

Министерство образования и науки Российской Федерации
Санкт-Петербургский государственный политехнический университет

—
Институт компьютерных наук и технологий
Кафедра «Информационная безопасность компьютерных систем»

**ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3**

«Сетевые службы. Защита сетевых ресурсов»

по дисциплине «Операционные системы»

Выполнил
студент гр. 23508/4

Проценко Е.Г.

Проверил
ст. преподаватель

Резединова Е.Ю.

Санкт-Петербург
2016

1 ФОРМУЛИРОВКА ЗАДАНИЯ

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

<i>Имя компьютера</i>	<i>Платформа</i>	<i>Сетевое конфигурирование</i>	
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.

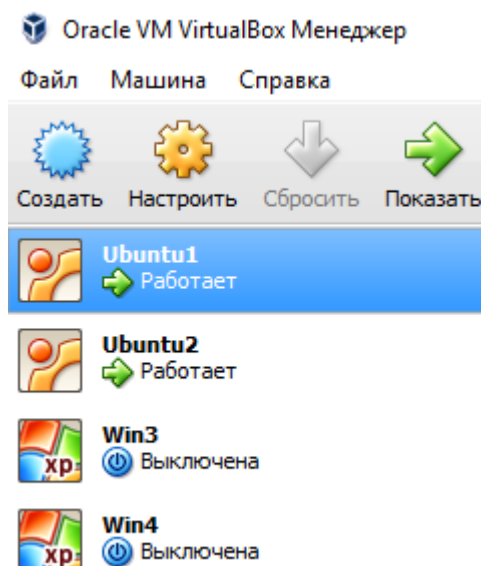
Создать файлы, которые отображаются при возникновении какой-либо ошибки на стороне сервера. Поместить в них сообщение об ошибке и ее описание.

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

2 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”) :

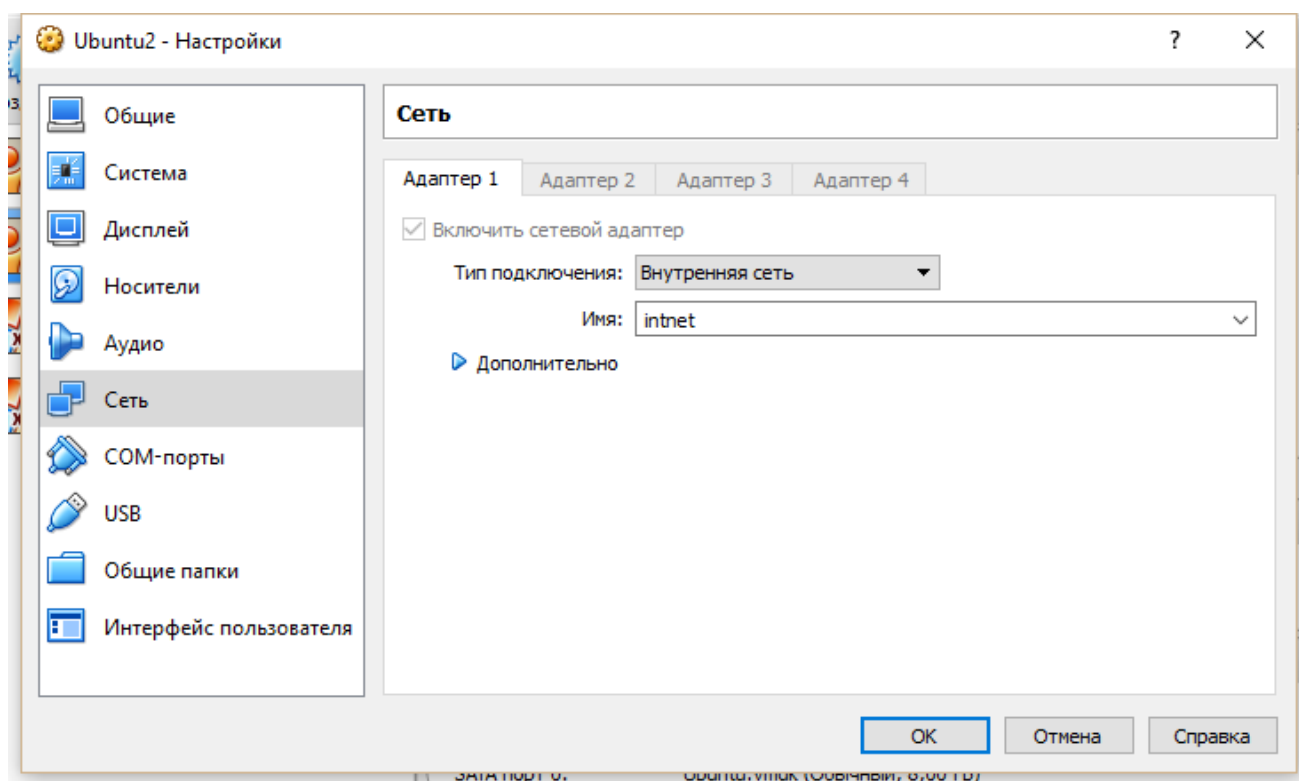


Рисунок 1 - Настройка внутренней сети между виртуальными машинами VirtualBox

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:

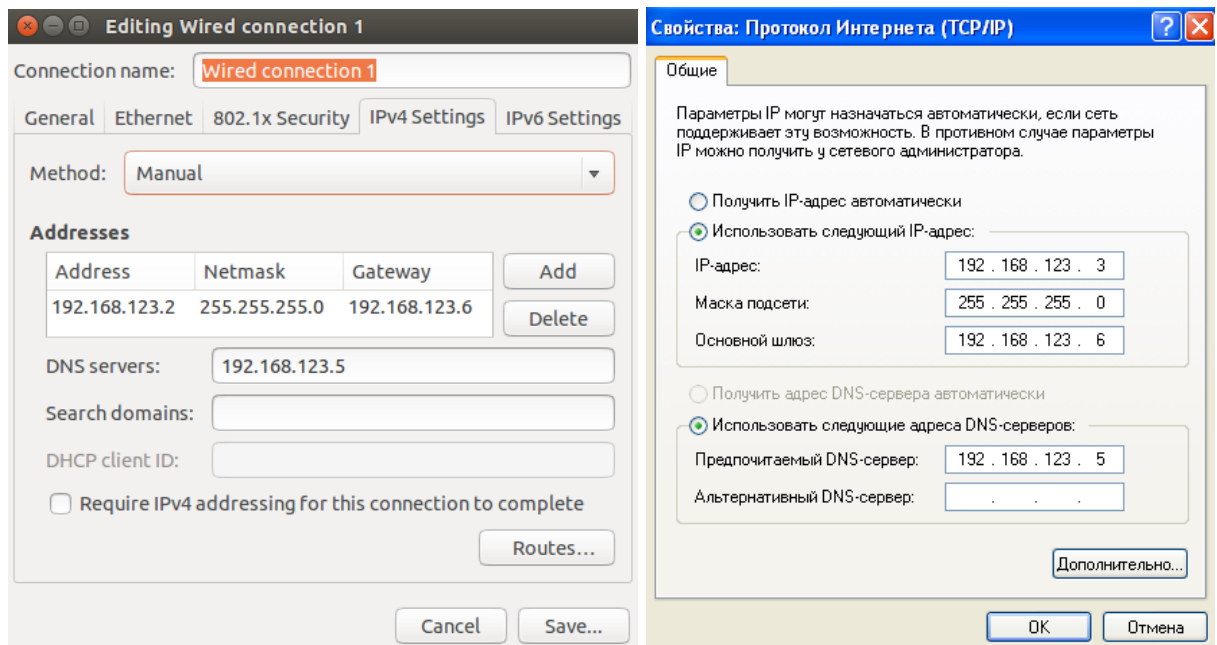


Рисунок 2 - Окно конфигурации параметров сети в Ubuntu и MS Windows XP SP2

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.

```
japroc@japroc-VirtualBox:~$ sudo ping 192.168.123.3
[sudo] password for japroc:
PING 192.168.123.3 (192.168.123.3) 56(84) bytes of data.
 64 bytes from 192.168.123.3: icmp_seq=1 ttl=128 time=0.936 ms
 64 bytes from 192.168.123.3: icmp_seq=2 ttl=128 time=0.288 ms
 64 bytes from 192.168.123.3: icmp_seq=3 ttl=128 time=0.301 ms
 64 bytes from 192.168.123.3: icmp_seq=4 ttl=128 time=0.320 ms
 64 bytes from 192.168.123.3: icmp_seq=5 ttl=128 time=0.316 ms
 64 bytes from 192.168.123.3: icmp_seq=6 ttl=128 time=0.290 ms
 64 bytes from 192.168.123.3: icmp_seq=7 ttl=128 time=0.289 ms
 64 bytes from 192.168.123.3: icmp_seq=8 ttl=128 time=0.280 ms
 64 bytes from 192.168.123.3: icmp_seq=9 ttl=128 time=0.265 ms
 64 bytes from 192.168.123.3: icmp_seq=10 ttl=128 time=0.294 ms
 64 bytes from 192.168.123.3: icmp_seq=11 ttl=128 time=0.292 ms
```

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 надпись 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 %%.

3 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 абстрактный механизм (например, написание правил) реализуется на выбранной платформе.

4 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.

5 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
```