Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Эксплуатация объектов сетевой инфраструктуры

ЛЕКЦИИ

Пятигорск

Содержание

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними
«Ознакомление программой Virtual Box»

1. **Цель работы**: Освоить технологию создания новой виртуальной машины в **Virtual Box**.

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками и выбором параметров виртуальной машины в Virtual Box.
2. научить учащихся основным способам настройки виртуальной машины;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Сейчас многие хотят попробовать свои силы в изучении новой для них операционной системы, традиционно это Linux. Но не у всех есть желание установить её на компьютер параллельно с другой системой, или, же попросту человек не уверен в своих силах и боится чего-то сделать с жестким диском. И тут на помощь приходит класс программ под названием «виртуальные машины». Виртуальную машину, можно использовать для тестирования работоспособности своей программы, которая работает с записями из реестра, но поскольку может нарушиться работа системы, имеет смысл установить собственное творение на «виртуалку» и более спокойно экспериментировать там. Одной из таких машин является **Sun Virtual Box**.

Программа была создана компанией Innotek с использованием исходного кода Qemu. Первая публично доступная версия VirtualBox появилась 15 января 2007 года. В феврале 2008 года Innotek был приобретён компанией Sun Microsystems, модель распространения VirtualBox при этом не изменилась.

1 Возможности Virtual Box.

Программа Virtual Box позволяет эмулировать x86-совместимый ПК, на который можно установить большое число гостевых ОС, среди которых все семейство Windows, начиная с Windows 3.x и заканчивая Vista, DOS, Linux на основе ядра версий 2.4 и 2.6 и OpenBSD. Сама же виртуальная машина может предоставлять системе доступ в сеть,
позволять работать с периферийными устройствами. Помимо прочего стоит отметить достаточно удобные инструменты для обмена файлами. Есть возможность выбора языка интерфейса (поддерживается и русскоязычный интерфейс).

2 Запуск Virtual Box.

Запуск программы осуществляется выбором пунктов меню «Пуск»: Пуск — Все программы — Oracle VM VirtualBox — Oracle VM VirtualBox. Программа требует бесплатную регистрацию, которая заключается в простом вводе своего имени и E-mail, ее можно отменить.

4.3 Создание виртуальной машины.

Главное меню программы (рис. 1) состоит из трех пунктов:

- Файл
- Машина
- Справка

-

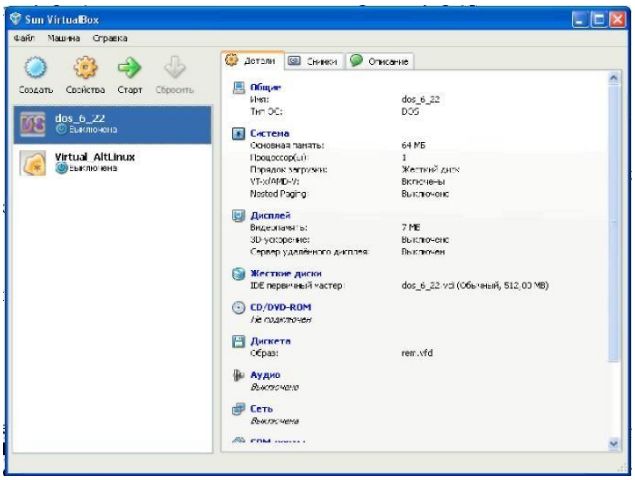


Рис. 1. Главное окно программы

Меню «Файл», в свою очередь, делится на «Менеджер виртуальных дисков», «Настройки» и «Выход».

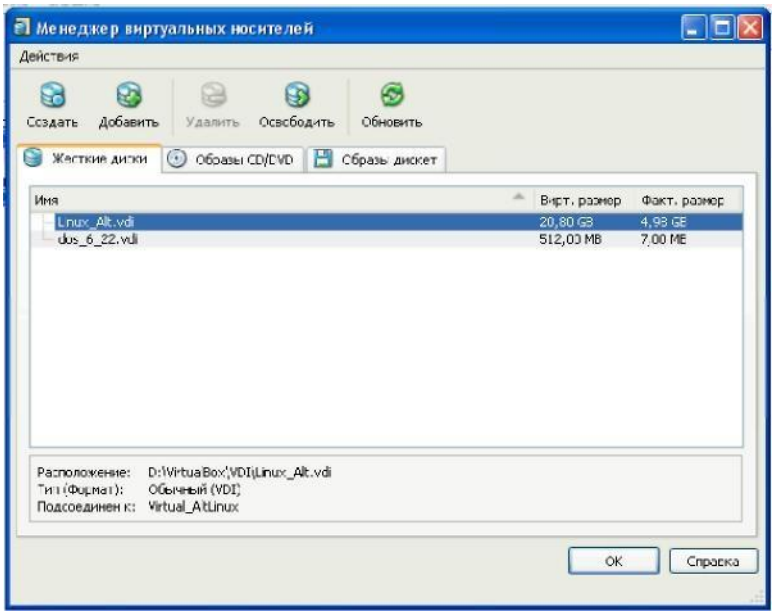


Рис. 2. Менеджер виртуальных дисков

Рассмотрим их поподробнее. Первый пункт - это менеджер виртуальных дисков (рис. 2), при помощи которого можно создавать, добавлять, освобождать или удалять «виртуалки». Также можно подключать образы CD/DVD для последующей установки системы из образа.

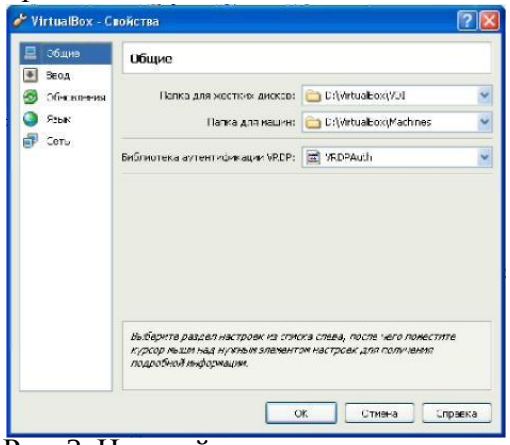


Рис. 3. Настройки

Второй пункт - это «Настройки» (рис. 3). Большого количества настроек здесь нет, но те, которые присутствуют, помогают настроить «индивидуальность» программы.

Также при помощи пункта **«Настройки»** можно выбрать так называемую хост-клавишу, ту клавишу, при нажатии на которую можно активизировать курсор Windows и впоследствии переключаться на другие запущенные программы (или просто открытые окна) в среде Windows. Еще в пункте **«Настройки»** можно выбрать язык программы.

Следующий пункт в Главном меню программы - это **«Машина»**. При помощи данного пункта можно управлять и следить за состоянием вашей виртуальной машины. Также при помощи данного пункта можно создать новую «виртуалку» (рис. 4).

Создание новой «виртуалки» происходит в режиме мастера. То есть делится на несколько регламентированных шагов при помощи которых и создается виртуальная машина.

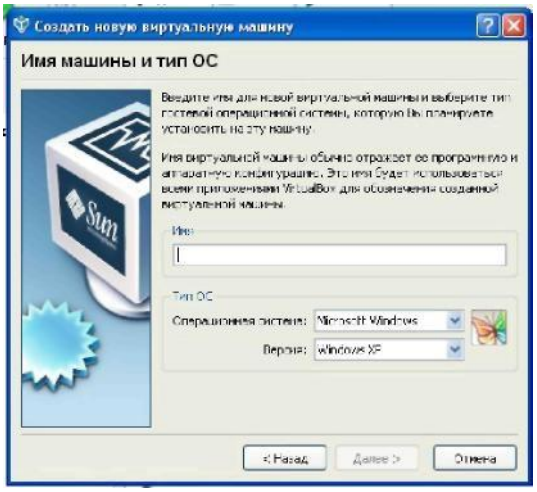


Рис. 4. Мастер создания новой виртуальной машины

Рассмотрим эти пункты:

- Выбор названия виртуальной машины и типа ОС;
- Выбор основной памяти для выделения виртуальной машине;
- Создание/подключение виртуального диска;
- Диалог с указанием успеха. После создания виртуального раздела общий вид программы меняется и становится

более функциональным.

В правой части окна можно посмотреть текущее состояние машины, а также наличие подключения CD/DVD привода, Аудио, Сети, USB. В тот момент, когда виртуальная машина неактивна, можно выбрать дополнительные параметры и свойства, нажав на кнопочку вверху окна по имени **«Свойства»**. Например, выбрать порядок загрузки, тип буфера (двунаправленный - из системы в виртуальную машину, или только внутри «виртуалки»).

Можно подключить звук из основной системы, который будет эмулироваться с помощью Windows Direct Sound. Можно включить контроллер USB.

Во время работы системы у каждого пользователя есть возможность делать так называемые снимки состояния системы. С возможным последующим откатом к раннему состоянию системы. Если во время работы с виртуальной системой у вас возникла необходимость срочно (или не совсем срочно) выйти из нее, то по нажатии на хост-клавишу и затем по нажатии комбинации **ALT+F4** можно выбрать один из пунктов завершения работы системы:

- Сохранить состояние машины;
- Послать сигнал завершения (равносильно завершению работы с последующим выключением компьютера в среде Windows);
- Выключить машину.

Удаление «виртуалки» не вызывает никаких трудностей. После выделения нужной

виртуальной машины нажимаете на кнопку **«Удалить»**, и вам задают следующий вопрос: хотите ли вы удалить текущую виртуальную машину? Если вы уверены, то нажимайте **«Удалить».**

Порядок работы

1. Внимательно ознакомьтесь с кратким и справочно-информационным материалом по теме занятия.
2. Создайте папки C:\HardDisks\<Ваш логин> и C:\Machines\<Ваш логин>.
3. Запустите VirtualBox.
4. Виберите пунк меню Файл — Настройки.
5. На вкладке Свойства, в разделе общие измените: а) Папка для жестких дисков — C:\HardDisks\<Ваш логин>; б) Папка для машин — C:\Machines\<Ваш логин>. Сохраните изменения.
6. Создайте новую виртуальную машину, со следующими параметрами: Имя: <Ваш логин>_lr1; Операционная система: Other; Версия: DOS; Память: 128 Мб; Загрузочный диск: Первичный (мастер), Создать новый жесткий диск; Динамически расширяющийся образ; Размер 2 Гб.
7. Измените параметры виртуального компьютера, на вкладке Детали. Порядок загрузки: Дискета, Жесткий диск; Аудио: Выключено, Сеть: Выключена, USB: Выключен.

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 2 «Прокладка кабеля UTP»

Цель работы: Получить представление о видах структурированных кабельных систем (СКС) и оборудовании, применяемом для их монтажа;

В процессе занятия решаются следующие задачи:

- Получить практические навыки монтажа кабельных систем на основе сетевых карт **Ethernet / FastEthernet**;
- Изучить назначение прямого и кроссированного соединения (**T568A** и **T568B**).

Краткие теоретические и справочно-информационные материалы по теме занятия.

Кабельная система (КС) – это совокупность линий связи и пассивного соединительного оборудования, предназначенная для передачи одного или нескольких типов сиг-налов. КС стандартизируются соответствующими типами документов: IEEE, ISO,

ГОСТ. Структурированные кабельные системы - особые КС, удовлетворяющие таким требованиям как модифицируемость, надежность, емкость. СКС делят на горизонтальные, вертикальные и сети кампуса (табл. 1).

Таблица 1

Вид КС	Назначение	Требования
Горизонтальная	Соединение устройств в пределах помещения/этажа	модифицируемость, надежность, универсальность
Вертикальная	Соединение ГКС в пределах здания	Емкость, надежность
Сеть кампуса	Соединение ВКС между зданиями	Емкость, надежность

К пассивному оборудованию горизонтальной кабельной системы относятся:
- линии связи (кабели);
- розетки;
- Patch-panel (фактически розетки с большим количеством портов);
- patch-cord (кабели с установленными на них вилками, соединяющие активное и пассивное оборудование);
- прочее оборудование (стойки и кроссы).

Основной тенденцией развития ГКС является рост универсальности систем. По одним и тем же каналам могут передаваться сигналы аналоговой и цифровой телефонии, компьютерные данные, сигнал сетей вещания, видеосигнал, сигналы сетей сигнализаций. Достигается эта возможность за счет применения промежуточного пассивного оборудования – кроссов и Patch-panel.

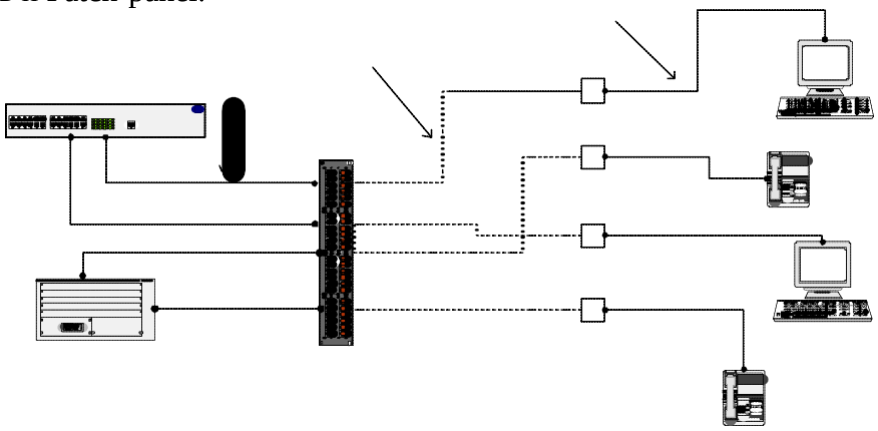
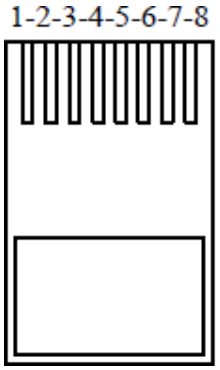


Рисунок 1

На рисунке 1 представлено использование одной кабельной системыдля соединения разнородного активного оборудования. Так, заменяя только патч-корды, мы по одним и тем же линиям передаем по нашему желанию или голосовой аналоговый трафик, или компьютерные данные. Причем эта конфигурация может изменяться произвольно. При необходимости могут соединяться отдельные порты на патч-панели, для непосредственного соединения активного оборудования. Патч-корд – кабель для соединения пассивного и активного оборудования.

Различают патч-корды для компьютерных сетей (8 контактов) с вилкой RJ45, для телефонных сетей с вилками RJ16 (4 контакта) и RJ11 (2 контакта). Термин «RJ45» ошибочно применяется к восьмиконтактному разъему 8P8C. На самом деле настоящий RJ45 физически несовместим с 8P8C, так как использует схему 8P2C. Однако, общеупотребительным является термин «RJ45».

Для распределения контактов внутри коннектора существуют два стандарта T568A и T568B. Порядок проводов по цветам представлен на рисунке 2.



T568A: БЗ-З-БО-С-БС-О-БК-К
T568B: БО-О-БЗ-С-БС-З-БК-К

Рисунок 2

В соответствии с этими стандартами разводятся кабели на патч- панелях и розетках.

Для соединения двух разнородных устройств (компьютера и коммутатора) используется прямое соединение, то есть используется один стандарт на окончаниях всех соединениях. Для соединения двух однородных устройств (компьютера и компьютера или коммутатора и коммутатора) используется перекрестное соединение, когда один раз по ходу линии используется соединение со сменой стандартов (А-В). Это может быть перекрестный патч-корд или перекрестное соединение розетки и патч-панели.

Порядок работы

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

Часть 1.1. Соединение компьютеров на физическом уровне

1. Определить, какой стандарт соединения требуется для связи двух **однородных устройств**, например, компьютеров.
2. Удалить внешнюю оболочку кабеля на длину **12-13 мм** (1/2 дюйма). В обжимном инструменте имеется специальный **нож и ограничитель**.
3. Расплести кабель и расположить провода для **перекрёстного** соединения.
4. Повернуть вилку **металлическими контактами вверх** или пластмассовым «хвостиком» вниз и вставить в неё кабель. Проверить **правильность расположения** проводов и зубьев каждого контакта.
5. Используя обжимной инструмент, обжать вилку с кабелем.
6. С помощью кабельного тестера **проверить правильность** соединения коннекторов.

Часть 1.2. Соединение компьютеров на физическом уровне с помощью пач-панели

1. На **рисунке 3** представлена схема сети, которую необходимо собрать.
2. Составить **план сети**, определив и отметив на плане стандарты соединений.
3. Используя монтажный инструмент, собрать сеть.
4. Соединить два компьютера собранной сетью. Признаком наличия соединения будут горящие **индикаторы Link** на сетевых адаптерах.
5. В случае если сеть не работает, использовать кабельный тестер для **локализации неисправностей**.

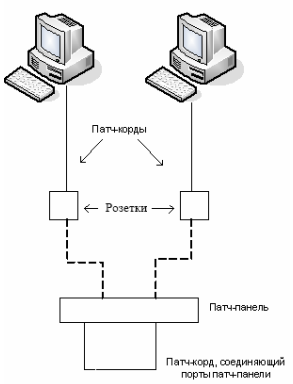


Рисунок 3

Часть 2. Разработка плана кабельной системы этажа (в соответствии с введенными стандартами)

Руководствуясь положениями из **СНИП 2.09.04-87**, по данному плану помещения определить положение сетевых розеток (локальная сеть, телефония). Исходя из соответствующих **стандартов**, составить схему проводки кабелей, установки розеток, а также таблицу спецификаций материалов.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Зачем нужна смена стандартов при соединении однородных устройств?
2. Чем отличаются стандарты витой пары категорий 5, 5e, 6, 7?
3. Заполнить таблицу параметров кабельных сегментов в соответствии с их типом и назначением:

Тип кабеля	Названия стандартов, регламентирующих применение данных линий связи (ISO/IEC)	Основные области применения	Максимальная длина кабельного сегмента для сетей Ethernet (без использования повторителя)
Коаксиальный кабель			
Оптоволоконный кабель			
Витая пара категории 5			
Витая пара категории 5e			
Витая пара категории 6			
Витая пара категории 7			

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

«Установка и настройка файервола KerioWinRoute ox»

Цель работы: Научиться устанавливать и настраивать Kerio WinRoute Firewall

В процессе занятия решаются следующие задачи:

1. познакомить с основными настройками и выбором Kerio WinRoute Firewall.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Kerio WinRoute Firewall - пакет маршрутизации и обеспечения сетевой безопасности. Предназначен для защиты от внешних атак и вирусов и дает возможность ограничения доступа к вебсайтам, в зависимости от их содержания. В состав пакета входят программный маршрутизатор, брэндмауэр (файрвол), прокси-сервер, URL filter (позволяющий запретить посещение определенных Web-страниц) и т.д.

Kerio WinRoute Firewall дает возможность точно настраивать правила для проверки входящего и исходящего трафика с учетом состояния протокола, обеспечивая при этом полную безопасность. Kerio WinRoute Firewall предоставляет возможность сканирования входящего и исходящего HTTP и FTP трафика на наличие вирусов. Кроме встроенной в версию защиты McAffee, доступно еще несколько антивирусов, на выбор.

Kerio WinRoute Firewall дает возможность параллельно использовать H.323 и SIP протоколы для того, чтобы не афишировать в Интернете инфраструктуру VoIP. Проверка протоколов помогает использовать некоторые приложения с протоколами, не предназначенными изначально для работы с firewall, в защищенных локальных сетях. Большинство протоколов можно сканировать, фильтровать или модифицировать, таким образом, повышая степень защиты.

Порядок работы

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

1. Настройка сетевых интерфейсов

Выбор IP-адресов для локальной сети (LAN)

Вы можете использовать следующие варианты при выборе адресов для вашей локальной сети:

- " публичные IP-адреса. Провайдер выделяет диапазон IP-адресов и устанавливает правила маршрутизации.
- " частные IP-адреса и IP-трансляция (NAT). Мы рекомендуем использовать данную опцию, так как это позволяет упростить администрирование и техническую поддержку.

Частные адреса представляют из себя специальные IP-диапазоны, зарезервированные для использования исключительно в локальных сетях (частные сети). Данные адреса не должны существовать в адресном пространстве сети Интернет (Интернет-маршрутизаторы обычно настраиваются на блокировку прохождения всех пакетов, содержащих эти адреса).

Для частных сетей зарезервированы следующие IP-диапазоны:

- 10.x.x.x, сетевая маска 255.0.0.0
- 172.16.x.x, сетевая маска 255.240.0.0
- 192.168.x.x, сетевая маска 255.255.0.0

Предупреждение: Не используйте другие адреса в частной сети, т.к. в этом случае некоторые веб-сайты (работающие на тех же адресах) могут быть недоступны.

В нашем примере для локальной сети используется адрес 192.168.1.0 и сетевая маска 255.255.255.0.

