МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования

Ульяновский государственный технический университет

ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Сборник лабораторных работ
для студентов направления 11.03.02

Составитель: Дементьев В.Е.

Ульяновск 2015

СОДЕРЖАНИЕ

ОСНОВНЫЕ ПРАВИЛА ПО ТЕХНИКЕ БЕЗОПАСНОСТИ

К выполнению лабораторных работ допускаются студенты, прослушавшие инструктаж по технике безопасности и расписавшиеся в журнале по технике безопасности. При нарушении правил техники безопасности студент отстраняется от выполнения лабораторной работы.

Перед началом работы необходимо ознакомиться с рабочим местом, используемыми приборами и оборудованием. Убедится, что все переключатели электрических схем и приборов находятся в исходном состоянии. Включение приборов и исследуемой схемы производится только после проверки их преподавателем.

Во время занятий запрещается отвлекать товарищей, громко разговаривать, покидать без необходимости рабочее место.

По окончании работы необходимо установить все переключатели в исходное состояние и выключить все приборы на рабочем месте.

Запрещается: оставлять без надзора включенное оборудование, загромождать рабочее место посторонними предметами, вскрывать и передвигать приборы, прикасаться одновременно к двум различным приборам.

При несчастном случае необходимо: обесточить оборудование и снять напряжение с электрощита лаборатории, оказать первую помощь пострадавшему, сообщить преподавателю и вызвать по телефону 03 скорую помощь.

ВВЕДЕНИЕ

Основной целью лабораторных работ по курсу «Теория информационной безопасности» является:

– закрепление теоретических знаний и более детальная проработка основных моментов теории информационной безопасности;

– изучение методов контроля безопасности информационных систем;

– приобретение навыков работы со специализированными программами;

– изучение методов обработки экспериментальных данных.

СОДЕРЖАНИЕ ОТЧЕТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

ОТЧЕТ ДОЛЖЕН СОДЕРЖАТЬ СЛЕДУЮЩИЕ РАЗДЕЛЫ:

1. Цель работы.
2. Описание используемого ПО и эксплуатируемых особенностей информационных систем.
3. Таблицы и графики результатов расчетов и измерений.
4. Выводы по проделанной работе, которые должны содержать анализ полученных результатов.

1. Лабораторная работа № 1
ОСОБЕННОСТИ РАБОТЫ С ВИРТУАЛЬНЫМИ МАШИНАМИ MICROSOFT VIRTUAL PC

1.1. Цель работы

Изучение среды Microsoft Virtual PC для создания и настройки виртуальных операционных систем.

1.2. Краткие теоретические сведения

При решении различных задач, связанных с настройкой и администрированием локальных вычислительных сетей часто требуется выполнить проверку работоспособности различных параметров (программ, настроек и т.д.) потенциально опасных для работоспособности системы. Для минимизации рисков и точного учета возможных последствий приянтия тех или иных решений применяют технологии виртуализации. В широком смысле, виртуализация представляет собой процесс отделения реализации какого-либо объекта или процесса от его представления для пользователя.

Виртуализация операционных систем тоже бывает разная, однако нас интересует такое её представление для пользователя: в операционной системе физического компьютера (её принято называть хостовой ОС): как обычная программа, устанавливается платформа виртуализации, с помощью которой создаются виртуальные машины, в которых, в свою очередь, устанавливаются различные операционные системы (их принято называть гостевыми ОС). Гостевые системы и хостовая ОС работают одновременно, обмениваются данными и участвуют в сетевом взаимодействии не только с хостовой ОС, но и с внешней по отношению к физическому компьютеру сетью.

Вариантами использования виртуальных машин на настольных компьютерах пользователей могут быть:

- Работа в виртуальной машине со старыми приложениями, не поддерживающими хостовую операционную систему вашего компьютера.
- Создание защищенных пользовательских окружений для работы с сетью (всевозможные вирусы и вредоносное программное обеспечение сможет лишь повредить гостевую операционную систему виртуальной машины, не затронув реальную систему).
- Возможность работать одновременно в нескольких системах, осуществлять сетевое взаимодействие между ними.

- Простота создания резервной копии операционной системы (не надо создавать никаких образов диска, всего лишь требуется скопировать папку с файлами виртуальной машины).
- Возможность иметь на одном компьютере неограниченное число виртуальных машин с совершенно разными операционными системами и их состояниями.
- Отсутствие необходимости перезагрузки для переключения в другую операционную систему.

Для настольных систем компании VMware и Microsoft предлагают пользователям 2 продукта: VMware Workstation и Microsoft Virtual PC. Что касается производительности и надежности, эти два продукта приблизительно равны, однако продукт VMware Workstation, хоть и превосходящий несколько Microsoft Virtual PC по возможностям, является платным и ориентирован прежде всего на IT-профессионалов. Поэтому для настольных компьютеров большего всего подходит бесплатная платформа Virtual PC, тем более, что поскольку производителем платформы является сама компания Microsoft, то поддержка хостовых и гостевых операционных систем Windows видится более полной.

1.3. Задание к лабораторной работе

1.3.1.Установка учебной ОС Windows XP в виртуальной машине Microsoft Virtual PC

1. Запустите программу Пуск->Программы->Microsoft VirtualPC
2. После запуска программы появится мастер создания новой виртуальной машины. Нажмите «Next», чтобы приступить к ее созданию.
3. В появившемся окне мастера выберите «Create a virtual machine», чтобы создать новую виртуальную машину, и нажимаем «Next» (рис 1).

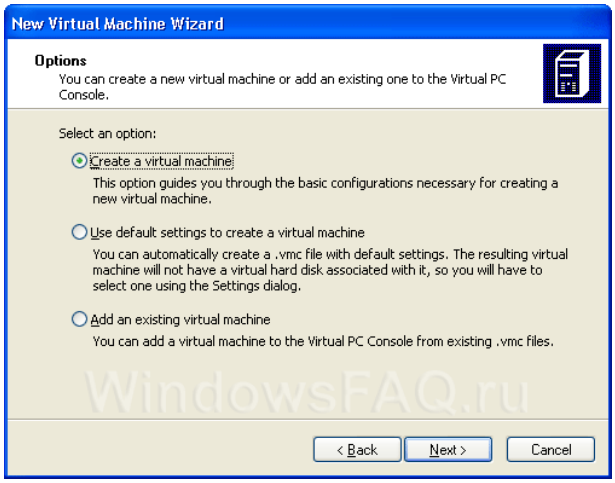


Рис 1. Создание виртуальной машины

4. В следующем окне выбирете расположение и имя файла с конфигурацией виртуальной машины. Учитывайте, что файл конфигурации виртуальной машины настоятельно рекомендуется хранить в той же папке, что и виртуальный диск, который будет создан позднее, а значит на диске, на котором вы сохраните файл, должно быть достаточно места для установки гостевой ОС.

5. На следующем шаге нужно выбрать тип гостевой операционной системы. Очень важно выбрать правильный тип гостевой ОС, так как ее производительность напрямую зависит от этого. Если вашей системы нет в списке, это еще не значит, что ее нельзя установить. Выберите пункт «Other», если устанавливаемой ОС нет в списке. (рис. 2)

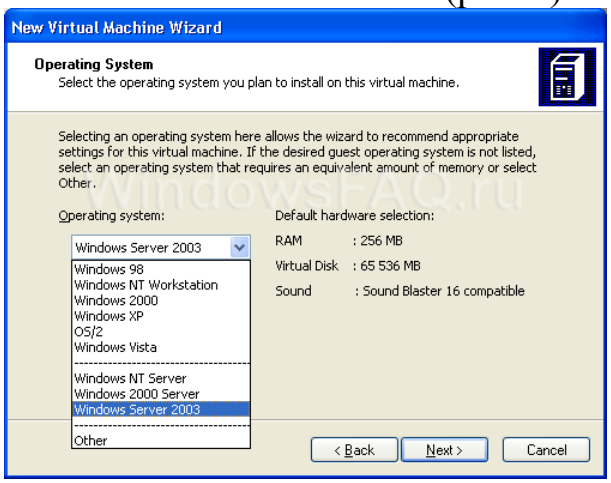


Рис 2. Выбор устанавиваемой ОС

6. В следующем окне мастера необходимо выбрать количество оперативной памяти, которая будет выделена гостевой системе. Можно выбрать пункт «Using the recommended RAM», в случае если вы сомневаетесь, сколько памяти выделять гостевой ОС. При выборе пункта «Adjusting the RAM» можно вручную установить количество выделенной оперативной памяти. Выделяя память, принимайте во внимание минимальные требования устанавливаемой системы к объему RAM, а также объем физической памяти вашей машины и планируемое количество одновременно запущенных гостевых систем.

7. На следующем шаге выберите, использовать ли уже имеющийся виртуальный жесткий диск («An existing virtual hard disk») или создать новый («A new virtual hard disk»).

8. Следующий этап это выбор размера виртуального жесткого диска. По умолчанию, Virtual PC предлагает создать диск объемом 65536 Мб. Этой величиной определяется максимальный объем диска виртуальной машины, а сам файл, в котором содержатся данные виртуального диска, будет расти по мере заполнения диска в виртуальной машине (рис 3).

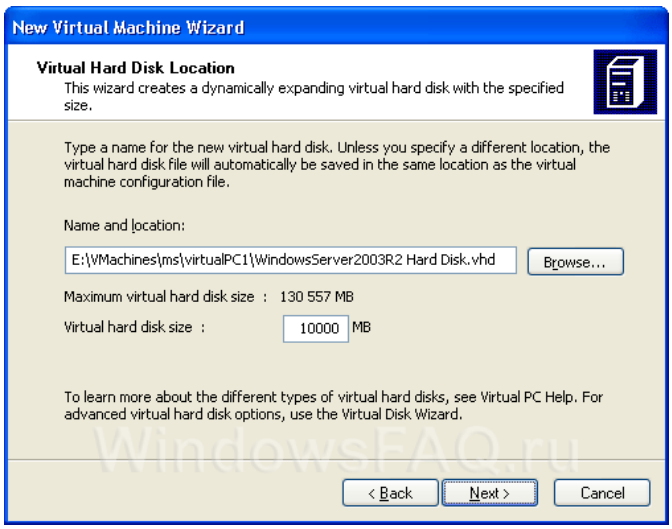


Рис. 3 Установка размера виртуального жесткого диска

9. На завершающем шаге мастера проверьте атрибуты виртуальной машины и, если все в порядке, нажмите «Finish».

10. После нажатия кнопки «Finish», в окне Virtual PC будет следующая картина (рис 4):

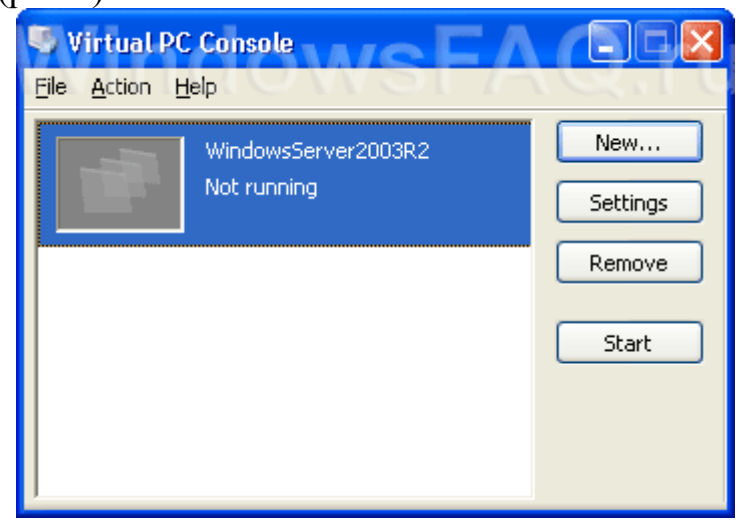


Рис. 4 Консоль управления виртуальными машинами

11. В главном окне программы, «Virtual PC Console», нажмите кнопку «Start». Начнется загрузка виртуальной машины.

