подсети, выполняя операцию AND над IP-адресом и маской подсети.

Компьютер А:

00011010. 11011011. 01111011. 00000110 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000

26 192 0 0

Компьютер B:

00011010. 11011010. 01100110. 00011111 11111111. 11000000. 00000000. 00000000 00011010. 11000000. 00000000. 00000000

26 192 0 0

Ответ: номера подсетей двух IP-адресов совпадают, значит компьютеры A и B находятся в одной подсети. Следовательно, между ними, возможно, установить прямое соединение без применения шлюзов.

Задание 2. Определить количество и диапазон IP-адресов в подсети, если известны номер подсети и маска подсети.

Номер подсети - 26.219.128.0, маска подсети - 255.255.192.0.

Указания к выполнению

Переведите номер и маску подсети в двоичный вид.

Номер подсети: 26.219.128.0= 00011010. 11011011. 10000000.00000000

Маска подсети: 255.255.192.0= 11111111. 11111111. 11000000. 00000000

По маске определите количество бит, предназначенных для адресации узлов (их значение равно нулю). Обозначим их буквой K.

Общее количество адресов равно 2 . Но из этого числа следует исключить комбинации, состоящие из всех нулей или всех единиц, так как данные адреса являются особыми. Следовательно, общее количество узлов подсети будет равно 2 - 2.

В рассматриваемом примере K = 14,2 -2 = 163 82 адресов.

Чтобы найти диапазон IP-адресов нужно найти начальный и конечный IP-адреса подсети. Для этого выделите в номере подсети те биты, которые в маске подсети равны единице. Это разряды, отвечающие за номер подсети. Они будут совпадать для всех узлов данной подсети, включая начальный и конечный:

Номер подсети: 26.219.128.0 = 00011010. 11011011. 10000000. 00000000

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Чтобы получить начальный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить нулями, за исключением крайнего правого бита, который должен быть равен единице. Полученный адрес будет первым из допустимых адресов данной подсети:

Начальный адрес: 26.219.128.1 = 00011010. 11011011. 10000000. 00000001

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

6. Чтобы получить конечный IP-адрес подсети нужно невыделенные биты в номере подсети заполнить единицами, за исключением крайнего правого бита, который должен быть равен нулю. Полученный адрес будет последним из допустимых адресов данной подсети:

Конечный адрес: 26.219.191.254= 00011010. 11011011. 10111111. 11111110

Маска подсети: 255.255.192.0 = 11111111. 11111111. 11000000. 00000000

Ответ: Для подсети 26.219.128.0 с маской 255.255.192.0:

количество возможных адресов: 16 382,

диапазон возможных адресов: 26.219.128.1 -26.219.191.254.

Задание 3. Организации выделена сеть класса С: 212.100.54.0/24. Требуется разделить данную сеть на 4 подсети с количеством узлов в каждой не менее 50. Определить маски и количество возможных адресов новых подсетей.

Указания к выполнению

В сетях класса С (маска содержит 24 единицы - 255.255.255.0) под g

номер узла отводится 8 бит, т. е. сеть может включать 2 - 2 = 254 узла.

Требование деления на 4 подсети по 50 узлов в каждой может быть выполнено: 4-50 = 200 < 254. Однако число узлов в подсети должно быть кратно степени двойки. Относительно 50 ближайшая большая степень - 26 = 64. Следовательно, для номера узла нужно отвести 6 бит, вместо 8, а маску расширить на 2 бита - до 26 бит (см. рис. 3).

В этом случае вместо одной сети с маской 255.255.255.0 образуется 4 подсети с маской 255.255.255.192 и количеством возможных адресов в каждой - 62 (не забывайте про два особых адреса).

Номера новых подсетей отличаются друг от друга значениями двух битов, отведенных под номер подсети. Эти биты равны 00, 01, 10, 11.

Ответ: маска подсети - 255.255.255.192, количество возможных адресов - 62.

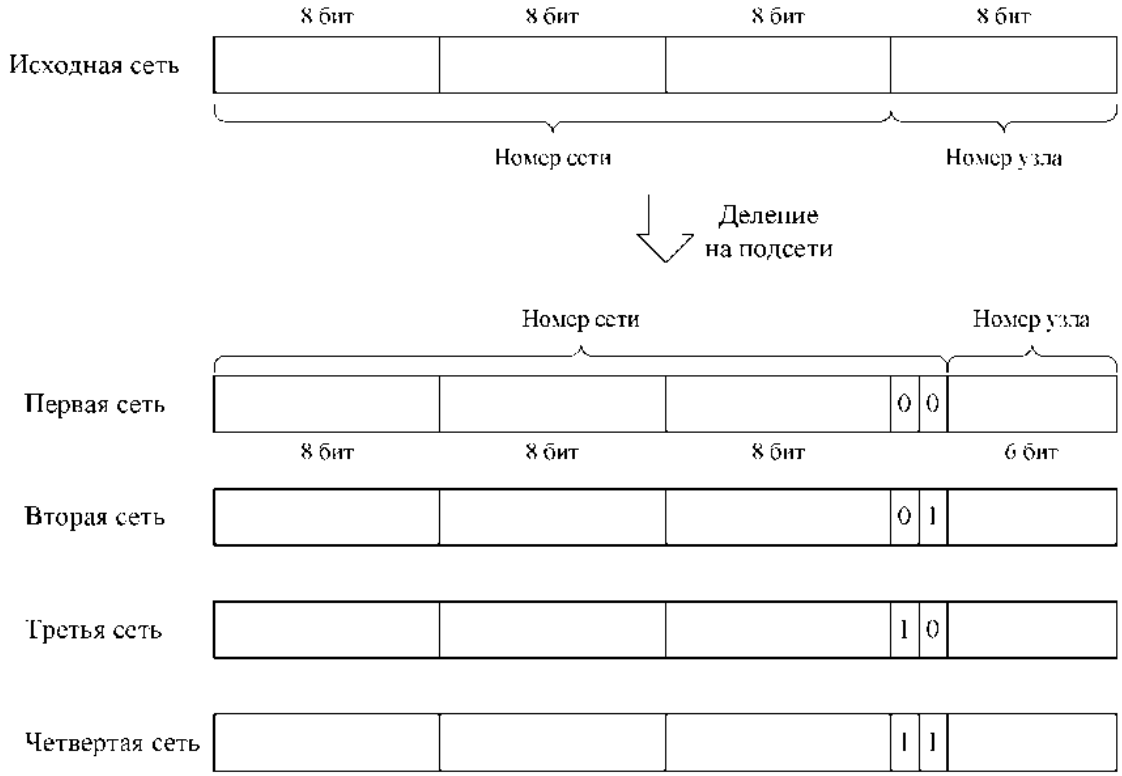


Рис. 3. Адреса подсетей после деления

Самостоятельная работа

Задание 1. Определить, находятся ли два узла А и В в одной подсети или в разных подсетях.

IP-адрес компьютера А: 94.235.16.59; IP-адрес компьютера В: 94.235.23.240; Маска подсети: 255.255.240.0.

IP-адрес компьютера А: 131.189.15.6; IP-адрес компьютера В: 131.173.216.56; Маска подсети: 255.248.0.0.

IP-адрес компьютера А: 215.125.159.36; IP-адрес компьютера В: 215.125.153.56; Маска подсети: 255.255.224.0.

Задание 2. Определить количество и диапазон адресов узлов в подсети, если известны номер подсети и маска подсети.

Номер подсети: 192.168.1.0, маска подсети: 255.255.255.0.

Номер подсети: 110.56.0.0, маска подсети: 255.248.0.0.

Номер подсети: 88.217.0.0, маска подсети: 255.255.128.0.

Задание 3. Определить маску подсети, соответствующую указанному диапазону IP-адресов.

119.38.0.1 - 119.38.255.254.

75.96.0.1 -75.103.255.254.

48.192.0.1 -48.255.255.254.

Задание 4. Организации выделена сеть класса B: 185.210.0.0/16. Определить маски и количество возможных адресов новых подсетей в каждом из следующих вариантов разделения на подсети:

Число подсетей - 256, число узлов - не менее 250.

Число подсетей - 16, число узлов - не менее 4000.

Число подсетей - 5, число узлов - не менее 4000. В этом варианте укажите не менее двух способов решения.

Требования к отчету

В отчете запишите ответы на задания самостоятельной работы. Обоснуйте каждый шаг получения результата, аналогично тому, как это сделано в примерах.

Контрольные вопросы

Может ли быть IP-адрес узла таким? Укажите неверные варианты IP-адрес. Ответ обоснуйте.

192.168.255.0

167.234.56.13

224.0.5.3

172.34.267.34

230.0.0.7

160.54.255.255

Может ли маска подсети быть такой? Укажите неверные варианты. Ответ обоснуйте.

255.254.128.0

255.255.252.0

240.0.0.0

255.255.194.0

255.255.128.0

255.255.255.244

255.255.255.255

Можно ли следующие подсети разделить на N подсетей. Если это возможно, то укажите варианты разбиения с максимально возможным количеством подсетей или узлов в каждой подсети. Ответ обоснуйте.

165.45.67.0, маска 255.255.255.224, N=3

235.162.56.0, маска 255.255.255.224, N=6

234.49.32.0, маска 255.255.255.192, N=3

Лабораторная работа № 3. Маршрутизация в IP-сетях

Цели работы:

научиться объединять две сети исполняющего роль маршрутизатора;

научиться настраивать при помощи компьютера Windows Server 2003, в качестве маршрутизатора;

изучить возможности утилиты route.

Связь с проектом

Часто возникают задачи, когда необходимо к локальной сети подключить другую локальную сеть, причем номера подсетей у них разные. Например, возникла потребность к сети экономического факультета подключить сеть инженерного факультета. Экономический факультет имеет подсеть с номером 192.168.1.0/24, а инженерный - подсеть 192.168.2.0/24. Каким образом сделать так, чтобы, не меняя номера подсетей, компьютеры обоих факультетов могли соединяться друг с другом и использовать общие ресурсы?