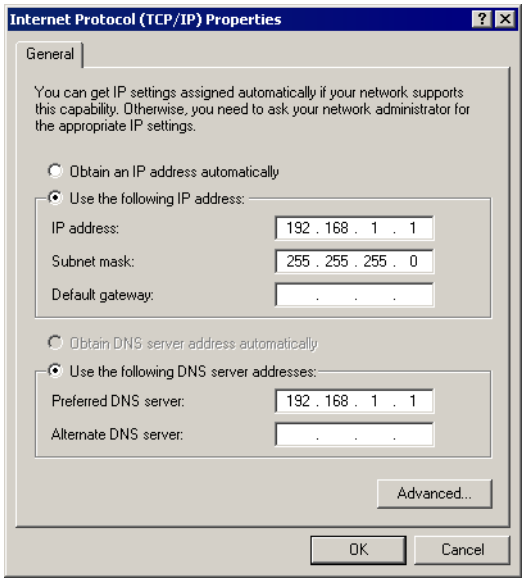
LAN-интерфейс

На LAN-интерфейсе должны быть сделаны следующие настройки:

- *IP address* — будет использоваться адрес 192.168.1.1
- *network mask* — 255.255.255.0
- *default gateway* —на данном интерфейсе параметр не должен быть установлен!
- *DNS server* — адрес DNS-сервера должен быть таким же, как и IP-адрес ин-

терфейса, подключенного к локальной сети, чтобы DNS-запросы между головным офисом и филиалами обрабатывались корректно а также дозвон по требованию с брандмауэра работал правильно.

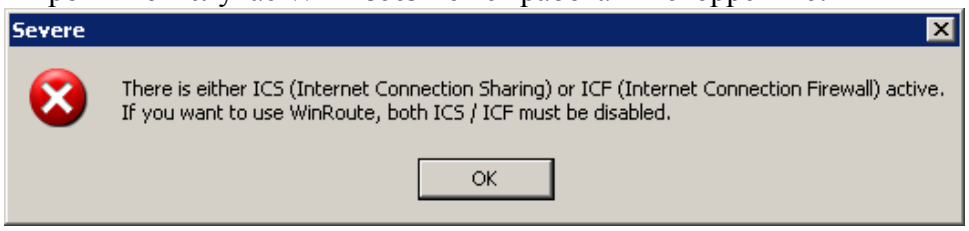
Укажите в параметре Preferred DNS server - 192.168.1.1



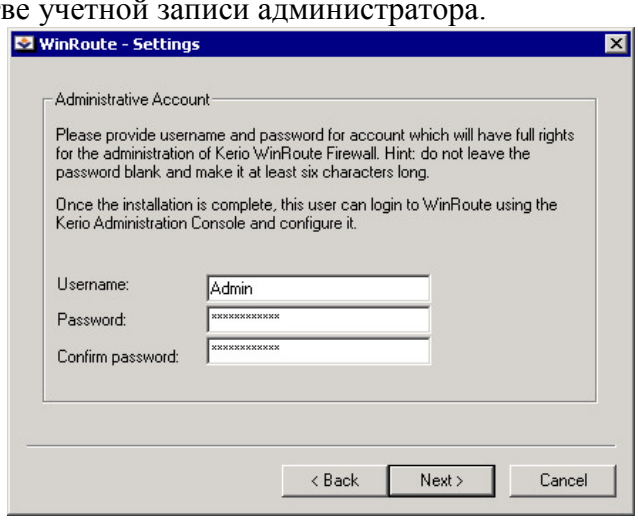
2. Установка WinRoute

Запустите файл установки WinRoute и выберите опцию Typical installation.

Отключите сервисы *Internet Connection Sharing* (Windows Me, 2000, XP) или *Internet Connection Firewall* (Windows XP), если таковые будут обнаружены инсталлятором, в противном случае WinRoute может работать некорректно.



Введите имя пользователя и пароль, которые будут использоваться в дальнейшем в качестве учетной записи администратора.



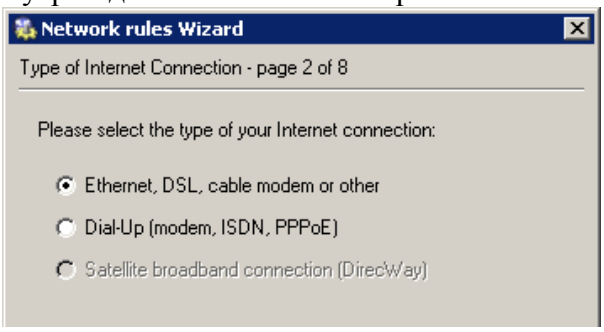
Перезагрузите компьютер после завершения процесса установки.

3. Базовая настройка политики трафика

После перезагрузки запустите консоль управления Kerio Administration Console

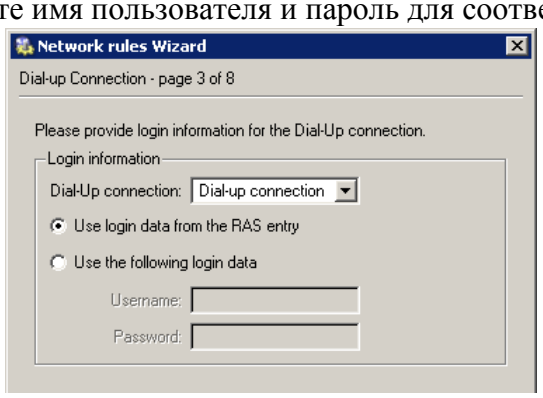
(Start / Programs / Kerio). Подключитесь к localhost (локальный компьютер), используя имя пользователя и пароль, заданные на этапе установки продукта. После первого входа в систему автоматически запустится мастер настройки сетевых правил Network Rules Wizard. Установите следующие параметры с помощью мастера:

- Тип Интернет-подключения (Шаг 2) - тип интерфейса, через который брандмауэр подключен к сети Интернет

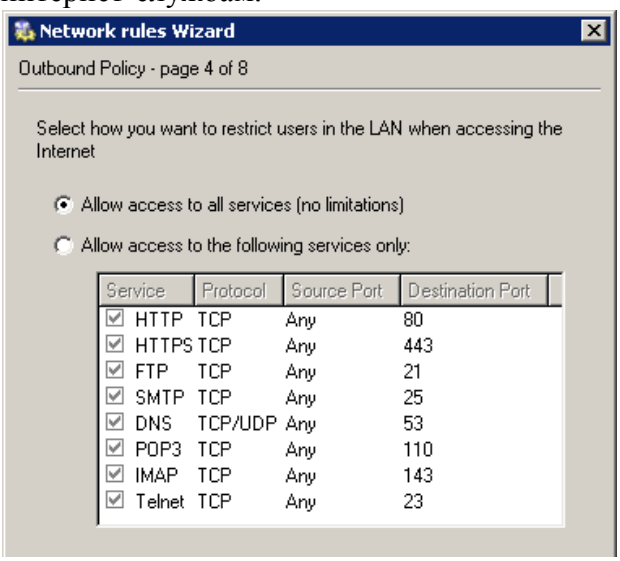


- Интернет-интерфейс (Шаг 3) - выберите Интернет-интерфейс или соответствующую запись диалап-соединения (в этом случае также необходимо указать имя пользователя и пароль).

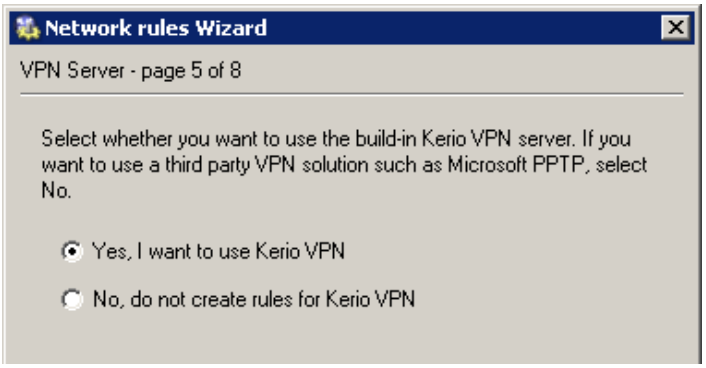
В случае диалап-соединения WinRoute требует указания соответствующего учетного имени пользователя и пароля. Указание этих данных необязательно в случае, если информация уже сохранена в операционной системе. Если нет (или вы не уверены, сохранена ли действительно данная информация), выберите опцию "Use the following login data" и укажите имя пользователя и пароль для соответствующей записи диалап-соединения.



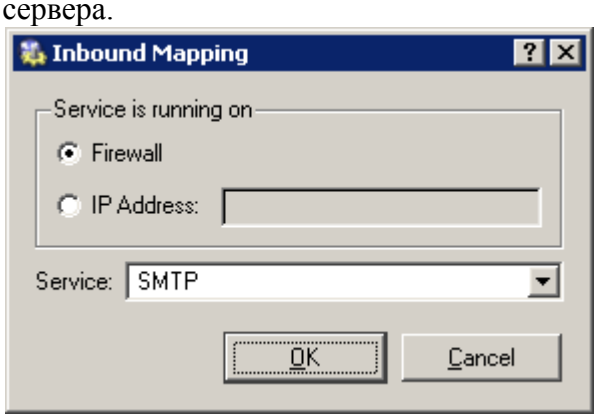
- Правила для исходящего трафика (Шаг 4) - данные правила разрешают доступ к интернет-службам.



- Политика *VPN-сервера* (Шаг 5) — выберите Yes, I want to use Kerio VPN для создания правил, разрешающих подключение мобильных пользователей и удаленных филиалов к головному офису

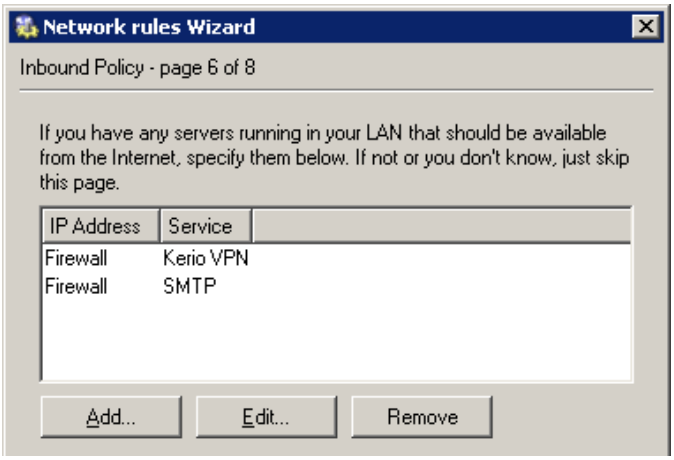


- Правила для входящего трафика (Шаг 6) — например, маппинг почтового SMTP сервера.



Примечание: На этом шаге вы можете также определить правила маппинга (подстановки портов, трансляции адреса получателя) для других поддерживаемых служб, например, FTP-сервера, с помощью второго метода - определение собственных правил.

- Общий доступ к Интернет-подключению (Шаг 7) — трансляция сетевых адресов (NAT) должна быть разрешена, если в локальной сети используются частные IP-адреса.



4. Настройка DHCP-сервера

Примечания к примеру

Для назначения IP-адресов локальным компьютерам могут быть использованы следующие методы:

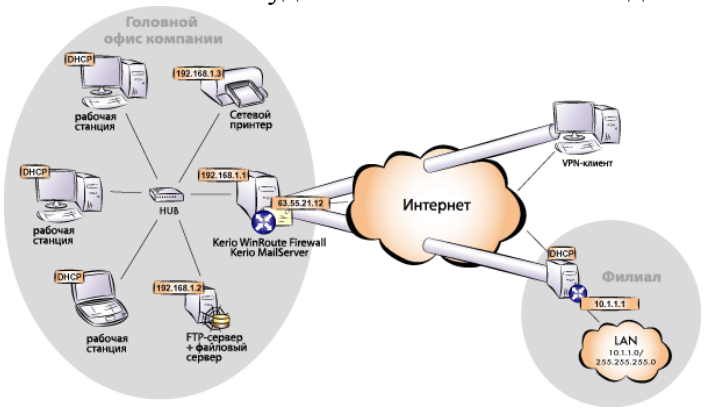
- Статический адрес 192.168.1.2 будет присвоен файловому/FTP серверу (его адрес не должен изменяться, иначе маппинг не будет работать).
- Статический адрес будет присвоен сетевому принтеру с помощью DHCP-сервера. Принетры не могут иметь динамические адреса, т.к. в случае изменения адреса они станут недоступными с клиентских машин.

Примечание: IP-адреса могут быть назначены принтерам вручную или с помощью DHCP-сервера. Если используется DHCP-сервер, то принеры настраиваются автоматиче-

ски и их адреса отображаются в таблице выделенных адресов сервера. В случае ручной настройки принтеры становятся независимыми от доступности DHCP-сервера.

- Динамические IP-адреса будут назначены локальным рабочим станциям (тем самым упрощается настройка).

В локальной сети будет использоваться DNS-домен company.com.



Примечание: Для сети филиала будут использоваться адреса 10.1.1.x, сетевая маска 255.255.255.0 и DNS-домен filial.company.com.

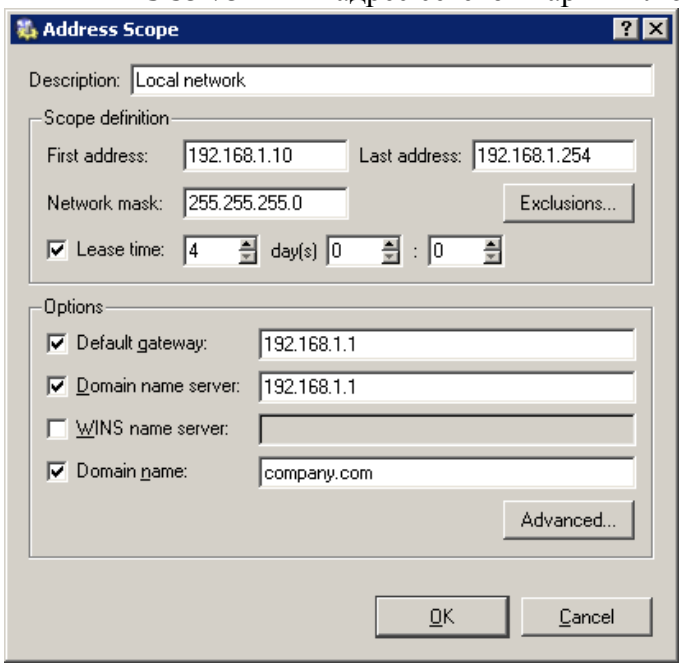
Настройка сервера DHCP

Перейдите в раздел Configuration / DHCP server консоли управления *Kerio Administration Console*. Откройте вкладку Scopes для создания IP-диапазона для машин, адреса которым будут присваиваться динамически (опция Add / Scope). Для настройки диапазона должны быть указаны следующие параметры:

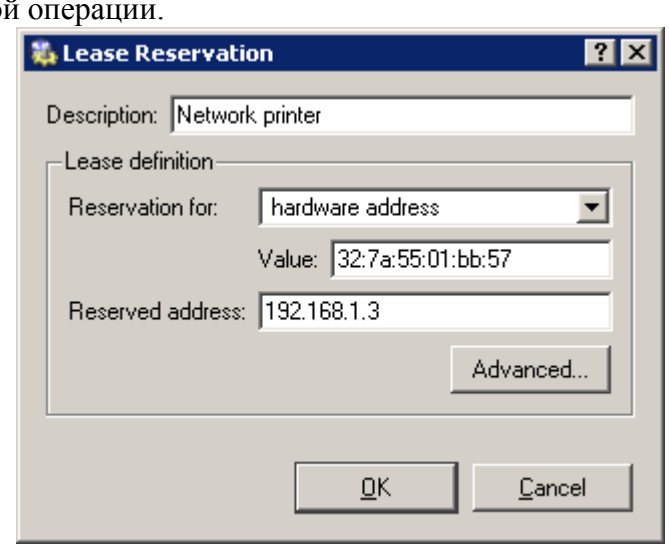
- First Address (Первый адрес) — выберите 192.168.1.10 (адреса с 192.168.1.1. до 192.168.1.9 будут зарезервированы для серверов и принтеров)
- Last Address (Последний адрес) — 192.168.1.254 (адрес с самым большим номером, который может использоваться в данной сети)
- Network mask (Сетевая маска) — 255.255.255.0
- Default gateway (Основной шлюз) — IP-адрес сетевой карты шлюза, подключенной к локальной сети (192.168.1.1).

Примечание: Основной шлюз определяет путь, по которому пакеты из локальной сети будут направлены в сеть Интернет. Направление пакетов через *WinRoute* позволит создать правила фильтрации трафика, авторизацию пользователей и т.п.

- DNS server — IP-адрес сетевой карты шлюза, подключенной к локальной



Зарезервируем адрес для сетевого принтера с помощью опции Add / Reservation... Резервируемый адрес не обязательно должен принадлежать диапазону, заданному ранее, однако, он должен находиться в той же сети (в данном примере резервируется адрес 192.168.1.3). Вам необходимо знать аппаратный (MAC) адрес принтера для осуществле- ния данной операции.



Подсказка: Не рекомендуется делать ручное резервирование адреса для принтера, если вы точно не знаете его аппаратный адрес. Запустите DHCP-сервер и подключите принтер к сети. Принтеру будет выделен адрес из диапазона, определенного ранее. Найдите этот адрес на вкладке Leases и используйте кнопку Reserve... для того, чтобы от- крыть диалоговое окно, в котором и будет указан аппаратный адрес. Укажите необходи- мый IP-адрес (и описание в случае необходимости) и нажмите на кнопку OK. Перезапу- стите принтер. Требуемый IP-адрес будет назначен принтеру DHCP-сервером.

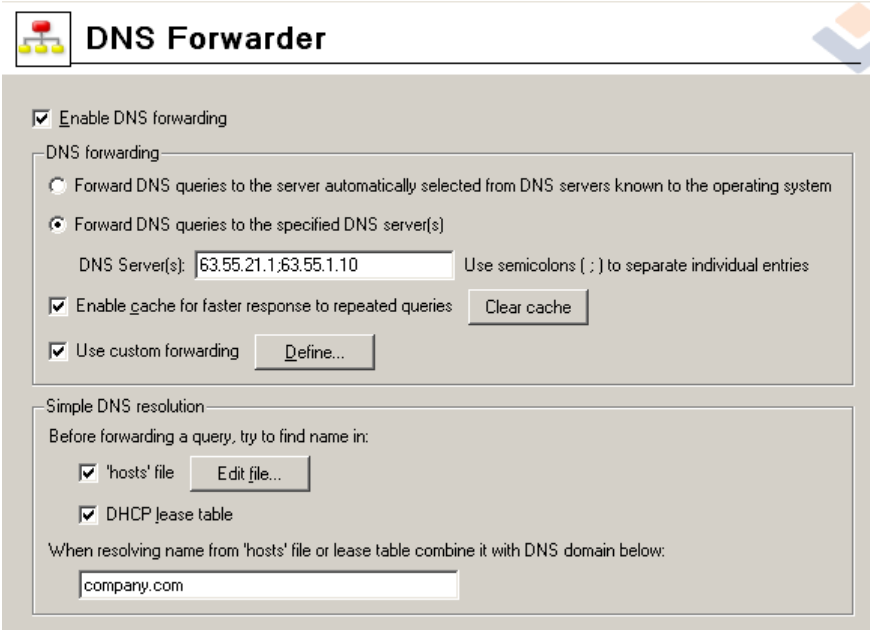
Примечания:

1. Не используйте DHCP-сервер, пока вы не определили все диапазоны и не зарезервировали все необходимые адреса.
2. Вы также можете использовать другой DHCP-сервер для автоматической настройки сетевого оборудования. Задайте IP-адрес внутреннего интерфейса шлюза в качестве параметра Default gateway и DNS server в настройках DHCP-сервера для выбранного диапазона адресов.

5. Настройка DNS Форвардера

Перейдите в меню Configuration / DNS Forwarder для настройки DNS-серверов, на которые будут перенаправляться DNS-запросы. Выберите опцию "Check the Forward DNS queries to the specified DNS servers" и укажите один или несколько серверов в сети Интернет. Обычно лучшим выбором является указание DNS-серверов провайдера. Для получения данных адресов свяжитесь с вашим провайдером.

Внимание: Автоматический выбор DNS-серверов невозможен, т.к. DNS-сервер на сетевой карте, подключенной к локальной сети, использует тот же IP-адрес, что и DNS-сервер на брандмауэре— DNS-сервера всегда должны быть указаны в *DNS форвардере*, в противном случае *DNS Форвардер* не будет работать правильно.

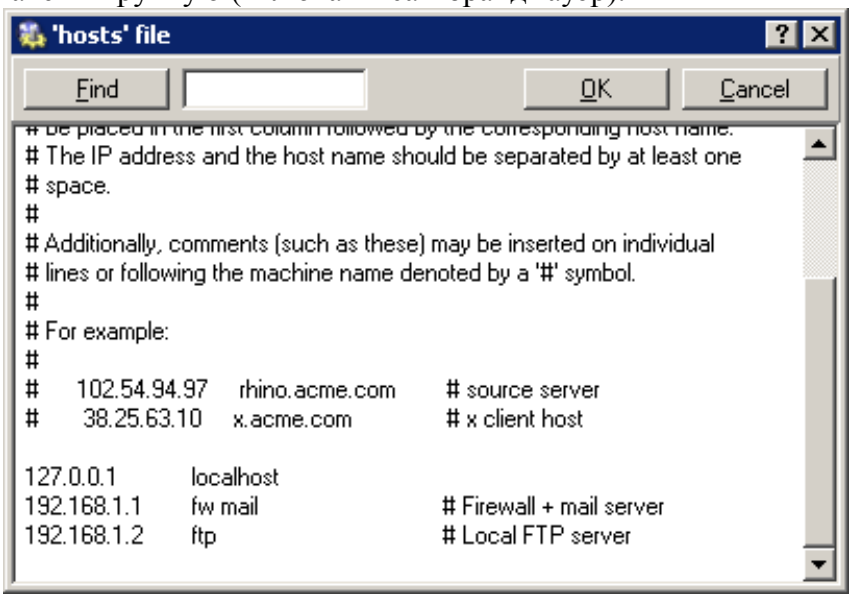


Дополнительные параметры *DNS Форвардера*:

- Рекомендуется включить опцию Enable cache... (это уменьшит время ответа на повторяющиеся DNS-запросы).
- Включите опцию Use custom forwarding для установки параметров, необходимых для корректной пересылки DNS-запросов между сетью головного офиса и сетью филиалов.
- Обе опции 'hosts' file и DHCP lease table должны быть включены (*DNS Форвардер* использует файл hosts и/или таблицу аренды DHCP для поиска имен и IP-адресов локальных машин).

