ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Программное обеспечение вычислительной техники и автоматизированных систем»

Учебно-методическое пособие

по дисциплине

«СЕТИ И ТЕЛЕКОММУНИКАЦИИ»

Автор
Кудинов Н.В.

Ростов-на-Дону, 2018

Аннотация

Учебно-методическое пособие предназначено для студентов очной формы обучения направления 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Авторы

к.т.н., доцент,
каф. ПОВТиАС
Кудинов Н.В.

Оглавление

1. ЛАБОРАТОРНАЯ РАБОТА №1

Тема работы: Изучение сетевого окружения с использованием утилит управления, диагностики, мониторинга ОС Unix, Linux, Windows.

Цель работы: изучить навыки настройки односегментных сетей, студенты должны уметь сконфигурировать сеть, распределить адреса, протестировать конфигурацию и доступность сетевых ресурсов. Получить навыки организации обмена файлами (в том числе и кросплатформенного). Исследовать процессы разрешения ip-адресов и символических имён хостов (протоколы NMB и DNS), получить навыки перезапуска системных сервисов (демонов) и определения сервиса, который необходимо перезапустить для разрешения тех или иных проблем)

Изучению подлежат: команды сетевого администратора для ОС Linux и Windows, утилиты диагностики сетей, назначение сетевых и функциональность служб ОС.

Таблица 1. Команды сетевого администрирования ОС Windows и ОС Linux

net use smbclient	команда монтирования общедоступного (по сети) сетевого директории (ресурса) или предоставления информации о уже настроенных общедоступных каналов (точек подключения) удалённых файловых систем. Смонтированне каналы выходы в удалённую файловую систему представлены в ОС Windows сетевыми виртуальными дисками. Функционирование дисков поддерживается так называемым файловым редиректором, реализуемом службой Workstation.
net share smbd	управляет «точками» сетевого входа в локальную файловую систему. Назначенные точки считаются общими сетевыми ресурсами. При вызове команды без параметров выводятся сведения обо всех общих ресурсах компьютера, который получил и исполняет эту команду. Доступ к точкам «входа» осуществляется файловым сервером, называемом в ОС Windows просто Server.

net view smbclient	выводит список имён компьютеров, доступных для определения по протоколу NetBIOS и общих файловых ресурсов выбранного сетевого узлы. Вызванная без параметров, команда net view выводит список компьютеров доступных в локальном сегменте сети. Оперативная информация поддерживается службой Browser.
net start /etc/init.d/	Запуск служб, в том числе и сетевых. При запуске команды net start без параметров выдается список запущенных служб. Служба, как и любая программа при запуск считывает параметры из энергонезависимой памяти(в Windows параметры хранятся в специальной СУБД — системном реестре).
net stop /etc/init.d/	Остановка работы службы. Может приводить к освобождению программно-аппаратных ресурсов.
Nbtstat	используется для отображения информации протокола NetBIOS over TCP/IP (NetBT) и в основном применяется при решении проблем, возникающих при наличии в сети на основе Windows 2000 и более старых систем.
nbtstart -RR	
arp	Отображает, добавляет или удаляет записи в таблицах трансляции сетевых адресов в физические адреса. Таблицы используются при работе протокола ARP.
nslookup	Отправляет запрос и отображает сведения, которые предоставляет служба DNS. Система используется для диагностики логической структуры сети на уровне адресно-именной информации.
route	Выводит на экран и изменяет записи в локальной таблице IP-маршрутизации.
ping	Команда диагностики сетевых соединений, посредством отправки сообщений и получения эхо-ответа на него. Эта функциональность обеспечивается протоколом ICMP, который позволяет проверять соединение или целостность логической связи на уровне протокола IP.

tracert traceroute	Задействует системно-сетевые механизмы маршрутизации для передачи тестовых пакетов с частичным их «отражением» на межсетевых шлюзах. Позволяет промоделировать и отобразить маршрут передачи трафика к выбранному узлу локальной сети. Используются сообщения формата ICMP с постоянным увеличением параметра срока жизни (Time to Live, TTL).
Ipconfig, ifconfig	Отображает актуальные параметры настройки конечных участков сети TCP/IP, относящихся к локальному компьютеру. Эти оконечные участки называются сетевыми интерфейсами и поддерживаются на программно-аппаратном уровне (драйверы, адаптеры). Обеспечивает конфигурирование сетевых интерфейсов. Также команда ipconfig в особом режиме обновляет параметры этих сетевых интерфейсов по протоколу DHCP. Команда ipconfig без параметров выводится только IP-адрес, маску подсети и основной шлюз для каждой подключённой сети.
netstat	Отображает активные подключения сетевых портов (точек подключения) протокола управления связью (TCP) и передачи датаграм пользователя (UDP) друг к другу, статус этих портов и статистики упомянутых протоколов.
Netsh ip	Является диалоговой средой настройки параметров сетевого окружения. Особенно полезна на нач льном этапе настройки в контексте interface ip

Ход выполнения работы

1. Подготовить необходимые информационные ресурсы — образы загрузочных дисков сетевых операционных систем в варианте сборки AllKid или WinPE (Windows XP) и ASP Liunx.