12. Теперь необходимо определиться с расположением дистрибутива гостевой операционной системы. Если он находится на загрузочном CD или DVD диске, вставьте его в привод, так как с него по умолчанию пытается загрузиться виртуальная машина, после этого нажмите «Enter». Если дистрибутив операционной системы у вас в виде загрузочного образа ISO, откройте меню CD консоли виртуальной машины, выберите пункт «Capture ISO Image» и укажите путь к образу. После этого начнется загрузка операционной системы (рис. 6).

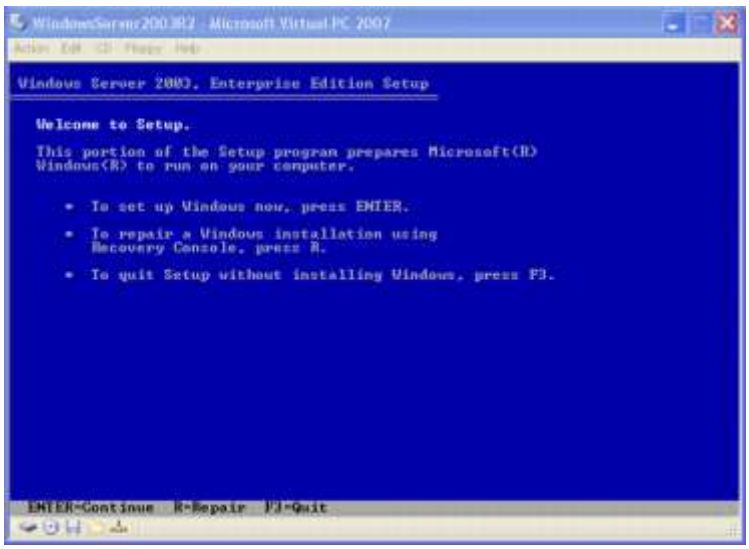


Рис.6 Инсталляция операционной системы

Затем устанавливайте вашу гостевую систему так, как будто бы вы устанавливаете ее на физическую машину

Настройка виртуальной машины.

В меню «Action» консоли виртуальной машины выберите пункт «Close», при этом появится меню, в котором можно выбрать один из трех пунктов:

- Shutdown Windows Server 2003 (корректное завершение работы гостевой ОС).
- Turn off (аналог кнопки Power на физической машине).
- Save state (виртуальная машина как бы ставится на паузу, что-то вроде режима Hibernate на физической машине).

Выберите пункт «Shutdown» и, когда гостевая операционная система выключится, в главном окне программы Virtual PC Console нажмите кнопку «Settings» - перед вами появится окно настроек виртуальной машины (рис 7).

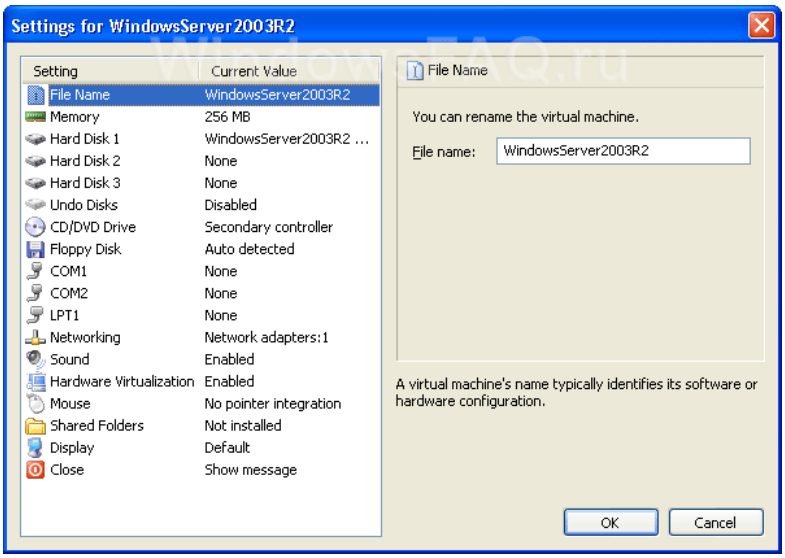


Рис 7. Настройки виртуальной машины

Рассмотрим каждый из пунктов настроек, кроме пункта «Networking», который мы рассмотрим отдельно.

- File Name – здесь вы можете изменить имя файла настроек виртуальной машины (соответственно, изменится и имя самой машины).
- Memory – здесь вы можете изменить количество физической памяти хоста, выделяемой гостевой системе.
- Hard Disk – здесь вы можете изменить уже имеющийся или добавить новый виртуальный жесткий или Floppy-диск. При нажатии на кнопку «Virtual Disk Wizard» откроется мастер создания и изменения дисков.
- Undo Disks – если поставить галку напротив этого пункта, то все изменения, которые произошли на дисках во время работы с виртуальной машиной, в конце сеанса работы с ней можно будет либо подтвердить, либо отменить. Включение таких дисков потребует наличие дополнительного места на физическом жестком диске.
- CD/DVD Drive - позволяет смонтировать физические CD и DVD приводы в виртуальную машину. Отметьте чекбоксы у тех приводов, которые вы хотите подключить к виртуальной машине.
- Floppy Disk – отключите автообнаружение флоппи-дисков, если вам не требуется их использование.
- COM и LPT. Эти пункты позволяют подключить порты COM и LPT в виртуальную машину и пользоваться устройствами, подключенными к ним.
- Sound. Позволяет проигрывать звук в виртуальной машине, используя физический аудиоконтроллер хоста. Уберите галку напротив этого пункта, если вам не требуется такая возможность.
- Hardware Virtualization. Позволяет виртуальной машине использовать инструкции аппаратной виртуализации вашего физического процессора. Рекомендуется оставлять эту галку включенной, если такая возможность аппаратной виртуализации поддерживается процессором.
- Mouse. Интеграция указателя мыши с гостевой системой. Такая возможность появляется с установкой Virtual Machine Additions.
- Shared Folders. Эта опция позволяет создавать общие папки для обмена файлами между гостевой и хостовой ОС и доступна только при установленных Virtual Machine Additions. Создавать папки можно только при включенной гостевой системе. Для создания папки нажмите кнопку Share Folder и выберите папку в хостовой ОС, которую вы хотите подключить к гостевой системе. После создания, папка будет доступна как сетевой диск в гостевой системе.
- Display. Здесь вы можете выбрать поведения экранных настроек гостевой системы и, в частности, возможность старта в полноэкранном режиме, настройки разрешения и окна консоли гостевой системы. Кстати, комбинация клавиш Alt-Enter, во время работы с гостевой системой, позволяет переходить в полноэкранный режим и обратно.

- Close. Здесь можно выбрать действие, автоматически совершаемое при закрытии гостевой системы, а также отредактировать меню, возникающее при выборе пункта «Close».

Настройка сетевого взаимодействия виртуальных машин Virtual PC

Один из самых интересных вариантов использования виртуальных машин – организация на одном физическом компьютере виртуальной сети, где одновременно работают несколько виртуальных машин. Откройте настройки (Settings) виртуальной машины и перейдите на вкладку «Networking» (рис 8).

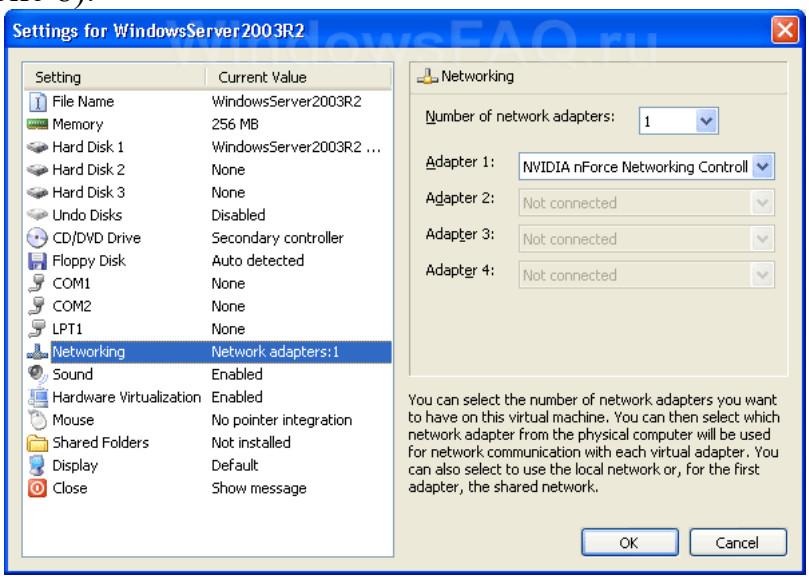


Рис 8. Настройки сети

В строчке Adapter 1 выберите сетевой адаптер вашего компьютера, это значит, что платформа Virtual PC позволяет гостевым и хостовой системам совместно использовать ресурсы физического сетевого адаптера с помощью трех различных моделей сетевого взаимодействия, а также полностью оградить виртуальную машину от сетевого взаимодействия.

Если в строчке Adapter выбран физический сетевой адаптер, это значит, что сетевой адаптер виртуальной машины напрямую подключен к сетевому адаптеру хоста. При таком типе сетевого взаимодействия виртуальная машина будет видеться из внешней сети и вести себя так, будто бы это отдельный компьютер в сети. Если в сети используется DHCP-сервер, виртуальная машина получит самостоятельный IP адрес в этой сети. Такой тип сетевого взаимодействия применяется, когда из внешней сети необходимо обращаться к ресурсам виртуальной машины и работать с ней, как с полноценным клиентом сети (например, гостевая система является файл-сервером). Иногда такой тип сетевого взаимодействия также называют Bridged Networking.

При выборе варианта Local only виртуальные машины на одном хосте смогут взаимодействовать между собой, но им будут недоступны внешние сетевые соединения хоста. Такой тип сетевого взаимодействия применяется, когда требуется построить какую-либо модель сетевого взаимодействия между несколькими машинами, однако внешние сетевые со-

единения не требуются (например, такой тип взаимодействия идеален для проверки работы связки «сервер приложений» - «сервер баз данных»).

Вариант Not connected означает, что виртуальная машина не будет принимать участие в сетевом взаимодействии и виртуальный сетевой адаптер как устройство не будет включен.

Последний вариант сетевого взаимодействия, который может быть выбран для виртуальной машины, это «Shared Networking». При использовании такого варианта, программа Virtual PC, действуя как DHCP-сервер, выдает виртуальной машине IP-адрес из диапазона 192.168.131.1 - 192.168.131.253. Также Virtual PC при этом является ещё и NAT -сервером (NAT - Network Address Translation). То есть виртуальные машины, использующие этот тип сетевого взаимодействия, спрятаны за NAT-сервером по отношению к внешней сети хоста и могут инициировать соединения с её клиентами, но члены внешней сети не могут инициировать соединения с виртуальными машинами хоста. Такой тип сетевого взаимодействия идеален, когда требуется, например, выходить в Интернет из виртуальной машины, максимально при этом спрятав виртуальную машину от атак извне.

2.4. Контрольные вопросы

1.Что такое виртуализация? В каких случаях она необходима?