Укажите локальный домен company.com в поле When resolving name... *DNS Форвардер* при этом сможет правильно отвечать на запросы, ссылающиеся на имена в локальной сети (например, `fw`) или на полные DNS-имена машин (например, `fw.company.com`).

Нажмите кнопку Edit file... для редактирования системного файла hosts. В этом диалоговом окне укажите все IP-адреса и имена компьютеров, для которых IP-адреса были назначены вручную (включая и сам брандмауэр).

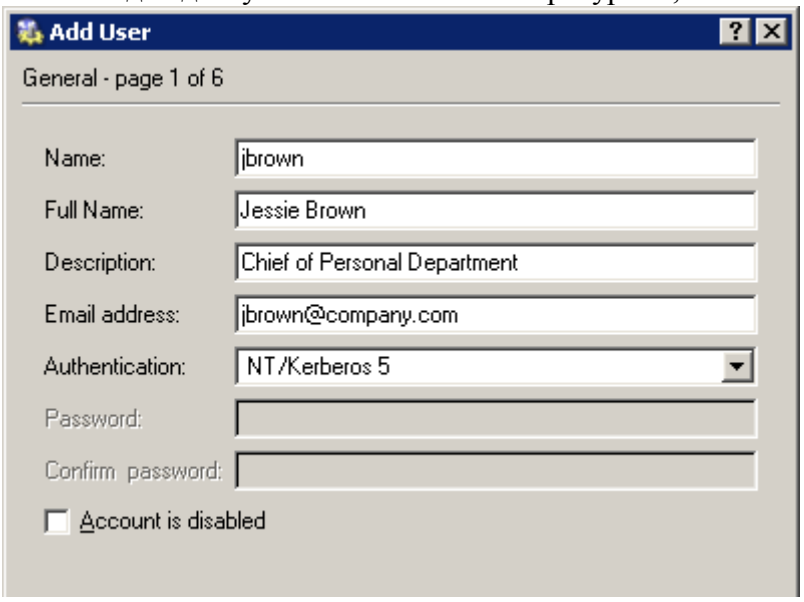


6. Создание учетных записей пользователей и групп

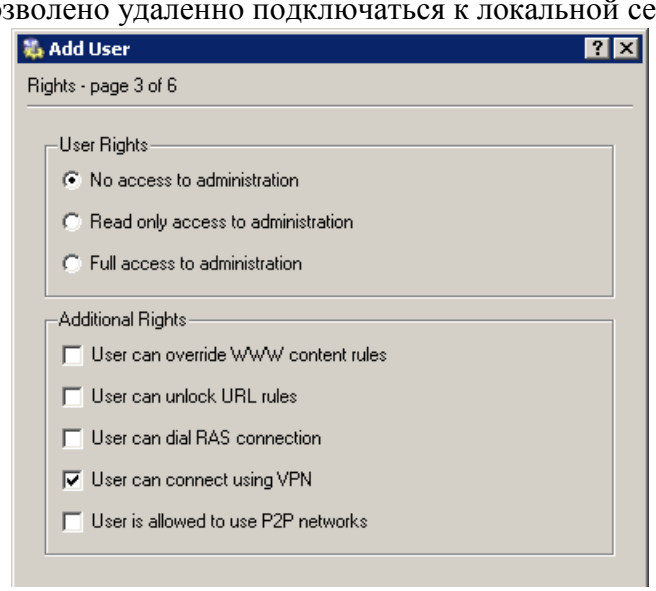
Перейдите в раздел Users and Groups / Users для создания учетных записей для всех пользователей в локальной сети.

Если сеть построена на базе доменов Windows NT или Windows 2000, то пользова-

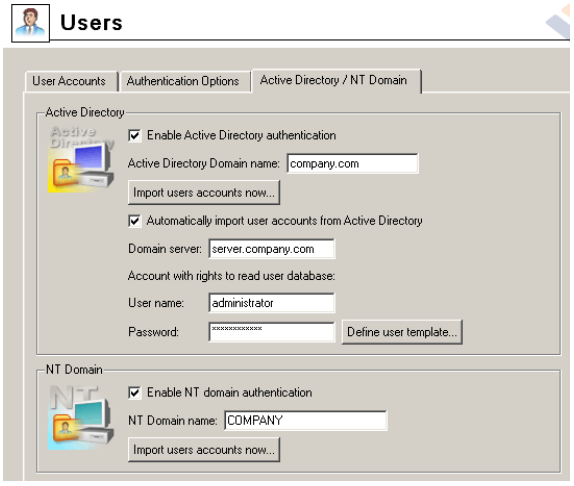
тели могут быть импортированы из данных доменов. Имена и пароли пользователей будут использоваться для доступа к любым сетевым ресурсам, в том числе и к сети Интернет.



Установите права доступа к VPN-серверу для каждого пользователя, которому будет позволено удаленно подключаться к локальной сети.



Если планируется использовать автоматическую авторизацию, то имя домена Windows NT/Windows 2000 должно быть указано в соответствующем поле диалога Advanced Options / User Authentication.

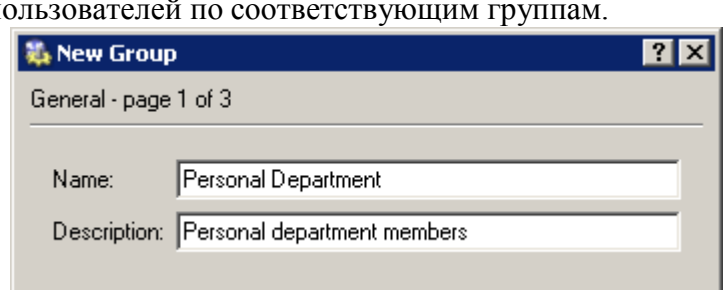


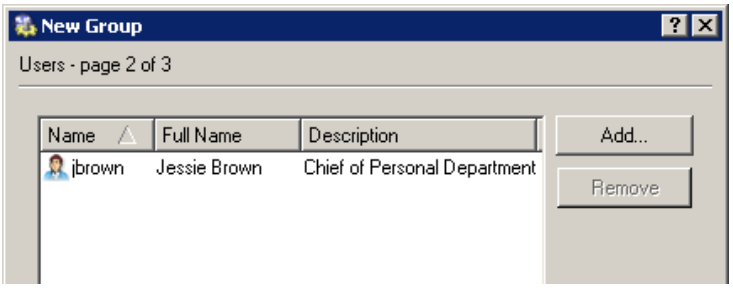
Подсказка:

1. Также возможно импортировать учетные записи пользователей из домена NT или из Active Directory. Это позволит сэкономить время и упростить задачу администрирования.

2. Для автоматического импорта учетных записей из Active Directory необходимо указать IP-адрес сервера AD, а также имя пользователя и пароль с соответствующими правами (может быть использона учетная запись любого пользователя домена). Кроме того, можно создать шаблон настроек (группы, права, квоты и т.п.), применяемый автоматически ко всем новым пользователям при их первой авторизации на сервере.

Перейдите в раздел Users and Groups / Groups для создания групп пользователей, которые будут использоваться для управления доступом к интернет-ресурсам. Распределите пользователей по соответствующим группам.

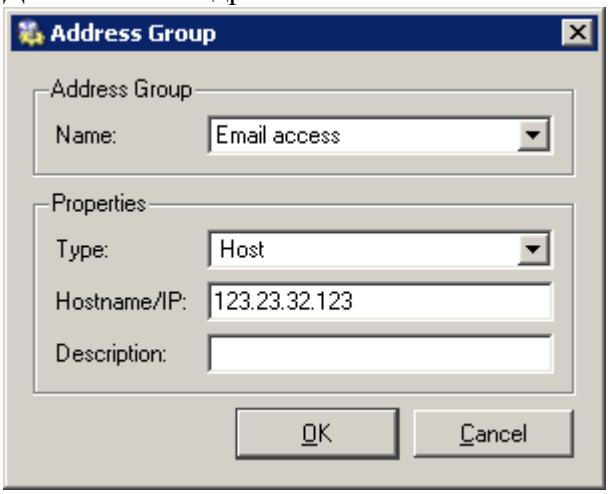




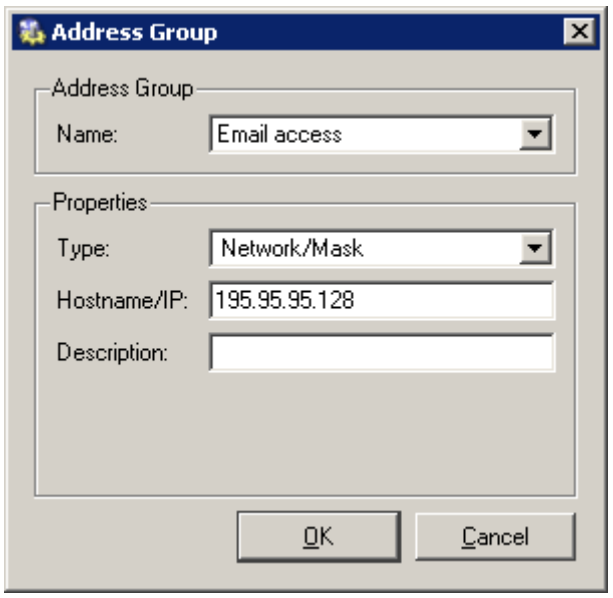
7. Адресные группы и временные интервалы

Перейдите в раздел Definitions / Address Groups для создания IP-групп, которые будут использоваться для ограничения доступа к почтовым учетным записям. Эта группа будет состоять из адресов 123.23.43.123 и 50.60.70.80, а также из полной сети 195.95.95.128 с маской 255.255.255.248.

Добавляем IP-адрес:

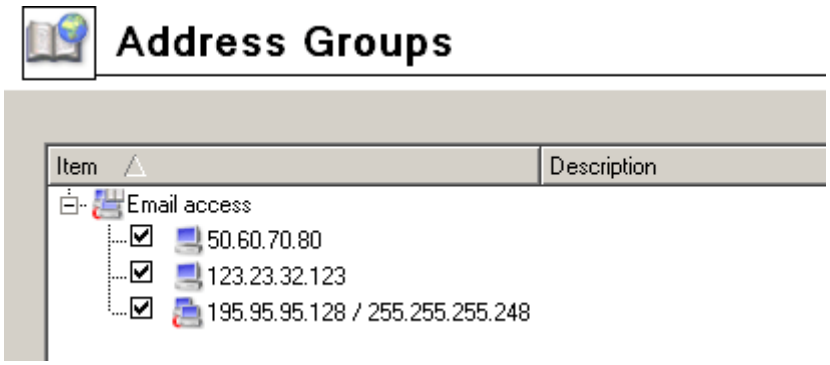


Добавляем сеть:



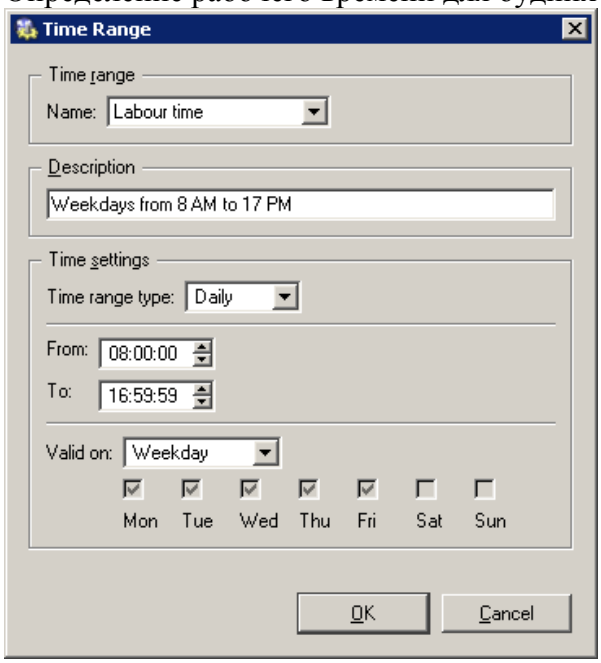
Примечание: Имя должно быть одинаковым для всех элементов, чтобы все записи были добавлены к одной и той же группе.

В конечном итоге мы должны получить следующее:

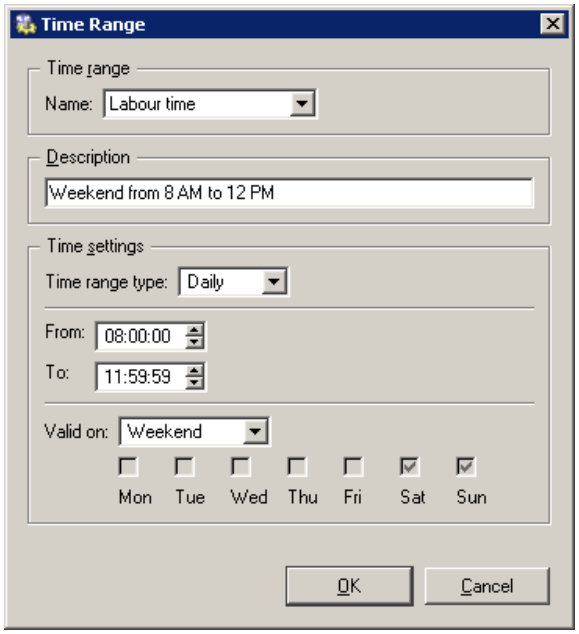


Перейдите в раздел Definitions / Time Ranges для создания интервала времени, ограничивающего интернет-доступ в рабочее время (с понедельника по пятницу с 8 часов утра до 17-00, в субботу и воскресенье с 8 до 12 часов).

Определение рабочего времени для будних дней (с понедельника по пятницу):



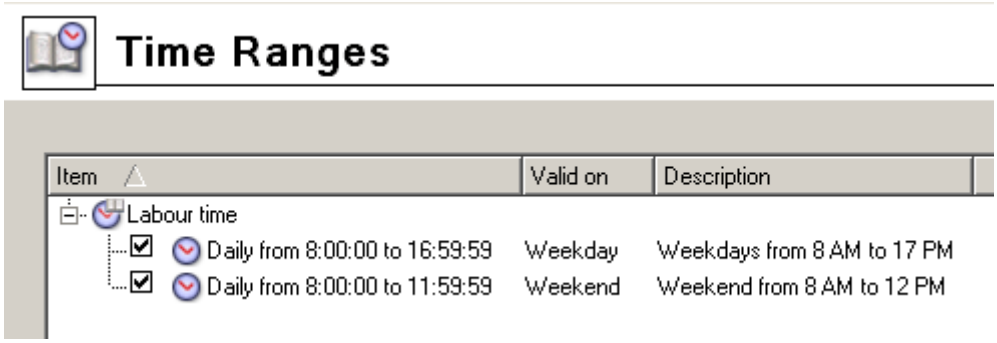
Определение рабочего времени для выходных дней (суббота и воскресенье):



Примечание:

1. Вы можете использовать готовые группировки дней (Weekday или Weekend) для настройки параметра Valid on — при этом нет необходимости индивидуально выделять каждый день.
2. Имя записей должно быть идентично, чтобы был создан только один временной интервал.

На рисунке приведен итоговый результат определения интервала времени Labor time:



8. Определение Web-правил

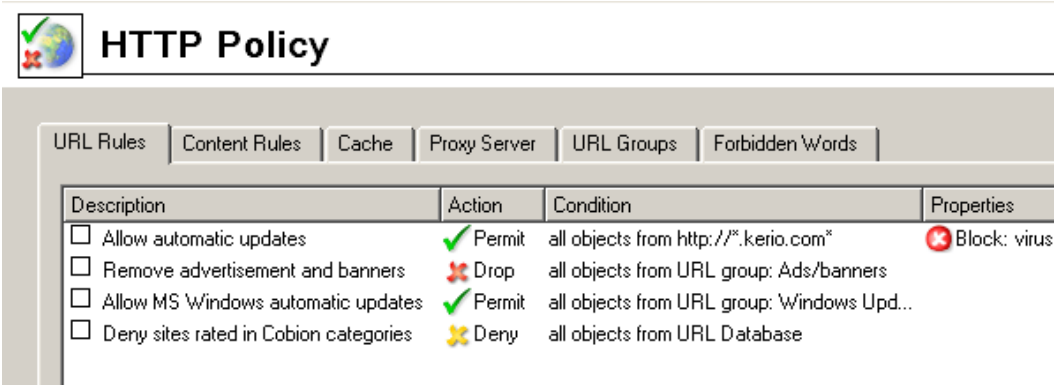
Требования

Доступ к web-страницам будет ограничен согласно следующим правилам:

- на web-страницах фильтруется реклама;
- доступ к эротическому/сексуальному контенту запрещен;
- доступ к страницам с предложениями работы запрещен (исключение делается только для пользователей из отдела кадров (Personal Department);
- для получения доступа к сети Интернет пользователи должны авторизоваться на шлюзе (это позволит проводить мониторинг просмотренных пользователями страниц).

Предопределенные HTTP-правила

Следующие HTTP-правила предопределены при установке и доступны на вкладке URL Rules в разделе Configuration / Content Filtering / HTTP Policy:



Allow automati updates (Разрешить автоматические обновления)

Данное правило разрешает производить автоматическое обновление *WinRoute* и антивируса *McAfee* с сайта Kerio Technologies.

Remove advertisement and banners (Удалять рекламу и баннеры)

Фильтрация рекламы и баннеров. Согласно этому правилу блокируются все объекты, подпадающие под определение группы Ads/banners. Щелкните на данном правиле для его активации.

Примечание: Иногда может так случиться, что страница, на которой нет рекламы, будет заблокирована. В этом случае удалите соответствующую запись из группы Ads/banners или создайте правило-исключение для подобных страниц (мы рекомендуем именно второй метод).

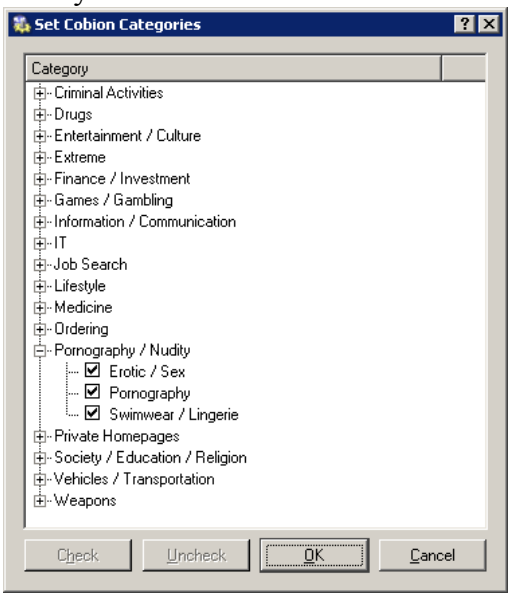
Allow MS Windows automatic updates (Разрешить автоматические обновления Windows)

Правило разрешает автоматические обновления операционной системы Windows с серверов Microsoft.

Deny sites rated in Cobion categories (Запретить сайты по категориям Cobion)

Данное правило запрещает доступ к Web-сайтам, входящим в выбранные категории фильтра *Cobion Orange Filter*.

Нажмите кнопку Select Rating... для выбора блокируемых категорий. Отметьте соответствующие категории в разделе Pornography для запрета доступа к страницам с эротическим/сексуальным контентом.



Примечание:

1. Базовая лицензия *WinRoute* не включает систему *Cobion* (необходимо приобрести специальную версию лицензии). Однако данная система доступна в триальной версии *WinRoute*.

2. Система *Cobion*, включенная в поставку *WinRoute*, должна иметь возможность установки соединения с серверами баз данных в сети Интернет. Это означает, что политика трафика должна разрешать доступ к сервису *COFS* (6000/tcp) со шлюзовой машины. Разрешающее правило создается автоматически мастером настройки политики.

3. Вы можете создать несколько URL-правил, использующих технологию *Cobion Orange Filter*. Несколько категорий может быть выбрано для каждого правила.

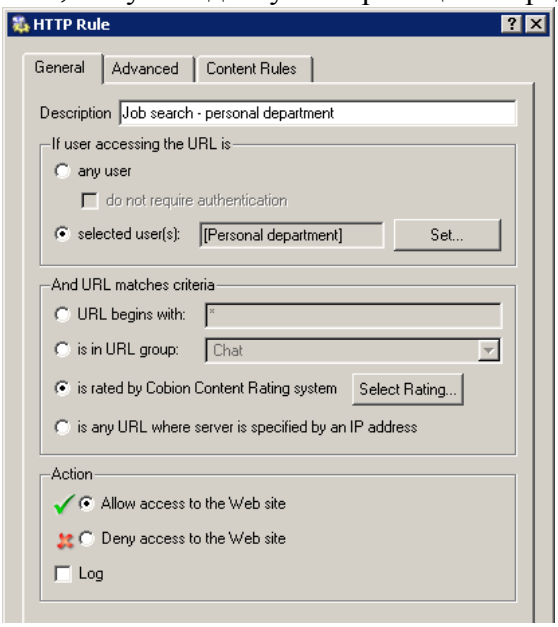
4. Мы рекомендуем включить опцию “unlock” в правилах, использующих технологию *Cobion Orange Filter*, так как отдельные страницы могут быть классифицированы неверно и важная информация в некоторых случаях может блокироваться. Все запросы на разблокировку доступа сохраняются в журнале *Filter* — это позволяет вам отслеживать, были ли подобные запросы правомерны.