Примечание: в качестве альтернативы ASP-дитрибутиву системы GNU/Linux можно выбрать: Unix DesktopBSD, Unix Dragon Fly, Ubuntu (при наличии доступа к основным репозитариям или его кешу), Slackware, minix, BackTrack (Kali), ALT Linux workstation, CAE Linux, Neth server, SLAX Linux; в качестве альтернативы сборки Alkid может быть выбрана сборка ZverDVD, BartPE или Win PE.

2. Запустить на выполнение ПО моделирующее вычислительные машины Oracle Virtual Box, настроить две машины с такими параметрами: Объём ОЗУ не более четверти установленной в

HOST-машине (не виртуальная), без жёсткого диска, в устройство чтения CD/DVD дисков установлен виртуальный диск для загрузки операционной системы, сетевые адаптеры с номером один включены и сконфигурированы на подключение к виртуальному мосту, допускающему связь с host-машиной. Концептуальная модель: два компьютера - две операционные системы.

3. Включить виртуальные компьютеры, загрузить операционные системы. В ОС Windows включить поддержку сетевых интерфейсов, активировав пиктограмму "Сеть вкл."

4. Проверить настройки сетевых интерфесов, осуществить перекрёстную проверку связи с проэтапным просмотром таблицы ARP-протокола.

5. Просмотреть перечень компютеров, находящихся в одном сетевом сегменте, см. net view;

6. Открыть директорию PROGRAMS файловой системы iso9660, расположенную на системном томе X: ОС Windows. Для справки см. net share /? в интерпретаторе cmd;

7. Найти директорию PROGRAMS с сетевом окружении с другого компьютера сети. См. комаду net view;

8. Подключить открытую сетевую директорию на host машине. Для справки см. net use /? в интерпретаторе cmd.

9. Просмотреть таблицу TCP и UDP портов. Останавливая службу Server найти порты отвечающие за работу сетевой файловой системы.

10. Последовательно останавливая службу server проследить за доступностью файловой системы на сетевом диске. Запустить длительный процесс копирования файлов с сетевой файловой системы и определить интервал времени на который можно отключить сетевой интерфейс (см. Панель управления\Сетевые подключения) в виртуальной машине под управлением ОС Windows

11. Подключить сетевой каталог в системе Linux, используя команду mount для файловой системы smbfs. Для справки см. man mount в эмуляторе терминала. Общий формат записи команды такой: mount -t cifs -o utf8,username=admin,passwd=123 //<IP_сервера>/PROGRAMS /mnt

12. Организовать "загрузку" файлов с файлового сервера и организовать просмотр сетевого трафика на уровне протокола tcp при помощи утилиты tcpdump (в Linux).

13. Запросить университетский сервер имён о расположении домена ec.dstu.local, см. команду nslookup

Сделать выводы по отдельным этапам и работе в целом.

Провести анализ применимости команд, приведённых в таблице для администрирования ОС Linux и ОС Windows, определить, какие команды носят одинаковую функциональность при одинаковых ключах запуска, для каких ключи различаются для реализации одинаковых функций, для каких команд в парной ОС нет аналогов: синтаксических и/или функциональных.

Содержание отчёта

1. Цель работы
2. Описание хода выполнения работы с выводами и листингами командно-диалоговых журналов (возможно использовать снимки экрана).

Примечание: Для выполнения работы понадобятся два загрузочных образа:
1. http://rutracker.org/forum/viewtopic.php?t=471746
2. http://rutracker.org/forum/viewtopic.php?t=560432

2. ЛАБОРАТОРНАЯ РАБОТА №2

Тема работы: Установка, настройка и тестирование маршрутизируемой сетевой среды.

Цель работы: Исследовать механизм маршрутизации в сетях TCP/IP, получить представление о структуре таблицы маршрутизации и организации трансляции транзитного сетевого трафика.

Порядок выполнения работы:

1. Создать и запустить три виртуальные машины с управляющей операционной системой Linux, которые отличаются от обычных следующими признаками:

-отсутствует локальный жесткий диск. Загрузка ОС производиться с CD-диска. В VB подобная загрузка реализуется через подключение образа диска ASP Linux, находящегося в общем студенческом каталоге.

-установлены два сетевых адаптера, тип первого адаптера задан как "Соединение типа Мост", а для второго как "адаптер Virtual Box host only" (для свзи с несущей (host) машиной).

Настроить и запротоколировать параметры сетевого окружения -

ip-адреса, нанести параметры на схему.