Данная задача решается при помощи настройки маршрутизатора, соединяющего обе подсети, причем в роли маршрутизатора может выступать компьютер с Windows Server 2003, имеющий две сетевые карты: одна подключена к сети факультета информатики, другая - к сети факультета математики.

В результате требуется получить следующую схему сети:

Рис. 4. Схема сети с маршрутизатором

Задание 1. Переместить виртуальную машину с Windows XP в другую подсеть с номером 192.168.2.0/24.

Указания к выполнению

Подключите виртуальную машину с Windows XP к внутренней сети виртуальных машин: в разделе Сетевые параметры настроек виртуальной машины выберите подключение сетевого адаптера к внутренней сети виртуальных машин (Local only).

Таким образом, образовалось две физические подсети (см. рис. 4).

Запустите виртуальную машину с Windows XP. Измените сетевые параметры виртуальной машины следующим образом:

IP-адрес: 192.168.2.20;

маска подсети: 255.255.255.0.

Таким образом, виртуальная машина находится сейчас в подсети 192.168.2.0/24.

Поместите в отчет окно с установленными сетевым параметрами.

Проверьте, что виртуальная машина не способна установить соединение с физическим компьютером с помощью утилиты ping:

ping 192.168.1.10

Поместите в отчет скриншот окна командной строки с информацией о невозможности установить соединение.

Задание 2. Настроить виртуальную машину с Windows Server 2003 в качестве маршрутизатора.

Указания к выполнению

Установите два сетевых адаптера на виртуальную машину с Windows Server 2003 (Раздел Networking настроек виртуальной машины). Подключите первый адаптер к внутренней сети виртуальных машин (Local only), второй - к адаптеру Microsoft замыкания на себя.

Запустите виртуальную машину. Откройте окно Сетевых подключений. В этом окне должно быть два подключения по локальной сети, первое из них (соответствует тому адаптеру, который подключен к внутренней сети виртуальных машин, второе соответствует адаптеру Microsoft замыкания на себя.

Настройте IP-адреса обоих подключений согласно рис. 4. Проверьте, что физический компьютер имеет соединение с сервером и наоборот, а также, что виртуальная машина с Windows XP имеет связь с сервером и наоборот. При этом физический компьютер и виртуальная машина с Windows XP соединиться не могут, так как находятся в разных подсетях.

Поместите в отчет скриншот окна командной строки с информацией о невозможности установить соединение.

На виртуальной машине с Windows Server 2003 настройте службу маршрутизации. Для этого откройте оснастку Маршрутизация и

удаленный доступ: Пуск - Программы - Администрирование - Маршрутизация и удаленный доступ.

В контекстном меню сервера выберите пункт Сконфигурировать и активировать маршрутизацию и удаленный доступ. В окне мастера Routing and Remote Access Server Setup Wizard выберите пункт Конфигурация пользователя. Установите флажок LAN routing. На предложение запустить службу нужно ответить Yes.

Просмотрите таблицу маршрутизации, действующую сейчас на сервере: щелкните на значке сервера, затем на IP маршрутизация, в контекстном меню элемента Статические маршруты выберите Показать таблицу маршрутизации. Эта таблица соответствует той таблице, которая выводится в командной строке при запуске утилиты route с ключом /print.

Сохраните в отчете скриншот с таблицей, полученной из оснастки и скриншот с таблицей, полученной с помощью утилиты route.

Теперь следует добавить в таблицу маршрутизации записи, которые позволят компьютерам из разных подсетей связываться друг с другом. В контекстном меню элемента Статические маршруты выберите пункт Новый статический маршрут. В появившемся окне введите следующие параметры:

Интерфейс - Local Area Connection;

Адрес назначения - 192.168.2.0;

Маска подсети - 255.255.255.0;

Шлюз- 192.168.2.1;

Метрика - 1.

Таким образом, настроен маршрут для передачи пакетов из подсети 192.168.2.0 в подсеть 192.168.1.0.

Создайте ещё один статический маршрут и по аналогии настройте его для передачи пакетов из подсети 192.168.1.0 в подсеть 192.168.2.0.

Поместите в отчет скриншоты с окнами обоих маршрутов и результат в окне Статические маршруты.

Просмотрите созданные записи в разделе Статические маршруты и в таблице маршрутизации.

Задание 3. Осуществить подключение виртуальной машины с Windows XP к физическому компьютеру через маршрутизатор.

Указания к выполнению

Настройте для виртуальной машины с Windows XP шлюз по умолчанию в соответствии с рис. 4. Для этого откройте окно настроек параметров TCP/IP (то окно, в котором следует менять IP-адрес компьютера). В строке Основной шлюз введите IP-адрес 192.168.2.1.

Сохраните скриншот окна в отчете.

Проверьте (с помощью утилиты IPconfig), что на физическом компьютере установлен шлюз по умолчанию 192.168.1.1. Если это не так, измените шлюз по умолчанию.

Сохраните скриншот окна в отчете.

Проверьте способность виртуальной машины с Windows XP соединяться с физическим компьютером с помощью утилиты ping.

Аналогичным образом проверьте способность физического компьютера соединяться с виртуальной машиной.

Поместите скриншоты командной строки в отчет. Запишите в отчете выводы.

Задание 4. Вернуть исходные настройки.

1. Верните следующие настройки:

IP-адрес виртуальной машины с Windows XP;

подключение сетевой карты виртуальной машины с Windows XP к адаптеру Microsoft замыкания на себя;

количество сетевых карт виртуальной машины с Windows Server 2003 сделайте равным 1;

подключите сетевую карту виртуальной машины с Windows Server 2003 к адаптеру Microsoft замыкания на себя.

Самостоятельная работа

Объедините две подсети 192.168.1.0/24 и 192.168.2.0/24 при помощи маршрутизатора на основе виртуальной машины с Windows XP. В этом случае для просмотра таблицы маршрутизации, добавлении и удалении новых маршрутов придется использовать исключительно утилиту route.

Зафиксируйте процесс объединения в отчете с помощью скриншотов, аналогично тому, как делали в работе.

Контрольные вопросы

1. Назовите протоколы маршрутизации, реализованные в Windows Server 2003.
2. Что такое таблица маршрутизации?
3. Какие записи создаются в таблице маршрутизации по умолчанию?

4. Чем отличаются возможности Windows Server 2003 от возможностей Windows XP в области маршрутизации?
5. Какое максимальное количество сетей можно соединить, используя один компьютер с Windows Server 2003 в качестве маршрутизатора?

Лабораторная работа № 4. DHCP-сервер: установка и управление

Цели работы:

научиться устанавливать и удалять DHCP-сервер;

научиться настраивать область действия DHCP-сервера;

научиться выполнять резервирование адресов.

Примечание. Если виртуальная машина подключена к сетевому адаптеру на физическом компьютере (не Microsoft Loopback Adapter), т. е. имеет выход в реальную сеть, перед выполнением работы необходимо отключить физический компьютер от сети, потому что установка DHCP- сервера на виртуальной машине может вызвать ошибки в работе реальной сети.

Связь с проектом

Целью данной лабораторной работы является установка DHCP-сервера для локальной сети факультета. Значение адреса узла, на котором будет работать DHCP-сервер, равно 192.168.1.1 и зарезервировано, а диапазон динамически выдаваемых адресов 192.168.1.11 - 192.168.1.100.

Задание 1. Назначить серверу сетевые параметры.

Указания к выполнению

Запустите виртуальную машину с Windows Server 2003. Будем называть эту машину сервером сети.

Назначьте виртуальной машине IP-адрес 192.168.1.1, маска подсети 255.255.255.0.

Проверьте с помощью утилиты IPconfig правильность настройки сетевых параметров.

На физическом компьютере проверьте доступность виртуальной машины с помощью утилиты ping.

Поместите скриншоты командной строки для обеих утилит в отчет.

Задание 2. Установите DHCP-сервер на виртуальной машине.

Указания к выполнению

1. Для установки DHCP-сервера проделайте следующие действия:

Откройте Панель управления, затем Установка и удаление программ.

На вкладке Установка компонентов Windows найдите Сетевые службы и нажмите Состав.

Поставьте галочку около Протокол Динамической конфигурации хостов и подтвердите свой выбор.

Дождитесь завершения установки сервера.

Проверьте, что после установки сервера в меню Администрирование добавилась новая оснастка - DHCP. Эта оснастка используется для настройки DHCP-сервера. Если в оснастке DHCP нет вашего сервера, то в меню нужно выбирать команду Добавить сервер, а затем указать имя DHCP-сервера или найти его с помощью клавиши Обзор.

Запуск и остановка DHCP-сервера производятся при помощи пункта контекстного меню DHCP-сервера Все задачи.

Заметьте, что перед использованием DHCP-сервера в сети с установленной службой каталога Active Directory, его нужно авторизовать.

Сохраните в отчете скриншот оснастки DHCP.

Задание 3. Создать область действия DHCP-сервера со следующим диапазоном IP-адресов: 192.168.1.11 - 192.168.1.100.

Указания к выполнению

Запустите оснастку DHCP.

В контекстном меню конфигурируемого DHCP-сервера выберите пункт Создать область (New Scope).

В окне Имя области определите имя для создаваемой области действия и дайте ей краткое описание. Используйте понятные имена, которые позволяют легко определить область действия в том случае, если на DHCP-сервере хранится несколько областей.

В окна мастера Диапазон адресов определите пул IP-адресов, для которых создается область действия. Пул задается путем указания начального (192.168.1.10) и конечного адреса (192.168.1.100) диапазона. Также указывается маска подсети (255.255.255.0).

В окне Добавление исключений можно определить исключения из только что определенного диапазона, при этом можно исключать как отдельные адреса, так и целые диапазоны. Для исключения одиночного IP-адреса необходимо указать его в поле Начальный IP-

адрес. Поле Конечный IP-адрес необходимо оставить в этом случае пустым. После нажатия кнопки Добавить введенный адрес будет добавлен в список исключенных из диапазона адресов.