Примечание: Вы можете указать информацию, которая будет отображена на странице блокировки, на вкладке Advanced (URL Rules) или перенаправить пользователей на другую страницу при попытке доступа к запрещенной странице.

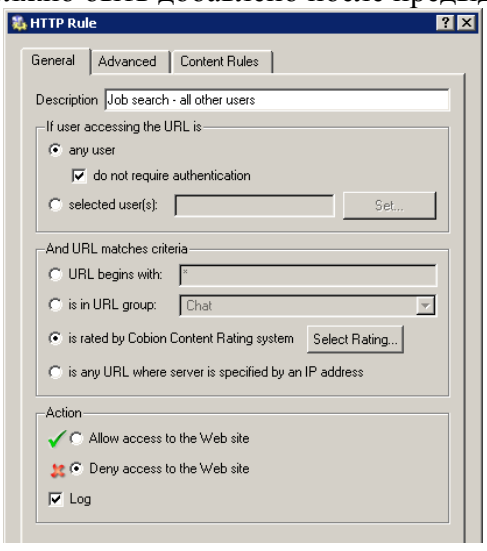
Создание собственных URL-правил

Правила, которые будут применяться для отдельных пользователей или групп, могут быть добавлены после правила, требующего авторизацию от всех пользователей.

Вы можете добавить правило, разрешающее пользователям из группы *Personal Department*, получать доступ к страницам с предложениями работы.

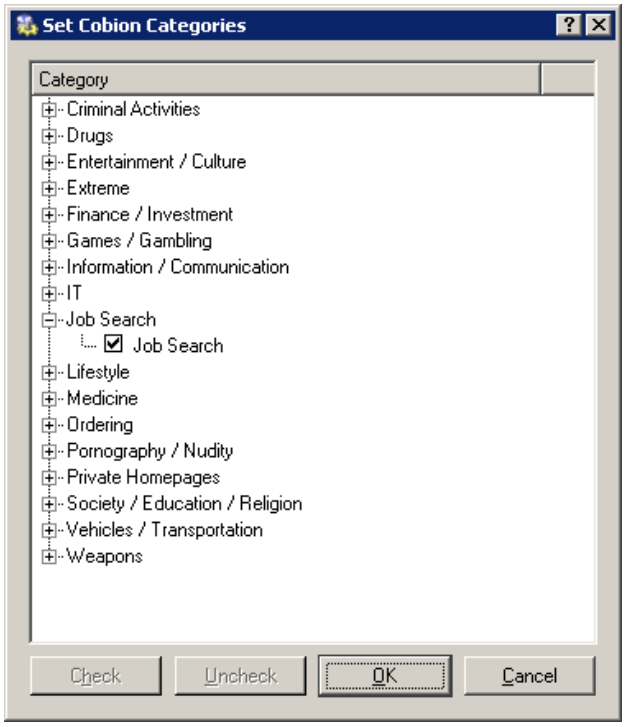


Правило, запрещающее доступ всем остальным пользователям к данным страницам, должно быть добавлено после предыдущего правила.



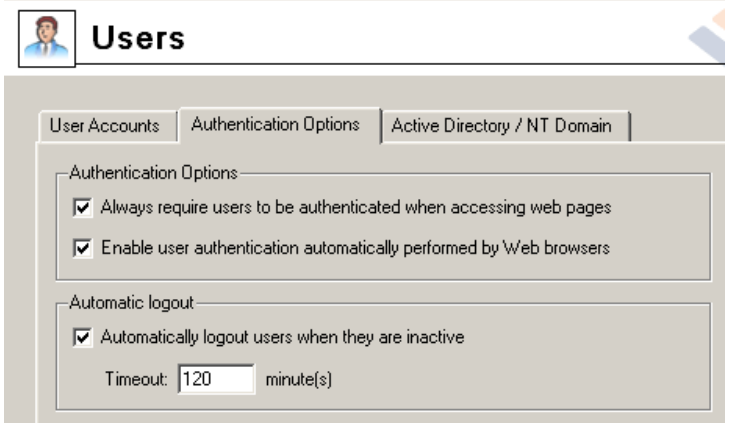
Примечания:

1. Рекомендуется включить опцию "do not require athentication" для данного запрещающего правила, так как в противном случае пользователи будут направлены на страницу авторизации до того, после чего получат информацию о запрете.
2. В двух вышеописанных правилах должна быть выбрана только категория JobSearch.



Авторизация пользователей для доступа к веб-сайтам

Последнее опциональное ограничение - требование авторизации для доступа к веб-сайтам. Активируйте опцию Always require users to be authenticated when accessing web pages на вкладке Authentication Options в разделе Users and groups / Users.



Настройка кэша HTTP

Кэш ускоряет доступ к повторно открываемым веб-страницам, при этом одновременно уменьшая интернет-трафик. Кэш может быть активирован с помощью опций Enable cache on transparent proxy и Enable cache on proxy server в разделе Configuration / Content Filtering / HTTP Policy. Установите желаемый размер кэш-области с учетом свободного дискового пространства. По умолчанию установлено значение 1 Гб (1024 Мб), максимальное значение - 2 Гб (2048 Мб).

Настройка политики FTP

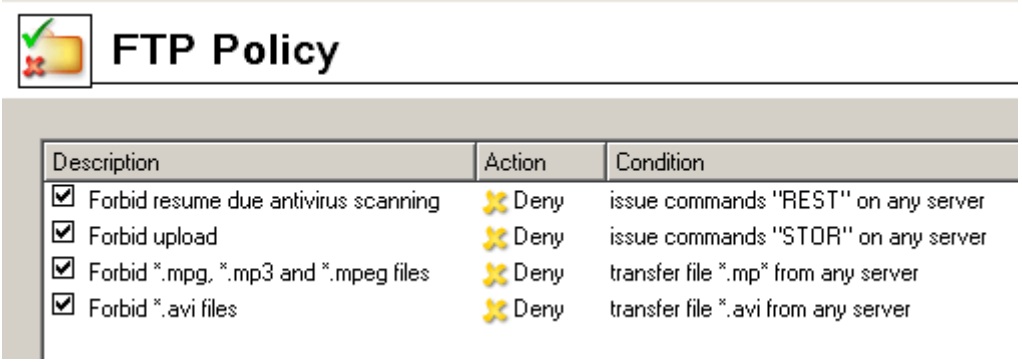
Требования

Доступ к FTP будет ограничен согласно следующим правилам:

- передача музыкальных файлов в формате MP3 запрещена
- передача видео-файлов (*.avi) запрещена в рабочее время
- загрузки на удаленные FTP-сервера запрещена — защита важной корпоративной информации

Предопределенные правила FTP

Перейдите в раздел Configuration / Content Filtering / FTP Policy для настройки ограничений FTP. Следующие правила являются предопределенными и могут быть использованы для всех оговоренных ограничений.



Forbid resume due antivirus scanning (запрет возобновления из-за антивирусного сканирования)

Данное правило запрещает восстановление (продление с текущего места) прерванных сеансов передачи данных (например, из-за сетевого сбоя). Если файлы, передаваемые по FTP, сканируются на предмет наличия вирусов, то рекомендуется включить данное правило (файлы, передаваемые частями, не могут быть надежно просканированы).

Forbid upload (запрет загрузки на удаленные сервера)

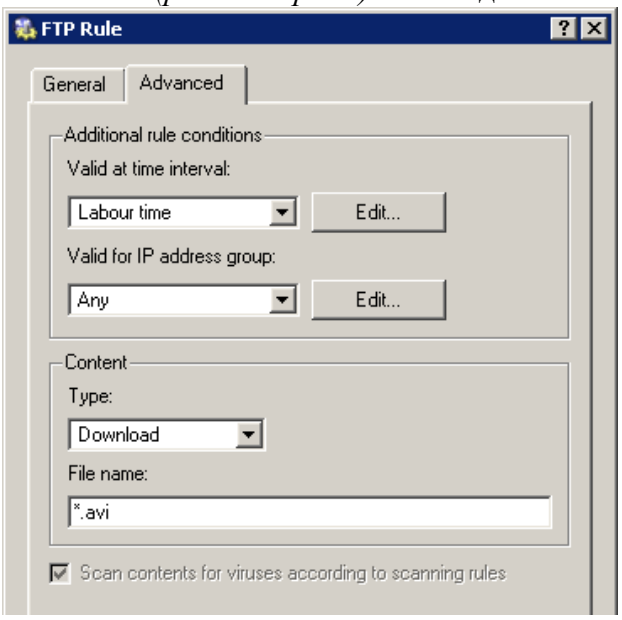
Запрет сохранения данных на FTP-серверах — это правило уже определено и достаточно просто его включить.

Forbid *.mpg, *.mp3 and *.mpeg files (запрет файлов *.mpg, *.mp3 and *.mpeg)

Данная опция запрещает передачу звуковых файлов перечисленных форматов. Данное правило также уже существует и достаточно просто его включить.

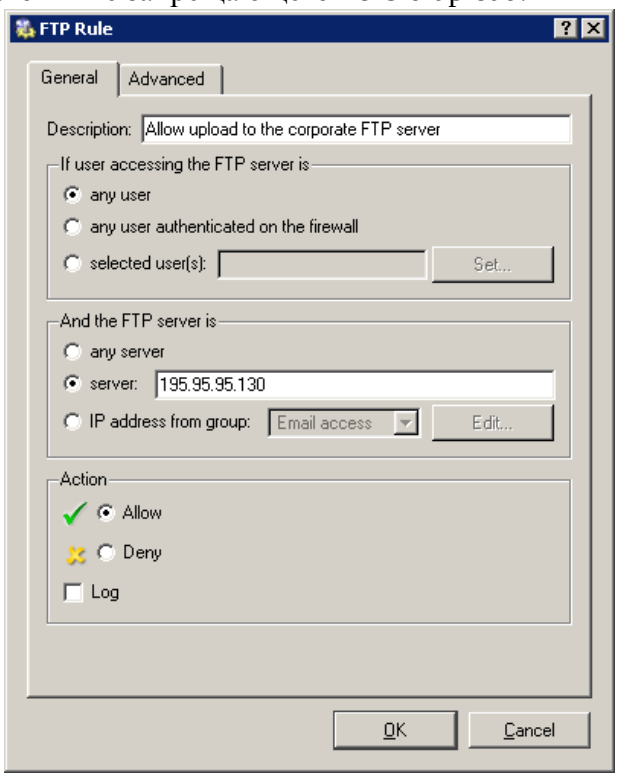
Forbid *.avi files (запрет файлов *.avi)

Это правило будет запрещать передачу видео-файлов. Включите данное правило, нажмите кнопку Edit для того, чтобы открыть диалоговое окно, и укажите временной интервал *Labor time (рабочее время)* на вкладке Advanced.



Внимание: Политика FTP распространяется только на FTP-трафик, обрабатываемый инспектором протокола FTP.

В нашем примере мы планируем разрешить доступ к локальному FTP-серверу из сети Интернет. Правило Forbid upload запрещает также загрузку файлов и на наш сервер, что не всегда желательно. Поэтому мы должны создать разрешающее правило и поместить его выше запрещающего Forbid upload.



:

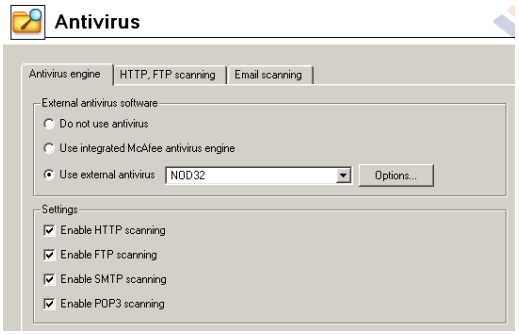
Примечания

1. IP-адрес машины, на которой работает FTP-сервис, должен быть указан в поле адреса сервера. Нельзя в данном правиле задать адрес внешнего интерфейса шлюза, с которого мы настраивали маппинг (трансляция IP-адреса производится ДО применения фильтрующих правил)!
2. Данный метод может быть использован для разрешения загрузки на любой из FTP-серверов в сети Интернет, при этом оставляя запрет на остальные сервера.

10. Настройка антивирусного сканирования

Любые поддерживаемые внешние антивирусные приложения, которые Вы намереваетесь использовать, должны быть сначала установлены. Антивирусное приложение McAfee интегрировано в WinRoute, и для дальнейшего его использования Вы должны приобрести специальную лицензию.

Выберите соответствующее антивирусное приложение во вкладке Antivirus в **Configuration / Content filtering /Antivirus** и выберите протоколы, которые будут сканироваться. Все исполняемые файлы и файлы Microsoft Office сканируются по умолчанию.



Вкладки **HTTP, FTP scanning** и **Email scanning** допускают детализированную

конфигурацию сканирования этих протоколов. В большинстве случаев настройки по умолчанию являются оптимальными.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Как открыть порт в Kerio Winroute Firewall для торрентов?
2. Как закрыть одному человеку или группе людей некоторые сайты оставив их открытыми для других?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними **«Поиск и устранение неисправностей коммутатора» Цель работы:** производить поиск и устранение неисправностей сетевого оборудования.

В процессе занятия решаются следующие задачи:

1. Построение сети и настройка базовых параметров устройства
2. Поиск и устранение неполадок статического NAT
3. Поиск и устранение неполадок динамического NAT;

Краткие теоретические и справочно-информационные материалы по теме занятия.

Топология

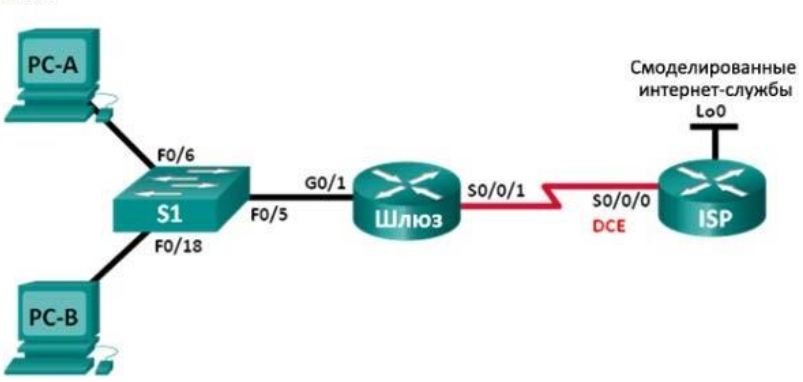


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	209.165.200.225	255.255.255.252	N/A
Интернет-провайдер	S0/0/0 (DCE)	209.165.200.226	255.255.255.252	N/A
	Lo0	198.133.219.1	255.255.255.255	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.4	255.255.255.0	192.168.1.1

Маршрутизатор Gateway был настроен неопытным сетевым администратором из вашей компании. Из-за нескольких ошибок в настройках возникли проблемы с процессом NAT. Начальник попросил вас найти неисправности, устранить ошибки конфигурации и составить отчёт о проделанной работе. Убедитесь в том, что сеть соответствует следующим требованиям:

- Компьютер PC-A работает в качестве веб-сервера со статическим NAT и будет доступен извне через адрес 209.165.200.254.
- Компьютер PC-B функционирует в качестве узлового компьютера и динамически получает IP- адрес от созданного пула адресов под названием NAT_POOL, который использует диапазон 209.165.200.240/29.

Порядок работы

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

Часть 1: Построение сети и настройка базовых параметров устройства

В первой части вам предстоит настроить топологию сети и настроить базовые параметры на маршрутизаторах (используйте эмулятор сетей Cisco Packet Tracer). Дополнительные конфигурации NAT прилагаются.

В конфигурации NAT для шлюзового маршрутизатора (Gateway) содержатся ошибки, которые вам нужно найти и исправить в процессе выполнения этой лабораторной работы.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Шаг 4: Настройте базовые параметры каждого маршрутизатора.

a. Отключите поиск DNS.

b. Присвойте имена устройствам в соответствии с топологией.

c. Настройте IP-адреса в соответствии с таблицей адресов.

d. Установите тактовую частоту на 128000 для всех последовательных интерфейсов DCE.

e. Назначьте cisco в качестве пароля консоли и виртуального терминала VTY.

f. Назначьте class в качестве зашифрованного пароля доступа к привилегированному режиму EXEC.

g. Настройте logging synchronous, чтобы сообщения от консоли не могли прерывать ввод команд.

Шаг 5: Настройте статическую маршрутизацию.

a. Создайте статический маршрут от маршрутизатора интернет-провайдера до маршрутизатора Gateway, используя диапазон публичных сетевых адресов 209.165.200.224/27. *ISP(config)# ip route 209.165.200.224 255.255.255.224 s0/0/0*

b. Создайте маршрут по умолчанию от маршрутизатора Gateway к маршрутизатору ISP. *Gateway(config)# ip route 0.0.0.0 0.0.0.0 s0/0/1*

Шаг 6: Загрузите настройки маршрутизатора.

В вашем распоряжении конфигурации для маршрутизаторов. Ошибки содержатся в конфигурации для маршрутизатора Gateway. Определите и исправьте ошибки конфигурации.
Конфигурация шлюзового маршрутизатора

```
interface  g0/1
ip nat outside
no shutdown
interface s0/0/0
ip nat outside
interface s0/0/1
no shutdown
ip nat inside source static 192.168.2.3 209.165.200.254
ip nat pool NAT_POOL 209.165.200.241 209.165.200.246 netmask 255.255.255.248
ip nat inside source list NAT_ACL pool NATPOOL
 ip access-list standard NAT_ACL
permit 192.168.10.0 0.0.0.255
banner motd $AUTHORIZED ACCESS ONLY$
end
```

Шаг 7: Сохраните текущую конфигурацию в загрузочную конфигурацию

Часть 2: Поиск и устранение неполадок статического NAT

Во второй части вам нужно исследовать статический NAT для компьютера PC-A, чтобы оценить правильность его настройки. Выполняйте поиск и устранение неполадок, пока статический NAT не будет настроено правильно.

a. Чтобы устранить неполадки в NAT, используйте команду debug ip nat. Включите отладку NAT, чтобы видеть преобразования через маршрутизатор Gateway в реальном времени.
Gateway# debug ip nat

b. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

c. На маршрутизаторе Gateway введите команду, которая позволит увидеть все текущие преобразования NAT на данном маршрутизаторе. Запишите команду в строке ниже.

Почему вы видите преобразования NAT в таблице, хотя при отправке эхо-запроса от компьютера PC-A на интерфейсе loopback маршрутизатора интернет-провайдера этого не было? Что необходимо сделать, чтобы исправить эту проблему?

_____

d. Запишите все команды, необходимые для исправления ошибки в конфигурации статического NAT.

_____

_____

e. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

_____

f. На маршрутизаторе Gateway введите команду, которая позволит увидеть общее количество текущих преобразований NAT. Запишите команду в строке ниже.

_____

Успешно ли проходит статическое преобразование NAT? Почему?

_____

_____

g. На маршрутизаторе Gateway введите команду, которая позволит увидеть текущую конфигурацию маршрутизатора. Запишите команду в строке ниже.

_____

h. Есть ли какие-либо проблемы в текущей конфигурации, которые препятствуют статическому NAT?

_____

i. Запишите все команды, необходимые для исправления ошибок в конфигурации статического NAT.

j. Отправьте эхо-запрос с PC-A на Lo0 маршрутизатора интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

_____

k. Чтобы убедиться в правильном функционировании статического NAT, используйте команду show ip nat translations verbose. Примечание. Период истечения времени для ICMP очень короткий. Если вы не видите все преобразования в выходных данных, повторите эхо-запрос. Успешно ли проходит статическое преобразование NAT?
_____ Если статическое преобразование NAT проходит неправильно, повторите вышеупомянутые действия, чтобы исправить неполадки в конфигурации.

Часть 3: Поиск и устранение неполадок динамического NAT
a. Отправьте эхо-запрос с PC-B на Lo0 на маршрутизаторе интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?

_____

b. На маршрутизаторе Gateway введите команду, которая позволит увидеть текущую конфигурацию маршрутизатора. Есть ли какие-либо проблемы в текущей конфигурации, которые препятствуют динамическому преобразованию NAT?

_____

_____

_____

c. Запишите все команды, необходимые для исправления ошибок в конфигурации динамического NAT.

_____

_____

_____

d. Отправьте эхо-запрос с PC-B на Lo0 на маршрутизаторе интернет-провайдера (ISP). Появляются ли какие-либо преобразования отладки NAT на маршрутизаторе Gateway?
_____ e. Чтобы отслеживать использование NAT, используйте команду show ip nat statistics. Успешно ли проходит NAT?_____Какой процент динамических адресов выделен?_____f. Отмените все операции отладки с помощью команды undebug all. Вопросы на закрепление 1. В чём заключаются преимущества статического NAT?

_____

_____

2. Какие проблемы могли бы возникнуть, если бы десять узловых компьютеров в этой сети попытались одновременно наладить связь через Интернет?