2. Каким образом взаимодействуют гостевые (виртуальные) системы и хостовая ОС

3. Каковы преимущества и недостатки применения виртуальных машин

4. Какие программы, предназначенные для работы с виртульными машинами вы знаете?

5. Сколько необходимо места на виртуальном жестком диске для установки операционной системы.

6. Какие варианты расположения дистрибутива ОС могут быть при использовании программы Microsoft Virtual PC.

6. Какие типы сетевого взаимодействия предусмотрены в программе Microsoft Virtual PC.

Лабораторная работа № 2
СТАНДАРТНЫЕ КОМАНДЫ И ПРОГРАММЫ WINDOWS ДЛЯ РАБОТЫ С ЛОКАЛЬНОЙ СЕТЬЮ

2.1. Цель работы

Изучение среды Microsoft Virtual PC для создания и настройки виртуальных операционных систем.

2.2. Краткие теоретические сведения

При возникновении неполадок связи можно воспользоваться стандартными командами и программами Windows для мониторинга сети и исправления ошибок. Для использования этих команд обычно используют

режим командной строки в Windows. Для запуска командной строки нажмите Пуск/Выполнить (рис 9), введите команду «cmd» и нажмите кнопку OK (рис. 10).

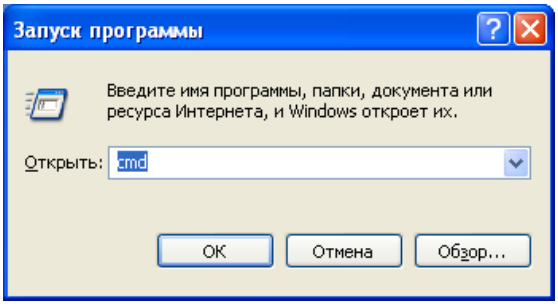


Рис.9. Запуск программ

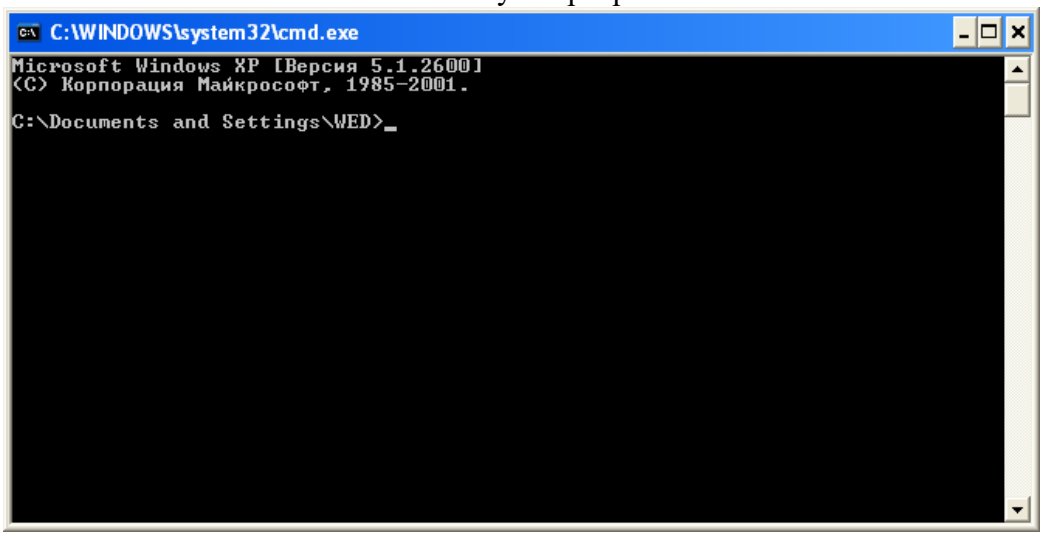


Рис. 10. Режим командной строки

В появившуюся строку вводу необходимо ввести название команды или программы с заданными параметрами. Результат выполнения обычно можно просмотреть в этом же окне. Ниже перечислены и описаны основаные еоманды и программы Windows, предназначенные для работы с локальной сетью.

Утилита ipconfig

В операционных системах Microsoft Windows и Windows NT, ipconfig — это утилита командной строки для вывода деталей текущего соединения и контроля над клиентским сервисом DHCP.

Доступные ключи командной строки в Windows

Ключ	Описание
/all	Отображение полной информации по всем адаптерам.
/release [адаптер]	Отправка сообщения DHCPRELEASE серверу DHCP для освобождения текущей конфигурации DHCP и удаления конфигурации IP-адресов для всех адаптеров (если адаптер не задан) или для заданного адаптера. Этот ключ отключает протокол TCP/IP для адаптеров, настроенных для автоматического получения IP-адресов.
/renew [адаптер]	Обновление IP-адреса для определённого адаптера или если адаптер не задан, то для всех. Доступно только при настроенном автоматическим получением IP-адресов.
/flushdns	Очищение DNS кэша.
/registerdns	Обновление всех зарезервированых адресов DHCP и перерегистрация

	имен DNS.
/displaydns	Отображение содержимого кэша DNS.
/showclassid адаптер	Отображение кода класса DHCP для указанного адаптера. Доступно только при настроенном автоматическим получением IP-адресов.
/setclassid адаптер [код_класса]	Изменение кода класса DHCP. Доступно только при настроенном автоматическим получением IP-адресов.

На рис. 11 представлен результат выполнения инструкции ipconfig /all.

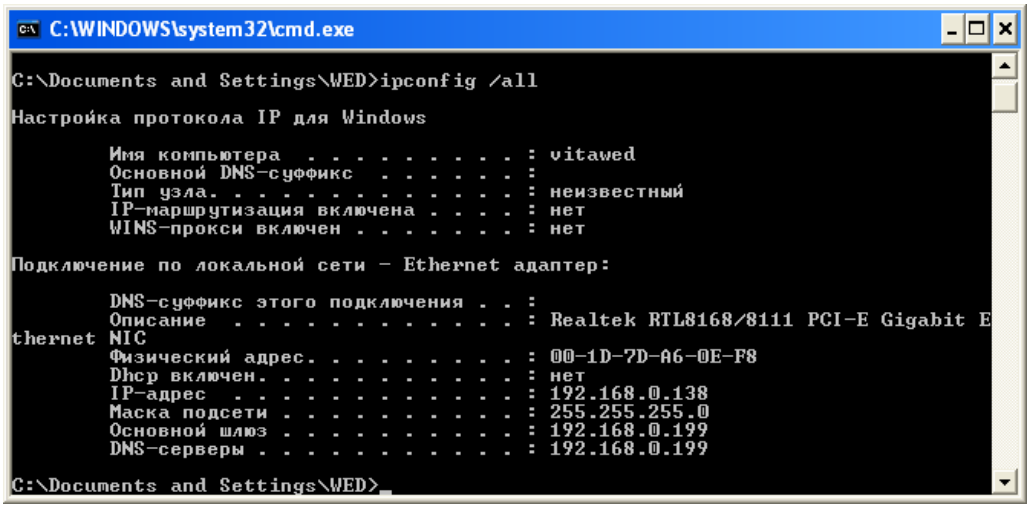


Рис. 11 Команда ping.

При возникновении неполадок связи можно воспользоваться командой ping для проверки IP-адреса назначения и вывода результатов этой проверки на экран. Команда ping сообщает, ответил ли опрошенный узел и сколько времени прошло до получения ответа. Если при доставке пакета узлу назначения произошла ошибка, команда ping выводит сообщение об ошибке.

С помощью команды ping можно выполнять следующие операции.

- - обращение к своему компьютеру (по адресу, а не по имени узла) для проверки работоспособности TCP/IP. (Обращение командой ping к своему компьютеру не проверяет работоспособность сетевого адаптера.)
- - обращение к локальному маршрутизатору для проверки его работоспособности.
- - обращение за пределы локального маршрутизатора.

В далее показаны некоторые полезные параметры команды ping операционной системы windows (они подойдут для большинства других ОС)

Параметр	Использование
-n счетчик	Задает число отправляемых эхо-запросов. По умолчанию отправляется 4 запроса.
-w интервал	Задает период ожидания в миллисекундах. По умолчанию период ожидания равен 1000 миллисекунд (1 секунде).
-l размер	Задает размер пакета, посылаемого командой ping. По умолчанию размер пакета равен 32 байтам.

-f	Устанавливает бит запрета фрагментации для пакета ping. По умолчанию фрагментация пакетов ping разрешена.

Сообщение «Заданная сеть недоступна» означает, что отсутствует маршрут к сети назначения. Необходимо проверить таблицу маршрутизации на маршрутизаторе, адрес которого указан в сообщении «Заданная сеть недоступна».

Ответ «Превышен интервал ожидания для запроса» означает, что от данного узла в течение заданного времени ожидания (по умолчанию — 1 секунда) не был получен ответ. Это может происходить по следующим причинам.

- Отключен маршрутизатор. Чтобы проверить маршрутизаторы на пути между источником и приемником, воспользуйтесь командой tracert.
- Отключен узел назначения. Физически проверьте, включен ли узел, или попробуйте установить связь с ним по другому протоколу.
- Отсутствует обратный маршрут к вашему компьютеру. Если узел работает, проверьте обратный маршрут, просмотрев адрес основного шлюза и таблицу маршрутизации на узле назначения.
- Время, необходимое для получения ответа, превышает используемый период ожидания. Для увеличения периода ожидания используйте параметр -w команды ping. Например, чтобы ответ ожидался в течение 5 секунд, используйте команду ping –w 5000.

На рис. 12 представлен результат выполенения команды ping ya.ru.

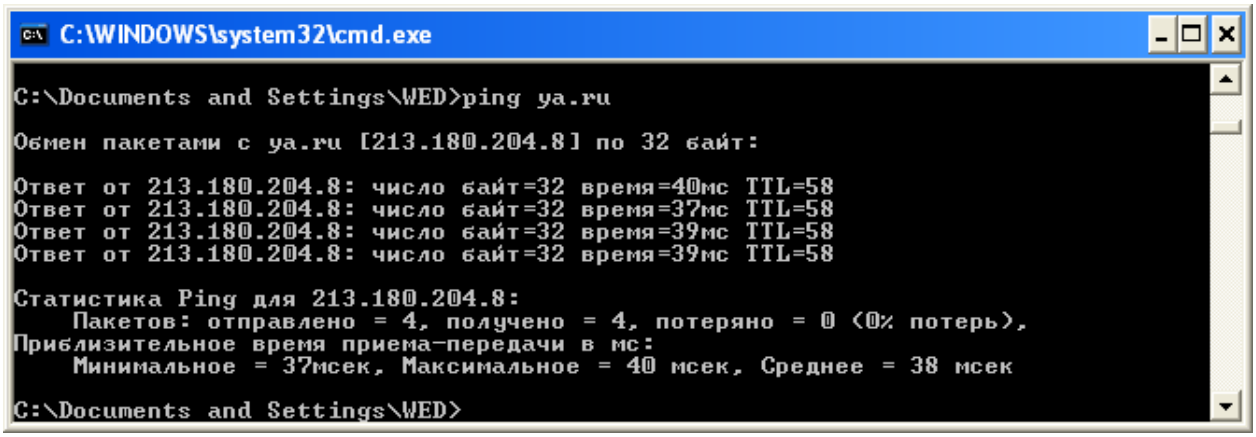


Рис. 12. Команда tracert.