В окне Время аренды определяется время аренды IP-адресов (по умолчанию - 8 дней).

На следующей странице мастера будет задан вопрос - требуется ли определить опции DHCP для создаваемой области действия непосредственно в ходе работы мастера или это будет сделано администратором впоследствии. Определите опции сразу же:

Адрес шлюза по умолчанию - поставьте адрес сервера (нажмите клавишу Add, чтобы он появился в списке);

DNS сервер - добавьте адрес сервера;

WINS server - добавьте адрес сервера или оставьте пустым, если служба WINS в сети не работает.

В конце работы мастера необходимо выбрать Активизировать область действия сейчас.

Если служба DHCP-сервера функционирует нормально, на значке сервера должна появиться зеленая стрелка. Красная стрелка указывает, что служба не работает, в этом случае следует обновить информацию о сервере (контекстное меню сервера - Обновить) или перезапустить службу (контекстное меню сервера – Все задачи - Перезапустить).

Поместите в отчете скриншот оснастки DHCP.

Задание 4. Проверить работу DHCP-сервера.

Указания к выполнению

Запустите виртуальную машину с Microsoft Windows XP. Эта машина будет являться DHCP-клиентом, будем называть её рабочей станцией.

Настройте рабочую станцию на автоматическое получение IP-адреса и имени DNS-сервера.

Откройте окно свойств Подключение по локальной сети и выберите Протокол Интернета (TCP/IP).

Установите переключатель в положение Получить IP-адрес автоматически.

Выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила сетевые параметры от DHCP- сервера.

Поместите в отчете скриншот командной строки.

Задание 5. Зарезервируйте для рабочей станции постоянный IP-адрес 192.168.1.20.

Указания к выполнению

Запустите оснастку DHCP.

Для просмотра текущих аренд откройте раздел Аренды адресов и найдите аренду для рабочей станции.

Определите MAC - адрес станции (столбец Unique ID) и запишите его.

В контекстном меню раздела Резервирования выбираем Новое резервирование... и вводим параметры - имя резервирования, необходимый IP-адрес (192.168.1.20), MAC - адрес станции.

Поместите в отчет скриншот окна.

На рабочей станции выполните утилиту IPconfig с ключом /renew, а затем с ключом /all, и убедитесь в том, что рабочая станция получила зарезервированный IP-адрес от DHCP-сервера.

Поместите в отчете скриншот командной строки.

Задание 6. Зарезервируйте для рабочей станции адрес вне текущей области действия DHCP-сервера.

Указания к выполнению

Выполните резервирование для рабочей станции IP-адреса вне области действия DHCP-сервера, например, 192.168.1.200.

Проверьте на рабочей станции, получила ли она новые параметры.

Поместите в отчете скриншоты выполненных действий.

Задание 7. Настройте мониторинг DHCP-сервера.

Указания к выполнению

Служба DHCP-сервера ведет мониторинг своих действий, записывая их в журнал аудита. Этот журнал можно использовать при решении проблем с DHCP-сервером.

Чтобы включить журнал, откройте окно свойств DHCP-сервера (контекстное меню сервера - Свойства. На вкладке Общие выберите пункт Разрешить мониторинг DHCP.

Файлы журнала находится в следующем каталоге: C:\Windows\system32\dhcp. Файлы создаются ежедневно и называются по следующему принципу: к постоянному имени DhcpSrvLog добавляется

обозначение дня недели, например, журнал понедельника называется DhcpSrvLog-Mon.log.

Просмотрите файл журнала за текущий день. В начале журнала приводятся значения кодов событий. Затем указывается точное время и краткое описание события.

Найдите в журнале записи, соответствующие вашим действиям в этой лабораторной работе.

Сохраните в отчете текст файла журнала.

Самостоятельная работа

Сохраняйте в отчете скриншоты каждого действия.

Установите диапазон адресов для DHCP-сервера 172.16.0.1 - 172.16.0.10, маска подсети 255.240.0.0. Проверьте работу DHCP-сервера.

Установите зарезервированный за рабочей станцией IP-адрес 172.16.0.20. Проверьте получение станцией адреса.

Используйте вкладку альтернативной конфигурации рабочей станции на случай отключения службы DHCP. Протестируйте полученные настройки.

Что такое автоматические частные адреса? Протестируйте их получение и работу сети в случае, если DHCP-сервер оказывается недоступным.

Контрольные вопросы

Для чего предназначена служба DHCP?

Что означает термин «аренда адреса»?

Для каких компьютеров сети следует применять резервирование адреса?

Какой IP-адрес шлюза по умолчанию определяют для подсети DHCP-сервера?

Какой IP-адрес вы дадите шлюзу по умолчанию для компьютера-арендатора адреса, находящегося в другой подсети (маска 255.255.240.0), если IP-адрес DHCP-сервера 201.212.96.1, а маска подсети 255.255.240.0?

Какой IP-адрес шлюза по умолчанию вы определите для подсети DHCP-сервера, IP-адрес которого 201.212.96.1, а маска подсети 255.255.240.0?

Установите соответствия между протоколами и выполняемыми ими функциями:

Протоколы	Функции протоколов
DHCP	Отображение IP-адресов на MAC-адреса.
DNS	Присвоение IP-адресов клиентским

	компьютерам
ARP	Отображение доменных имен на IP-адреса

Лабораторная работа № 5. DNS-сервер: установка и управление

Цели работы:

1. научиться устанавливать службу DNS;
2. научиться конфигурировать зоны DNS;
3. научиться тестировать службу DNS;
4. научиться применять файл HOSTS.

Связь с проектом

Служба DNS предназначена для преобразования символьных доменных имен в IP-адреса и обратно. В сети, где работает служба DNS, пользователи могут без труда обращаться к различным сетевым ресурсам по доменным именам, а не по IP-адресам. Также, устанавливая эту службу, мы готовим платформу для установки Active Directory.

Требования к отчету

Отчет должен включать скриншоты каждого шага выполнения установки и проверки работоспособности DNS-сервера.

Задание 1. Установите сервер DNS на виртуальную машину с Windows Server 2003.

Указания к выполнению

Выполните предварительную конфигурацию компьютера, на котором будет установлен сервер DNS: проверьте, что серверу DNS назначен статический IP-адрес (например, 192.168.1.1).

Для установки сервера DNS воспользуйтесь одним из двух способов.

й способ.

Откройте Панель управления, затем Установка/удаление программ.

На вкладке Установка/удаление компонентов Windows найдите Сетевые службы и нажмите Подробно.

Выберите компонент Domain Name System (DNS) и подтвердите свой выбор.

Дождитесь завершения установки сервера.

й способ.

Откройте Панель управления - Администрирование.

Запустите Управление сервером.

Выберите Добавить или удалить роль и выберите DNS Server.

Дождитесь завершения установки сервера.

3. Для дальнейшей настройки DNS-сервера используется оснастка главного системного меню Администрирование - DNS.

Задание 2. Создайте зону прямого просмотра myzone.ru.

Указания к выполнению

Откройте оснастку DNS.

Разверните узел DNS, далее разверните узел <Имя компьютерам

Для создания нового домена щелкните правой кнопкой по Зоны прямого просмотра и выберите пункт Новая зона.

В окне Тип зоны укажите Основная зона и нажмите Далее.

В окне Имя зоны укажите имя зоны - myzone.ru и нажмите Далее.

В окне Файл зоны убедитесь, что выбран переключатель Создать новый файл с этим именем и имя создаваемого файла - myzone.ru.dns.

Просмотрите сводку выбранных параметров и щелкните кнопку Готово.

Убедитесь, что в Forward Lookup Zones появился новый узел myzone.ru и сгенерированы записи Начальная запись зоны, Сервер имен и Хост А.

Для добавления нового узла (хоста) в созданную зону, щелкните правой кнопкой по узлу myzone.ru и выберите New Host (Новый хост). В поле Name (Имя) введите имя узла - server. Поле IP Address установите равным IP-адресу вашего компьютера. Нажмите Add Host (Добавить хост).

Задание 3. Протестируйте работу службы DNS.

Указания к выполнению

Запустите виртуальную машину с Windows XP. Выполните в ней команду ping server.myzone.ru.

Убедитесь, что такой узел был найден, и отображается его IP-адрес. Если ping не проходит, нужно исправить настройки.

Для преобразования IP-адреса в доменное имя выполните утилиту nslookup с параметром, равным IP-адресу виртуальной машины. Объясните, почему появилась ошибка.

Задание 4. Создайте зону обратного просмотра (для преобразования IP-адреса в доменное имя).

Указания к выполнению

В узле Reverse Lookup Zones (Зоны обратного просмотра)

щелкните правой кнопкой мыши и выберите New zone (Мастер создания новой зоны).

В окне Zone Type (Тип зоны) укажите Primary Zone (Основная зона) и нажмите Next.

Убедитесь, что выбран переключатель Network ID (Номер сети). В поле под ним введите адрес вашей сети (например, 192.168.1). Поле Reverse Lookup Zone Name (Имя зоны обратного просмотра) внизу окна должно выглядеть так: 1.168.192.in-addr.arpa.

Завершите работу мастера, оставив все настройки по умолчанию.

Щелкните правой кнопкой мыши по новому узлу в Reverse Lookup Zones (например, 192.168.1.x Subnet) и выберите New Pointer (Новый указатель). Последнее число установите равным последнему числу в IP-адресе. В поле Host name (Имя хоста) запишите полное имя узла, например server.myzone.ru.

Задание 5. Создайте псевдоним для узла server.myzone.ru.

Указания к выполнению

Щелкните правой кнопкой мыши по узлу myzone.ru и выберите New Alias (Новый псевдоним). В поле Alias name (Имя псевдонима) укажите псевдоним узла (например, MyServer). В поле Fully qualified domain name (Полное доменное имя) впишите полное имя server.myzone.ru

Задание 6. Протестируйте работу службы DNS.