Сводная таблица интерфейсов маршрутизаторов

Сводная информация об интерфейсах маршрутизаторов				
Модель маршрутизатора	**Интерфейс Ethernet №1**	**Интерфейс Ethernet №2**	**Последовательный интерфейс №1**	**Последовательный интерфейс №2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
Примечание. Чтобы узнать, каким образом настроен маршрутизатор, изучите интерфейсы с целью определения типа маршрутизатора и количества имеющихся на нём интерфейсов. Эффективного способа перечисления всех комбинаций настроек для каждого класса маршрутизаторов не существует. В данной таблице содержатся идентификаторы возможных сочетаний Ethernet и последовательных (Serial) интерфейсов в устройстве. В таблицу не включены какие-либо иные типы интерфейсов, даже если на определённом маршрутизаторе они присутствуют. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это принятое сокращение, которое можно использовать в командах Cisco IOS для представления интерфейса.				

Время выполнения работы 90 мин;

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 5 «Настройка параметров беспроводного адаптера»

Цель работы: познакомиться с принципами подключения к сети Ethernet беспроводной точки доступа, работающей по одному из стандартов Wi-Fi

В процессе занятия решаются следующие задачи:

1. Настройка сетевое взаимодействие между проводными и беспроводными клиентами.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Беспроводной связь - это передача информации на расстояние без использования электрических проводников или «проводов». Это расстояние может быть как малой (несколько метров, как в телевизионном дистанционном управлении), так и очень большим

(тысячи или даже миллионы километров для телекоммуникаций). Беспроводная связь обычно рассматривается как отрасль телекоммуникаций.

Беспроводная технология в общем используется для оборудования мобильных информационных технологий. В их состав входят мобильные телефоны, наладонники (PDA) и беспроводные сети. Другие примеры *беспроводных технологий*включают устройства глобального позиционирования, устройства дистанционного открывания гаража, беспроводные компьютерные мыши и клавиатуры, спутниковое телевидение и мобильные и радиотелефоны.

Развитие беспроводных технологий

В последние годы направление беспроводных компьютерных сетей и удаленного доступа потерпел бурного развития. Это связано с распространением блокнотных компьютеров, систем поискового вызова (так называемых пейджеров) и появлением систем класса «персональный секретарь» (Personal Digital Assistant (PDA)), расширением функциональных возможностей сотовых телефонов. Такие системы должны обеспечить деловое планирование, расчет времени, хранение документов и поддержание связи с удаленными станциями. Девизом этих систем стало anytime, anywhere, т.е. предоставление услуг связи вне зависимости от места и времени. Кроме того, беспроводные каналы вязкую актуальные там, где невозможно или дорого прокладку кабельных линий и значительные расстояния. До недавнего времени большинство беспроводных компьютерных сетей передавала данные со скоростью от 1.2 до 14.0 Кбит / с, зачастую только короткие сообщения (передача файлов больших размеров или длинные сеансы интерактивной работы сбазой данных были недоступны). Новые технологии беспроводного передачи оперируют со скоростями в несколько десятков мегабит в секунду.

Классификация беспроводных сетей

В зависимости от технологий и передающих сред, которые используют, можно определить следующие классы беспроводных сетей:

- сети на радиомодема;
- сети на сотовых модемах;
- инфракрасные системы;
- системы VSAT;
- системы с использованием низкоорбитальных спутников;
- системы с технологией SST;
- радиорелейные системы;
- системы лазерной связи.

Федеральная комиссия по электросвязи США (FCC) определила следующие категории PCS (Personal Communication Services) и соответствующие полосы частот:

- узкополосные PCS (диапазон 900-901, 930-931, 940-941 МГц) для скоростных пейджерных сетей, двунаправленного передачи сообщений, передача сообщений вещания;
- широкополосные PCS (120, 1850-2200 МГц);
- сотовую связь;
- цифровое передачи речи и данных;
- нелицензированные PCS (40 МГц, от 1890 до 1930 МГц);
- беспроводные ЛМ и АТС организаций в ближайшем радиусе действия;
- в пределах одного здания или группы зданий.

Нелицензированные PCS обеспечивают передачу данных со скоростью до 10 Мбит / с.

Сети на радиомодема

Для передачи данных используют полосы частот радио-и ультракоротковолнового диапазона. Каждый радиомодем имеет антенну и передатчик для направленного передачи сигналов. Самыми популярными технологиями беспроводной передачи этого класса является:

- радио Ethernet (IEEE 802.11);

- HIPERLAN ;
- Bluetooth.

IEEE 802.11

Подробнее в статье IEEE 802.11

IEEE 802.11 - это семья технологий беспроводной передачи в радиодиапазоне. Сегодня самая популярная технология стандарта IEEE 802.11b; она позволяет передавать данные со скоростью 11 Мбит / с на расстояние от нескольких до десятков километров. Выходная скорость зависит от уровня помех, оборудование. На базе IEEE 802.11b строят беспроводные локальные сети Wireless LAN (WLAN)).

Группа стандартов IEEE 802.11 фактически определяет физический и канальный уровень протоколов передачи. Стандарты отличаются реализациями физических уровней передачи, обеспечивают разные скорости.

- IEEE 802.11 - это предварительная версия стандарта, известная как радио Ethernet (Wireless Ethernet); сегодня уже устарела.
- IEEE 802.11b обеспечивает максимальную скорость передачи 11 Мбит / с и использует 14 каналов в диапазоне 2.4 ГГц.
- IEEE 802.11a обеспечивает скорость передачи 54 Мбит / с. Работает в диапазоне 5 ГГц. Имеет 12 каналов передачи. В ней используются два поддиапазона передачи 5.15-5.25, 5.25-5.35 ГГц.
- IEEE 802.11g - обеспечивает скорость передачи 22 Мбит / с. Работает в диапазоне 2.4 ГГц. Полностью совместим с IEEE 802.11b, однако предлагает три новые методыкодирования, которые позволяют увеличить скорость.

Организация Wireless Ethernet Compatibility Alliance (WECA) сертифицирует оборудование на соответствие IEEE 802.11b и ставит на нем отметку Wi-Fi Compatible (Wireless Fidelity).

HIPERLAN

Подробнее в статье HIPERLAN

HIPERLAN (High Performance Radio Local Area Network) разработана Европейским институтом стандартов по телекоммуникационным технологиям (European Telecommunications Standards Institute). Она является аналогом IEEE 802.11, который используется в Европе, и бывает таких разновидностей:

- HiperLAN / 1 - скорость до 20 Мбит / с в диапазоне 5 ГГц;
- HiperLAN / 2 - скорость до 54 Мбит / с в диапазоне 5 ГГц.

Bluetooth

Bluetooth - это интерфейсная беспроводная технология. Диаметр сети 10-30 м (в перспективе - 100 м). Работает в багатопунктовому режиме, не обязательно в зоне прямой видимости. Главное назначение - создание бытовых сетей, присоединения мультимедийной периферии, стиральных машин, холодильников и т.д.. Концепция сети Bluetooth разработала 1994 шведская фирма Ericsson. Название технологии происходит от прозвища, которое дали Викингу Геральду Блатанду, который в X в. объединил разрозненные земли, создав Датское королевство. В 1997 г. созданы первые приемники-передатчики. В 1998 г. сформирована группа SIG, в которую вошли Ericsson, IBM, Intel, Nokia, Toshiba. В 1999 р. выпущено спецификации на оборудование. Подробнее о технологии Bluetooth. Новые технологии беспроводного передачи (Ultra Wideband (UWB)) предлагают скорости передачи, превышающие 100 Мбит / с, и требуют минимальных затрат энергии.

Технология SST

В технологии SST (Spread Spectrum Technology) использовано распределение сигнала по спектру частот. Это позволяет значительно повысить пропускные способности канала благодаря большей помехоустойчивости. Технологию SST уже длительный период применяли в военных целях. Есть две разновидности сетей SST:

- FH-SS. Приемник и передатчик синхронно перескакивают с частоты на частоту;

- DH-SS. В каждый момент времени сигнал «размазано» по широкому диапазону частот. Технология SST позволяет не только увеличить пропускные способности сети, но и лучше реализовать защиту информации от прослушивания. Внешний наблюда- тель такую информацию воспринимает как «белый шум».

Спутниковые технологии

Технология VSAT

Технология VSAT (Very Small Aperture Terminal) использует для передачи данных геостационарные спутники, размещенные над экватором Земли на высоте 40 тыс. км.Наземные станции для связи со спутником применяют эллиптические антенны диаметром 3 м. Канал VSAT:

- обеспечивает скорость передачи данных до 2 Мбит / с;
- позволяет реализовать сочетание на большие расстояния с переходом государственных границ;
- соизмеримый по цене с кабельными каналами такой же пропускной способности. Одновременно этот канал отличается значительными задержками передачи данных, обусловленными большим расстоянием до спутника (задержка составляет примерно 250 мкс, тогда как для кабельных сетей - 15 мкс). Поэтому канал VSAT нельзя использовать в системах реального времени и оперативной связи.

Поскольку стоимость спутникового канала велика, то поставщик услуг покупает у владельца спутника канал связи большой емкости и продает части пропускной способности канала. Итак, сеть с использованием звеньев VSAT имеет звездную структуру.

Системы низкоорбитальных спутников

Системы на базе низкоорбитальных спутников LEO (Low Earth Orbit), как и системы VSAT, для передачи используют спутник. Спутник находится на высоте около 100 км на обычной, а не геостационарной орбите. В этом случае уменьшается задержка в передаче данных. Кроме того, вывести такой спутник на орбиту гораздо дешевле, чем геостационарный. Вместе с тем для поддержания постоянной связи нужно использовать большое количество таких низкоорбитальных спутников. Среди имеющихся проектов LEO можно выделить систему Iridium, которая использует 66 спутников.

В первом варианте предполагали, что в системе будет 77 спутников. Именно столько электронов содержит атом иридия. Позже оказалось, что достаточно 66. Однако название решили оставить (название элемента с 66 электронами диспрозия происходит от латинского disprosius - труднодостижимой).

Корпорация Teledesic, владельцами которой являются Bill Gates и Greg MacCaw, планирует создать всемирную систему передачи мультимедийной информации на основе LEO-технологии. Планируется, что такая сеть будет использовать 840 спутников и предоставлять пользователям каналы пере ¬ пускнои способности от 62 Кбит / с до 2 Мбит / с.

Сети на сотовых модемах

Сети на сотовых модемах используют существующую инфраструктуру сотовой телефонии. Они работают в особо тяжелых условиях больших помех, периодического пропадания сигнала.

Среди методов доступа выделяют аналоговые, использующие для передачи аналоговый сигнал. Это классические методы доступа в сотовых сетях FDMA (Frequency Division Multiple Access), TACS (Total Access Communication System).

Главный ресурс сотовой сети - это предназначенный для нее диапазон частот. Аналоговые методы доступа выделяют для каждого передачи отдельный канал - полосу ча- стот в предназначенном для сети диапазоне. В этом случае соседние сотовые ячейки не могут работать в одном и том же диапазоне частот (иначе передачи в соседних ячейках мешали бы друг другу). Частотный диапазон делят на семь частей.

Среди методов доступа, которые используют цифровое передачи, популярны различные модификации TDMA (Time Division Multiple Access). Они применяют известный принцип распределения времени передачи на отдельные временные слоты. К этой группе

методов относятся AMPS (Advanced Mobile Phone Service) (частотные каналы шириной 30 кГц делятся на три временные слоты), NAMPS (Narrowband AMPS), PDC (каналы по 25 кГц, три слота), GSM (диапазон 200 кГц, восемь слотов).

CDMA

Передовой сегодня является технология CDMA (Code Division Multiple Access), которая использует цифровое передачи.

CDPD

Технология CDPD (Cellular Digital Packet Data) реализует как пакетное передачи (протокол TCP / IP), так и модемный интерфейс (AT-команды). В отличие от радиомодемов, сотовые модемы используют не специальные антенны и приемники-передатчики, а соответствующие устройства сотового телефона. При передаче данных применяют протоколы MNP-10 или ETC. Протокол MNP-0 динамически оптимизирует скорость передачи данных и уровень сигнала, имеет развитые средства працювання ошибок.

ETC

Протокол ETC предложила 1993 г. фирма AT & T Paradyne. Он основывается на состояние ¬ Дарти V.32bis (14.4 Кбит / с) и позволяет поддерживать связь с другими модемами стандарта ETC и другими протоколами. По сравнению с MNP-10 совершеннее технически. Развитие технологий на более высоких уровнях протокола выраженный в организации доступа к Internet. Этот доступ возможен благодаря использованию WAP-технологий.

Системы на базе инфракрасных каналов

Системы на базе инфракрасных каналов отличаются небольшой стоимостью приемников и передатчиков (от 1.5 до 4.5 дол. США), высокими скоростями передачи. Однако инфракрасные каналы работают только в условиях прямой видимости. Ассоциация Infrared Data Communications разработала стандарт передачи инфракрасным каналом со скоростью 115.2 Кбит / с.

Радиорелейная связь

Радиорелейные станции (РРС) используют для передачи аналогового сигнала в телевидении и цифрового в последовательном коде по стандарту ITU G.703 в телефонии. Канал G.703 имеет пропускной способностью 2 Мбит / с. Его можно использовать, например, для соединения сегментов Ethernet. Современные цифровые РРС имеют полосу перепуска 2-34 Мбит / с. Поэтому часто ее разделяют на несколько каналов. Максимальное расстояние для связи РРС - 60-80 км. Для наземных РРС используют частотные диапазоны 1, 5, 7, 15, 23, 34 ГГц. Взаимодействия маршрутизатора и РРС постигают при помощи конвертера V.35/G.703.

Порядок работы

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

Примечание. Эта часть задания выполняется на одном из компьютеров, с помощью которого будет настроена точка доступа. Поскольку настройка беспроводной точки доступа обычно осуществляется через веб-интерфейс с использованием стандартного сетевого Ethernet-соединения, выбранный компьютер нужно подключить к точке доступа, а затем правильно сконфигурировать параметры протокола IP на этом компьютере.

1. Возьмите беспроводную точку доступа и, используя разъем для коннектора RJ-45, соедините с помощью кабеля «витая пара» точку доступа с одним из компьютеров класса.

Примечание. Как правило, точки доступа имеют порты с автоопределением MDI/MDI-X, поэтому тип кабеля (прямой или перекрестный) обычно не имеет значения. Однако желательно проверить, поддерживает ли ваша точка доступа эту функцию, в ее руководстве пользователя.

1. Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы».

2. В меню **Пуск** щелкните правой кнопкой мыши на пункте **Сетевое окружение** и в появившемся контекстном меню выберите пункт **Свойства**.

3. В открывшемся окне **Сетевые подключения** щелкните правой кнопкой мыши на значке **Подключение по локальной сети** и в появившемся контекстном меню выберите пункт **Свойства**.

4. В окне свойств сетевого подключения щелкните мышью на строке **Протокол Интернета (TCP/IP)** в списке **Компоненты, используемые этим подключением**, а затем щелкните мышью на кнопке **Свойства**.

5. В окне настройки параметров протокола IP выберите радиокнопку **Использовать следующий IP-адрес** и введите следующие параметры:

- IP-адрес — 192.168.1.200;
- маска подсети — 255.255.255.0.

Примечание. Как правило, точка доступа имеет предварительно установленный IP-адрес в сети 192.168.1.0 (обычно 192.168.1.1 или 192.168.1.254). Желательно проверить в руководстве пользователя, какой IP-адрес и пароль входа настроены изготовителем для вашей точки доступа.

6. Дважды щелкните мышью на кнопках **OK**, чтобы закрыть окна настройки сетевого подключения. Закройте окно **Сетевые подключения**.

7. В меню **Пуск** выберите пункт **Интернет**.

8. В открывшемся окне программы **Microsoft Internet Explorer** в поле **Адрес** введите строку http://*IP-адрес вашей точки доступа* (например, http://192.168.1.1) и щелкните мышью на значке **Переход**.

9. В окне авторизации введите пароль, указанный в документации к вашей точке доступа.

Примечание. Дальнейшие действия зависят от конкретной точки доступа, поэтому ниже приведены

лишь общие шаги настройки, позволяющие добиться сетевого взаимодействия с беспроводными клиентами. Следует обратить внимание, что для упрощения подключения здесь приведены такие параметры настройки, которые не рекомендуется применять в реальной работе (в частности, здесь включается режим оповещения и отключается защита при беспроводном доступе).

10. Найдите в меню управления точкой доступа раздел **Wireless Settings** («настройки беспроводного взаимодействия») или аналогичный и настройте следующие (или аналогичные) параметры:

- **Channel** («канал») — оставьте установленным по умолчанию;
- **SSID** («идентификатор») — введите название вашей точки доступа, например, ClassAP;
- **SSID Broadcast** («оповещение») — для упрощения обнаружения вашей точки доступа беспроводными клиентами этот режим лучше включить (**Enable**);
- **Wireless Mode** («стандарт, используемый точкой доступа») — для совместимости лучше указать смешанный режим 802.11b/g.

11. Щелкните мышью на кнопке **Apply** («применить»). Перейдите к разделу **Encryption** («шифрование») или аналогичному и выберите следующий (или аналогичный) параметр:

- **Security Mode** («режим защиты») — отключен (**Disabled**).

Внимание! Отключение защиты производится в этом задании только для упрощения настройки! На практике такие параметры беспроводного взаимодействия применять нельзя.

12. Щелкните мышью на кнопке **Apply** («применить») и закройте окно программы **Internet Explorer**.

Настройка беспроводного адаптера и подключение к точке доступа

Примечание. Эта часть задания выполняется на компьютере, не имеющем проводного подключения к сети.

1. Возьмите беспроводной сетевой адаптер и установите его в один из компьютеров сети.

Примечание. Если это PCI-совместимый адаптер, то процедуру установки адаптера в разъем следует проводить, как описано в задании 2 лабораторной работы 3. Если это USB-адаптер, его можно подключить к любому порту USB работающего компьютера.

2. Включите компьютер и войдите в систему с учетной записью, входящей в локальную группу «Администраторы».

Примечание. Поскольку ОС Windows XP Professional пока не имеет в своем комплекте драйверов для большинства беспроводных адаптеров, после входа в систему или подключения USB-адаптера должен запуститься **Мастер нового оборудования**. Если этого не произошло, то проверьте в **Диспетчере устройств**: возможно, ваш адаптер автоматически определен ОС и драйверы для него уже установлены. В этом случае соответствующие пункты этого раздела можно пропустить.

На странице **Мастер нового оборудования** выберите радиокнопку **Нет, не в этот раз** и щелкните мышью на кнопке **Далее**

3. На странице **Если с устройством поставляется установочный диск, вставьте его** убедитесь, что выбрана радиокнопка **Автоматическая установка (рекомендуется)**, вставьте компакт- или флоппи-диск (из комплекта беспроводного адаптера) с драйвером и щелкните мышью на кнопке **Далее**.

Примечание. Если после установки диска запустится какая-либо программа, то закройте ее.

4. Мастер нового оборудования должен найти на диске подходящий для вашего адаптера драйвер. На странице **Выберите наиболее подходящее программное обеспечение для вашего оборудования** щелкните мышью на кнопке **Далее**.

Примечание. Если появится предупреждение, что устанавливаемое программное обеспечение не тестировалось на совместимость с Windows XP, щелкните мышью на кнопке **Все равно продолжить**.

5. На странице **Мастер завершил установку программ для** щелкните мышью на кнопке **Готово**.

Примечание. Если все операции выполнены правильно, то в Панели задач появится значок беспроводного сетевого подключения.

6. Щелкните правой кнопкой мыши на значке **Беспроводное сетевое соединение** в Панели задач и выберите в меню пункт **Просмотр доступных беспроводных сетей**.

7. На странице **Выберите беспроводную сеть** выберите сеть с названием, указанным в поле **SSID** при настройке вашей точки доступа (например, ClassAP**)**, и щелкните мышью на кнопке **Подключить**.

Примечание. Если появится предупреждение, что сеть является незащищенной, то щелкните мышью на кнопке **Подключить**. Подключение к беспроводной сети должно установиться, однако оно корректно не заработает, пока не будут настроены совместимые IP-адреса.

8. Выполните двойной щелчок мышью на значке **Беспроводное сетевое соединение (ClassAP)** в Панели задач.

9. В окне **Состояние Беспроводное сетевое соединение** щелкните мышью на кнопке **Свойства**.

10. В окне свойств беспроводного сетевого подключения щелкните мышью на строке **Протокол Интернета (TCP/IP)** в списке **Компоненты, используемые этим подключением**, а затем щелкните мышью на кнопке **Свойства**.

11. В окне настройки параметров протокола IP выберите радиокнопку **Использовать следующий IP-адрес** и введите параметры:

- IP-адрес — 192.168.1.150;
- маска подсети — 255.255.255.0.

12. Дважды щелкните мышью на кнопках **ОК** и закройте все окна.

Подключение точки доступа к сети Ethernet и проверка взаимодействия в гетерогенной сети

Примечание. Эта часть задания выполняется на компьютерах, подключенных к сети Ethernet, построенной в ходе выполнения задания 1 данной лабораторной работы.

1. Используя кабель «витая пара», подключите беспроводную точку доступа к порту RJ-45 коммутатора Fast Ethernet.
2. Настройте на компьютерах сети параметры протокола IP, совместимые с теми, которые вы использовали при настройке беспроводной точки доступа и компьютера с беспроводным адаптером, например, следующие:

- IP-адрес — 192.168.1.10*x*, где *x* — номер компьютера в классе;
- маска подсети — 255.255.255.0.