(Tracert) — данная команда дает возможность оценить длину пути, который проходит ваш запрос до интересующего ресурса, то есть какое количество промежуточных компьютеров (роутеров) проходят данные, прежде чем попасть к вам. Чем меньше этот показатель, тем лучше, хотя его влияние на качество связи менее заметно, да и разница в длине пути у различных провайдеров не столь уж значительна. При слишком длинных маршрутах возрастает вероятность того, что один из промежуточных роутеров по пути будет перегружен, вследствие чего скорость связи снизится. Пример применения команды tracert представлен на рис. 13.

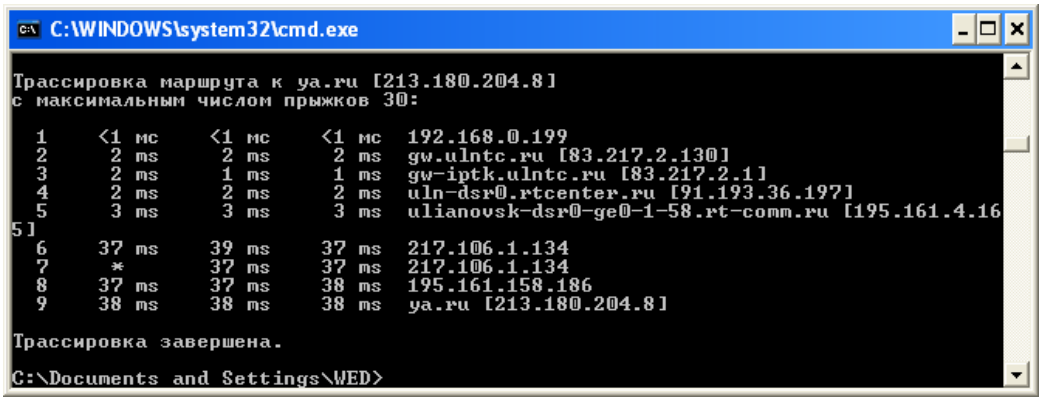


Рис. 13. Команда arp

Команда arp предназначена для работы с arp кэшем локального компьютера.

Параметр	Использование
-a	Команда отображает все записи в arp таблице
-d	Команда удаляет все записи в arp таблице
-s	Добавляет запись в arp таблицу. При использовании этой опции необходимо указать имя хоста и Ethernet адрес, IP адрес, соответствующий имени хоста, и Ethernet адрес добавляются в кэш. Подобная запись делается на постоянной основе (она не будет удалена из кэша по тайм-ауту), если только в конце командной строки не будет использовано ключевое слово temp.
-s pub	Ключевое слово pub в конце командной строки с опцией -s приведет к тому, что система будет функционировать как ARP агент для этого хоста. Система будет отвечать на ARP запросы для IP адресов, соответствующих имени хоста, при этом ответ будет содержать указанный Ethernet адрес. Если объявленный адрес это адрес самой отвечающей системы, это означает, что система работает как уполномоченный агент ARP для указанного имени хоста.

На рис. 14 показана arp таблица, полученная с помощью команды arp –a.

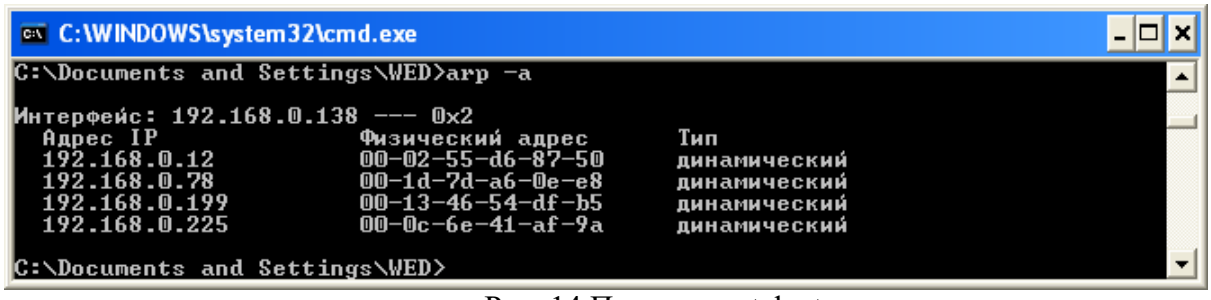


Рис. 14 Программа telnet

Программа telnet позволяет вам залогиниться на удаленную машину, и работать на ней, как-будто вы сидите за терминалом, подключенным непосредственно к ней. У команды telnet есть "горячий ключ" "Ctrl-]" , который переводит telnet в командный режим. В этом режиме можно менять параметры работы telnet'a. Выход из командного режима - ENTER. Обычно telnet используют для проверки доступности заданных портов выбранного хоста. Пример попытки соединения локального компьютера с хостом ya.ru по порту 400 с помощью команды telnet ya.ru 400 показан на рис. 15.

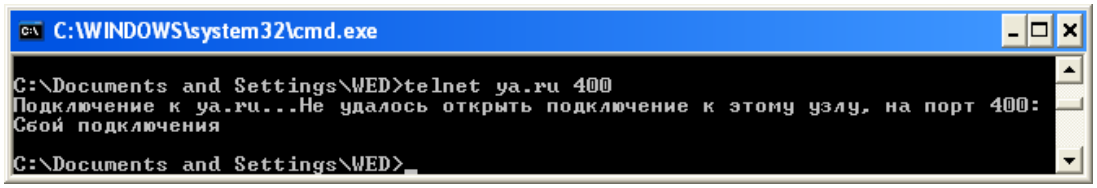


Рис. 15 Команда netstat

Команда netstat показывает содержимое различных структур данных, связанных с сетью, в различных форматах в зависимости от указанных опций Первая форма команды показывает список активных сокетов (sockets) для каждого протокола. Вторая форма выбирает одну из нескольких других сетевых структур данных. Третья форма показывает динамическую статистику пересылки пакетов по сконфигурированным сетевым интерфейсам; аргумент интервал задает, сколько секунд собирается информация между последовательными показами.

Параметр	Использование
-a	Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются.
-A	Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки.
-i	Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются.
-n	Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа.
-r	Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации.
-s	Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации.
-f семейство адресов	Ограничить показ статистики или адресов управляющих блоков только указанным семейством адресов, в качестве которого можно указывать: inet Для семейства адресов AF_INET, или unix Для семейства адресов AF_UNIX.
-I интерфейс	Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объемом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле конфигурации системы, например, emd1 или lo0.
-p имя_протокола	Ограничить показ статистики или адресов управляющих блоков только протоколом с указанным именем_протокола, например, tcp.

Примеры использования команды netstat представлены на рис. 16, 17 и 18.