Указания к выполнению

Используйте утилиты ping, nslookup.

В дереве консоли откройте свойства узла через команду контекстного меню Properties (Свойства).

Перейдите на вкладку Monitoring (Наблюдение).

В группе Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS-серверу) и Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS- серверам). Щелкните кнопку Test Now (Тестировать).

В списке Test Results (Результаты теста) против обеих записей вы увидите PASS (тест пройден). Если вы работаете на автономном сервере, напротив Recursive Query (Рекурсивный запрос) вы увидите FAIL (ошибка).

Задание 7. Сконфигурируйте клиента для использования службы DNS.

Указания к выполнению

1. На клиенте откройте диалоговое окно его свойств TCP/IP. Настройте систему для автоматического получения адреса DNS (это обеспечивает сервер DHCP) или вручную укажите IP-адреса предпочтительного и дополнительного серверов DNS.

2. Для настройки дополнительных параметров DNS щелкните кнопку Advanced (Дополнительно). Чтобы задать параметры DNS, в диалоговом окне Advanced TCP/IP Settings (Дополнительные параметры TCP/IP) перейдите на вкладку DNS. Здесь можно сконфигурировать и параметры, обеспечивающие разрешение имен узлов, для которых не было указано полное доменное имя, и настроить параметры регистрации DNS.

Задание 8. Задайте разрешение имен с использованием файла HOSTS для случаев отказа службы DNS и для возможности использования коротких имен при доступе к удаленным узлам.

Указания к выполнению

На сервере найдите системный файл HOSTS и откройте его в текстовом редакторе.

Какая запись уже присутствует в файле по умолчанию и что эта запись означает? Что это за адрес и для чего он используется?

Выясните IP-адрес узла www.microsoft.com.

Внесите запись в файл, указав полученный IP-адрес и имя - www.microsoft.com. Сохраните изменения.

Проверьте через браузер доступность узла www.microsoft.com.

Внесите в файл IP-адрес своего сервера и имя в формате computer.domain. Сохраните изменения.

Остановите службу DNS через утилиту Services.

Проверьте, доступно ли это имя в формате computer.domain через утилиту ping.

Самостоятельная работа

Установите DNS-сервер для домена faculty.ru. Настройте прямую и обратную зоны, протестируйте сервер с помощью оснастки DNS, командной строки и виртуальной машины с Windows XP.

Зафиксируйте все шаги установки, настройки и тестирования DNS-сервера с помощью скриншотов в отчете.

Контрольные вопросы

1. Для чего предназначены прямые и обратные запросы поиска?
2. Опишите назначение компонентов DNS: зона, сервер имен, доменное пространство имен.

3. Назовите основные типы зон и их назначение.
4. Назовите основные правила именования доменов.
5. Какова максимально допустимая длина имени домена?
6. Какова максимально допустимая длина имени FQDN?
7. С какой целью используют несколько серверов имен?
8. Приведите примеры использования утилиты nslookup.
9. Можно ли одному IP-адресу нужно присвоить несколько имен? Перечислите все способы.
10. Для чего используется файл HOSTS?
11. В каком порядке нужно располагать записи в файле HOSTS - упорядоченными по какому-либо параметру или произвольно?

Лабораторная работа № 6. Создание домена Windows Server 2003

Цели работы:

научиться создавать домен Windows Server 2003;

научиться устанавливать службу каталога Active Directory;

изучить структуру службы каталога Active Directory.

Связь с проектом

Для централизованного управления факультетской сетью необходимо создать домен на основе Microsoft Windows Server 2003.

Примечание. В процессе установки может потребоваться вставить в дисковод установочный компакт-диск Windows Server 2003. Можно использовать физический компакт-диск или /ло-образ установочного диска операционной системы.

Задание 1. Установить на сервере службу каталога Active Directory, создать домен mydomain.ru.

Указания к выполнению

Запустите мастер установки Active Directory Start - Run - dcpromo.

Следуя шагам мастера установки, выберите следующие параметры установки:

в окне Domain Controller Type (Тип контроллера домена) - переключатель Domain controller for a new domain (Контроллер домена в новом домене);

в окне Create New Domain (Создать новый домен) - переключатель Domain in a new forest (Домен в новом лесу);

в окне Install or Configure DNS (Установка или настройка DNS) - переключатель No, just install and configure DNS on this computer (Нет,

DNS уже установлена и настроена на этом компьютере), если служба DNS уже установлена на сервере, или Yes, I will configure the DNS client (Да, я буду конфигурировать клиента DNS);

в окне New Domain Name (Новое доменное имя) наберите mydomain.ru в строке Full DNS Name For New Domain (Полное DNS-имя нового домена);

в окне NetBIOS Domain Name (Доменное имя NetBIOS) должна появиться запись MYDOMAIN;

убедиться, что для размещения базы данных и протокола выбран путь C:\WINDOWS\NTDS, а для размещения каталога SYSVOL указан путь C:\WINDOWS\SYSVOL;

в окне Permissions (Разрешения) выберите Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems (Разрешения, совместимые только с операционными системами Windows 2000 или Windows Server 2003);

в окне Directory Services Restore Mode Administrator Password (Пароль администратора для режима восстановления) введите пароль, который хотите присвоить этой учетной записи сервера Administrator в случае, если компьютер загрузится в режиме Directory Services Restore (Режим восстановления);

в окне Summary (Сводка) изучите список выбранных вами параметров установки и дождитесь завершения процесса установки Active Directory.

3. В окне Completing The Active Directory Installation Wizard (Завершение работы мастера установки Active Directory), щелкните кнопку Finish (Готово), а затем кнопку Restart Now (Перезагрузить компьютер сейчас).

Задание 2. Просмотреть созданный домен одним из способов.

Указания к выполнению

1-й способ.

Откройте My Network Places - Entire Network - Microsoft Windows Network (Мое сетевое окружение - Вся сеть - сеть Microsoft Windows).

Убедитесь, что появилась запись о домене mydomain, в котором содержится один компьютер - Server.

2-й способ.

В меню Start - Programs - Administrative Tools (Пуск - Программы - Администрирование) выберите Active Directory Users And

Computers (Пользователи и компьютеры Active Directory). Откроется одноименная оснастка.

В дереве оснастки дважды щелкните на mydomain.ru (или на имени вашего домена), чтобы увидеть содержимое узла mydomain.ru.

В разделе Domain Controllers (Контроллеры домена) дерева оснастки просмотрите название контроллера домена и его полное имя DNS (например, если имя изолированного сервера было server, то после установки домена должно стать server.mydomain.ru).

В разделе Users (Пользователи) просмотрите список встроенных учетных записей пользователей и групп пользователей домена.

Активизируйте встроенную учетную запись Guest (Гость) и попробуйте войти в систему. Удалась ли попытка сделать это? На контроллеры домена разрешен вход только администраторам домена.

Закройте консоль Active Directory Users And Computers.

^ Сохраните в отчет скриншоты по результатам обоих способов.

Задание 3. Проверить работу службы DNS с помощью оснастки DNS.

Указания к выполнению

Откройте консоль DNS командой Start - Programs - Administrative Tools - DNS (Пуск - Программы - Администрирование - DNS).

В дереве консоли DNS щелкните правой кнопкой по имени вашего сервера и выберите команду Properties (Свойства). Откроется окно свойств SERVER (если у сервера другое имя, то в заголовке окна будет значиться оно).

Перейдите на вкладку Monitoring (Наблюдение).

В списке Select A Test Type (Выберите тип теста) пометьте флажки A Simple Query Against This DNS Server (Простой запрос к этому DNS- серверу) и A Recursive Query To Other DNS Servers (Рекурсивный запрос к другим DNS-серверам) и щелкните Test Now (Протестировать). В окне свойств Server в списке результатов тестирования должна появиться надпись PASS (Пройден успешно) или FAIL (Не пройден) - в столбцах Simple Query (Простой запрос) и Recursive Query (Рекурсивный запрос). Объясните полученные результаты.

Задание 4. Удалить службу Active Directory.

Указания к выполнению

Запустите мастер установки и удаления Active Directory Start - Run - dcpromo.

Самостоятельная работа

Согласно заданию проекта установите домен с именем faculty.ru, где контроллером домена является server.faculty.ru, IP-адрес которого 192.168.1.1.

^ Отразите в отчее с помощью скриншотов все этапы установки.

Контрольные вопросы

1. Опишите различия между рабочей группой и доменом.
2. Каково основное различие между ОС Windows XP и Windows Server 2003?
3. Возможно ли создать домен в сети, где все компьютеры сети работают под управлением ОС Windows XP?
4. Дайте определение контроллера домена.
5. Перечислите известные Вам встроенные учетные записи пользователей и групп пользователей домена и опишите их назначение.
6. Что означает термин «изолированный» сервер?
7. Опишите различия между рабочей группой и доменом.
8. Почему встроенная учетная запись Guest (Гость), как правило, бывает отключена?

Лабораторная работа № 7. Создание и администрирование учетных записей пользователей и групп

Цели работы:

научиться создавать, изменять удалять учетные записи и группы;

научиться задавать и изменять пароли;

научиться добавлять учетные записи в группы.

Связь с проектом

Требования проекта для пользователей и групп пользователей приведены во введении к лабораторному практикуму.

Задание 1. Создайте доменную учетную запись декана:

имеет доступ ко всем ресурсам сети,

может осуществлять вход на любой компьютер.

Указания к выполнению

Выполните команду Start - All Programs - Administrative Tools - Active Directory Users and Computers (Пуск - Программы - Администрирование - Пользователи и компьютеры Active Directory).

Раскройте папку faculty.ru в левой панели окна. Во вложенных папках выберите Users (Пользователи).

В меню Action (Действие) выберите команду New - User (Содать - Пользователь).