То есть, первый компьютер должен иметь IP-адрес, равный 192.168.1.101, второй — 192.168.1.102 и т. д.

3. Попытайтесь обратиться к общим ресурсам на компьютерах сети (особенно интересно проверить, работает ли обращение к ресурсам компьютеров с беспроводными адаптерами).

Удалось ли вам обратиться к ресурсам какого-либо из компьютеров сети?

4. Закройте все окна и завершите работу с компьютером.

Время выполнения работы 90 мин;

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 6 «Поиск неисправностей технических средств»

Цель работы: Освоить технологию определения неисправностей технических средств.

В процессе занятия решаются следующие задачи:

1. Научиться определять основные технические характеристики аппаратных средств
2. Изучить методические указания и рекомендуемую литературу.
3. При помощи спец. программы собрать данные о технических характеристиках персонального компьютера.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Классификация неисправностей АПС

Для выбора метода диагностики и определения первичных и вторичных симптомов отказа необходимо уметь классифицировать неисправность, т. к. первичный отказ часто

вызывает целый спектр отказов вторичных, являющихся следствием первичного и затеняющих причину неисправности.

Предлагаемая классификация охватывает ошибки и отказы, вызванные электронными узлами *системной платы*, как наиболее сложной части PC, и может быть распространена на весь клон IBM PC.

С позиции аппаратных и программных средств, используемых в PC, неисправности подразделяются на аппаратные, программные и аппаратно-программные.

Аппаратные неисправности, т. е. неисправности аппаратных средств, в свою очередь, подразделяются на случайные, мягкие и жесткие ошибки.

К **случайным** ошибкам относят:

1) плавающие ошибки;
2) корректируемые отказы;
3) некорректируемые отказы (технические остановы).

Потенциально, любая неисправность, связанная со случайными ошибками, может привести к жесткой ошибке. Случайная ошибка, приобретшая фактор стабильности и делающая невозможной дальнейшую эксплуатацию системы классифицируется как жесткая, не корректируемая и требует анализа и диагностики неисправности АПС. Нередко, после коррекции условий эксплуатации ВС (температурно-климатические, вибрационные и т. д.), такие ошибки исчезают, но, по истечении некоторого времени, появляются снова. Та- ким образом, это – не метод устранения ошибок, и задача инженера или техника по ТО – наоборот, *ужесточить условия эксплуатации ВС на время диагностики,* с целью выявления ошибки и выделения отказавшего узла. Наиболее неприятны отказы, связанные с факторами нестабильности и неопределенности – плавающие ошибки.

Порядок работы

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

Запустить программу Everest на тестируемом компьютере и с помощью мастера отчетов (меню «Отчёт») сформировать отчет об ап- паратном обеспечении.

2. Заполнить табл. 1.

1. Результаты выполнения работы

№	Наименование компонента системного блока или характеристика	Найденное обозначение или характеристика
1	Тип ЦП, частота	
2	Тип системной платы, форм-фактор	
3	Чипсет системной платы	
4	Тип жесткого диска, объем	
5	Тип сетевого адаптера	
6	Тип видеоадаптера	
7	Тип звукового адаптера	
8	Разъемы ОЗУ	
9	Разъемы расширения системной платы	
10	Объем кэш-памяти процессора	

Время выполнения работы 90 мин;

Контрольные вопросы

1. Назначение и компоненты системной платы.
2. Что такое северный мост? Его назначение.
3. Что такое южный мост? Его назначение.
4. Что такое форм-фактор материнской платы?

5. Назначение центрального процессора.

6. Что такое многоядерный процессор?

7. Что такое кэширование?

8. Оперативное запоминающее устройство. Его назначение.

9. Что такое энергозависимые и энергонезависимые запоминающие устройства?

10. Универсальная последовательная шина USB. 11. Шина ввода-вывода PCI и PCI-Express.

12. Шина AGP.

13. Видеокарта. Назначение и устройство.

14. Сетевой адаптер. Назначение, типы, параметры и функции.

15. Назначение и типы оптических приводов. 16. Жёсткий диск. Назначение и устройство.

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 7 «Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы, коммутационное оборудование»

Цель работы: изучить основные блоки и периферийные устройства персонального компьютера, способы их соединения, конструктивы (разъемы), основные характеристики (название, тип разъема, количество контактов, скорость передачи данных, дополнительные свойства);

.

В процессе занятия решаются следующие задачи:

1. научиться определять по внешнему виду типы разъемов, подключаемое к ним оборудование;
2. знать основные устройства персонального компьютера, их назначение и основные характеристики;
3. научиться определять компоненты системного блока по внешнему виду, уяснить порядок и способы их соединения.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Периферийное устройство — аппаратура, которая позволяет вводить информацию в компьютер или выводить ее из него.

Периферийные устройства являются опциональными, и, технически, могут быть отключены от компьютера без потери его работоспособности. Однако абсолютное большинство компьютеров используются вместе с теми или иными периферийными устройствами.

Выделяют три основных типа периферийных устройств:

- Устройства ввода, использующиеся для ввода информации в компьютер: мышь, клавиатура, сенсорный экран, сканер, веб-камера и видеозахват
- Устройства вывода, например мониторы, принтеры
- Устройства хранения, служащие для накопления информации, обрабатываемой компьютером: НЖМД, НГМД, ленточные и дисковые устройства,накопители "флеш"

Иногда периферийное устройство относится к нескольким типам, например Устройство ввода-вывода.

Отдельно взятое устройство из класса периферийных устройств компьютера. Класс *периферийных* устройств появился в связи с разделением вычислительной машины на внутренние и внешние устройства. Внутренние — это вычислительные (логические) блоки (то есть процессоры) и память хранения выполняемой программы. Внешние устройства — это и есть периферийные устройства, вместе с подключающими их интер- фейсами. Таким образом, периферийные устройства, расширяя возможности ЭВМ, не из- меняют её архитектуру.

Периферийными устройствами также можно считать внешние по отношениюк системному блоку компьютера устройства.

Порядок работы

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

1. Убедитесь в том, что компьютерная система обесточена (при необходимости, отключите систему от сети).
2. Разверните системный блок задней стенкой к себе.
3. По наличию или отсутствию разъемов USB установите форм-фактор материнской платы (при наличии разъемов USB - форм-фактор ATX, при их отсутствии -AT).
4. Установите местоположение и снимите характеристики следующих разъемов:
    - питания системного блока;
    - питания монитора;
    - сигнального кабеля монитора;
    - клавиатуры;
    - последовательных портов;
    - параллельного порта (если есть);
    - других разъемов.
5. Убедитесь в том, что все разъемы, выведенные на заднюю стенку системного блока, не взаимозаменяемы, то есть каждое базовое устройство подключается одним единственным способом.
6. Изучите способ подключения мыши.

    Мышь может подключаться к разъему последовательного порта или к специальному порту PS/2, имеющему разъем круглой формы. Последний способ является более современным и удобным. В этом случае мышь имеет собственный выделенный порт, что исключает возможность ее конфликта с другими устройствами, подключаемыми к последовательным портам. Последние модели могут подключаться к клавиатуре через разъем интерфейса USB.

7. Заполните таблицу:

Разъем	Тип разъема	Количество контактов	Примечания

8. Определить наличие основных устройств персонального компьютера.
9. Установите местоположение блока питания, выясните мощность блока питания (указана на ярлыке).
10. Установите местоположение материнской платы.
11. Установите характер подключения материнской платы к блоку питания.
    Для материнских плат в форм-факторе AT подключение питания выполняется двумя разъемами. Обратите внимание на расположение проводников черного цвета - оно важно для правильной стыковки разъемов.
12. Установите местоположение жесткого диска.
    Установите местоположение его разъема питания. Проследите направление шлейфа проводников, связывающего жесткий диск с материнской платой. Обратите внимание на местоположение проводника, окрашенного в красный цвет (на жестком диске он должен быть расположен рядом с разъемом питания).
13. Установите местоположения привода CD-ROM (DVD-ROM).
    Проследите направление их шлейфов проводников и обратите внимание на положение проводника, окрашенного в красный цвет, относительно разъема питания.
14. Установите местоположение платы видеоадаптера.
    Определите тип интерфейса платы видеоадаптера.
15. При наличии прочих дополнительных устройств выявите их назначение, опишите характерные особенности данных устройств (типы разъемов, тип интерфейса и др.).
16. Заполните таблицу:

Устройство	**Характерные особенности**	**Куда и при помощи чего подключается**

Время выполнения работы 90 мин;

Контрольные вопросы

1. Архитектура вычислительных систем.
2. Состав системного блока.
3. Назначение, основные характеристики, интерфейс устройств персонального компьютера (по каждому устройству), входящих в состав системного блока.
4. Устройство жесткого диска
1. Базовая аппаратная конфигурация;
2. Основные характеристики монитора;
3. Характеристики (тип разъема, количество контактов, скорость передачи данных) разъемов: видеоадаптера; последовательных портов; параллельного порта; шины USB; сетевой карты; питания системного блока; питания монитора.
4. Типы периферийных устройств.

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

2. Работа оценивается на «четыре балла» если допущена 1 ошибка в выполнении

последовательности выполнения работы т.е.команды введены правильно, но в ходе выполнения действия команды возникли затруднения, выводы сделаны правильно

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 8 «Тестирование кабелей»

Цель работы: Освоить технологию определения неисправностей СКС.

В процессе занятия решаются следующие задачи:

1. Научиться определять неисправности СКС используя кабельный тестер

Краткие теоретические и справочно-информационные материалы по теме занятия.

Трассоискатель кабельный тестер NF-806B

Модель NF-806B совмещает в себе функции трассоискателя и кабельного тестера. Трассоискатель предназначен для поиска нужного провода, прослеживания трассы его прокладки до коммутационной панели без повреждения изоляции. Тестер состоит из двух приборов – эмиттера (передатчика) и приемника. Функции кабельного тестера заключаются в исследовании витой пары на правильность разводки, замыкания обрывы.

Порядок работы

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

Функция обнаружения телефонного провода

1. Подключите телефонную линию к разъему RJ11 эмиттера.

2. Переведите трехпозиционный переключатель в положение “SCAN”, начнет мигать индикатор “STATUS”, что обозначает нормальную работу эмиттера.

3. Нажмите и удерживайте кнопку «PUSH TO TEST” на приемнике, поднесите щуп пробника к другому концу обследуемого провода.

4. Во время проведения измерений нажатием на кнопку переключения функций передатчика можно изменять двухтоновый сигнал.

5. Сравните громкость звукового сигнала и яркость индикатора приемника. Они будут максимальными для искомого провода.

Вариант 1: Обнаружение провода в коммутаторе

Подключите эмиттер к разъему телефонного кабеля, который нужно обнаружить. При помощи приемника найдите другой его конец в коммутаторе.

Вариант 2: Обнаружение провода на кроссовой панели

Подключите эмиттер к разъему телефонного кабеля, который нужно обнаружить. При помощи приемника найдите другой его конец на кроссовой панели.

Функция обнаружения витой пары

1. Подключите сетевой кабель к разъему RJ45 эмиттера.
2. Переведите трехпозиционный переключатель в положение “SCAN”, начнет мигать индикатор “STATUS”, что обозначает нормальную работу эмиттера.
3. Нажмите и удерживайте кнопку «PUSH TO TEST” на приемнике, поднесите щуп пробника к другому концу обследуемого провода. 4. Сравните громкость звукового сигнала и яркость индикатора. Они будут максимальными для искомого провода.

Вариант 1: Обнаружение провода на роутере

Подключите эмиттер к разъему сетевого кабеля, который нужно обнаружить. При помощи приемника найдите другой его конец на роутере.

Вариант 2: Обнаружение провода в пучке

Подключите эмиттер к разъему сетевого кабеля, который нужно обнаружить. Вызвоните провод в пучке.

Функция обнаружения электрического провода

1. Подключите сетевой провод при помощи зажимов «Крокодилы» к эмиттеру.
2. Повторите пункты 2 – 5 из раздела тестирования телефонного провода.

Примечание: прибор запрещается использовать для проверки многоамперных проводов.

Функция тестирования витой пары

1. Вставьте разъемы RJ45 в соответствующие гнезда на эмиттере и приемнике.
2. Переведите трехпозиционный переключатель в положение “TEST”, начнет мигать индикатор “VERIFY”, что обозначает нормальную работу эмиттера.
3. В соответствии с 16 последовательностями определите наличие короткого замыкания, обрыва, незамкнутой цепи и перекрестные пары.
4. Во время проведения измерений нажатием на кнопку переключения функций можно выбирать быстрый и медленный режим

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 9 «Тестирование коммутационного оборудования»

Цель работы: Освоить технологию определения неисправностей технических средств.

В процессе занятия решаются следующие задачи:

1. Научиться определять основные технические характеристики аппаратных средств
2. Изучить методические указания и рекомендуемую литературу.
3. При помощи спец. программы собрать данные о технических характеристиках персонального компьютера.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Тестирование ЛВС осуществляется на стадии завершения работ по монтажу сети ЛВС и представляет собой осмотр созданной сети на предмет ее соответствия принятым стандартам. Серьезный и грамотный подход к тестированию ЛВС обеспечивает гарантию длительной, устойчивой и полноценной работы локальной сети и позволяет свести к минимуму работы в соответствии с таким немаловажным этапом, как диагностика сети.

Тестирование ЛВС включает в себя следующие этапы:

- проверка кабель-каналов
- осмотр рабочих узлов
- тестирование коммутационного оборудования

На этапе осмотра кабельных каналов проверяется целостность кабеля, правильность расположения кабельных жгутов, а также расположение кабельных трасс относительно источников помех и соответствие кабельной системы требованиям стандартов. Осмотр рабочих мест выявляет правильность прокладки кабеля вблизи розеточных модулей, а также наличие маркировки. Тестирование коммутационного оборудования определяет текущее состояние сети на предмет ее соответствия документации.

По результатам тестирования составляется отчет – документ, содержащий в себе выводы о техническом состоянии лвс и перечень рекомендаций по устранению выявленных неполадок, текущей эксплуатации и путям развития и модернизации сети в будущем.

Диагностика ЛВС и средства ее осуществления

Диагностика ЛВС является важной составляющей администрирования локальной сети и представляет собой процесс поиска неисправностей, замедляющих работу программного обеспечения и сети в целом. Последние можно условно разделить на три основные группы:

- физические неисправности
- ошибки в работе сетевых протоколов
- перегрузки в сети

Неисправности физического уровня связаны с выходом из строя сетевых устройств и компонентов. Перегрузки возникают вследствие невозможности сетевых устройств справиться с объемом поступающих к нему запросов. Ошибки в работе протоколов ведут к проблемам взаимодействия сетевых устройств друг с другом.

Для осуществления качественной диагностики ЛВС в мире разработано множество различных диагностических средств, позволяющих быстро определять причины сбоев в работе сетей. В области сетевой диагностики применяется, в частности, специализированное оборудование, такое как анализаторы сетевых протоколов, приборы мониторинга функционирования сети, кабельные и сетевые тестеры, а также специализированное тестирующее программное обеспечение. Так, обнаружить физическую неисправность можно с помощью простейших тестеров, проверяющих работу канала, а инструментальная диагностика ошибок, связанных с перегрузками и некорректной работой сетевых протоколов, осуществляется при помощи сетевых тестеров и анализаторов протоколов.

Значительная часть вышеперечисленных приборов имеет достаточно высокую цену, и это является одной из главных причин воспользоваться для проведения диагностики лвс услугами сторонних компаний, уже имеющих в своем распоряжении данное оборудование. Кроме того, даже если Вы решите приобрести такое оборудование и заниматься диагностикой лвс Вашего предприятия, что называется, «не отходя от кассы», совершенно не факт, что Ваш штатный системный администратор успешно справится с подобной задачей: ведь опыт и интуицию, в отличие от кабельных тестеров, не купишь.

Компания «Флайлинк» специализируется на разработке, установке и тестировании ЛВС, а также диагностике и обслуживании не первый год. В нашем распоряжении – самое передовое оборудование и технологии, а многочисленные положительные отзывы Клиентов подтверждают высочайшую квалификацию наших специалистов и качество выполненных работ.

Порядок работы

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

1) В работе приведены описания нескольких систем, для которых необходимо подобрать активное оборудование.
2) В описаниях указаны транспортные задачи, которые должно решить оборудование, а также дополнительные требования к разворачиваемой системе.
3) При подборе оборудования необходимо соблюдать принцип минимизации финансовых затрат.
4) Ограничения по производителям оборудования нет, однако рекомендуется обратить внимание на оборудование 3Com, CISCO и D-LINK.

Задание 1 – подобрать коммутационное оборудование для сети небольшого офиса. В состав сети входят 15 компьютеров с равным уровнем доступа. Максимальная нагрузка на сеть возможна при одновременном доступе к файловой базе данных объемом 96 Мб.

Задание 2 – подобрать коммутационное оборудование для проведения чемпионата России по киберспорту. Планируется обеспечить совместную работу 80 компьютеров. Следует избежать ситуации задержек в игре из-за недостаточной производительности коммутационного оборудования. Считайте, что пиковый трафик, генерируемый средней современной сетевой игрой составляет 10 Мб\с. Возможна компактная установка коммутационного оборудования в одной стойке.

Задание 3 – подобрать коммутационное оборудование для сети крупного предприятия. Требуется организовать изолированные потоки данных для разных отделов предприятия и высокоскоростной back-bone для связи отделов и доступа к сервисам предприятия. Примем количество отделов 5, по 30 компьютеров в каждом отделе.

Задание 4 – подобрать коммутационное оборудование для сети студии киномонтажа. В студии создан вычислительный кластер для обсчета цифрового видео из 4 компьютеров. Оборудование должно быть гарантированно неблокирующем, то есть обладать внутренней шиной такой производительности, чтобы гарантированно обработать максимально возможные потоки между всеми нагруженными портами коммутатора.

Задание 5 – подобрать коммутационное оборудование для ядра крупной корпоративной сети. Обеспечить коммутацию 18 стомегабитных каналов от подразделений. Необходимо реализовать фильтрацию на основе IP адресов и поддержку протоколов маршрутизации RIP2.

Задание 6 – подобрать коммутационное оборудование для использования в качестве узловых точек растущей сети провайдера кабельного домашнего Internet. Необходимо обеспечить удаленное управление устройством.

Задание 7 – подобрать коммутационное оборудование для оператора сети. Через сеть в среднем передается 4 Терабайта в день. Необходимо обеспечить соединение сетей с разными канальными протоколами (FastEthernet, GigabitEthernet и FDD).

Время выполнения работы 90 мин;

Контрольные вопросы

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 10-11-12 «Резервное копирование. Организация бесперебойной работы системы резервного копирования. Восстановление работоспособности сети после сбоя»

Цель работы: Изучение процесса резервного копирования, восстановления системы после сбоя

В процессе занятия решаются следующие задачи:

1. Научиться восстанавливать систему из копий «backup».

Краткие теоретические и справочно-информационные материалы по теме занятия.

Что из себя представляет система резервного копирования?

Система резервного копирования – это один из дополнительных компонентов операционной системы Windows Server 2008, позволяющий выполнять надежное резервное копирование и восстановление операционной системы, а также файлов и папок, расположенных на сервере. В состав системы резервного копирования входит соответствующая оснастка консоли MMC, а также средства командной строки.

Важно.

Необходимая для этих целей оснастка консоли MMC не входит в состав операционной системы Windows Server 2008 Standard. Чтобы иметь возможность управлять резервным копированием непосредственно на компьютере, работающем под управлением этой операционной системы, Вам необходимо воспользоваться средствами командной строки, либо для удаленного управления резервным копированием воспользоваться соответствующей оснасткой на другом компьютере.

Что нового в системе резервного копирования?

В систему резервного копирования внесены следующие улучшения:

- **Ускоренная технология резервного копирования.** Для выполнения резервного копирования и восстановления операционной системы, файлов и папок, а также томов система резервного копирования использует службу теневого копирования томов (Volume Shadow Copy Service, VSS) и технологию резервного копирования на уровне блоков. После создания первой полной резервной копии Вы можете настроить систему на автоматическое создание инкрементных резервных копий, в которые будут включаться только изменения, внесенные с момента последнего резервного копирования. Даже в том случае, если Вы выберете вариант создания полных резервных копий каждый раз, сам процесс создания будет занимать гораздо меньше времени, чем он бы занимал в более ранних версиях операционной системы Windows.
- **Упрощенное восстановление.** Вы можете восстанавливать только необходимые элементы из резервной копии путем начального выбора самой резервной копии и последующего указания необходимых в ней элементов. Вы можете восстановить только необходимые Вам файлы и папки, или же все содержимое папки целиком. Кроме того, если ранее для восстановления необходимых данных из инкрементных резервных ко- пий Вам необходимо было выполнить последовательное восстановление из всех инкре- ментных резервных копий, то теперь достаточно просто указать дату создания резерв- ной копии, содержащей данные, которые Вам необходимо восстановить.