3. Проверить связность сети при помощи команд ping и arp -a (для выяснения вопроса, с какого адаптера пришел тестовый пакет).

4. Выбрать одну из виртуальных машин в качестве межсетевого шлюза - маршрутизатора (случайно).

5. Выключить один из сетевых интерфейсов для получения однозначного маршрута прохождения пакета.

5. Проверить, пропускает ли шлюз сетевые тестовые пакеты в удаленную сеть.

6. Описать на одной из ОС, сеть как удаленную, расположенную за шлюзом.

7. Проверить возможность выхода в удаленную сеть.

8. Если выхода нет то ввести на шлюзе команду, разрешающею трансляцию транзитного трафика:

```
echo "1">/proc/sys/net/ipv4/ip_forvard
```

9. Организовать доступ с одной машины до удаленной через межсетевой шлюз. Объект доступа - сервер ssh, выполняемый от имени процесса sshd. Необходимо проверить, открыт ли порт протокола ssh на выбранной серверной машине. Кроме того необходимо пользователю root административно задать пароль для организации сетевого доступа.

10. На виртуально маршрутизаторе(шлюзе) организовать прослушивание сетевого трафика, введя команду

tcpdump -i eth0

11. Проанализировать журнал tcpdump, разобрать действия протокола arp и ssh.

12. Организовать сетевую логическую петлю, запустив tcpdump поверх удаленной сессии ssh.

13. Сделать выводы по работе.

3. ЛАБОРАТОРНАЯ РАБОТА №3

Тема: «Электронная почта. Настройка и отладка взаимодействия MUA и MTA. Создание пользователей и групп рассылки».

Цель работы: Получить навыки настройки системы обмена электронной почтой, установки и настройки почтовых серверов и

отладки их работы.

Системные требования к лабораторной установке: Три компьютера:

1. 1-2 серверных под управлением Linux live CD, например Back Track 3.0 и ASP Linux greenhorn (128Mb RAM). Желательно всё проверить в двух обозначенных дистрибутивах.

2. Клиентский: для отправки почты (клиентский терминал) из The Bat под управлением Windows (256Mb RAM) или Thunderbird под управлением ubuntu. Клиентским компьютером может выступать физический host-компютер. При этом почтовые программы класса MUA могут закупаться в portable режиме с сетевого или переносного накопителя.

Краткая теория: Так получилось, что узлы пересылки почты в глобальных сетях были основаны на ОС Unix. Наиболее сложным элементом системы транспорта почты был сервер исходящей почты (предоставляющий доступ по протоколу SMTP). Он позволял обрабатывать списки рассылки, почтовые псевдонимы, правила подстановки для подмены адреса отправителя и получателя, таблицы настройки безопасности. Наиболее стабильным сервером исходящей почты, поддерживающий перечисленные сервисы оказался sendmail.

Для доставки входящей почты в компьютеры пользователей используется протокол POP3 (Post Offce Protocol версии 3). Программное обеспечение предоставляющее клиентам доступ по этому протоколу, как правило, является более простым и как следствие этого мнее затратным по ресурсам. Такой сервер запускается на порядок быстрее чем sendmail. По этой причине чаще всего программа запускается по мере необходимости, для более рационального использования ресурсов многозадачного планировщика процессов. Такой запуск - по необходимости – реализуется суперсервером служб интернет – inetd (xinetd).

Это программное обеспечение опираться, в своей функциональности на базовые элементы архитектуры ОС Unix – система учета и авторизации пользователей и личные (домашние - home) каталоги пользователей.

В данной работе студенту даются готовые конфигурационные файлы почтовых серверов, которые он должен передать (выгрузить) на сервер, для выгрузки можно использовать протоколы (и соответствующие серверные программы) – FTP и SSH. Для выполнения лабораторной работы используется виртуальная маши-

на Virtual Box и образ загрузочного диска — Linux Live CD, как наиболее быстрый способ быстро получить сконфигурированную и рабочую Linux среду. Недостаток такого подхода – все изменения произведенные на сервере в ходе сеанса работы теряются, поэтому необходимо сразу готовить отчёт по работе, отмечая достаточно мелкие детали и на первый взгляд несущественные проблемы.

Замечание по подготовке лабораторного стенда: Между компьютерами должна быть установлена локальная есть, если используется VirtualBox, лучше всего переключить вирт. адаптеры на режим Virtual Box host only. Предварительно сеть нужно проверить при помощи ping <IP>, если логически видно, что ip-адреса в разных сетях, нужно перезапросить процедуру переустановки сетевых интерфейсов командой: dhclient eth0 или dhcpcd eth0, возможно придётся удалить файл хранимой блокировки с расширением ".pid", если запрос завершается ошибкой нужно остановить процесс блокирующий это действие: killall dhcpcd. У всех виртуальных компьютеров должны быть одинаковые настройки сетевых адаптеров.