Введите необходимые сведения о пользователе. В разделе User logon name (Имя пользователя при входе в систему) введите dean (декан). Обратите внимание на то, что при создании доменной учетной записи, в отличие от локальной, после имени пользователя отображается имя домена, отделенное от последнего знаком @. Таким образом, полное имя пользователя (User logon name) - dean@faculty.ru.

При определении пароля пользователя обязательно установите флажок User must change password at next logon (Пользователь должен сменить пароль при следующем входе в систему).

Завершите создание учетной записи.

В правой панели найдите учетную запись. Дважды щелкните по ней, чтобы внести дополнительные сведения (адрес, организация и т. д.).

Убедитесь в том, что декан может входить в систему в любое время (вкладка Account - Logon Hours (Учетная запись - Часы входа)).

Попробуйте войти в домен под учетной записью декана. Почему попытка не удалась?

Запишите в отчет причину отказа.

10.Зарегистрируйтесь в системе как администратор.

Посмотрите свойство учетной записи декана, снова выполнив команду Start - All Programs - Administrative Tools - Active Directory Users and Computers. В окне свойств учетной записи выберите вкладку Member of (Членство в группах) и добавьте учетную запись декана в глобальную группу Администраторы домена с помощью следующих команд Add... - Advanced... - Find now... (Добавить... - Дополнительно... - Найти...) из полученного списка выберите Domain Admins (Администраторы домена).

Повторите попытку войти в домен под учетной записью декана.

После входа в систему под учетной записью администратора смените пароль декана и снова задайте необходимость смены пароля при следующем входе в систему.

Внесите в отчет скриншоты окон для пунктов 5, 8, 9, 13.

Задание 2. В соответствии с требованиями политики безопасности сети, в группу администраторов не рекомендуется включать других пользователей домена, кроме лиц, непосредственно выполняющих функции администрирования. Исключите учетную запись декана из группы администраторов.

Указания к выполнению

Выполните команду Start - All Programs - Administrative Tools - Active Directory Users and Computers.

Раскройте папку faculty.ru в левой панели окна. Во вложенных папках выберите Users.

В правой панели найдите учетную запись. Дважды щелкните по ней, и перейдите на вкладку Member of (Членство в группах). Среди списка групп выберите Domain Admins и нажмите Remove.

"23ч Внесите в отчет скриншот окна, запрещающего вход в домен.

Задание 3. Разрешить учетной записи декана осуществлять вход на контроллер домена, не включая его в группу администраторов.

Указания к выполнению

Добавить учетную запись декана в группу Print Operators, члены которой могут осуществлять вход на контроллер домена.

Войдите в домен под учетной записью декана

Предложите другой способ, разрешающий вход на контроллер домена.

"ЙЭк Внесите в отчет скриншот окна главного меню после входа декана на контроллер домена. Опишите другой способ разрешения входа на контроллер домена декану.

Задание 4. Создайте глобальную группу Teachers (Преподаватели):

тип группы - группа безопасности;

преподаватели могут осуществлять вход на любой компьютер сети, кроме сервера;

для каждого из преподавателей существует собственная учетная запись и настройки, которые конфигурируется лично преподавателем.

Указания к выполнению

Выполните команду Start - All Programs - Administrative Tools - Active Directory Users and Computers.

Раскройте папку faculty.ru в левой панели окна. Во вложенных папках выберите Users.

В меню Action выберите команду New - Group (Новое - Группа).

В поле Group Name (Имя группы) введите Teachers.

В области Group Scope (Область действия группы) щелкните переключатель Global (Глобальная), а в области Group Type (Тип группы) - переключатель Security (Безопасность).

Щелкните ОК.

Задание 5. Добавьте в группу Teachers (Преподаватели) члена группы - учетную запись декана.

Указания к выполнению

Убедитесь, что открыта оснастка Active Directory Users and Computers и выбран контейнер Users.

В окне свойств группы Teachers выберите вкладку Members (Члены группы), а затем последовательно кнопки Add... - Advanced... - Find now...

из полученного списка выберите учетную запись декана.

В окне свойств учетной записи декана найдите информацию о членстве в группе Teachers.

Внесите в отчет скриншот соответствующего окна.

Самостоятельная работа

Задание 1. Составьте списки встроенных локальных, глобальных доменных, локальных доменных групп и изучите описание каждой встроенной группы.

Задание 2. Заполните таблицы, содержащие сведения о членах домена. Таблицы должны помогать планировать и создавать учетные записи домена.

Пример заполнения таблиц для группы пользователей Деканат и учетной записи Студент смотрите ниже.

Таблица 1. Планирование групп

Группа пользователей	Тип группы	Количество членов группы	Полное имя пользователей группы
Деканат	Глобальная	4	Сидоров Иван Петрович Иванов Петр Петрович Соболева Елена Анатольевна Смирнова Надежда Владимировна

Таблица 2. Расписание входа в систему

Полное имя пользователя	Имя пользователя для входа в систему	Членство в группах	Когда пользователю разрешен вход в систему	С каких компьютеров пользователю разрешен вход в систему

Сидоров Иван Петрович	dean	Деканат Преподаватели Print Operators	В любое время	Все компьютеры домена
Иванов Петр Петрович	grishin	Деканат Преподаватели	В любое время	Все компьютеры, кроме контроллера домена
Студенты	student		Рабочие дни 7.30-21.30 Запрет - воскресенье	

Таблица 3. Планирование паролей

Имя входа пользователя	Пользователь должен сменить пароль при следующем входе в систему	Возможность изменять свой пароль	Срок действия пароля	Пароль
dean	Да	Да	Не ограничен	weerwtbjh
ivanov	Да	Да	60 дней	fhfhgouut
student	Нет	Нет	Не ограничен	

Придумайте не менее трех пользователей из каждой группы и в соответствии с требованиями проекта заполните таблицы 1-3. Внесите таблицы в отчет.

Задание 3. Создайте в соответствии со своими вариантам таблиц 1-3 необходимые по заданию проекта учетные записи пользователей и групп пользователей.

"ЙЭк Внесите в отчет скриншот раздела Users оснастки Active Directory Users and Computers.

Задание 4. Проведите тестирование учетных записей. Например, измените системное время на 6.00 и попытайтесь войти в домен под учетной записью студента. Попытайтесь сменить пароль данной учетной записи.

Внесите в отчет описание проводимых тестов и соответствующие им скриншоты окон выдаваемых сообщений.

Контрольные вопросы

1. Опишите различия между локальной и доменной учетными записями.
2. С какой целью создают группы пользователей?
3. Объясните назначение локальных, глобальных и универсальных групп.
4. Объясните назначение групп безопасности и групп распространения.
5. Дайте определение и приведите примеры для следующих терминов: «права пользователей», «привилегии пользователей», «разрешения доступа пользователей».
6. Перечислите известные вам встроенные учетные записи пользователей и групп пользователей домена и опишите их назначение.
7. В какую встроенную группу пользователей, отличную от группы администраторов, нужно включить учетную запись, чтобы пользователь мог осуществлять вход на рабочую станцию? Существуют ли другие способы сделать это?
8. Как запретить вход в систему в выходные дни и нерабочее время?
9. Как ограничить срок действия учетной записи?
10. Как отключить учетную запись сотрудника, например, во время его болезни?
11. Назовите длину пароля минимально рекомендуемую и максимально возможную.
12. Как изменить пароль пользователя?
13. Как запретить изменение пароля пользователем?
14. Каковы последствия удаления группы?

Лабораторная работа № 8. Присоединение компьютеров к домену. Публикация ресурсов в Active Directory

Цели работы:

научиться присоединять компьютеры к домену;
изучить способы публикации ресурсов;
научиться задавать и изменять права доступа;
запускать приложения от имени другого пользователя.

Связь с проектом

Кроме пользователей членами домена являются компьютеры. Вы должны обеспечить подключение всех компьютеров факультета к домену faculty.ru.

Основной целью создания компьютерной сети является совместное использование ресурсов. В факультетской сети основным видом ресурсов являются файлы и папки. Их следует предоставить в общий доступ. Для предотвращения конфликтных ситуаций администратору следует назначить всем пользователям домена права доступа к общим ресурсам, соответствующие их полномочиям.

Задание 1. Задайте следующие сетевые параметры рабочей станции:

имя рабочей станции - userl;

IP-адрес назначьте из той же подсети, что и контроллер домена (если не работает сервер DHCP).

Задание 2. Убедитесь в возможности установления связи между контроллером домена и рабочей станцией.

Поместите в отчет скриншот, в котором отражено подтверждение установления связи между компьютерами.

Задание 3. Включите рабочую станцию в домен.

Рассмотрим процесс на примере включения рабочей станции userl в домен faculty.ru

Указания к выполнению

1. Для присоединения компьютера к домену на рабочей станции следует открыть окно System Properties (Свойства системы), выполнив одну из команд Settings (Настройка) - Control Panel (Панель управления) - System (Система) или вызвать из контекстного меню окно свойств папки My Computer (Мой компьютер).

Перейдите на вкладку Computer Name (Имя компьютера).

Выберите Network ID (Идентификация). Откроется мастер сетевой идентификации Network Identification Wizard. Нажмите Next (Далее).

На вкладке Connecting to the Network (Подключение к сети) выберите This computer is part of a business network, and I use it to connect to other computers at work (Компьютер входит в корпоративную сеть, и во время работы я использую его для соединения с другими компьютерами). На этой вкладке существует второй вариант. Какой? В каких случаях он применяется?

Выберите тип сети - My company uses a network with domain (Моя организация использует сеть с доменами).

В окне Network Information (Сетевая информация) изучите, какие сетевые параметры понадобятся.

В окне User Account and Domain Information (Сведения об учетной записи и домене) оставьте все без изменения. Нажмите Next.

В окне Computer Domain (Домен компьютера) запишите имя домена и узла - Computer name (Имя компьютера) - userl, a Computer domain (Домен компьютера) - faculty. Нажмите Next.

