1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский государственный политехнический университет
3. —
4. Институт компьютерных наук и технологий
5. **Кафедра «Информационная безопасность компьютерных систем»**

**ОТЧЕТ**

**по лабораторной работе № 3**

1. **«Сетевые службы. Защита сетевых ресурсов»**
2. по дисциплине «Операционные системы»
3. Выполнил
4. студент гр. 23508/4 Проценко Е.Г.
5. Проверил
6. ст. преподаватель Резединова Е.Ю.
7. Санкт-Петербург
8. 2016

# Формулировка задания

Настроить сеть с учетом следующих параметров (вариант работы 18).

|  |  |  |  |
| --- | --- | --- | --- |
| *Имя компьютера* | *Платформа* | *Сетевое конфигурирование* | |
| RedHatServer1 | Red Hat Enterprise Linux 4 | IP | 192.168.123.1 |
| RedHatServer2 | Red Hat Enterprise Linux 4 | IP | 192.168.123.2 |
| WinXPServer1 | WindowsXP SP2 | IP | 192.168.123.3 |
| WinXPServer2 | WindowsXP SP2 | IP | 192.168.123.4 |

Маска подсети 255.255.255.0; Основной шлюз 192.168.123.8;

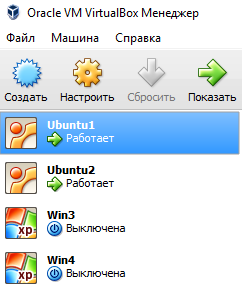
Компьютеры должны находиться в одной сетевой группе.

Проверить сетевое взаимодействие ОС с помощью команды ping.

Создать файлы, которые отображаются при возникновении какой-либо ошибки на стороне сервера. Поместить в них сообщение об ошибке и ее описание.

Создать запросы с машины под управлением OC UNIX, так чтобы отобразились созданные файлы.

# Результаты работы

Для выполнения данной лабораторной работы было выбрано ПО Oracle VirtualBox.

Для виртуализации понадобились два экземпляра ОС Windows XP и два OS Ubuntu.

**Соединение виртуальных машин в единую сеть**. Для обеспечения возможности взаимодействия наших виртуальных машин необходимо в настройках каждой виртуальной машины зайти во вкладку Сеть и сделать так как на картинке: выбрать внутреннюю сеть, главное теперь, чтобы имя у всех было одинаковое (в нашем случае “intnet”) :

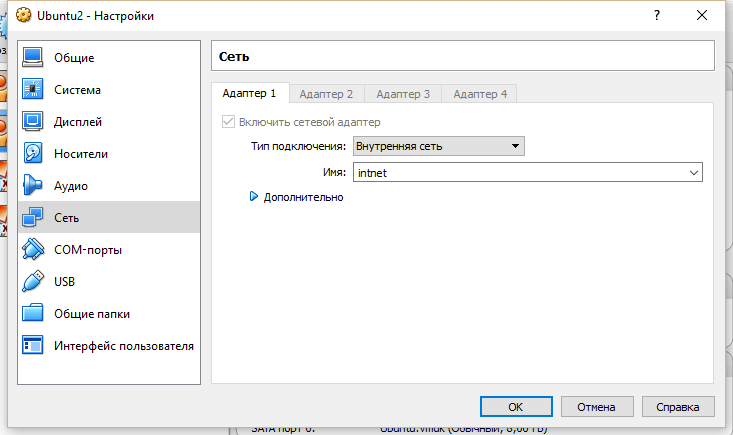


Рисунок 1 - Настройка внутренней сети между виртуальными машинами VirtualBox

Подключив каждую машину к созданной нами сети "UNIX-Windows-Network" (изначально каждая подключена к сети хостового компьютера через NAT), получаем внутреннюю сеть между 4 виртуальными машинами. Теперь необходимо сконфигурировать каждую машину в отдельности в соответствии с заданием лабораторной работы:

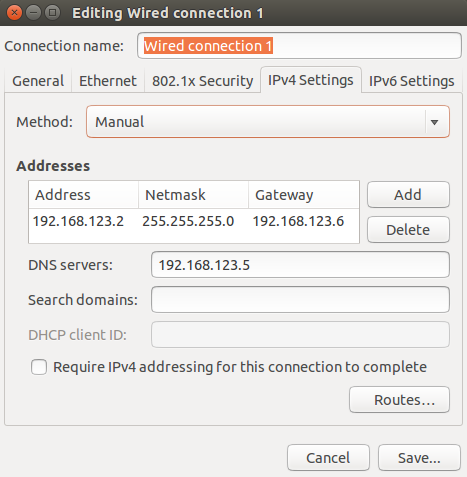
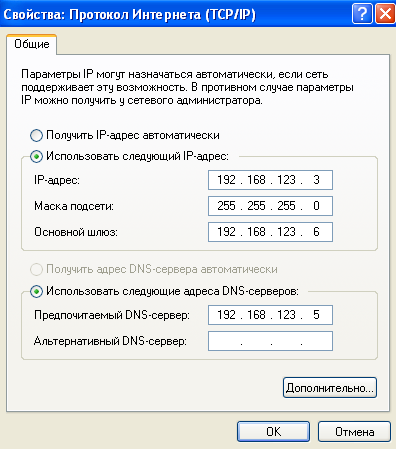
 

Рисунок 2 - Окно конфигурации параметров сети в Ubuntu и MS Windows XP SP2

Для того, чтобы проверить возможность взаимодействия машин, необходимо выполнить команду "ping", указав адреса остальных компьютеров в сети. В процессе выполнения лабораторной работы было установлено, что все компьютеры в нашей сети отвечают друг другу на команду "ping", как это и должно быть при правильной настройке. Для отсутствия проблем при ping-е необходимо отключить фаервол на каждой машине.

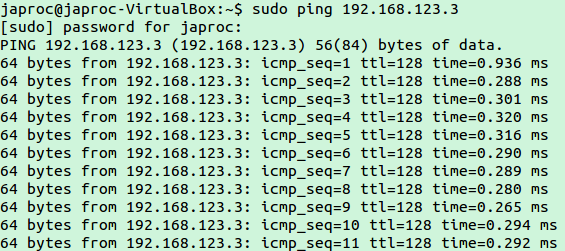


Рисунок 3 – Демонстрация того, как машины пингуются.

На машину с MS Windows XP SP2 и IP-адресом 192.168.123.3 был установлен HTTP-сервер Apache версии 2.2.11.

Для демонстрации работоспособности сервера нужно зайти с одной из виртуальных машин на наш сервер, там же мы должны увидеть надпис It Works! После, я добавил папки, чтобы показать, что они будут отображаться.

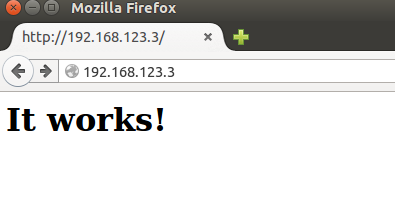
 

Рисунок 4 – Демонстрация работоспособности сервера.

В Apache можно вести лог ошибок. Стандартный файл httpd.conf имеет раздел логов с комментариями для каждой директивы. директиву настройки лога ошибок в httpd.conf:  
  
ErrorLog logs/error\_log

Уровень ошибок, попадающих в лог, устанавливается следующим образом:  
  
LogLevel warn  
  
В Apache определены следующие уровни ошибок:  
  
- emerg - экстренный – система не функционирует;  
- alert - ошибку необходимо немедленно исправить;  
- crit - критическая ошибка;  
- error – ошибка;  
- warn – предупреждение;  
- notice - уведомление (нормальное функционирование);  
- info - информационное сообщение;  
- debug - сообщение отладки.