- **Упрощенное восстановление операционной системы.** Система резервного копирования работает теперь с новыми средствами восстановления Windows, что позволяет упростить восстановление операционной системы. Вы можете выполнить восстановление системы на том же сервере, на котором создавалась эта резервная копия, либо в случае возникновения аппаратного сбоя можете восстановить операционную систему на новый сервер, не содержащий операционной системы.
- **Возможность восстановления приложений.** Для защиты данных приложений система резервного копирования использует функциональные возможности VSS, встроенные в такие приложения, как Microsoft SQL Server™ и Windows SharePoint® Services.
- **Улучшенный планировщик.** В состав системы резервного копирования включен мастер, который проведет Вас через все шаги процесса создания ежедневных резервных копий. Тома, содержащие системные компоненты, автоматически включаются во все плановые резервные копии, благодаря чему обеспечивается надежная защита данных в случае сбоев.
- **Возможность хранения резервных копий отдельно от сервера для защиты от аварий.** Вы можете сохранять резервные копии по очереди на несколько дисков, что позволяет выносить их для хранения за пределы местонахождения сервера. Для этого подключите диски и укажите их в качестве разрешенного места создания плановых резервных копий. При этом если первый из списка диск будет отключен и помещен в отдельное хранилище за пределами местонахождения сервера, система резервного копирования автоматически создаст резервную копию на следующем диске из списка.

- **Удаленное администрирование.** Система резервного копирования использует оснастку консоли MMC, предоставляя, таким образом, в Ваше распоряжение знакомую и единообразную по виду интерфейса среду для управления резервным копированием. После того, как Вы установите оснастку **Система архивации данных Windows Server**, Вы сможете получать к ней доступ через диспетчер сервера, либо через новую, или имеющуюся консоль MMC, предварительно добавив в нее эту оснастку. После этого Вы можете использовать данную оснастку для управления резервными копиями на других серверах. Для этого в меню **Действие** необходимо выбрать пункт **Подключиться к другому компьютеру**.
- **Автоматическое управление использованием дисков.** После того, как Вы настроите создание резервных копий по расписанию, система резервного копирования самостоятельно начнет следить за использованием дискового пространства. Благодаря этому Вам не нужно будет заботиться о наличии свободного места на диске из-за создания нескольких резервных копий, поскольку при создании новых резервных копий система резервного копирования будет автоматически повторно использовать дисковое пространство, занимаемое более ранними резервными копиями. При этом в средстве управления будет отображаться информация об имеющихся резервных копиях и об объеме дискового пространства. Это может помочь Вам в планировании предоставления дополнительного дискового пространства в том случае, если необходимо иметь резервные копии, созданные за более длительный период времени.
- **Расширенная поддержка командной строки.** Система резервного копирования включает в себя расширенную поддержку командной строки и документацию, позволяющие Вам выполнять большинство из тех задач, которые Вы можете выполнять с помощью соответствующей оснастки консоли MMC. Вы также можете автоматизировать процесс создания резервных копий с помощью сценариев.
- **Поддержка DVD-дисков**. Вы можете в ручном режиме создавать резервные копии томов прямо на DVD-дисках. Это позволяет создавать резервные копии, которые затем можно легко перенести в отдельное хранилище за пределами расположения сервера. Этот способ создания резервных копий также позволяет создавать резервные копии в ручном режиме с сохранением их на локальных и сетевых дисках. Обратите внимание на то, что резервные копии, создаваемые по расписанию, всегда должны размещаться на локальных дисках.

Примечание.

Система резервного копирования, входящая в состав Windows Server 2008, не позволяет использовать средства хранения на магнитной ленте (стримеры). Поддерживается использование только внешних и внутренних жестких дисков, DVD-дисков и общих па- пок. Не смотря на это, в Windows Server 2008 все еще включена поддержка драйверов для средств хранения на магнитной ленте.

Кто должен использовать систему резервного копирования?

Система резервного копирования предназначена для широкого круга пользователей – от владельцев малого бизнеса, до системных администраторов на крупных предприятиях. Однако упрощенный интерфейс позволяет также использовать эту систему в более мелких организациях, а также теми, кто не является специалистами в области информационных технологий.

Данное пошаговое руководство предназначено для:

- Владельцев малого бизнеса, планирующих использовать систему резервного копирова-

ния.

- ИТ-специалистов крупных предприятий, занимающихся планированием и анализом информационной инфраструктуры, оценивающих функциональные возможности продукта.
- Специалистов, осуществляющих раннее внедрение Windows Server 2008.
- Архитекторов безопасности, ответственных за реализацию концепции защищенных информационных систем (trustworthy computing).

Преимущества от использования системы резервного копирования

Вы можете использовать систему резервного копирования Windows Server 2008 для защиты всего сервера без необходимости применения сторонних технологий резервного копирования. Встроенные мастера проведут Вас через все шаги процесса настройки автоматического создания резервных копий по расписанию, создания резервных копий в ручном режиме (в случае необходимости), а также восстановления определенных элементов или целых томов. С помощью системы резервного копирования Вы можете создавать резервные копии всего сервера целиком, или только необходимых томов.

В случае возникновения проблем с жестким диском или других неполадок, из-за которых сервер невозможно запустить, Вы можете воспользоваться мастерами и прочими компонентами системы резервного копирования, а также средством восстановления Windows (Windows Complete PC Restore), которые помогут Вам преодолеть возникшие проблемы, проведя через весь процесс восстановления работоспособности сервера. Данный способ восстановления позволяет значительно сократить время вынужденного простоя по сравнению с тем, если бы для восстановления работоспособности сервера была переустановлена операционная система и затем было бы произведено восстановление данных из резервных копий.

Меры безопасности

Поскольку в резервных копиях содержится копия Вашей операционной системы и прочие важные данные, следует соблюдать меры предосторожности, направленные на предотвращение доступа к этим данным неавторизованных пользователей. Для этого рекомендуем воспользоваться следующими советами:

- Ограничьте физический доступ к резервным копиям, поместив их для хранения в защищенное место. Данную меру предосторожности следует соблюдать даже в том случае, если у Вас имеется резервная копия зашифрованных томов, поскольку данные, находящиеся в этой резервной копии, не являются зашифрованными.
- Ограничьте количество пользователей, входящих в группу Администраторы или Операторы Архива на сервере. Члены указанных групп могут пользоваться системой создания резервных копий.
- Использование удаленной общей папки в качестве места хранения резервных копий требует наличия у пользователя, выполняющего резервное копирование, следующих прав и полномочий:

  - Наличие прав на запись в сетевую папку.
  - Членство в группе Операторы архива или Администраторы на том сервере, на котором выполняется создание резервных копий.

Предоставьте этой учетной записи минимально необходимые права для работы, с целью уменьшения вероятности несанкционированного доступа третьих лиц к ресурсам сети во время создании резервных копий с использованием данной учетной записи.

- При использовании сетевой папки в качестве места хранения резервных копий ограничьте к ней доступ, предоставив необходимые права только тем пользователям, которым необходим доступ ко всем резервным копиям, содержащимся в данной папке. Файлы, создаваемые в общей папке в процессе резервного копирования, наследуют все права доступа данной папки.

Порядок работы

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

Установка системы резервного копирования

Вы можете установить систему резервного копирования с помощью средства Задачи начальной настройки, или с помощью диспетчера сервера.

Чтобы установить систему резервного копирования с помощью средства Задачи начальной настройки, выполните следующие действия:

1. Для запуска средства Задачи начальной настройки в командной строке введите: **oobe**
2. В разделе **Настроить этот сервер** щелкните по ссылке **Добавить компоненты.** Это приведет к запуску мастера добавления компонентов.
3. На странице **Выбор компонентов** выберите из списка пункт **Возможности системы архивации данных Windows Server**, разверните его, нажав на значок [+], и отметьте флажком пункт **Система архивации данных Windows Server**, после чего нажмите кнопку **Далее**.
4. На странице **Подтвердите выбранные элементы** нажмите кнопку **Установить.**
5. Нажмите кнопку **Закрыть**.

Чтобы установить систему резервного копирования с помощью диспетчера сервера, выполните следующие действия:

1. Нажмите кнопку **Пуск**, после чего щелкните по элементу **Диспетчер сервера**.
2. В разделе **Сводка компонентов** щелкните по ссылке **Добавить компоненты** для запуска мастера добавления компонентов.
3. На странице **Выбор компонентов** выберите из списка пункт **Возможности системы архивации данных Windows Server**, разверните его, нажав на значок [+], и отметьте флажком пункт **Система архивации данных Windows Server**, после чего нажмите кнопку **Далее**.

4. На странице **Подтвердите выбранные элементы** нажмите кнопку **Установить.**
5. Нажмите кнопку **Закрыть.**

Сценарий 1. Создание резервных копий на внешних жестких дисках по расписанию

В данном сценарии рассматривается процесс создания резервных копий на внешних жестких дисках. В случае использования планировщика резервные копии будут создаваться ежедневно. При настройке планировщика Вы можете указать:

- Создавать резервные копии всего сервера целиком или только его определенных томов. Вы можете создавать резервные копии всех томов сервера, или исключать тома, не содержащие операционной системы или приложений. В целях защиты сервера в резерв- ные копии автоматически включаются тома, содержащие операционную систему и приложения.
- Периодичность создания резервных копий (ежедневное, либо более частое создание резервных копий). Создание резервных копий по расписанию выполняется, по крайней мере, раз в день, однако при необходимости Вы можете создавать их и чаще.

Примечание.

Система резервного копирования позволяет хранить на одном диске до 512 резервных копий (из-за ограничений VSS). Реальное же число копий может быть меньше из-за объема диска, а также из-за величины изменений, присутствующих в каждой резервной копии. В случае, если Вам необходимо иметь большее число резервных копий, Вы можете разместить их на нескольких дисках.

Вы можете запустить мастер расписания архивации в любое время, чтобы изменить ранее созданное расписание создания резервных копий. При создании плановых резервных копий эти копии будут автоматически записываться на тот диск, который использовался последним. В случае, если этот диск не обнаруживается, в качестве места хранения выбирается диск, который использовался перед ним.

Необходимые условия для сохранения плановых резервных копий на внешних дисках

Прежде, чем Вы сможете настроить сохранение плановых резервных копий на внешние жесткие диски, необходимо убедиться, что соблюдаются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования. Для получения информации о процессе установки системы резервного копирования обратитесь к разделу "Установка системы резервного копирования", представленному ранее в данном руководстве.
- Вы являетесь членом группы Администраторы (только члены группы Администраторы могут назначать или изменять расписание создания резервных копий. Следует учесть, что и члены группы Операторы архива при необходимости могут создавать резервные копии, однако при этом будут использоваться те же настройки, которые используются при создании резервных копий по расписанию).
- К серверу подключен внешний жесткий диск, имеющий интерфейс USB 2.0 или IEEE 1394. Объем жесткого диска должен, по крайней мере, превышать в 2.5 раза объем дан-

ных, подлежащих резервному копированию. Поскольку система резервного копирования предварительно форматирует жесткий диск перед размещением на нем резервных копий, то этот диск должен быть либо пустым, либо на нем могут находиться ненужные Вам данные, которые могут быть потеряны.

Необходимые шаги для настройки автоматического создания плановых резервных копий на внешних жестких дисках

Для настройки автоматического создания плановых резервных копий на внешних жестких дисках Вам необходимо:

- Решить, следует ли создавать резервную копию всего сервера или только его определенных томов.
- Решить, как часто следует создавать резервные копии: раз в день или чаще.
- После запуска процесса резервного копирования следить за его ходом с помощью раздела Состояние и Сообщения начальной страницы оснастки. В данном разделе отображаются все созданные и восстановленные резервные копии за последние семь дней.

Для указания внешних дисков в качестве места хранения резервных копий, создаваемых автоматически по расписанию, выполните следующие действия:

1. Нажмите кнопку **Пуск**, откройте меню **Администрирование**, после чего нажмите **Система архивации данных Windows Server**.
2. В меню **Действие** начальной страницы оснастки **Система архивации данных Windows Server (Локальный)** выберите пункт **Расписание архивации** (аналогичные действия можно выполнить, используя боковую панель **Действия**, если она отображается). При этом запустится мастер расписания архивации.
3. На странице **Приступая к работе** нажмите кнопку **Далее.**
4. На странице **Выбор конфигурации архивации** установите переключатель в одно из положений, указанных ниже, после чего нажмите кнопку **Далее:**

    1. Положение **Весь сервер (рекомендуется)** позволит создать резервные копии всех томов сервера.
    2. Положение **Настраиваемый** позволит выбрать необходимые тома. После выбора этого положения нажмите кнопку **Далее**. На странице **Выбор элементов для архивации** выберите тома, резервную копию которых необходимо создать.

    Примечание.

    Тома, содержащие операционную систему или приложения, по умолчанию добавляются в резервные копии и не могут быть исключены из них.

5. На странице **Укажите время архивации**, установкой переключателя выберите один из представленных ниже режимов создания резервных копий, после чего нажмите кнопку **Далее**:

    1. Режим **Раз в день.** При этом необходимо будет указать время начала ежедневного создания резервной копии.
    2. Режим **Больше одного раза в день**. В списке **Доступное время** указаны возможные варианты времени, при наступлении которых может стартовать процесс создания резервной копии, а в списке **Запланированное время** указано назначенное время создания плановых резервных копий. Чтобы переместить значение времени из списка **Доступное время** в список **Запланированное время** необходимо выделить время начала создания резервной копии, после чего нажать кнопку **Добавить.** Повторяйте данное действие столько раз, сколько необходимо, после чего нажмите кнопку **Далее.**

6. На странице **Выберите диск назначения** укажите внешний диск, на который вы желаете сохранить резервную копию, после чего нажмите кнопку **Далее.**

> **Примечание.**
>
> В случае, если тот внешний диск, который Вы подключили, не отображается в списке **Доступные диски** на странице **Выберите диск назначения**, нажмите кноп- ку **Показать все доступные диски**, после чего отметьте флажком все диски, кото- рые должны присутствовать на странице **Выберите диск назначения.**

7. Будет показано сообщение, информирующее Вас о том, что выбранный диск будет отформатирован, и все данные на нем будут потеряны. В случае согласия нажмите кнопку **Да.**
8. На странице **Маркировка диска назначения** будут представлены все отмеченные Вами диски. В качестве метки у каждого диска будут указаны такие данные, как Ваше имя пользователя, текущая дата, текущее время, а также имя диска. Нажмите кнопку **Далее**.

> **Важно.**
>
> Мы рекомендуем наносить на каждый внешний жесткий диск наклейки с данными меток. При восстановлении данных из резервных копий, расположенных на этом диске, информация из метки будет служить идентификатором данного диска.

9. На странице **Подтверждение операций** нажмите кнопку **Готово**, чтобы изменения вступили в силу**.** Мастер выполнит форматирование диска, что может занять некоторое время (зависит от объема диска).
10. На странице **Сводка** прочтите выведенную итоговую информацию и нажмите кнопку **Закрыть**.

Использование нескольких внешних жестких дисков для создания плановых резервных копий

Вы также можете использовать несколько внешних жестких дисков для хранения данных. При этом Вы можете сохранять резервные копии по очереди на несколько дисков, что позволит их выносить для хранения за пределы местонахождения сервера. Это поможет Вам лучше подготовиться к возможным неприятностям, позволив восстановить данные в случае физического повреждения серверного оборудования. Высокая вероятность пожаров или прочих природных бедствий (таких как землетрясений или наводнений) является веской причиной для хранения резервных копий в удаленном хранилище. Но и менее драматическое событие, например такое, как ложное срабатывание системы пожаротушения, может вывести из строя Ваше оборудование.

Вы также можете использовать эту стратегию резервного копирования для увеличения числа резервных копий. На каждом внешнем диске можно хранить до 512 резервных копий (реальное число зависит от объема данных в каждой резервной копии). Вы можете увеличить число резервных копий, используя для хранения несколько внешних дисков.

Для обеспечения наилучшей защиты данных мы рекомендуем Вам использовать принцип ротации дисков при повседневном создании резервных копий. Для этого Вам следует посетить удаленное хранилище, чтобы оставить там жесткий диск с самой последней резервной копией и взять жесткий диск с самой старой, после чего необходимо этот диск подключить к серверу.

Сценарий 2. Создание резервных копий на DVD-дисках в ручном режиме для восстановления разделов или системы

В данном сценарии описывается процесс создания резервных копий томов на DVD- дисках в ручном режиме. Данный тип резервных копий позволяет Вам восстанавливать все тома, которые содержатся в резервной копии. Данный тип резервных копий использу-ется только в том случае, когда Вам необходимо восстановить целые тома (при этом Вы не можете восстановить только необходимые Вам файлы и папки, или данные приложе- ний непосредственно из резервной копии, сохраненной на DVD-дисках). Данный тип резервного копирования следует использовать для восстановления операционной системы, или, например, для защиты данных при поломке жесткого диска, либо для защиты от возможных природных бедствий.

При сохранении резервных копий на DVD-дисках данные сжимаются. Из-за этого размер данных в резервной копии на DVD-диске может быть меньше, чем размер данных на томе

сервера.

В том случае, если в резервной копии содержатся важные тома (тома с системными компонентами, необходимыми для восстановления операционной системы), Вы можете использовать эту резервную копию для восстановления операционной системы на сервере, выполнив восстановление тома. Для получения подробных инструкций по восстановления системы, обратитесь к сценариям 5 и 6 данного руководства.

Необходимые условия для создания резервных копий на DVD-дисках в ручном режиме для восстановления разделов

Прежде, чем Вы попытаетесь создать резервную копию на DVD-дисках, убедитесь, что выполняются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования. Для получения информации о процессе установки системы резервного копирования обратитесь к разделу "Установка системы резервного копирования", представленному ранее в данном руководстве.
- Вы являетесь членом группы Администраторы или Операторы архива.
- Устройство записи DVD-дисков подключено к серверу.
- Количество чистых DVD-дисков, имеющихся в Вашем распоряжении, достаточно для сохранения данных выбранных разделов.

Шаги, необходимые для создания резервной копии на DVD-дисках в ручном режиме для восстановления разделов

Для создания резервной копии на DVD-дисках выполните действия, указанные ниже.

Для создания резервных копий на DVD-дисках в ручном режиме:

1. Нажмите кнопку **Пуск**, откройте меню **Администрирование**, после чего нажмите **Система архивации данных Windows Server**.
2. В меню **Действие** начальной страницы оснастки **Система архивации данных Windows Server (Локальный)** выберите пункт **Однократная архивации** (аналогичные действия можно выполнить, используя боковую панель **Действия**, если она отображается). При этом запустится мастер однократной архивации.
3. На странице **Параметры архивации** установите переключатель в положение **Другие параметры**, после чего нажмите кнопку **Далее**.
4. На странице **Выбор конфигурации архивации** установите переключатель в одно из положений, указанных ниже, после чего нажмите кнопку **Далее**:

    1. Положение **Весь сервер (рекомендуется)** позволяет создать резервные копии всех томов сервера.
    2. Положение **Настраиваемый** позволяет выбрать необходимые тома. После выбора этого положения нажмите кнопку **Далее**. На странице **Выбор элементов для архивации** выберите тома, резервную копию которых необходимо создать.

Чтобы иметь возможность восстановить систему из данной резервной копии, установите флажок **Включить восстановление системы**.

Примечание.

Если Вы выберете том, содержащий операционную систему, то в резервную копию также автоматически будут включены тома, содержащие компоненты этой операционной системы.

5. На странице **Укажите тип места назначения** установите переключатель в положение **Локальные диски,** после чего нажмите кнопку **Далее**.
6. На странице **Выбор места назначения архивации** выберите устройство записи DVD-дисков, после чего нажмите кнопку **Далее**.
7. На странице **Подтверждение** просмотрите результирующую информацию, после чего нажмите кнопку **Архивировать**. Первая часть процесса создания резервной копии займет несколько минут (за это время мастер подготовит тома для создания резервной копии).

Примечание.

Если Вы закроете окно мастера однократной архивации прежде, чем процесс будет завершен, на начальной странице оснастки в разделе **Сообщения** будет отображаться сообщение **Ожидание носителя информации**, информирующее о том, что мастер выполнил все необходимые предварительные действия для записи DVD-дисков. Чтобы продолжить процесс записи DVD-дисков, на начальной странице оснастки в разделе **Состояние** в колонке **Последняя архивация** щелкните по ссылке **Показать подробности,** после чего нажмите кнопку **Далее**.

8. После того, как будет выведено соответствующее сообщение, подпишите маркером пустой DVD-диск, указав следующую информацию: метку диска, текущую дату, текущее время и название DVD. Вставьте пустой DVD-диск в устройство записи DVD-дисков, после чего нажмите кнопку **OK**.

Примечание.

В зависимости от объема данных может понадобиться несколько DVD-дисков для записи резервной копии. В этом случае каждый раз, прежде чем вставить новый DVD-диск, мастер попросит Вас его подписать.

9. На странице **Ход архивации** будет отображаться информация о текущем процессе записи данных на DVD-диск, информация о проверке данных и о завершении процесса создания резервной копии. Нажмите кнопку **Закрыть** для выхода из мастера.

Сценарий 3. Восстановление файлов и папок

В данном сценарии описан процесс восстановления файлов и папок из резервной копии, находящейся на внешнем жестком диске или в удаленной общей папке.

Необходимые условия для восстановления файлов и папок

Прежде чем Вы начнете выполнять данную задачу, убедитесь, что соблюдаются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования. Для получения информации о процессе установки системы резервного копирования обратитесь к разделу "Установка системы резервного копирования", представленному ранее в данном руководстве.
- Вы являетесь членом группы Администраторы или Операторы архива.
- На внешнем жестком диске или на сетевом ресурсе имеется хотя бы одна резервная копия.
- Внешний жесткий диск, на котором находится резервная копия, подключен к серверу, а при использовании сетевой папки к ней имеется доступ по сети.