Появится окно, в котором нужно ввести имя и пароль учетной записи, которая имеет разрешение на добавление пользователей в домен. Например, в нашем случае это будут:

User name - Administrator

Password - пустой (или текущий пароль администратора)

Domain - faculty.ru

В окне User Account будет предложено добавить новых пользователей. Выберите переключатель Do not add user at this time (Не добавлять пользователей в это время).

Нажмите Finish (Готово) и перезагрузите компьютер.

Внесите в отчет скриншот окна Computer Name (Имя компьютера) рабочей станции.

Задание 4. На рабочей станции войдите в систему под одной из доменных учетных записей.

Внесите в отчет скриншоты окон Log on to Windows и главного системного меню после входа пользователя на рабочую станцию.

Задание 5. Откройте общий доступ к папке Users, расположенной на сервере. Папка будет служить для временного размещения файлов всех пользователей сети. В ней любой пользователь сети сможет сохранять свои файлы и папки, просматривать ее содержимое, но не должен иметь прав на изменение доступа к ней.

Указания к выполнению

Создайте на сервере папку UserDocs. Поместите в нее текстовый файл, содержащий ваши личные данные.

В контекстном меню папки выберите Sharing & Security... (Общий доступ и безопасность).

На вкладке Sharing (Доступ) выберите Share this folder... (Предоставить в общий доступ). В пункте Share name... (Имя папки общего доступа) наберите имя Студенты - под таким именем папка UserDocs будет доступна пользователям сети.

На вкладке Security (Безопасность) назначьте группам пользователей домена права чтения и записи на эту папку

(установите соответствующие флажки в столбце Allow (Разрешить)), но не разрешайте полный доступ.

Если в разделе Group or user names (Имена групп или пользователей) присутствуют не все учетные записи и группы, то их можно добавить помощью следующих команд Add... - Advanced... - Find now... (Добавить - Дополнительно - Найти). Из полученного списка выберите необходимые объекты доступа.

Внесите в отчет скриншот окна Security (Безопасность) с соответствующими установками для каждого пользователя домена.

Почему не рекомендуется устанавливать полный доступ на папку Студенты для пользователей домена? Запишите в отчет ответ.

Задание 6. Получите доступ к папке Студенты с рабочей станции домена.

Указания к выполнению

На рабочей станции войдите под любой доменной учетной записью.

Получить доступ к папке можно одним из следующих способов:

в сетевом окружении найдите папку Users;

выполните команду Start - Run (Пуск - Выполнить) и введите имя в формате \\<имя сервера>\<имя папки>. Например: \\server\users.

Убедитесь в том, что здесь вы сможете сохранять свои документы, изменять существующие, но вам отказано изменять права доступа на папку.

Внесите в отчет скриншот окна сообщения, запрещающего изменения прав доступа.

Задание 7. Подключите общую папку Студенты как сетевой диск G:.

Указания к выполнению

Войдите под учетной записью студента.

Откройте контекстное меню папки Студенты.

3. Воспользуйтесь командой My Network Places (Мое сетевое окружение) - Map Network Drive (Подключить сетевой диск).

Задание 8. Изучить использование команды Run As.

Указания к выполнению

Войдите на сервер под учетной записью администратора.

Поместите в папке Студенты с общим доступом приложение, ярлык программы или программу из Control Panel.

Запретите студенту доступ к данному объекту.

На рабочей станции войдите под учетной записью студента.

Откройте папку Студенты и попытайтесь открыть объект. Скопируйте в буфер окно, запрещающее доступ к объекту.

Выделите объект и, удерживая Shift, выберите в контекстном меню команду Run As (Запустить как).

Установите переключатель Run The Program As The Following User (Запустить программу от имени следующего пользователя).

В поле User name введите mydomain\Administrator, а в Password - пароль администратора. Нажмите ОК.

Запустите объект.

Внесите в отчет скриншоты окон:

запрещающее доступ к объекту,

Run As,

окно приложения или другого объекта после получения доступа к нему.

Задание 9. Удалите рабочую станцию из домена.

Указания к выполнению

На рабочей станции войдите под учетной записью администратора.

Вызовите окно свойств папки My Computer (Мой компьютер).

На вкладке Computer Name (Имя компьютера) нажмите Network ID (Идентификация).

На вкладке Connecting to the Network (Подключение к сети) выберите This computer is for home use and not a part of business network (Компьютер предназначен для домашнего использования и не входит в корпоративную сеть).

Внесите в отчет скриншот, запрещающий изменения прав доступа.

Предложите другой способ исключения рабочей станции из домена.

Самостоятельная работа

Задание 1. Включите в домен рабочую станцию compl.

Указания к выполнению

Переименуйте рабочую станцию userl в compl. Подключите станцию compl к домену.

Поместите в отчет скриншоты окон, в которых отражен каждый шаг процедуры включения рабочей станции в домен.

Задание 2. Создайте папки с общим доступом Документы, Задания, Отчеты. Установите для них разрешения согласно заданию проекта.

Внесите в отчет скриншоты окон Security (Безопасность) каждой папки с соответствующими установками для каждого пользователя домена.

Задание 3. Выполните проверку разрешений. Например, зарегистрируйтесь под разными учетными записями и попытайтесь получить к ним доступ.

Внесите в отчет описание проводимых тестов и соответствующие им скриншоты окон выдаваемых сообщений.

Контрольные вопросы

1. Как определить, является ли компьютер членом домена или рабочей группы?
2. Какие разрешения существуют для общих папок?
3. Как отменить наследование свойств объекта от родительской папки?
4. Может ли пользователь запретить доступ администратору к своей папке? Сможет ли администратор в этом случае вернуть права?
5. Опишите права субъектов доступа - Владелец и Администратор.
6. Какая утилита, не требующая смены пользователя, позволяет выполнять действия от имени другого пользователя?

Лабораторная работа № 9. Групповые политики

Цели работы:

изучить способы задания групповых политик;

изучить виды параметров групповых политик;

изучить объекты групповых политик;

научиться задавать групповые политики для разных объектов.

Связь с проектом

Групповые политики позволяют реализовать гибкое управление членами доменами - пользователями и компьютерами. В данной работе вам предстоит научиться использовать групповые политики и применять их для управления членами домена faculty.ru в соответствии с требованиями проекта.

Задание 1. Задайте в домене политику, в соответствии с которой на уровне всего домена при установке пароля пользователя требовалось бы следующее:

длина пароля - не менее 8 символов;

пользователь не может установить ни один из трех предыдущих паролей;

пароль должен отвечать требованиям сложности;

максимальный возраст пароля - 60 дней.

Указания к выполнению

Для запуска консоли управления MMC выполните команду Start - Run - mmc.

Для управления объектами групповой политики на уровне домена в консоли MMC добавьте оснастку Group Policy Object Editor командой File (Консоль) - Add (Добавить) - Remove Snap-in... (Добавить или удалить оснастку) - Add... (Добавить) и выберите из списка соответствующую оснастку.

Для определения объекта действия политики нажмите Browse... (Обзор...)

Изучите окно и перечислите объекты групповых политик.

Выберите Default Domain Policy. Нажмите Finish (Готово). В левом окне консоли должна появиться оснастка Default Domain Policy <имя контроллера домена> Policy.

Разверните оснастку и выберите Computer Configuration (Конфигурация компьютера) - Windows Settings (Конфигурация Windows) - Security Settings (Параметры безопасности) - Account Policies (Политики учетных записей) - Password Policy (Политика паролей).

Изучите политики паролей и установите настройки в соответствии с требованием задания.

Создайте нового пользователя и проверьте правильность настроек.

"23ч Запишите в отчет объекты групповых политик.

"23ч Внесите в отчет скриншот окна, отражающего установленные параметры политики.

Задание 2. Задайте политику на уровне всего домена, выполняющую блокировку учетных записей на 5 минут в том случае, если подряд было сделано не менее трех ошибок входа в систему.

Указания к выполнению

Соответствующая политика находится в следующем разделе: Computer Configuration (Конфигурация компьютера) - Windows Settings (Конфигурация Windows) - Security Settings (Параметры безопасности) - Account Policies (Политики учетных записей) - Account Lockout Policy (Политика блокировки учетной записи).

Проверьте правильность настроек политики путем нескольких попыток ввести неверный пароль пользователя на рабочей станции.

Зайдите на контроллер домена и разблокируйте учетную запись пользователя.

Внесите в отчет скриншоты окна, сообщающего о блокировке учетной записи на рабочей станции, и окно снятия блокировки.

Задание 3. Создайте организационное подразделение StudentSecurity.

Указания к выполнению

Выполните команду Start - Programs - Administrative Tools - Active Directory Users and Computers (Пуск - Программы - Администрирование - Пользователи и компьютеры Active Directory).

Раскройте папку faculty.ru в левой панели окна.

В меню Action выберите команду New - Organization Unit (Создать - Организационное подразделение).

В окне New Object - Organization Unit (Новый объект - Подразделение) в поле Name наберите StudentSecurity.

Поместите в организационное подразделение учетную запись студента.

Правой кнопкой щелкните по новому объекту, выберите Properties (Свойства) - Security (Безопасность).

Просмотрите список групп, обладающих правом доступа к подразделению StudentSecurity.

Внесите в отчет скриншоты окна свойств организационного подразделения.

Задание 4. Задайте политику на уровне организационного подразделения StudentSecurity, запрещающую менять картинку рабочего стола и загружающую общую для всех картинку.

Указания к выполнению

Откройте окно StudentSecurity.

Выполните команду User Configuration (Конфигурация пользователя) - Administrative Templates (Административные шаблоны) - Desktop (Рабочий стол) - ActiveDesktop, выберите параметр, запрещающий изменение картинки и задайте общую картинку рабочего стола для всего подразделения.

Убедитесь в правильности настройки.

Самостоятельная работа

Сохраняйте в отчет скриншоты основных шагов.