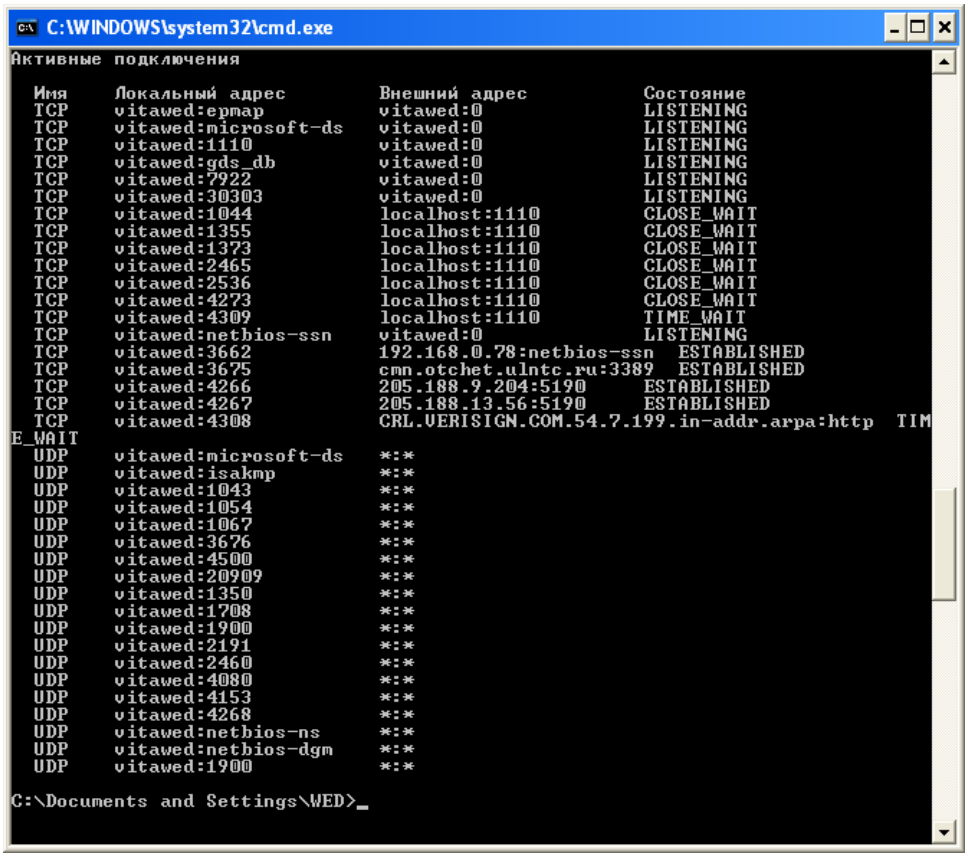


Рис. 16 Результат выполнения команды netstat -a

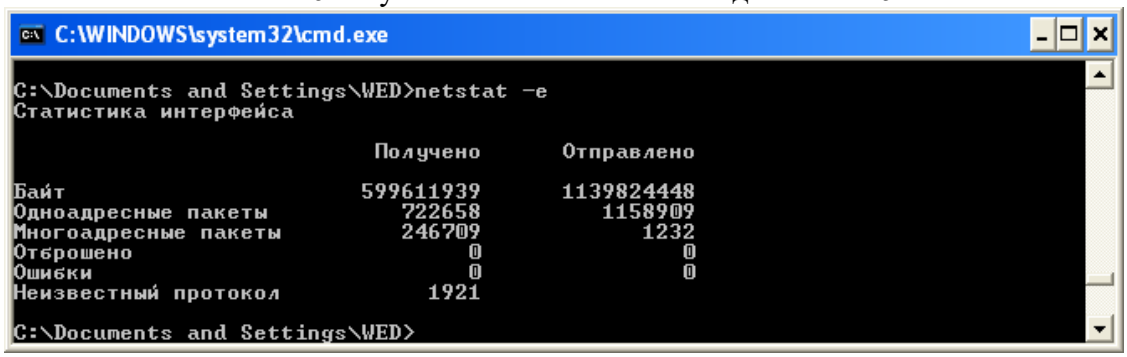


Рис. 17 Результат выполнения команды netstat -e

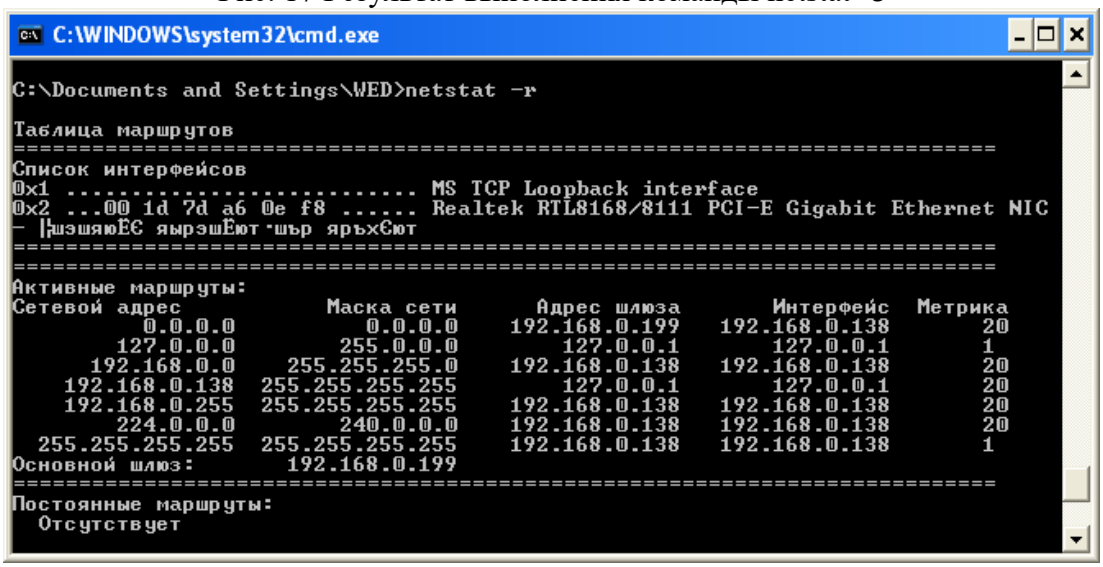


Рис. 18 Результат выполнения команды netstat –r

2.3. Задание на лабораторную работу

1. Запустить вируальную машину Windows XP.
2. Узнать имя и IP адрес своего компьютера и компьютера соседа
3. Проверить доступность компьютера соседа в сети с помощью команд ping и tracert
4. Последовательно изменяя размер покета в запросе ping проанализировать время доставки пакетов.
5. Определить IP адрес шлюза, через который идет работа с внешней сетью
6. Выполнить команды ping и tracert для любого внешеного хоста (например, yandex.ru). Проанализировать результаты.
7. Просмотреть arp таблицу своего компьютера
8. Удалить все записи из arp таблицы своего компьютера
9. Выполнить команду ping до любого компьютера класса.
10. Просмотреть arp таблицу своего компьютера. Проанализировать результаты.
11. Используя команду netstat определить открытые порты на своем компьютере.
12. С помощью программы telnet попробуйте подключится к открытым и закрытым портам на соседнем компьютере.
13. Определите список интерфейсов на данном компьютере, количество полученной и принятой информации по этим интерфейсам и сетевые маршруты.

2.4. Контрольные вопросы.

1. Что такое «командная строка» и для чего она необходима?
2. Каким образом можно получить из «командной строки» настройки сетевого подключения?
3. Можно ли определить из командной строки доступность заданного хоста и как это сделать?
4. Как можно определить маршрут до заданного хоста?
5. Каким образом можно узнать содержание arp таблицы локального компьютера?
6. Как можно определить статистику по заданному сетевому подключению?

Лабораторная работа № 3
ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПОДМЕНЫ ФИЗИЧЕСКОГО АДРЕСА КОМПЬЮТЕРА

3.1. Цель работы

Изучение различных способов изменения MAC-адреса сетевого адаптера в операционной системе Windows.

3.2. Краткие теоретические сведения

MAC-адрес (от англ. Media Access Control - управление доступом к среде, также Hardware Address) — уникальный идентификатор, присваиваемый каждой единице активного оборудования или некоторым их интерфейсам в компьютерных сетях Ethernet.

При проектировании стандарта Ethernet было предусмотрено, что каждая сетевая карта (равно как и встроенный сетевой интерфейс) должна иметь уникальный шестибайтный номер (MAC-адрес), «прошитый» в ней при изготовлении. Этот номер используется для идентификации отправителя и получателя фрейма; и предполагается, что при появлении в сети нового компьютера (или другого устройства, способного работать в сети) сетевому администратору не придётся настраивать этому компьютеру MAC-адрес вручную.

Уникальность MAC-адресов достигается тем, что каждый производитель получает в координирующем комитете IEEE Registration Authority диапазон из 16777216 (224) адресов и, по мере исчерпания выделенных адресов, может запросить новый диапазон. Поэтому по трём старшим байтам MAC-адреса можно определить производителя. Существуют таблицы, позволяющие определить производителя по MAC-адресу; в частности, они включены в программы типа arpalert.

В широковещательных сетях (таких, как сети на основе Ethernet) MAC-адрес позволяет уникально идентифицировать каждый узел сети и доставлять данные только этому узлу. Таким образом, MAC-адреса формируют основу сетей на канальном уровне модели OSI, которую используют протоколы более высокого (сетевого) уровня. Для преобразования MAC-адресов в адреса сетевого уровня и обратно применяются специальные протоколы (например, ARP и RARP в сетях IPv4, и NDP в сетях на основе IPv6).

Большинство сетевых протоколов канального уровня используют 1 из 3 пространств MAC-адресов, управляемых IEEE (или MAC-48, или EUI-48, или EUI-64); адреса в каждом из тех пространств, теоретически, должны быть глобально уникальными. Но не все протоколы используют MAC-адреса; и не все протоколы, использующие MAC-адреса, нуждаются в подобной уникальности этих адресов.

Адреса вроде MAC-48 наиболее распространены; они используются в таких технологиях, как Ethernet, Token ring, FDDI, WiMAX и других. Они состоят из 48 бит; таким образом, адресное пространство MAC-48 насчитывает 248 (или 281 474 976 710 656) адресов. Согласно подсчётам IEEE, этого запаса адресов хватит по меньшей мере до 2100 года.

EUI-48 от MAC-48 отличается лишь семантически: в то время как MAC-48 используется для сетевого оборудования — EUI-48 применяется для других типов аппаратного и программного обеспечения.

Идентификаторы EUI-64 состоят из 64 бит и используются в FireWire, а также в IPv6 (в качестве младших 64 бит сетевого адреса узла).

3.3. Задание на лабораторную работу

1. Запустить командную строку
2. Вывести текущие сетевые настройки командой ipconfig /all
3. Среди результатов найти MAC-адрес (если сетевых карт несколько, выбрать одну из них для дальнейшего исследования, ту, которая соединена с сетью класса).

Способ 1. Редактирование свойств сетевого адаптера

1. Вывести диалоговое окно настройки свойств сетевого адаптера Start->Settings->Network and Dial-up Connections. Далее выбрать сетевой адаптер и открыть окно его свойств (рис 19).

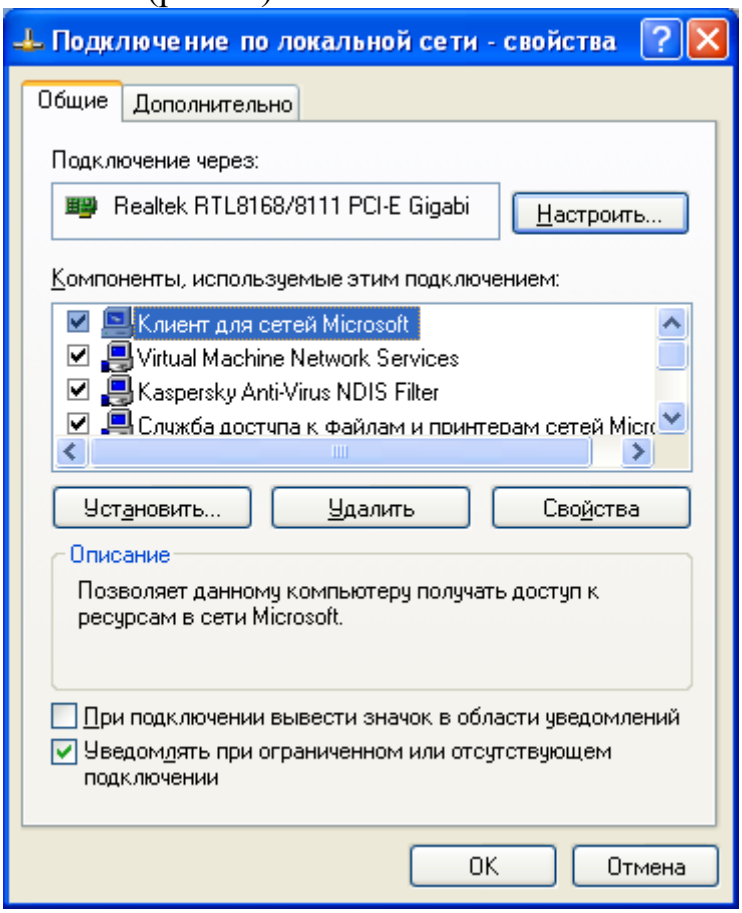


Рис 19. Параметры сетевого подключения

2. Нажать кнопку Configure, далее открыть закладку Advanced
3. В списке параметров выбрать Locally Administered Address (в разных версиях ОС Windows названия могут отличаться, например, Network Address).

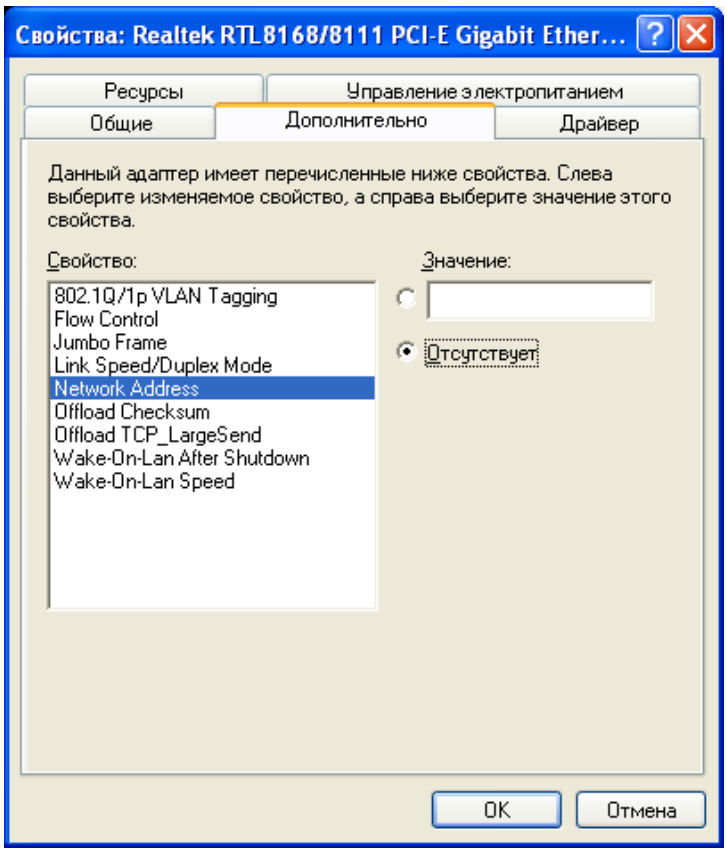


Рис 20. Параметры сетевого подключения

5. В поле Value вписать новое значение MAC-адреса (рис. 21)

Внимание! В некоторых случаях это значение не может быть произволы например, для некоторых сетевых адаптеров, встроенных в материнскую плс первые 24 бита менять нельзя. Кроме того, учитывайте возможные конфликт с соседними у злами. Рекомендуется сменить только последние 1-2 байта MAC-адреса.