Если ресурсов лабораторного компьютера недостаточно, в частности суммарно ОЗУ виртуальных машин занимают более 50% физического ОЗУ, то рационально проводить лабораторную работу в группе из нескольких участников, расположившихся в лаборатории за соседними компьютерами, используя общую физическую сеть. Для этого сетевые адаптеры VirtualBox должны быть в режиме "Сетевой мост". Для экономии ресурсов серверные системы нужно загружать в режиме "Text mode".

Ход выполнения работы:

1) Узнаем ip-адреса <IP> всех компьютеров системы, составляем карту адресов.

2) Если не запущен процесс sshd, запустим терминальный сервер (прим. при работе с ASP Linux запуск sshd не нужен)

/usr/sbin/sshd-generate

/usr/sbin/sshd

3) Подключится через putty к терминальному серверу или через ssh root@<IP>

4) Подготовить начальную конфигурацию почтового сервера:

4.1 Переводим командный интерпретатор в каталог конфигурации почтового сервера

командой cd /etc/mail

4.2 Даём разрешение на отправку почты

echo "<IP_NET_ADDR> RELAY" >./access

make access.db

4.3 Объявляем имя домена, для которого sendmail адреса почтовых ящиков будет считать локальными

echo -e "mail.ru\nmail" >local-host-names

echo "mail.ru mail" >domaintable

make domaintable.db

Это должно исключить попытки sendmail осуществить маршрутизацию почты при помощи DNS если вы укажете не объявленное имя домена то возможны такие ответы sendmail:

Deferred: mail.ru.: No route to host

Deferred: mail.ru.: Network is unreachable

5) Проверяем распознавание доменного имени, отправляем почту локально

echo -e "Hello world\!" | sendmail root@mail.ru

6) Если получено "Deferred: Connection refused by [127.0.0.1]", то нужно запустить MTAфоновым процессом: sendmail -bd -q25m (прим. при работе с ASP Linux запуск sshd не нужен, перезапуск делается через скрипты управления демонами /etc/init.d/sendmail restart)

7) Если получено "Cannot exec /usr/bin/procmail: No such file or directory Operating system error", то нужно скопировать файл утилиты procmail из другой установки ОС, напр. Другого LiveCD дистрибутива, в частности подойдёт ASP Linux live cd

8) Статус "Sent" означает что почта отправлена, проверьте содержимое каталога

/var/spool/mail

9) Если статус "Deferred: local mailer (/usr/bin/procmail) exited with EX_TEMPFAIL", то нужно независимо проверить работу процессора почты - procmail, моделируя доставку сообщения командой echo "Hellow world" | procmail root@mail.ru , Если файл не может быть создан в каталоге, то скорее всего каталог лучше удалить и создать заново. Перед этим выяснить, почему файл не создаётся введя ls -la <путь к каталогу>. Если какой-то файл не может быть прочитан, то его стоить создать командой touch <имя и путь к файлу>.

10) Результат доставки почты контролируйте при помощи утилиты mail, если её ответом является "No mail for root", то нужно указать файл который не мог быть записан в тесте пункта №9

11) Проверить возможность отправки почты с удалёного хоста,

для этого

-Найти номер порта sendmail командой: netstat -anp | grep sendmail . Из нескольких портов выбрать тот который описан в табл. /etc/services как номер потра протокола smtp

-Текстовым терминалом (telnet-ом) подключиться к tcp порту 25 почтового сервера (MTA) telnet <IP> 25. При удачном подключении telnet закрывается нажатием ctrl+"]".

-если соединение не удалось: найти адрес на котором открыт порт No25 командой netstat -an | grep 25 , понять является ли этот адрес адресом внешнего сетевого интерфейса, если нет перенастроить сервер командой vi /etc/mail/sendmail.cf <CR><LF> "/127.0.0.1" "x" 9 раз, "i" 0.0.0.0 ":wq". Принудительно снять с выполнения процесс MTA: killall sendmail и запустить его так как написано в п. No6

-на компьютере, работающего под управлением ОС Windows (Alkid), активировать

поддержку сети (сеть вкл.), при помощи приложения "The Bat!" отправить почту на адрес MTA (SMTP сервера), причём адрес сервера должен быть задан в десятично-цифровом формате.

Примечание: smtp сервер не требует аутентификации, а выбор POP3/IMAP является

несущественным.

-отправить почту из MUA (The Bat или Thuderbird) и проверить доставку через почтовый журнал: cat /var/log/maillog и при помощи утилиты mail. Результат зафиксировать.

ДОПОЛЕНИЕ: На оценку "ОТЛ" реализовать модель двузвенного (два сервера) транспорта электронной корреспонденции (для этого /etc/host на первом сервере должен содержать ссылку на домен получателя - адрес второго сервера).