Задание 1. Задайте на уровне организационного подразделения StudentSecurity следующие политики:

политика пароля, отличная от политики всего домена: длина пароля - не менее 0 символов, пароль не должен отвечать требованиям сложности, срок действия пароля не ограничен;

запретить менять пароль при помощи окна, вызываемого при помощи Ctrl-Alt-Del;

убирать пункт меню Properties (Свойства) из контекстных меню My Computer и My Documents;

из меню Start (Пуск) уберите пункт Run и Help.

Задание 2. Создайте организационное подразделение TeachersSecurity. Разрешите подразделению добавлять рабочие станции, но запретите менять дополнительные параметры стека TCP/IP.

Задание 3. На уровне домена запретить доступ к папке Network Connections (Сетевые подключения).

Контрольные вопросы

1. Дайте определение групповой политики.
2. К каким объектам можно применить групповые политики?
3. Где расположен объект локальной групповой политики?
4. Приведите примеры нелокальных объектов групповой политики.
5. В чем разница между конфигурационными и пользовательскими параметрами?
6. Перечислите требования к сложному паролю.

Лабораторная работа № 10. Сетевой анализатор Network Monitor и сети VPN

Цели работы:

научиться работать с сетевым анализатором кадров Network Monitor;

научиться устанавливать и настраивать сети VPN.

Связь с проектом

Сетевой анализатор Network Monitor, входящий в состав Microsoft Windows Server 2003, используется для анализа и обнаружения проблем в локальной сети. Network Monitor позволяет вести журнал сетевой активности, копию которого можно отослать профессиональным сетевым аналитикам или в службу поддержки. Кроме того, разработчики сетевого программного обеспечения

применяют Network Monitor для мониторинга и отладки своих приложений.

Виртуальные частные сети (Virtual Private Networks, VPN) позволяют обеспечить безопасный доступ к ресурсам сети. Допустим, декан факультета захотел иметь защищенное соединение с сервером, т. е. такое соединение, сообщения по которому не могут быть прочитаны даже при перехвате сообщения. Решением данной задачи является настройка VPN.

Задание 1. Установить сетевой анализатор Network Monitor.

Указания к выполнению

Запустите виртуальную машину с Windows Server 2003. В панели управления (Start - Control Panel) выберите пункт Add or Remove Programs (Добавление или удаление программ). Щелкните кнопку Add/Remove Windows Components (Добавление/удаление компонентов Windows).

В окне Windows Component Wizard (Мастер компонентов Windows) выберите Management And Monitoring Tools (Инструменты управления и мониторинга) и щелкните кнопку Details.

В окне Management And Monitoring Tools пометьте флажок Network Monitor Tools (Инструменты Сетевого монитора) и щелкните ОК.

В окне Мастера компонентов Windows щелкните Next.

Задание 2. Выполните мониторинг сетевых кадров с помощью Network Monitor.

Указания к выполнению

1. Запустите Network Monitor: Start - All Programs - Administrative Tools - Network Monitor (Пуск - Программы - Администрирование - Сетевой монитор).

Запустите мониторинг кадров: меню Capture - Start (Захват - Старт) или клавиша F10.

Окно Network Monitor содержит следующие элементы (Рис. 5):

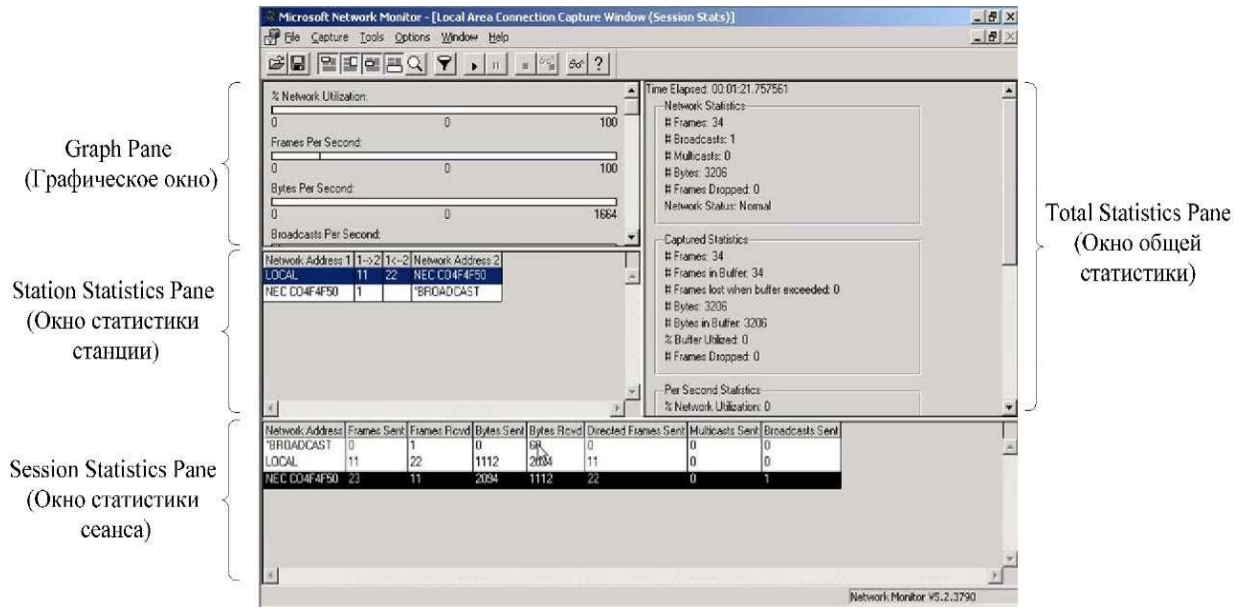


Рис. 5. Элементы окна Network Monitor

Network Monitor отображает общую статистику отслеживаемого трафика, в том числе следующую информацию:

сведения о широковещательных кадрах (Broadcast);

сведения о многоадресных кадрах (Multicast);

статистику использования сети;

количество полученных байт в секунду;

количество полученных кадров в секунду и т. д.

Запустите из командной строки утилиту ping и проверьте доступность физического компьютера:

ping 192.168.1.10

Остановите мониторинг в Network Monitor: меню Capture - Stop или клавиша F11. Просмотрите информацию о полученных кадрах: меню Capture - Display Captured Data (Захват - Просмотр собранных данных) или клавиша F12. В окне Summary (Общая информация) отобразится подробная информация обо всех собранных кадрах. Двойной щелчок на любом кадре откроет подробную статистику по этому кадру (рис. 6).

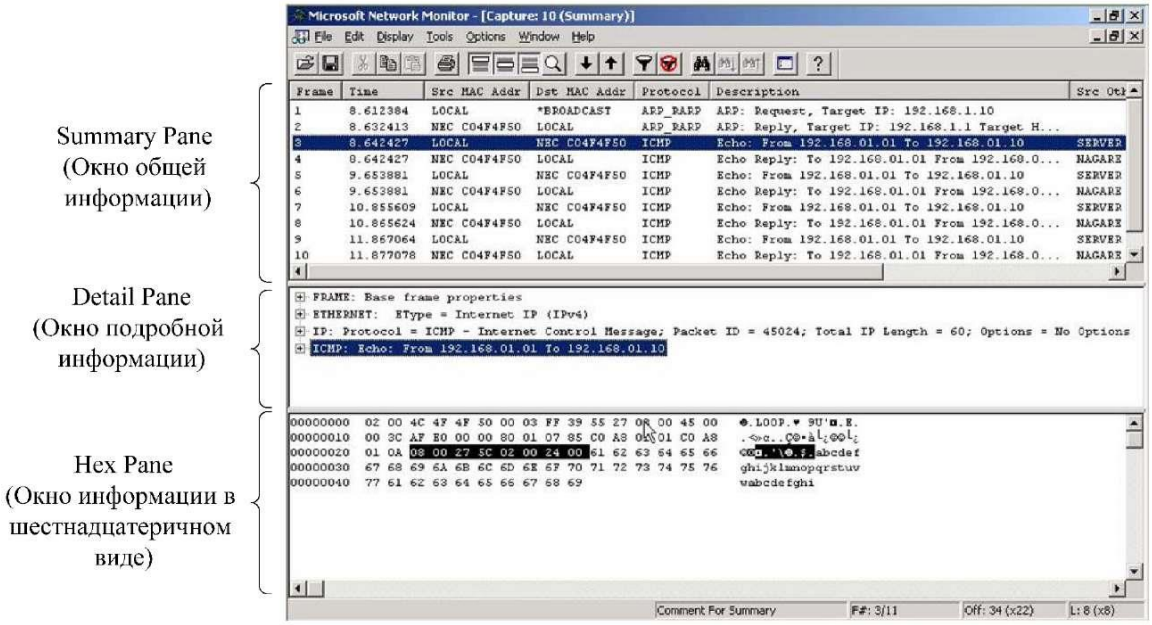


Рис. 6. Элементы окна Summary

В окне Summary Pane (Окно общей информации) отображается:

Frame - номер кадра;

Time - время захвата кадра;

Src MAC Addr - MAC-адрес источника;

Dst MAC Addr - MAC-адрес приемника;

Protocol - протокол, передавший кадр;

Description - описание кадра;

Src Other Addr - имя источника;

Dst Other Addr - имя приемника;

Type Other Addr - тип протокола нижнего уровня.

На рисунке видно, что Network Monitor захватил 10 кадров:

Первый кадр - широковещательный ARP-запрос на разрешение указанного в ping IP-адреса.

Второй кадр - ARP-ответ на запрос, содержащий требуемый IP-адрес.

Следующие восемь кадров - эхо-пакеты протокола ICMP и ответы на них.

Задание 3. Перехват текстовых сообщений.

Указания к выполнению

1. С помощью Network Monitor можно просматривать информацию, передаваемую по сети, если она незашифрована. В этом задании осуществим отправку текстового сообщения с помощью команды net send и перехватим её, используя Network Monitor.

Запустите мониторинг кадров в Network Monitor.

Из командной строки на сервере отправьте текстовое сообщение на клиентский компьютер с помощью команды net send:

net send 192.168.1.10 Hello!