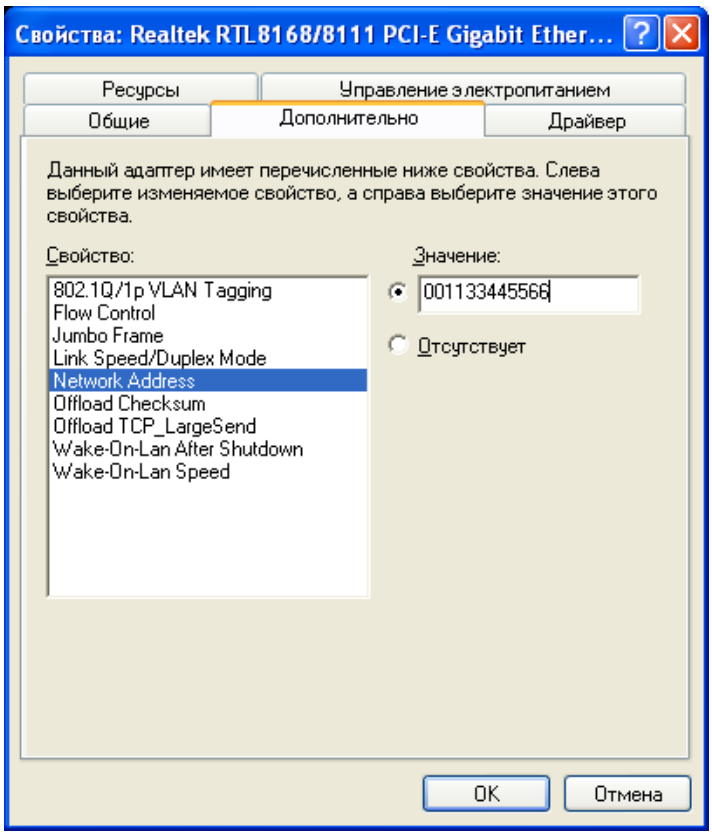


Рис. 21 Изменение MAC адреса

5. Нажать OK
6. Перейти в командную строку и вновь вывести параметры сети
7. Проверить, что MAC-адрес успешно изменился (в случае необходимости можно перезапустить сетевой интерфейс)

Способ 2. Редактирование параметров сетевого адаптера в реестре

1. Перейти в командную строку
2. Набрать команду net config rdr (рис 22)
3. Найти GUID сетевого адаптера, для которого был изменён MAC-адрес в предыдущей части работы (например, в данном случае это 522E599D-6389-4FFA-B8CE-2D85C8EC30C1)

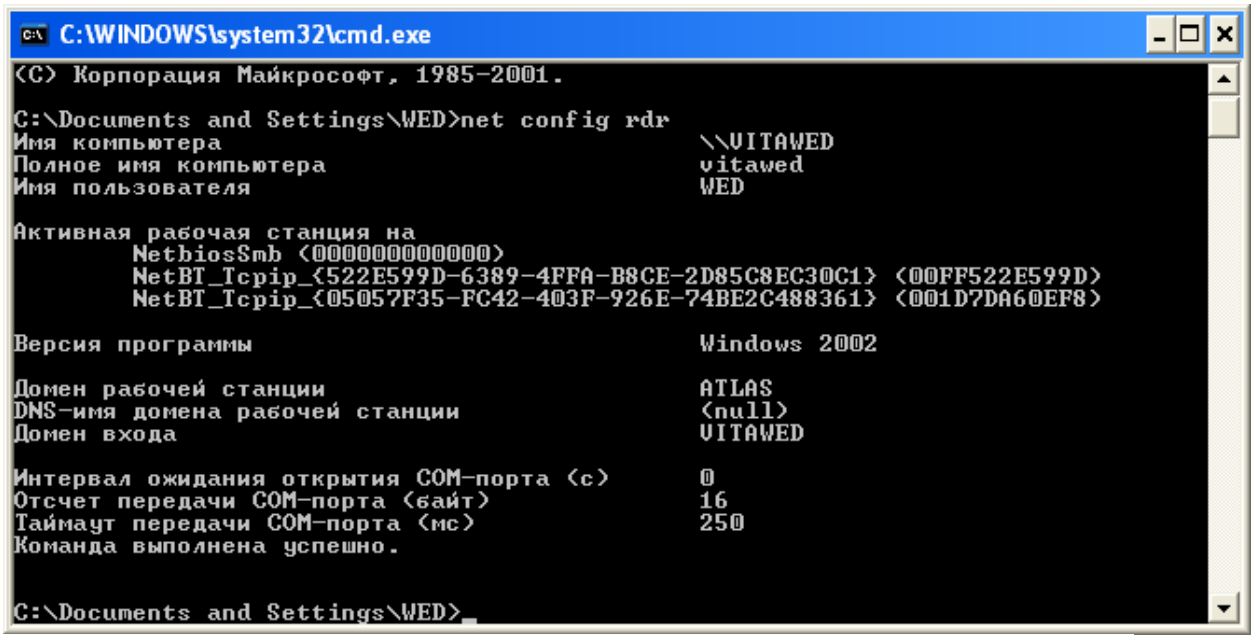


Рис 22. Результат выполнения команды net config rdr

4. Запустить редактор реестра Start -Run -regedit
5. Найти подключ "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ControI\Class\{4D36E965 -E325-11CE-BFC1-08002BE10318).
6. Раскрыть список подключен данного ключа (должен появиться список 0000,0 0002, 0003 и т. д.)
7. Просматривая каждый из подключен списка, по значению элемента DriverDesc найти требуемый сетевой адаптер (для контроля сравнить значение элемента NetCfg Instance ID с определённым в п. 3 GUID)

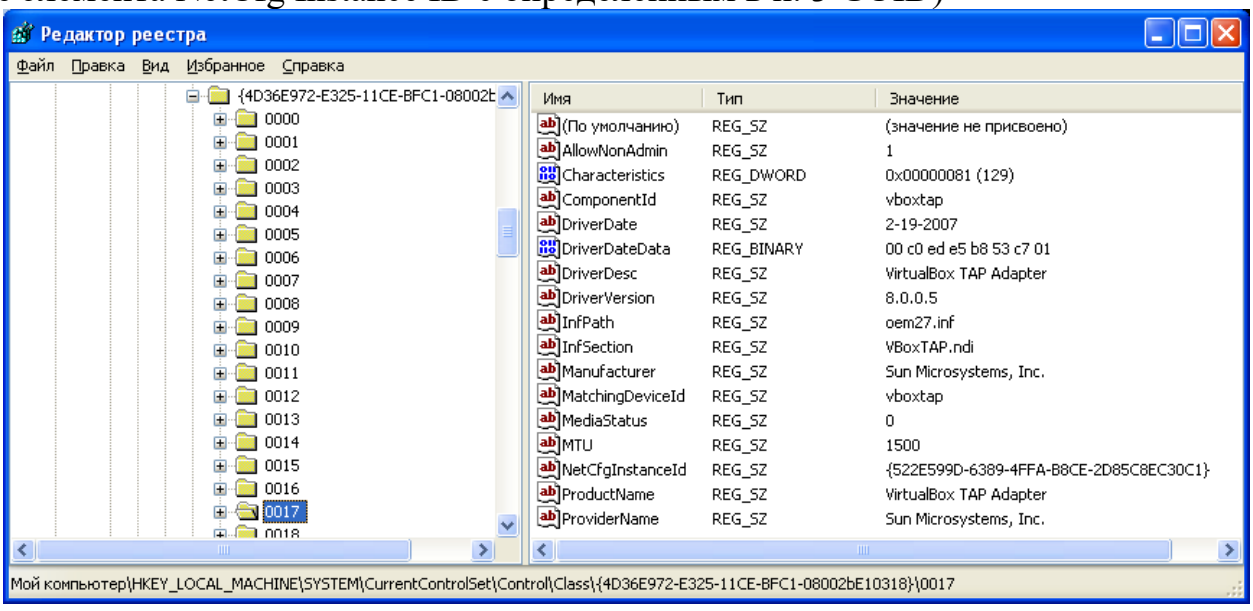


Рис 23. Реестр локального компьютера

8. Найти значимый элемент "NetworkAddress" (он должен содержать заданный в предыдущей части работы MAC-адрес)

Примечание: по умолчанию этот элемент не создаётся, и его необходимо добавлять вручную

Value Name: = NetworkAddress

Data Type: = REG_SZ

9. Задать новый MAC-адрес, например (рис. 25):

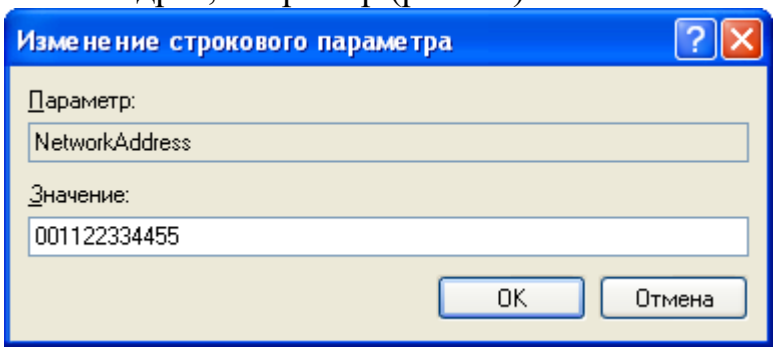


Рис 25. Изменение MAC адреса

10. Перезапустить сетевой интерфейс.

11. Перейти в командную строку и командой ipconflg /all проверить, что MAC-адрес был изменён

Дополнительно: воспользовавшись способом 1 или 2, задать некорректный MAC-щ (например, длиной 4 байта). Проверить, какой MAC-адрес получит в результате сетевой адаптер.

Способ 3. Использование бесплатной программы MakeUp.

1. Запустить программу MakeUp (рис. 26).