Шаги, необходимые для восстановления файлов и папок

Для восстановления файлов и папок, выполните шаги, указанные ниже.

Для восстановления файлов и папок:

1. Нажмите кнопку **Пуск**, откройте меню **Администрирование**, после чего нажмите **Система архивации данных Windows Server**.
2. В меню **Действие** начальной страницы оснастки **Система архивации данных Windows Server (Локальный)** выберите пункт **Восстановить** (аналогичные действия можно выполнить, используя боковую панель **Действия**, если она отображается). При этом запустится мастер восстановления.
3. На странице **Приступая к работе** выберите сервер, на котором хранится резервная копия, файлы или папки которой Вы хотите восстановить, после чего нажмите кнопку **Далее**.
4. На странице **Выбор даты архивации** выберите дату и время создания резервной копии, из которой Вы хотите восстановить данные, после чего нажмите кнопку **Далее**.

5. На странице **Выберите тип восстановления** установите переключатель в положение **Файлы и папки**, после чего нажмите кнопку **Далее.**
6. На странице **Выберите элементы для восстановления** в списке **Доступные элементы** спускайтесь по дереву папок, щелкая по значку [+] до тех пор, пока не перейдете к папке, которая Вам необходима. После щелчка по данной папке ее содержимое отобразится в правой панели. Выберите те элементы из папки, которые необходимо восстановить, после чего нажмите кнопку **Далее.**
7. На странице **Укажите параметр восстановления** в разделе **Конечные объекты восстановления** установите переключатель в одно из положений, указанных ниже:

    1. Положение **Исходное расположение** – для восстановления файла или папки в ту же папку, в которой они находились при создании резервной копии.
    2. Положение **Другое расположение** – для восстановления файла или папки в папку, отличающуюся от той, в которой они находились во время создания резервной копии. При этом необходимо ввести полный путь к указанной папке, либо нажать кнопку **Обзор**, чтобы выбрать ее вручную.

8. В разделе **Когда мастер обнаруживает файлы и папки в расположении восстановления** установите переключатель в одно из положений, указанных ниже:

    - **Создавать копии, чтобы иметь обе версии файла или папки**
    - **Перезаписывать существующие файлы при восстановлении файлов**
    - **Не восстанавливать эти файлы и папки**

9. В разделе **Параметры безопасности** установите флажок **Восстановление параметров безопасности** для приведения всех параметров безопасности к тем, что были у восстанавливаемого объекта во время создания резервной копии. Снятие флажка приведет к тому, что восстанавливаемый объект унаследует все параметры безопасности, имеющиеся у папки, в которую он восстанавливается. После этих действий нажмите кнопку **Далее.**
10. На странице **Подтверждение** просмотрите выведенную общую информацию, после чего нажмите кнопку **Восстановить**, чтобы восстановить выделенные данные. Появится страница **Ход восстановления**, на которой будет отображаться информация о процессе восстановления данных, после чего нажмите кнопку **Закрыть,** чтобы завершить работу мастера.

Сценарий 4. Восстановление всего тома из резервной копии, расположенной на DVD-диске

В данном сценарии описывается процедура восстановления всего тома из резервной копии, расположенной на DVD-диске. Когда Вы выполняете восстановление всего тома, восстанавливается все содержимое тома. При использовании резервной копии, расположенной на DVD-диске, Вы не можете выполнить выборочное восстановление только необходимых Вам папок и файлов.

Необходимые условия для восстановления всего тома из резервной копии, расположенной на DVD-диске

Прежде, чем Вы начнете выполнять действия, указанные в данном сценарии, убедитесь, что соблюдаются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования. Для получения информации о процессе установки системы резервного копирования обратитесь к разделу "Установка системы резервного копирования", представленному ранее в данном руководстве.
- Вы являетесь членом группы Администраторы или Операторы архива.
- Устройство записи DVD-дисков подключено к серверу.
- Все DVD-диски, на которых находится резервная копия, имеются в наличии и подписаны соответствующим образом.

Шаги по восстановлению всего тома из резервной копии, сохраненной на DVD-диске

Для восстановления всего тома выполните шаги, описанные ниже.

Для восстановления томов:

> **Важно.**
>
> При восстановлении тома, все имеющиеся в данный момент на нем данные будут потеряны.

1. Нажмите кнопку **Пуск**, откройте меню **Администрирование**, после чего нажмите **Система архивации данных Windows Server**.
2. В меню **Действие** начальной страницы оснастки **Система архивации данных Windows Server (Локальный)** выберите пункт **Восстановить** (аналогичные действия можно выполнить, используя боковую панель **Действия**, если она отображается). При этом запустится мастер восстановления.
3. На странице **Приступая к работе** выберите сервер, на котором хранится резервная копия тома, которой Вы хотите восстановить, после чего нажмите кнопку **Далее**.
4. На странице **Выбор даты архивации** выберите дату и время создания резервной ко-

пии, из которой Вы хотите восстановить данные, после чего нажмите кнопку **Далее.**

Примечание.

При выборе определенной даты на странице **Выбор даты архивации** по умолчанию отображается информация о последней резервной копии, созданной по расписанию. Чтобы отобразить информацию о резервной копии, созданной на DVD-диске, Вам необходимо выбрать время создания этой резервной копии.

5. На странице **Выберите тип восстановления** установите переключатель в положение **Тома**, после чего нажмите кнопку **Далее.**
6. На странице **Выберите тома** установите флажки рядом с тем разделом, информацию на котором Вам необходимо восстановить. После этого в столбце **Конечный том** выберите из списка тот том, на который Вы хотите восстановить данные. Нажмите кнопку **Далее.**
7. На странице **Подтверждение** убедитесь, что все параметры указаны верно, после чего нажмите кнопку **Восстановить,** чтобы начать восстановление данных. Появится страница **Ход восстановления**, на которой будет отображаться информация о процессе восстановления данных, после чего нажмите кнопку **Закрыть,** чтобы завершить работу мастера.

Сценарий 5. Восстановление операционной системы

В данном сценарии описана процедура восстановления серверной операционной системы с помощью средства Восстановление архива Windows Complete PC и резервной копии, созданной ранее с помощью системы резервного копирования (для доступа к инструменту Восстановление архива Windows Complete PC необходим установочный диск Windows Server 2008).

В данном сценарии Вы будете восстанавливать операционную систему путем восстановления всех важных для работы системы разделов. Разделы, не содержащие компоненты операционной системы, восстанавливаться не будут.

Необходимые условия для восстановления серверной операционной системы

Прежде чем Вы начнете выполнять действия, указанные в данном сценарии, убедитесь, что соблюдаются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования.
- Вы являетесь членом группы Администраторы или Операторы архива.
- У Вас имеется резервная копия всех критически важных для работы сервера разделов.

- У Вас имеется установочный диск Windows Server 2008 (в данном сценарии он необходим для доступа к функциям восстановления системы).

Шаги по восстановлению серверной операционной системы

Для восстановления серверной операционной системы выполните действия, указанные ниже.

Для восстановления серверной операционной системы:

1. Вставьте диск в устройство чтения CD или DVD-дисков, после чего перезагрузите к пьютер. Может понадобиться несколько минут для загрузки необходимых файлов.
2. После выбора языка установки в окне Установка Windows нажмите кнопку **Далее**, по чего щелкните по ссылке **Восстановление системы**.
3. Мастер выполнит поиск установленных на жестких дисках операционных сис Windows, после чего отобразит результаты в диалоговом окне **Параметры восстано ния системы**. Данный список должен быть пустым, если выполняется восстановлени новое оборудование. Нажмите кнопку **Далее**.
4. На странице **Параметры восстановления системы** щелкните по ссылке **Восстано ние архива Windows Complete PC**.
5. Установите переключатель в одно из следующих положений, после чего нажмите кно **Далее**:

   - **Использовать последний доступный архив (рекомендуется)**
   - **Восстановить другой архив**

6. При выборе второго варианта будут заданы дополнительные вопросы относительно п метров восстановления. В этом случае после выбора соответствующих опций нажм кнопку **Далее**.
7. На странице **Выберите тип восстановления резервной копии** нажмите кнопку **Уста вить драйверы**, если необходимо установить драйверы найденных жестких дисков. тем установите необходимые флажки, представленные ниже, и нажмите кнопку **Далее**

   1. **Форматировать и разбить на разделы диски.** Установка этого флажка позво удалить существующие разделы и переформатировать жесткие диски так, как необходимо для восстановления на них резервной копии.
   2. **Восстанавливать только системные диски.** Установка этого флажка позво восстановить только разделы, содержащие компоненты операционной системы. этом диски с данными восстанавливаться не будут.

8. При установке флажка **Форматировать и разбить на разделы диски** нажмите кнопку **Исключить диски**, после чего снимите флажки с тех разделов, которые не должны участвовать в процессе восстановления системы. Нажмите кнопку **Далее**.
9. Подтвердите все выбранные настройки восстановления, после чего нажмите кнопку **Готово**.

Сценарий 6. Полное восстановление сервера

В данном сценарии описана процедура полного восстановления сервера с помощью средства Восстановление архива Windows Complete PC и резервной копии, созданной ранее с помощью системы резервного копирования (для доступа к средству Восстановление архива Windows Complete PC необходим установочный диск Windows Server 2008).

При восстановлении данных с помощью данного сценария будет произведено переформатирование и повторное создание разделов на всех дисках, подключенных к серверу. Данный сценарий следует использовать в случае восстановления данных на новое оборудование, или в том случае, если все другие попытки восстановления на существующее оборудование потерпели неудачу.

Важно.
При выполнении данного сценария все имеющиеся на дисках данные, не включенные в резервную копию, будут потеряны. Изменения затронут все разделы, которые на момент выполнения операции использовались сервером, но данные из которых не были включены в резервную копию.

Необходимые условия для выполнения полного восстановления сервера

Прежде чем Вы начнете выполнять действия, указанные в данном сценарии, убедитесь, что соблюдаются следующие условия:

- На сервере, работающем под управлением операционной системы Windows Server 2008, установлена система резервного копирования.
- Вы являетесь членом группы Администраторы или Операторы архива.
- У Вас имеется резервная копия, содержащая данные со всех разделов сервера.
- У Вас имеется установочный диск Windows Server 2008. В данном сценарии для доступа к функциям восстановления системы необходим установочный диск.
- В случае, если Вы собираетесь выполнить восстановление данных на новое оборудование, имеющегося дискового пространства достаточно для восстановления всех разделов.

Шаги, необходимые для полного восстановления сервера

Для восстановления данных на новое оборудование выполните действия, указанные ниже.

Для восстановления сервера:

1. Вставьте диск в устройство чтения CD или DVD-дисков, после чего перезагрузите компьютер. Может понадобиться несколько минут для загрузки необходимых файлов.
2. После выбора языка установки в окне Установка Windows нажмите кнопку **Далее**, после чего щелкните по ссылке **Восстановление системы**.
3. Мастер выполнит поиск установленных на жестких дисках операционных систем Windows, после чего отобразит результаты в диалоговом окне **Параметры восстановле- ния системы**. Данный список должен быть пустым, если выполняется восстановление на новое оборудование. Нажмите кнопку **Далее**.
4. На странице **Параметры восстановления системы** щелкните по ссылке **Восстановление архива Windows Complete PC**.
5. Установите переключатель в одно из следующих положений, после чего нажмите кнопку **Далее**:

   - **Использовать последний доступный архив (рекомендуется)**
   - **Восстановить другой архив**

6. На странице **Выберите тип восстановления резервной копии** установите флажок **Форматировать и разбить на разделы диски**, после чего нажмите кнопку **Далее**.
7. Убедитесь, что выбраны верные параметры восстановления, после чего нажмите кнопку **Готово**.

Время выполнения работы 90 мин;

Контрольные вопросы

1. Что такое резервное копирование ?
2. Какие условия нужно соблюдать для сохранения плановых резервных копий на внешний диск?
3. Что нужно сделать, чтобы восстановить целый том?
4. Какие нужно проделать шаги для полного восстановления сервера?
5. Из за чего размер резервной копии на DVD диске может быть меньше чем том на сервере?

Сделайте выводы.

Составьте отчет о проделанной работе в тетради для самостоятельных работ.

Критерии оценки*:*

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

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

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

Рекомендуемая литература

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

Изучаемая тема: Объекты сетевой инфраструктуры и операции над ними

Практическая работа № 13-14 «Разработка плана восстановления. Использование схемы послеаварийного восстановления сети. Возврат к нормальному функционированию системы»

Цель работы: Научиться составлять план восстановления системы после сбоя.

В процессе занятия решаются следующие задачи:

1. Изучить методические указания и рекомендуемую литературу по составлению плана восстановления системы.

Краткие теоретические и справочно-информационные материалы по теме занятия.

Подробные планы действий в случае аварий и катастроф помогают действовать эффективно и гарантируют, что ни один важный аспект не будет упущен. *План аварийного восстановления – это подробный перечень мероприятий и действий, которые необходимо выполнить «до», «во время» и «после» возникновения чрезвычайной ситуации.* Здесь определяется порядок уведомления руководителей и ответственных сотрудников, а также излагаются детальные инструкции для исполнителей. Все это позволяет максимально быстро восстановить работоспособность важных информационных систем и сервисов. Сроки восстановления четко регламентируются в зависимости от требований и специфики работы компании-заказчика. Приемлемое для бизнеса время восстановления является одним из ключевых факторов, от которого зависит выбор стратегии резервирования оборудования и способа репликации данных.

Этапы разработки плана

Разработку плана обеспечения бесперебойной деятельности предприятия необходимо организовать в виде проекта, чтобы управлять задачами, сроками и конечными результатами.

Основными этапами типичного проекта являются:

Организация выполнения проекта;

Оценка риска, уменьшение нежелательных последствий от наступления событий, связанных с риском, анализ последствий для бизнеса;

Разработка стратегии восстановления деятельности;

Документирование плана;

Обучение;

Имитация бедствия.

Организация выполнения проекта

Организация выполнения проекта включает в себя административное управление проектом, определение допущений, проведение совещаний и разработку политики.

Оценка риска

При оценке риска выявляются типы бедствий, которые могут произойти в каждом конкретном месте. Обследуется физическая инфраструктура здания и его окружения. Для каждого типа бедствия делается оценка возможной продолжительности и присваивается относительная величина, соответствующая вероятности их появления. Используется шкала, например, от 0 до 3; где 0 означает невероятное событие, а 3 — весьма вероятное. В результате этого выявляются области, в которых следует провести дальнейшие исследо-

вания, чтобы уменьшить последствия событий, приводящих к риску. Анализ последствий для деятельности организации.

После оценки риска проводится анализ последствий бедствия для деятельности организации, в ходе которого определяются потери из-за невозможности продолжать нормальную деятельность. Они могут быть очевидными или носить более абстрактный характер, при котором руководству придётся сделать предположительную оценку потерь. В любом случае цель заключается не в том, чтобы получить точный ответ, а в том, чтобы выявить факторы, которые являются критически важными для продолжения деятельности компании. На этом этапе определяется масштаб плана обеспечения бесперебойной деятельности. Чрезмерные меры предосторожности потребуют лишних средств, а недостаточные — не обеспечат должной безопасности.

Разработка стратегии обеспечения бесперебойной деятельности

После определения требований можно принимать решение о том, как обеспечивать восстановление деятельности. Существует множество вариантов технических решений, в том числе: - Использование "горячего" резервного помещения. Поставщик предоставляет компании подготовленное рабочее помещение с оборудованием, средствами телекоммуникации, персоналом, осуществляющим техническую поддержку, и т.д., обычно по годовому контракту. Заказчики получают доступ к оборудованию по принципу "первый пришел — первым обслуживается". - Использование "холодного" резервного помещения. Компания организует работу в пустующем или арендуемом помещении, которое подготовлено к использованию. Сразу после бедствия в помещении развёртывается оборудование (возможно, закупаемое у поставщиков), программное обеспечение и службы обеспечения. - Использование внутренних резервов. Для предоставления услуг в чрезвычайных обстоятельствах используется оборудование компании, которое расположено в ином месте. - Заключение соглашения о взаимной поддержке. Заключается соглашение с другой компанией о коллективном использовании ресурсов после бедствия. При этом предполагается, что резервное оборудование всегда имеет нужную производительность и вас устраивает степень защиты информации при коллективной работе. В некоторых случаях можно использовать комбинацию этих вариантов. Крупные многонациональные компании чаще всего используют для локальных вычислительных сетей метод внутреннего резервирования. Поскольку количество имеющихся резервных помещений ограничено, может оказаться, что в случае чрезвычайных обстоятельств не окажется рабочего помещения, которое можно было бы использовать. Бедствие в масштабе региона может привести к тому, что все резервные помещения будут заняты и компании негде будет возобновить работу. Хорошо подготовленный план обеспечивает компанию пошаговыми инструкциями, соответствующими типу и тяжести бедствия. В нём указываются функциональные группы специалистов компании, подготовленные для реализации плана. Наличие хорошо проработанного плана гарантирует, что в стрессовой ситуации после возникновения чрезвычайных обстоятельств, критически важные факторы не будут упущены.

Документация

План может документироваться различными способами. Большинство компанийвсё еще применяют традиционные текстовые редакторы, другие используют коммерче- ское программное обеспечение. Какой бы метод ни был использован, важно обеспечить строгое выполнение процедур управления внесением изменений, чтобы поддерживать план в состоянии, соответствующем реальной текущей ситуации.

Обучение

Обучение "Группы восстановления" направлено на то, чтобы каждый сотрудник знал свои функции и обязанности в случае возникновения нештатных ситуаций.

Имитация бедствия

Большинство компаний проводят испытания плана минимум один раз в полгода. Имитируя бедствия можно проверить план, найти его слабые места и отработать взаимодействие участников. Обнаружение недостатков обычно влечёт за собой корректировку

плана. План должен регулярно проходить испытания и корректироваться. Лишь немногие планы обеспечения бесперебойной деятельности выполняются так, как это предусматривалось первоначально. Поскольку внесение поправок в план необходимо делать регулярно, должна быть максимально упрощена процедура корректировки плана.

Примерное содержание плана

Непременным условием быстрого и успешного восстановления деятельности организации после бедствия является предварительная разработка и регулярное обновление постоянно действующего плана обеспечения бесперебойной деятельности компании. В зависимости от специфики компании и принятой в ней политики подобный план мероприятий может иметь различные формы и названия. Он может состоять из нескольких разделов, отражающих различные направления работ: план подготовки к чрезвычайным ситуациям, план действий в чрезвычайной ситуации, план резервирования и восстановления информации, план восстановления деятельности и т.п. План может также детализироваться по категориям и продолжительности чрезвычайных обстоятельств. План включает следующие основные разделы:

1. Основные положения плана.
2. Оценка чрезвычайных ситуаций:

a. выявление уязвимых мест компании;
b. классификация возможных опасных событий и оценка вероятности их возникновения;
c. сценарии чрезвычайных ситуаций;
d. потенциальные источники отрицательных последствий каждой чрезвычайной ситуации и оценка величины ущерба;
e. набор критериев, на основании которых объявляется чрезвычайная ситуация.

3. Деятельность компании в чрезвычайной ситуации:
   - первоначальное реагирование на чрезвычайную ситуацию (оценка опасного события, объявление чрезвычайной ситуации, оповещение необходимого круга лиц, ввод в действие чрезвычайного плана);
   - мероприятия, обеспечивающие бесперебойность деятельности компании в чрезвычайной ситуации и восстановление ее нормального функционирования.
   - контроль правильности и корректировка содержания плана;
   - составление списка адресов и процедуры рассылки плана;
   - подготовка к опасным событиям, обеспечение безопасности и предотвращение бедствий;
4. Регулярное создание резервных копий данных, документации, бланков входных и выходных документов и основного программного обеспечения, их хранение в безопасном месте.
5. Информационное обеспечение:
   - приоритетные функции, выполняемые компанией;
   - списки внутренних и внешних ресурсов — технических средств, программного обеспечения, средств связи, документов, офисного оборудования и персонала;
   - учётная информация о техническом, программном и другом обеспечении, необходимом для восстановления деятельности организации в случае чрезвычайной ситуации;
   - список лиц, которых необходимо оповестить о чрезвычайной ситуации с указанием адресов и телефонов;
   - вспомогательная информация — планы и схемы, маршруты перевозок, адреса и т.п.;
   - описание детальных пошаговых процедур, обеспечивающих чёткое выполнение всех предусмотренных мер;
   - функции и обязанности сотрудников в случае возникновения непредвиденных обстоятельств;

- сроки восстановления деятельности в зависимости от типа возникшей чрезвычайной ситуации;
- смета расходов, источники финансирования.

6. Техническое обеспечение:
   - создание и поддержание базы технических средств, обеспечивающей бесперебойную деятельность компании в чрезвычайной ситуации;
   - создание и поддержание в надлежащем состоянии резервного производственного помещения.
7. Организационное обеспечение, состав и функции следующих групп, обеспечивающих бесперебойную деятельность в случае бедствия:
   - группы оценки чрезвычайной ситуации;
   - группы управления в кризисной ситуации;
   - группы для работ в чрезвычайной ситуации;
   - группы восстановления;
   - группы обеспечения работы в резервном производственном помещении;
   - группы административной поддержки.

Порядок работы

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

1. Составьте план послеаварийного восстановления системы.
2. Используя составленный план напишите порядок действия персонала в случае аварийной ситуации.

Критерии оценки*:*

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

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

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

1.