После передачи сообщения остановите мониторинг кадров. Откройте окно Summary для просмотра собранных кадров:

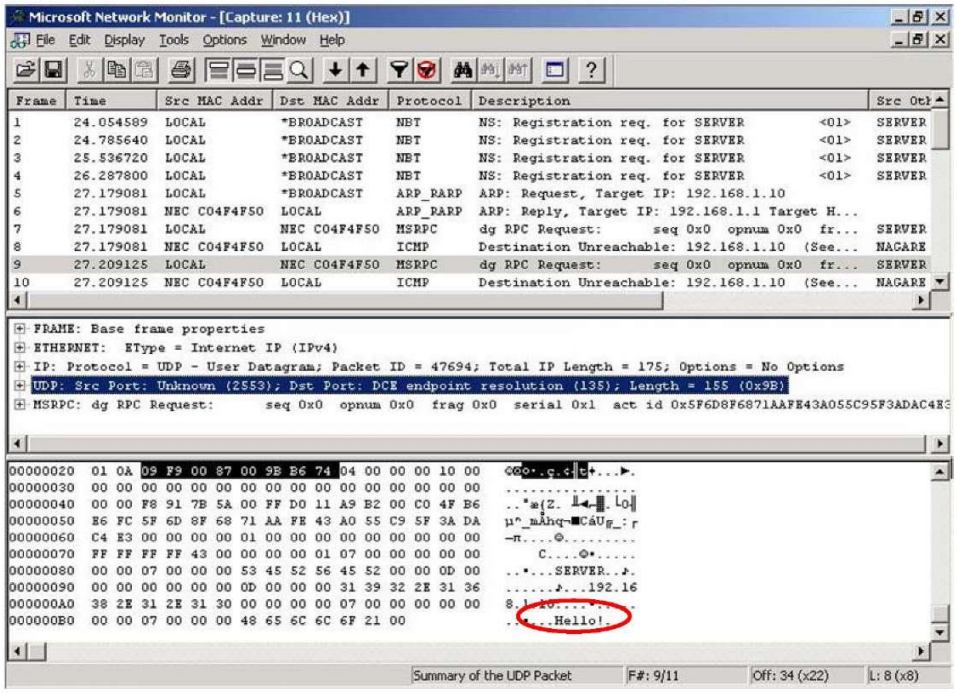


Рис. 7. Перехват текстового сообщения

На рис. 7 видно, что в одном из кадров можно прочитать посланное сообщение.

Если сообщение не удалось отправить, это свидетельствует, скорее всего, о том, что на сервере по умолчанию отключена служба Messenger (служба сообщений). Чтобы включить службу, откройте оснастку Services (Службы): Start - All Programs - Administrative Tools - Services. Найдите службу Messenger, щелкните по ней два раза, выберите в списке Startup type (Тип запуска) тип Manual (Вручную), нажмите кнопку Apply (Применить). Затем нажмите кнопку Start и кнопку ОК. Попробуйте послать сообщение ещё

Задание 4. Установка сервера виртуальной частной сети (VPN). Указания к выполнению

1. В предыдущем задании мы убедились, что передача текстовой информации в незашифрованном виде по открытым сетям небезопасна.

Решением данной проблемы является организация виртуальных частных сетей VPN.

Установите VPN-сервер. Для этого следует открыть оснастку Routing and Remote Access (Маршрутизация и удаленный доступ): Start - All Programs - Administrative Tools - Routing and Remote Access.

В контекстном меню сервера выберите пункт Configure and Enable Routing and Remote Access (Сконфигурировать и активировать маршрутизацию и удаленный доступ). В окне мастера Routing and Remote Access Server Setup Wizard выберите пункт Custom configuration (Конфигурация пользователя). Установите флажок VPN access (Доступ VPN). На предложение запустить службу нужно ответить Yes (Да).

Итак, VPN-сервер установлен и запущен. Сейчас следует установить диапазон IP-адресов, которые VPN-сервер может назначать VPN-клиентам. В контекстном меню сервера выберите пункт Properties (Свойства). Перейдите на вкладку IP, выберите Static address pool (Диапазон статических адресов). Нажмите кнопку Add (Добавить), введите начальный и конечный адреса диапазона, например 192.168.2.1 - 192.168.2.10 и нажмите ОК.

Следующим шагом будет активизация возможности удаленного подключения у одной из учетных записей. Откройте оснастку Active Directory Users and Computers (Пользователи и компьютеры Active Directory), выберите любую из существующих учетных записей (например, Administrator (Администратор)). В контекстном меню учетной записи выберите пункт Properties (Свойства), перейдите на вкладку Dial-in (Коммутируемый доступ), в разделе Remote Access Permission (Dial-in or VPN) (Разрешение удаленного доступа (коммутируемый или VPN)) выберите пункт Allow access (Разрешить доступ), щелкните ОК.

Задание 5. Настройка VPN-клиента.

Указания к выполнению

Для получения доступа к ресурсам удаленного компьютера следует настроить клиента VPN. Запустите виртуальную машину с Windows XP (те же действия при наличии разрешений можно выполнять на физическом компьютере).

Откройте окно сетевых подключений (Пуск - Панель управления - Сетевые подключения). Слева в разделе Сетевые задачи выберите Создание нового подключения. В Мастере новых подключений выберите Подключить к сети на рабочем месте, затем - Подключение к виртуальной частной сети.

В следующем окне введите название для подключений (например, «VPN»). Затем нужно выбрать Не набирать номер для предварительного подключения. В следующем окне следует ввести IP-адрес VPN-сервера (192.168.1.1). Нажмите кнопку Готово. VPN-клиент настроен.

Для подключения к VPN-серверу откройте созданное подключение и введите в поле имени пользователя имя той учетной записи, которой вы разрешили доступ к VPN-серверу. Если задан пароль, введите его. Нажмите кнопку Подключение. Если все правильно, должно установиться VPN- подключение, а в правом нижнем углу экрана должен появиться значок подключения.

4. Проверьте параметры подключения. Для этого в контекстном меню подключения выберите пункт Состояние. Перейдите на вкладку Сведения и выпишите параметры Тип сервера, Проверка подлинности, IP-адрес сервера и IP-адрес клиента. Убедитесь, что оба адреса принадлежат тому диапазону, который вы назначили на VPN-сервере.

Задание 6. Попытка перехвата сообщения в VPN-подключении.

Указания к выполнению

На виртуальной машине с Windows Server 2003 запустите мониторинг кадров в Network Monitor.

Передайте текстовое сообщение на VPN-клиент с помощью команды net send. Используйте IP-адрес клиента, выписанный с вкладки Сведения VPN-подкпючения, например:

net send 192.168.2.2 Hello!

После передачи сообщения остановите мониторинг в Network Monitor. Перейдите в окно Summary и попытайтесь найти ваше текстовое сообщение. По результатам сделайте выводы.

Самостоятельная работа

Сохраняйте в отчет скриншоты основных шагов.

Изучите возможности фильтрации кадров в Network Monitor (меню Capture - Filter). Настройте следующие фильтры:

захват кадров только между сервером и физическим компьютером;

захват кадров только по протоколу ARP.

Передайте небольшой текстовый файл с расширением txt в сети без VPN (например, пользуясь проводником Windows). Попробуйте его перехватить с помощью Network Monitor.

Настройте доступ к серверу по VPN учетной записи декана факультета.

Каким образом для соединения VPN можно выбрать тип используемого протокола аутентификации? Скриншот соответствующего окна поместите в отчет.

Контрольные вопросы

1. Для каких целей используется сетевой анализатор Network Monitor?
2. Какие виды фильтров позволяет применять Network Monitor?
3. Для чего служит VPN?
4. Назовите протоколы аутентификации, применяемые в VPN.
5. Каким образом в соединении VPN можно выбрать протокол соединения - PPTP или L2TP?
6. Как защищаются пакеты, передаваемые по VPN?

Литературные источники

1. Коннов, Н. Н. Анализ сетевых протоколов : лаб. практикум по курсу «Сети ЭВМ и телекоммуникации» / Н. Н. Коннов, В. Б. Механов. – Пенза :Изд-во ПГУ, 2010. – Ч. 1. – 68 с.
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 4-е изд. – СПб. : Питер, 2010.
3. Уилсон, Э. Мониторинг и анализ сетей. Методы выявления неисправностей / Э. Уилсон. – М. : ЛОРИ, 2002.

4. Филимонов, А. Протоколы Интернета / А. Филимонов. – СПб. : BHV-Санкт-Петербург, 2003.
5. Золотов, С. Протоколы Internet / С. Золотов. – СПб. : BHV-Санкт-Петербург, 1998.
6. Семенов, Ю. А. Telecommunication technologies – телекоммуникационные технологии (v3.3, 10 мая 2010 г.) / Ю. А. Семенов. – URL: http://book.itep.ru/
7. А.А. Кириченко / Вычислительные системы, сети и телекоммуникации: Практикум. / М., 2004. – 64с.
8. В.С.Микшина, Г.А. Еремеева, Н.Б. Назина и др.; Под ред. В.А. Острейковского / Лабораторный практикум по информатике: Учебное пособие для вузов / М.: Высш. шк., 2003. – 376с.: ил.
9. Программное обеспечение и Интернет-ресурсы:
10. http//www.citforum.ru/ (Новейшие компьютерные технологии)
11. http//www.iXBT.ru (Последние новости в компьютерном мире)
12. www.supercomputers.ru (Достижения суперкомпьютерной техники)
13. Технические средства и материально-техническое обеспечение дисциплины.
14. http://moodle.bgsha.com/course/view.php?id=32

Компьютерный набор произвел Никулин В.В.

Редактор Лебедева Е.М.

Подписано к печати Формат 60х84. 1/16. Бумага печатная
Усл.п.л. 3,56. Тираж 100 экз. Изд.№

Издательство Брянского государственного аграрного университета
243365, Брянская обл., Выгоничский район, п. Кокино, БГАУ