Перечень источников

1. file://s2/root/readonly/ForStud/kudinov/Сетевые техол/sendmail

2. http://ru.wikipedia.org/wiki/Sendmail

3. Настройка sendmail http://www.freebsd.org/doc/ru/books/handbook/sendmail.html

4. Дубровин Б.А. Установка суперсервера xinetd. http://www.ofnet.ru/prostye-lokalnye-seti/install-xinetd.html

Перечень вопросов ко второй лабораторной работе

1. Как различаются сервер входящей и исходящей почты? Это разные программы?
2. Почему sendmail может не отвечать на входящие запросы? Назовите причины.
3. Что нужно сделать, чтобы sendmail не отвергал исходящую электронную почту?
4. Что содержится в файле local-host-names.
5. Что содержится в файле domaintable.
6. Как проверить, что sendmail открыл 25-й порт на сервере?
7. Как убедится, что именно sendmail прослушивает 25-й порт?
8. Назовите простой способ создания почтовых ящиков.
9. Где находится очередь почтового сервера?
10. Что означают опции программы /sbin/sendmail –Ac –bd
11. Как увидеть, с какими параметрами запущен почтовый сервер?
12. Зачем и как перезапускают почтовый сервер?
13. Что такое список рассылок и как он обрабатывается почтовым сервером?
14. Зачем пользователи создают у себя в домашних каталогах файл .forward
15. Какая информация нужна почтовому серверу, чтобы принять решение о локальной доставке электронной почты?
16. Назовите простой способ локально проверить Ваш почтовый ящик.
17. Какие основные параметры учётных записей Outlook Express вводятся при настройке MUA.
18. Что такое MUA и MTA?
19. В случае неисправности, при отправке почты, зачем пинговать почтовый сервер?
20. Как получить актуальный файл access.db.
21. Что содержит файл почтовых псевдонимов aliases.
22. Может ли опытный пользователь обойтись без MUA?

4. ЛАБОРАТОРНАЯ РАБОТА №4

Тема работы: Изучение методов настройки сетевых экранов и технологии отображения портов.

Цель работы: Получить навыки настройки межсетевого экрана (netfilter) в ОС Linux. Выявить множество параметров, доступных для администрирования в межсетевом экране.

Порядок выполнения работы

В данной работе будет проведена установка и конфигурирование программного обеспечения фильтрации сетевого трафика. Рекомендуется придерживаться следующего плана выполнения:

1. Создать правило для использования межсетевого экрана в режиме запрета всех входящих передач с компьютера с адресом 10.44.0.66. При установленном пакете iptables это реализуется следующей командой:

iptables -A INPUT -s 10.44.0.66 -j DROP

В результате проделанных действий были заблокированы входящие пакеты приходящие от компьютера, имеющий IP адрес 10.44.0.66. Блокировка проверяется командной ping 10.44.0.30.

2. Удалить добавленное правило из цепочки правил командой:

iptables -D INPUT -s 10.44.0.66 -j DROP

Удаление правила соответствует разрешению прохождения пакетов на адрес 10.44.0.30.

Команда iptables –F очищает все правила в каждой цепочке.

3. Провести эксперимент с пробросим пакетов с сетевого порта одного компьютера на другой компьютер с заданным ip-адресом. Для этого запускаются две виртуальные машину под управление ОС Unix и ПО эмуляции виртуальной машины VirtualBox. В качестве типа внешней связи для сетевого адаптера выберем сетевой мост, что сосуществует прямому соединению с локальной сетью по схеме заезда.

4. На каждой из виртуальных машин необходимо узнать ip адреса, анализом вывода команды ifconfig. Необходимо выбрать среди виртуальных компьютеров сетевой шлюз волевым решением.

На шлюзе вводятся команды:

1) Iptables -t nat –A PREROUTING -p tcp –d 10.44.0.31 --dport 22 –j DNAT --to- distination 10.44.0.30:22

2) Iptables –A FORWARD –I eth0 –d 10.44.0.30 -p tcp –d 10.44.0.31 --dport 22 –j ACCEPT

Содержание отчета

1. Цель работы;
2. Ход вызволения работы с промежуточными выводами и графическими фрагментами копий экрана;
3. Выводы по работе и их возможные обобщения;

5. ЛАБОРАТОРНАЯ РАБОТА №5

Тема работы: Администрирование Windows 2003. Advanced Server. Изучение Active Directory.

Цель работы:

1. Научится администрированию сетевых операционных систем.
2. Ознакомится со свойствами объекта «Пользователь» и «Группа» в настоящих сетевых операционных системах. Научится правильно применять сочетания прав.
3. Ознакомится со списками пользователей, разработанными в соответствии со стандартом ITU-T X.400.
4. Ознакомится со структурой прав на файлы и каталоги в системе Windows 2000 Server. Ознакомление с маской наследуемых прав.