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined  
  
Строка начинается с LogFormat и сообщает Apache, что вы определили тип файла лога. Сейчас давайте взглянем на символы, которые составляют определение формата сообщения.

%h – IP-адрес клиента (удаленного хоста);  
%l - имя пользователя (от identd);  
%u - userid удаленного пользователя (полезно при использовании HTTP-авторизации);  
%t - дата и время запроса;  
%r - строка запроса;  
%s - код статуса, отсылаемый сервером клиенту (201, 301, 404, 500, и т.д.). Символ > перед s показывает, что в лог записывается только последний статус;  
%b - количество отправленных байтов клиенту (HTTP-заголовки не учитываются);  
%i - элементы, передаваемые в HTTP-заголовках. Таким образом, добавляя Referer и User-Agent можно отслеживать ссылающиеся URL и типы браузеров. Если запрошенная информация недоступна, то в логе она заменяется дефисом. Чтобы вставить в лог символ % необходимо использовать %%.

# Выводы

В данной лабораторной работе были исследованы основы внутрисетевого взаимодействия между четырьмя различными машинами. Работа показала, что наладить взаимодействие между клиентами сети достаточно нетрудно (однако надо найти работоспособную версию Apache для Windows) и всё упирается лишь в то, как какой-то очень асбтрактный механизм (например, написание правил) реализуется на выбранной платформе.

# Контрольные вопросы

* **Какие функции обеспечивают серверная и клиентская части сетевой ОС?**  
  Ответ: Средства предоставления собственных ресурсов и услуг в общее пользование — серверная часть ОС (сервер). Эти средства обеспечивают, например, блокировку файлов и записей, что необходимо для их совместного использования; ведение справочников имен сетевых ресурсов; обработку запросов удаленного доступа к собственной файловой системе и базе данных; управление очередями запросов удаленных пользователей к своим периферийным устройствам. Средства запроса доступа к удаленным ресурсам и услугам и их использования — клиентская часть ОС. Эта часть выполняет распознавание и перенаправление в сеть запросов к удаленным ресурсам от приложений и пользователей, при этом запрос поступает от приложения в локальной форме, а передается в сеть в другой форме, соответствующей требованиям сервера. Клиентская часть также осуществляет прием ответов от серверов и преобразование их в локальный формат.
* **Каковы основные отличия рекурсивных DNS-серверов от нерекурсивных?**Ответ: DNS-серверы бывают рекурсивные и не рекурсивные. Первые всегда возвращают клиенту ответ — они самостоятельно отслеживают отсылки к другим DNS-серверам и опрашивают их. Не рекурсивные сервера возвращают клиенту эти отсылки, так что клиент должен самостоятельно опрашивать указанный сервер.
* **Какие функции выполняют демоны Samba?**Ответ: Работа серверной части Samba основана на двух демонах: smbd — обеспечивает сетевой сервис файлов и печати, а также аутентификацию и авторизацию пользователей; nmbd — отвечает за службу имен NetBIOS.
* **Каким образом можно ограничить доступ к ресурсам web-сервера Apache?**Ответ: Существует множество настроек уровней прав доступа к различным ресурсам сервера Apache. Например, можно редактировать общую карту доступа к ресурсам сервера. Можно ограничивать доступ по определенным IP-адресам; к определенным каталогам и т.д. Более того, каждый пользователь, имеющий на сервере свой каталог, может управлять доступом других пользователей к данному каталогу посредством файла .htaccess.
* **С какой целью используется действие LOG межсетевого экрана netfilter/iptables?**Ответ: Как очевидно следует из названия, LOG - действие, служащее для журналирования отдельных пакетов событий. Информация журнала может быть прочитана, например, с помощью dmesg, syslogd.

# Приложение

Директории в файле httpd, отвечающие за ведение лога:  
ErrorLog "logs/error.log"

LogLevel warn

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined

LogFormat "%h %l %u %t \"%r\" %>s %b" common

CustomLog "logs/access.log" common