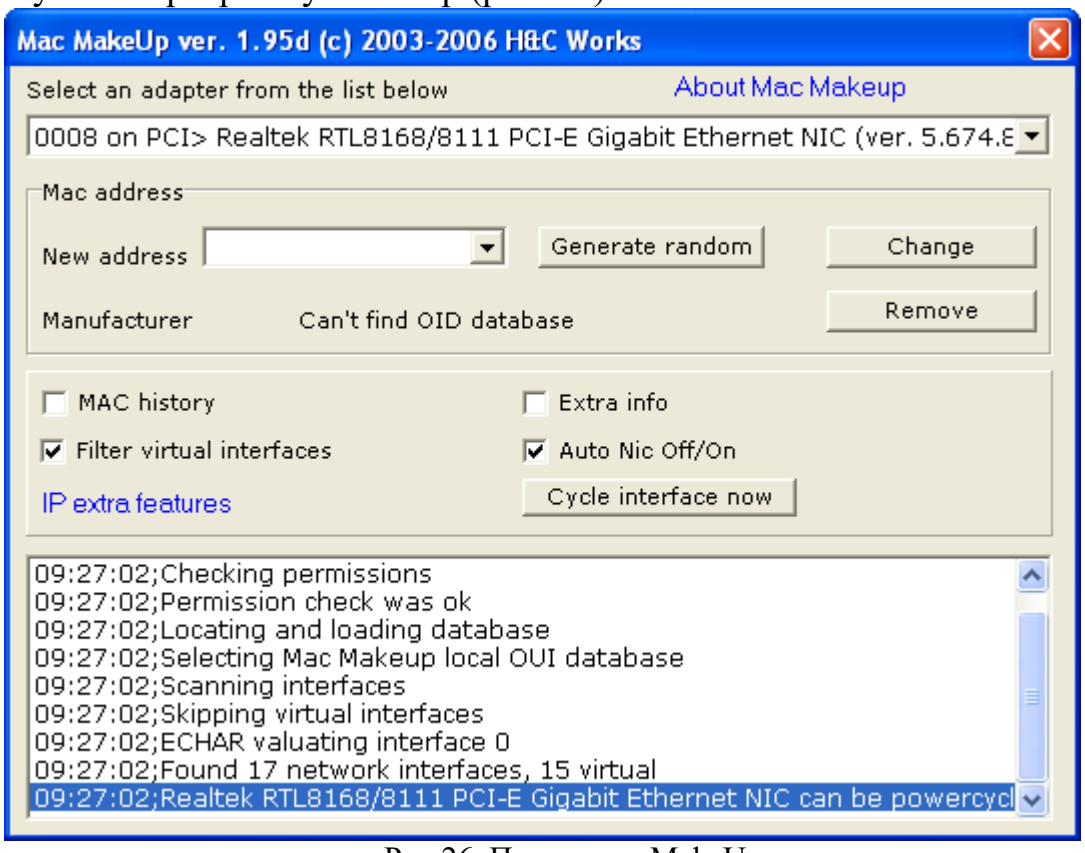


Рис 26. Программа MakeUp

2.В поле New Address ввести новое значение MAC-адреса

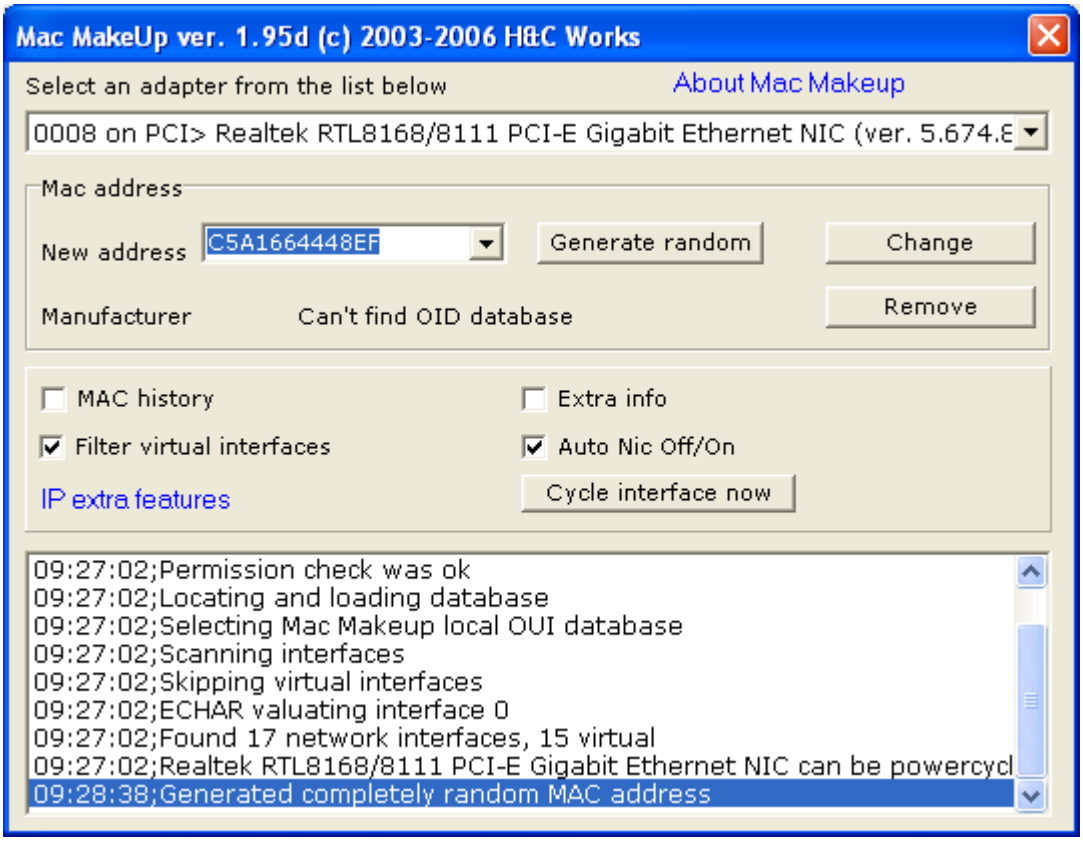


Рис 27. Изменение MAC адреса.

Для изменения MAC адреса можно использовать также и другие программы, например, SMAC.

3.4. Контрольные вопросы.

1. Зачем нужен MAC адрес и что он из себя представляет?
2. Можно ли менять MAC адрес устройства?
3. Может ли MAC адресом быть произвольное число?
4. В каких случаях может возникнуть необходимость смены MAC адреса?
5. Обязательно ли сетевая карта современного компьютера под управлением Microsoft Windows должно иметь MAC адрес?

Лабораторная работа № 4

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПЕРЕХВАТА ТРАФИКА С ПОМОЩЬЮ СЕТЕВОГО СНИФФЕРА

4.1. Цель работы

Изучение трафика, перехваченного при проведении атаки.

4.2. Краткие теоретические сведения

Сети Ethernet относятся к так называемым широковещательным сетям. Метод доступа, положенный в основу этой технологии, требует от узлов, подключённых к сети, непрерывного прослушивания всего сетевого трафика. Это означает, что узлы такой сети могут перехватывать информацию, адресованную своим соседям. Данная особенность технологии

Ethernet делает возможным проведение атак, использующих механизм «пассивного прослушивания». Средства для проведения таких атак - это анализаторы протоколов или снифферы.

Термин "сниффер" («нюхач») впервые был использован компанией Network Associates в названии известного продукта "Sniffer (r) Network Analyzer". В самом общем смысле, слово "сниффер" обозначает устройство, подключенное к компьютерной сети и записывающее весь ее трафик подобно телефонным "жучкам"", записывающим телефонные разговоры. Однако чаще всего "сниффером" называют программу запущенную на подключенном к сети узле и просматривающую весь трафик сетевого сегмента.

Работа "сниффера" использует основной принцип технологии Ethernet - общую среду передачи. Это означает, что любое устройство, подключенное к сетевому сегменту, может слышать и принимать все сообщения, в том числе предназначенные не ему.

Во втором случае фильтрация не осуществляется, и узел принимает все фреймы, передаваемые по сегменту.

Таким образом, в неселективном режиме сетевые адаптеры принимают все фреймы в том числе и не предназанченные данному узлу, единственное проверяемое условие 0 целостность фрейма.

Специализированные программы, переводящие сетевой адаптер в неселективный режим и собирающие весь трафик сети для последующего анализа, называются анализаторами протоколов или «снифферами». Собранный трафик сегмента может быть отображен на экране, записан в файл и т.п. Так как компьютеры обмениваются по сети двоичной информацией, в обязанности "сниффера" обычно входит так называемый структурный анализ протоколов (включающий разбиение пакета на заголовки и данные) и вывод информации в удобном (читаемом) виде.

Анализатор протоколов - программный продукт "двойного" применения. Он может быть использован специалистами и администраторами сетей для анализа происходящих в сети процессов и диагностики неисправностей, С другой стороны, снифферы используются злоумышленниками для проведения атак (механизм атаки -"пассивное прослушивание"). Кроме того, тот же принцип пассивного прослушивания трафика лежит в основе работы средств обнаружения сетевых атак.

Итак, анализаторы протоколов позволяют злоумышленнику просматривать весь трафик сетевого сегмента. Возможен ли перехват информации в случае нахождения злоумышленника в другом сегменте? С помощью анализатора протоколов это осуществить невозможно, однако для этого используются другие методы, позволяющие перенаправить трафик из другого сегмента на узел нарушителя и реализующие атаки типа «создание ложного объекта-посредника» на сетевом и транспортном уровнях модели OSI.

В сети Internet можно найти множество анализаторов протоколов для различных операционных систем. Далее перечислены некоторые из них:

- CommView
- Network Monitor
- Ethereal (Wireshark)
- tcpdump

Все они, обладая похожим функционалом, работают по изложенным выше принципам.

4.3. Задание на лабораторную работу

Для выполнения работы предлагается следующая последовательность действий.

1. На основной машине запустить программу CommView (Start > Programs > CommView > CommView)
2. Выбрать сетевой адаптер, с которого будет собираться трафик.
3. Нажать кнопку «Начать захват»
4. Дождаться перехвата трафика и остановить сбор трафика, нажав кнопку «Остановить захват».

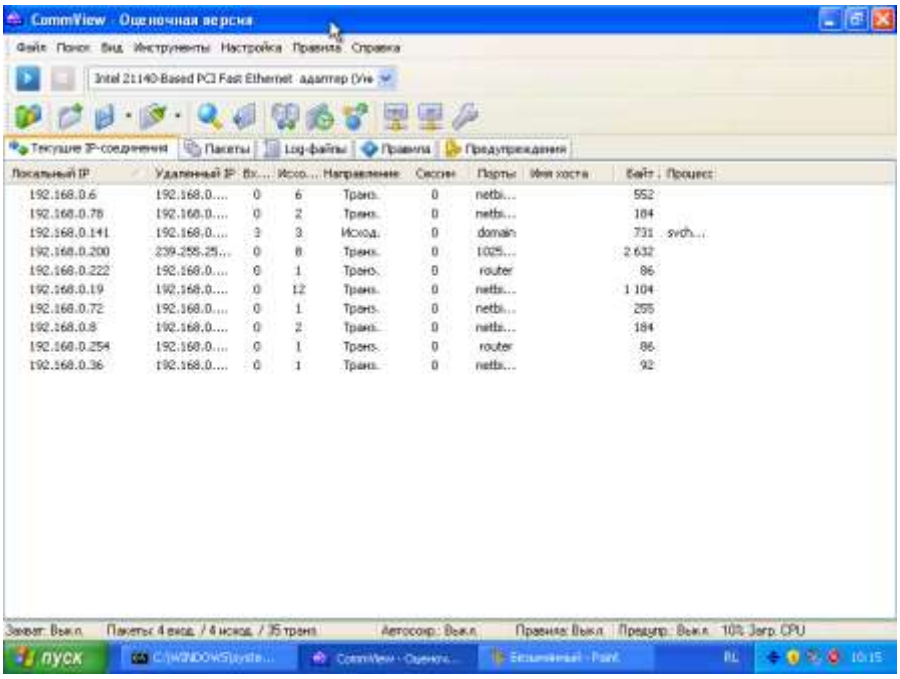


Рис 28. Внешний вид программы CommView

5. Открыть закладку «Пакеты». Просмотреть сведения о сетевых пакетах, котег расположены в трёх окнах. В верхнем окне отображена краткая информация с пакете, в среднем окне - шестнадцатеричный вариант, и. наконец, в нижнем показана информация из заголовков различных уровней.

Обычно не требуется перехват и просмотр всего трафика, поэтому целесообразно задавать различные способы фильтрации. Следующая часть работы посвящена заданию фильтра для перехвата ICMP-пакетов между вашим узлом и узлом преподавателя

6. Открыть закладку Правила.
7. В списке слева выбрать пункт IP-адреса.
8. Добавить адрес узла преподавателя два раза («В направлении к» и «В направлении от»).

9. В списке слева выбрать пункт Протоколы и направление.
10. Отметить в списке протокол ICMP и отключить захват транзитных пакетов.
11. Удалить собранные ранее пакеты (меню Файл > Очистить буфер пакетов)
12. Запустить перехват трафика
13. Запустить командную строку и ввести команду ping <узел основной машины>
14. Просмотреть перехваченные пакеты ICMP (Echo, Echo Reply). Их должно быть восемь (4 запроса, 4 ответа).
15. Изучить содержания различных пакетов, обращая внимание расположение и способ кодирования параметро Source MAC, Destination MAC, Source IP, Destination IP.