Ход выполнения работы:

1. В ПО Virtual Box организовать модель сети из двух компьютеров — одного клиентского, а другого серверного. Образы жестких дисков для загрузки операционных систем можно получить у преподавателя.
2. На серверной машине путем ввода команды

   dcpromo

активировать установку конфигурации службы Active Directory. Процесс создания конфигураций будет предварен диалогом с пользователем. Запрашивается имя домена, логин и пароль администратора домена.

3. Реализовать два варианта нахождения контроллера домена (сервера) по протоколу NetBIOS (в локальной сети) и с использованием указателей DNS.

ПРИМЕЧАНИЕ: Доступ к контроллеру домена первый раз производиться на рабочей станции пользователя при включении станции в домен (регистрация). В параметрах пиктограммы «Мой компьютер» выбрать диалоговую вкладку «Сетевая идентификация»\Домен и ввести имя.

4. После регистрации сведения о рабочей станции будут доступны при древовидном просмотре структуры базы данных Active Directory, который активизируется пиктограммой «Пользователи и компьютеры» в разделе «Администрирование» панели управления.

5. В интерфейсе «Пользователи и компьютеры» зарегистрировать виртуального пользователя с абстрактным именем и авторизоваться от имени этого пользователя на этой машине.

6. Далее необходимо реализовать задания по вариантам:

Вариант 1

1) Создать учетную запись для пользователя ANTONOV (с созданием домашнего каталога ANTONOV) Пользователь должен иметь все права на свой домашний каталог, кроме права супервизора.

2) Запретить пользователю самостоятельно изменять пароль.

3) Разрешить пользователю работать в сети до 21.10.2006.

4) Разрешить пользователю вход в сеть только в течение рабочего дня:

понедельник 8:00-17:00
вторник 8:00-17:00
среда 8:00-17:00
четверг 8:00-17:00
пятница 15:00-22:00
суббота выходной
воскресенье выходной

5) Установить сервер по умолчанию NW_DSTU.

6) Ограничить количество одновременных подключений пользователя одним.

7) Ограничить максимальный объем доступного дискового пространства в домашнем
каталоге 500K.

8) Проверить, создана ли группа MANAGERS, если её нет, то создать.

9) Включить в группу MANAGERS пользователей ANTONOV и BOKOV, если такой существует.

10) Создать каталог MANAGERS. С помощью утилиты RIGHTS назначить опекуном этого
каталога группу MANAGERS. Эта группа не должна иметь прав на удаление, изменение, создание файлов в этом каталоге, а также не должна иметь возможности назначить себе допол-

нительные права кроме назначенных администратором.

11) Создать файл в каталоге MANAGERS. Назначить опекуном этого файла пользователя ANTONOV. Он должен иметь возможность дописывать информацию в файл, но не иметь возможности его удалить.

Вариант 2

1) Создать учетную запись для пользователя BOKOV (без создания домашнего каталога).

2) Разрешить пользователю самостоятельно изменять пароль.

3) Установить дату истечения срока действия пароля 30.10.2006.

4) Запретить пользователю назначать себе пароль менее 7 символов.

5) Запретить пользователю назначать себе один и тот же пароль дважды.

6) Установить сервер по умолчанию NW_DSTU.

7) Разрешить пользователю работать в сети только 11 дней с момента создания.

8) Запретить пользователю вход в сеть до начала или после окончания рабочего дня:

понедельник 9:00-18:00
вторник 9:00-18:00
среда 8:00-17:00
четверг 9:00-18:00
пятница 16:00-22:00
суббота 10:00-14:00
воскресенье выходной

9) Ограничить количество одновременных подключений пользователя тремя.

10) Создать каталог BOKOV и назначить опекуном данного каталога пользователя BOKOV. Пользователь должен иметь все права на этот каталог, кроме права супервизора.

11) Ограничить максимальный объем доступного дискового пространства в созданном

каталоге 300K.

12) Проверить, создана ли группа HQ, если её нет, то создать.

13) Включить в группу HQ пользователей BOKOV и ANTONOV, если такой существует.

14) Создать каталог HQ. С помощью утилиты RIGHTS назна-

чить опекуном этого каталога группу HQ. Эта группа не должна иметь прав на удаление и изменение файлов в этом каталоге, а также не должна иметь возможности назначить себе дополнительные права кроме назначенных администратором.

15) Создать файл в каталоге HQ. Назначить опекуном этого файла пользователя BOKOV. Он должен иметь возможность дописывать информацию в файл и удалять его, зная его имя, но не иметь возможности найти его.

Вариант 3

1) Создать учетную запись для пользователя PETROV (с созданием домашнего каталога PETROV) Пользователь должен иметь все права на свой домашний каталог, кроме права супервизора.

2) Запретить пользователю самостоятельно изменять пароль.

3) Разрешить пользователю работать в сети до 11.11.2006.

4) Разрешить пользователю вход в сеть только в течение рабочего дня:

понедельник	7:00-16:00
вторник	7:00-16:00
среда	8:00-17:00
четверг	8:00-17:00
пятница	15:30-22:00
суббота	выходной
воскресенье	выходной

5) Отменить установку сервера по умолчанию.

6) Ограничить количество одновременных подключений пользователя четырьмя.

7) Ограничить максимальный объем доступного дискового пространства в
домашнем каталоге 300K.

8) Проверить, создана ли группа SALES, если её нет, то создать.

9) Включить в группу SALES пользователей PETROV и SIDOROV, если такой существует.

10) Создать каталог SALES. С помощью утилиты RIGHTS назначить опекуном этого ка-
талога группу SALES. Эта группа не должна иметь прав на удаление, изменение,
создание файлов в этом каталоге, а также не должна иметь возможности назначить

себе дополнительные права кроме назначенных администратором.

11) Создать файл в каталоге SALES. Назначить опекуном этого файла пользователя PETROV. Он должен иметь возможность дописывать информацию в файл, но не иметь возможности его удалить.

Вариант 4

1) Создать учетную запись для пользователя SIDOROV (без создания домашнего каталога).

2) Разрешить пользователю самостоятельно изменять пароль.

3) Установить период действия пароля 45 дней.

4) Запретить пользователю назначать себе пароль менее 8 символов.

5) Не запрещать пользователю назначать себе один и тот же пароль дважды.

6) Установить сервер по умолчанию NW_DSTU.

7) Разрешить пользователю работать в сети только 24 дня с момента создания.

8) Запретить пользователю вход в сеть до начала или после окончания рабочего дня:

понедельник	11:00-19:00
вторник	11:00-18:00
среда	11:00-19:00
четверг	10:30-18:30
пятница	16:30-22:00
суббота	10:00-14:00
воскресенье	выходной

9) Ограничить количество одновременных подключений пользователя четырьмя.

10) Создать каталог SIDOROV и назначить опекуном данного каталога пользователя SIDOROV. Пользователь должен иметь все права на этот каталог, кроме права супервизора.

11) Ограничить максимальный объем доступного дискового пространства в созданном каталоге 1300K.

12) Проверить, создана ли группа PD, если её нет, то создать.

13) Включить в группу PD пользователей SIDOROV и PETROV, если такой существует.

14) Создать каталог PD. С помощью утилиты RIGHTS назначить опекуном этого каталога группу PD. Эта группа не должна иметь прав на удаление и изменение файлов в этом каталоге, а также не должна иметь возможности назначить себе дополнительные права кроме назначенных администратором.

15) Создать файл в каталоге PD. Назначить опекуном этого файла пользователя SIDOROV. Он должен иметь возможность дописывать информацию в файл и удалять его, зная его имя, но не иметь возможности найти его.

Вариант 5

1) Создать учетную запись для пользователя BOSS (с созданием домашнего каталога BOSS) Пользователь должен иметь все права на свой домашний каталог, кроме права супервизора.

2) Разрешить пользователю самостоятельно изменять пароль.

3) Установить период действия пароля 38 дней.

4) Запретить пользователю назначать себе пароль менее 4 символов.

5) Не запрещать пользователю назначать себе один и тот же пароль дважды.

6) Установить сервер по умолчанию NW_DSTU.

7) Разрешить пользователю работать в сети только 44 дня с момента создания.

8) Запретить пользователю вход в сеть до начала или после окончания рабочего дня:

понедельник	10:30-19:00
вторник	10:30-18:00
среда	10:30-19:00
четверг	10:00-18:30
пятница	16:00-21:30
суббота	выходной
воскресенье	выходной

9) Ограничить количество одновременных подключений пользователя четырьмя.

10) Ограничить максимальный объем доступного дискового пространства в домашнем каталоге 550K.

11) Проверить, создана ли группа WH1, если её нет, то создать.

12) Включить в группу WH1 пользователей BOSS и ZAM, если такой существует.

13) Создать каталог WH1. С помощью утилиты RIGHTS

назначить опекуном этого каталога группу WH1. Эта группа не должна иметь прав на удаление, изменение, создание файлов в этом каталоге, а также не должна иметь возможности назначить себе дополнительные права кроме назначенных администратором.

14) Создать файл в каталоге WH1. Назначить опекуном этого файла пользователя BOSS. Он должен иметь возможность дописывать информацию файл, но не иметь возможности его удалить.

Вариант 6

1) Создать учетную запись для пользователя ZAM (без создания домашнего каталога).

2) Запретить пользователю самостоятельно изменять пароль.

3) Разрешить пользователю работать в сети до 15.12.2006.

4) Разрешить пользователю вход в сеть только в течение рабочего дня:

понедельник 8:30-17:00
вторник 8:30-17:00
среда 8:00-18:30
четверг 8:00-18:30
пятница 15:30-21:30
суббота выходной
воскресенье выходной

5) Отменить установку сервера по умолчанию.

6) Ограничить количество одновременных подключений пользователя тремя.

7) Создать каталог ZAM и назначить опекуном данного каталога пользователя ZAM.

Пользователь должен иметь все права на этот каталог, кроме права супервизора.

8) Ограничить максимальный объем доступного дискового пространства в созданном

каталоге 2M.

9) Проверить, создана ли группа WH2, если её нет, то создать.

10) Включить в группу WH2 пользователей ZAM и BOSS, если такой существует.

11) Создать каталог WH2. С помощью утилиты RIGHTS назначить опекуном этого каталога группу WH2. Эта группа не должна иметь прав на удаление и изменение файлов в этом ка-

талоге, а также не должна иметь возможности назначить себе дополнительные права кроме назначенных администратором.

12) Создать файл в каталоге WH2. Назначить опекуном этого файла пользователя ZAM. Он должен иметь возможность дописывать информацию в файл и удалять его, зная его имя, но не иметь возможности найти его.

Вариант 7

1) Создать учетную запись для пользователя CHEEF (с созданием домашнего каталога CHEEF) Пользователь должен иметь все права на свой домашний каталог, кроме права супервизора.

2) Разрешить пользователю самостоятельно изменять пароль.

3) Установить период действия пароля 18 дней.

4) Запретить пользователю назначать себе пароль менее 7 символов.

5) Запретить пользователю назначать себе один и тот же пароль дважды.

6) Установить сервер по умолчанию NW_DSTU.

7) Запретить пользователю работу в сети через 15 дней с момента создания.

8) Запретить пользователю вход в сеть до начала или после окончания рабочего дня:

понедельник	9:30-17:00
вторник	9:30-17:00
среда	9:30-17:30
четверг	9:00-18:30
пятница	16:00-21:30
суббота	выходной
воскресенье	выходной

9) Ограничить количество одновременных подключений пользователя тремя.

10) Ограничить максимальный объем доступного дискового пространства в домашнем каталоге 4M.

11) Проверить, создана ли группа ENGENEERS, если её нет, то создать.

12) Включить в группу ENGENEERS пользователей CHEEF и ELECTRO, если такой существует.

13) Создать каталог ENGENEER. С помощью утилиты RIGHTS назначить опекуном этого каталога группу ENGENEERS. Эта группа не должна иметь прав на удаление, изменение, создание файлов в этом каталоге, а также не должна иметь возможности

назначить себе дополнительные права кроме назначенных администратором.

14) Создать файл в каталоге ENGENEER. Назначить опекуном этого файла пользователя CHEEF. Он должен иметь возможность дописывать информацию в файл, но не иметь возможности его удалить.

Вариант 8

1. Создать учетную запись для пользователя ELECTRO (без создания домашнего каталога).

2. Запретить пользователю самостоятельно изменять пароль.

3. Запретить пользователю работать в сети после 01.12.2006.

4. Разрешить пользователю вход в сеть только в течение рабочего дня:

понедельник	8:30-17:30
вторник	8:30-17:30
среда	8:00-18:30
четверг	8:00-18:30
пятница	15:30-21:30
суббота	выходной
воскресенье	выходной

5) Установить сервер по умолчанию NW_DSTU.

6) Ограничить количество одновременных подключений пользователя двумя.

7) Создать каталог ELECTRO и назначить опекуном данного каталога пользователя ELECTRO. Пользователь должен иметь все права на этот каталог, кроме права супервизора.

8) Ограничить максимальный объем доступного дискового пространства в созданном каталоге 1М.

9) Проверить, создана ли группа MARKETING, если её нет, то создать.

10) Включить в группу MARKETING пользователей ELECTRO и CHEEF, если такой существует.

11) Создать каталог MARKET. С помощью утилиты RIGHTS назначить опекуном этого каталога группу MARKETING. Эта группа не должна иметь прав на удаление и изменение файлов в этом каталоге, а также не должна иметь возможности назначить себе дополнительные права кроме назначенных администратором.

12) Создать файл в каталоге MARKET. Назначить опекуном этого файла пользователя ELECTRO. Он должен иметь возмож-

ность дописывать информацию в файл и удалять его, зная его имя, но не иметь возможности найти его.

7. Создать в административной оснастке «Пользователи и компьютеры» контейнер Administration Unit.

8. Переместить пользователя и компьютер (рабочую станцию) в этот контейнер

9. Меняя параметры контейнера добиться изменения параметров пользователя и компьютера сразу. Сделать вывод.

Дополнительная литература:

1. http://ru.wikipedia.org/wiki/Active_Directory
2. http://www.mista.ru/articles1c/active.htm
3. http://habrahabr.ru/company/netwrix/blog/160837/

3. и ПО VirtualBox https://www.virtualbox.org/wiki/Downloads