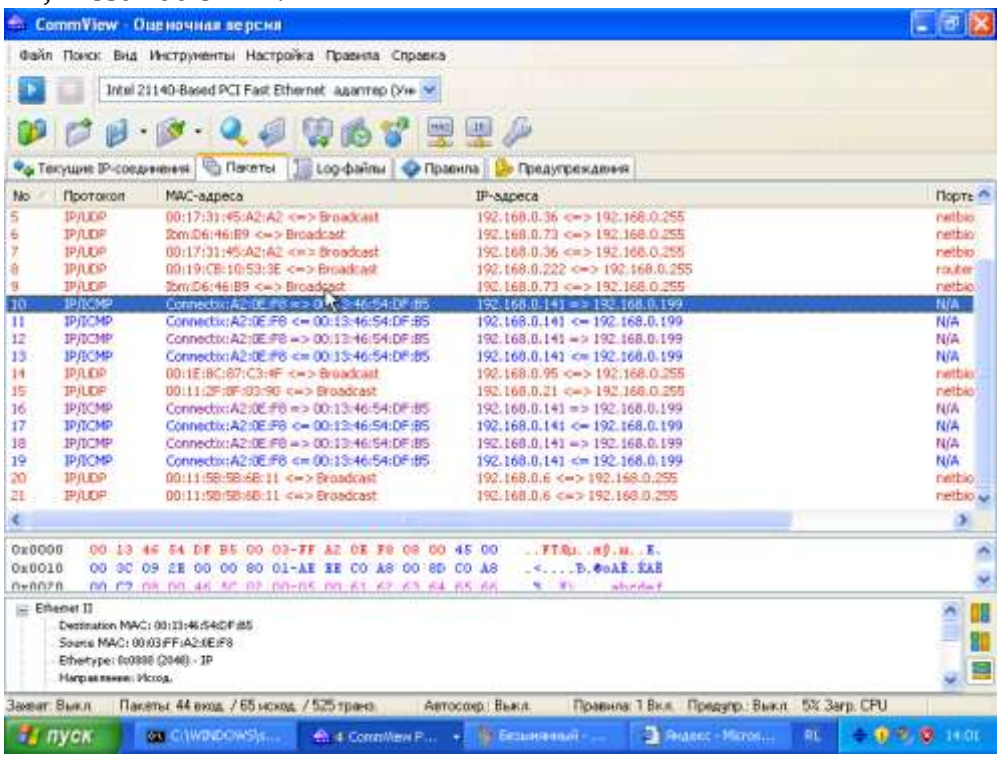


Рис 29. Перехват пакетов с помощью программы CommView

16. Для демонстрации возможностей перехвата данных в сети открыть в интернет-браузере любую WEB страницу.

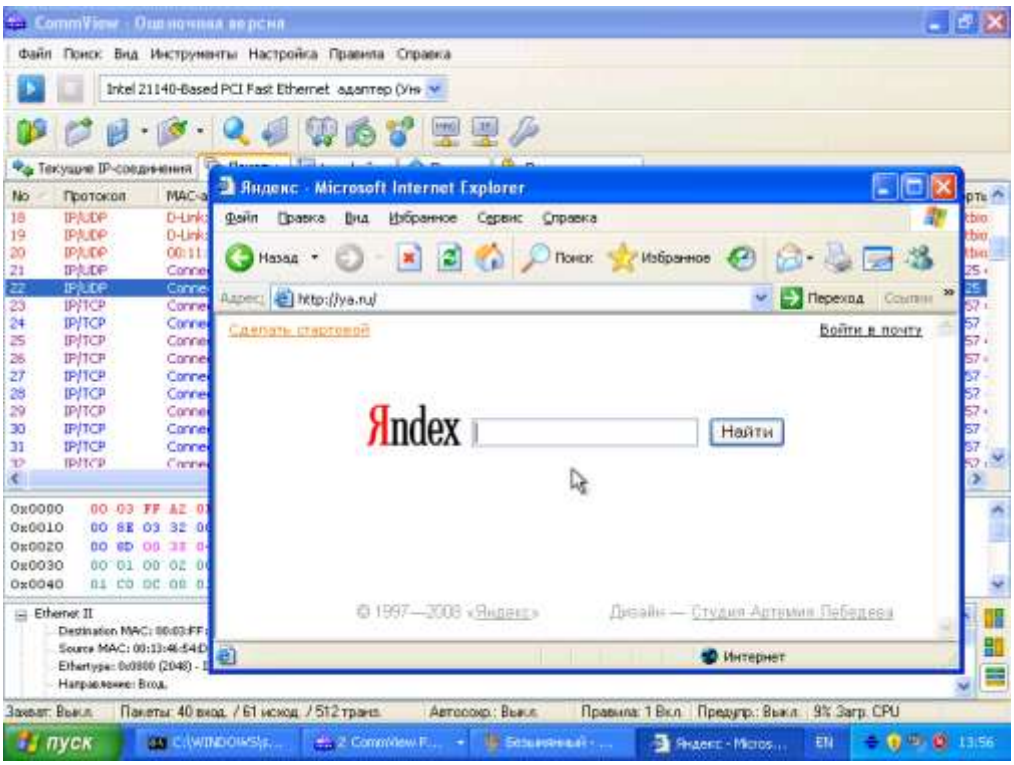


Рис 30. Перехват пакетов с помощью программы CommView

17. Найти среди перехваченной информации пакет TCP/IP и щеллкнуть по кнопке «Реконструкция TCP сессии»

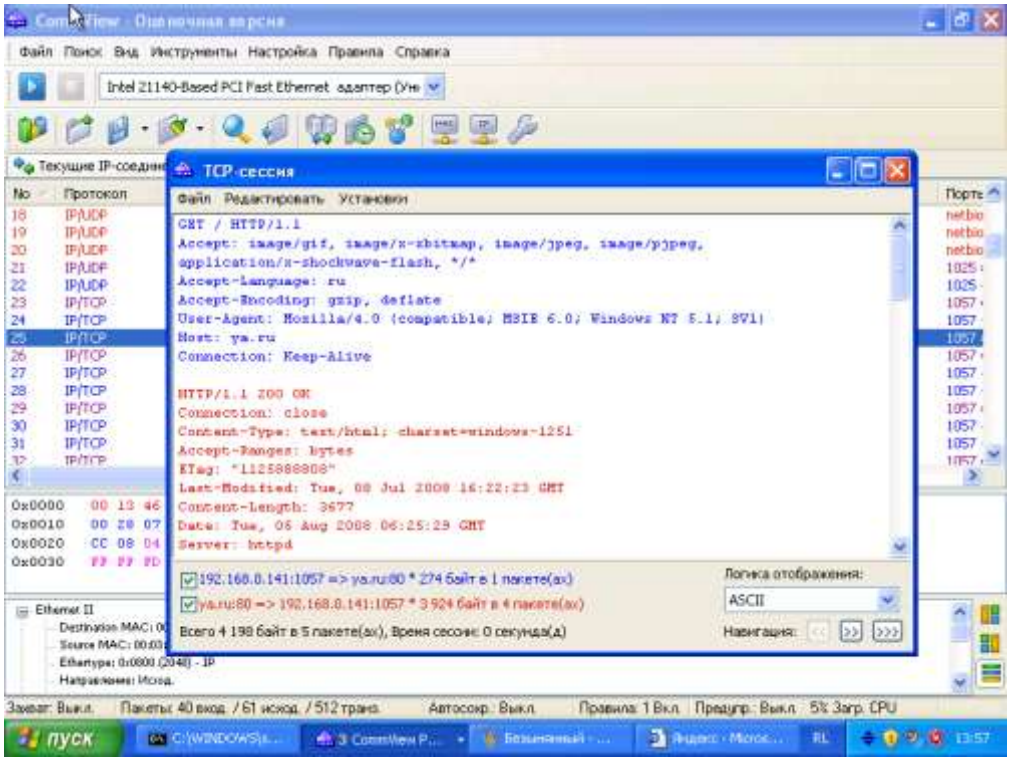


Рис 31. Реконструкция сессии с помощью программы CommView

18. Выбрать логику отображения HTML и убедится в том, что страница перехвачена.

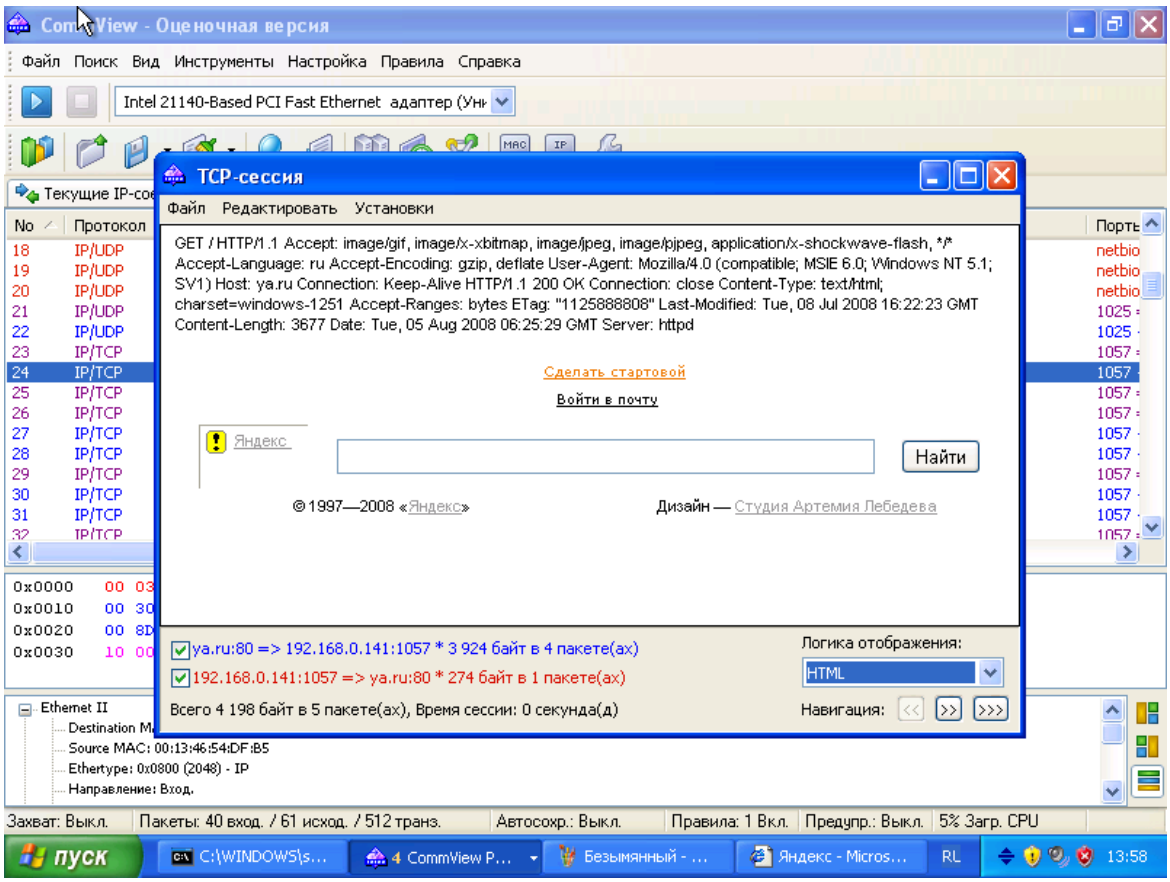


Рис 32. Реконструкция сессии с помощью программы CommView

19. Для выявления в сети узла с работающим сетевым анализатором запустите на виртуальной машине программу Cain, внизу выберите закладку Hosts, вверху – закладку Sniffer.
20. В меню Configure выберите сетевой адаптер, подключенный к сети учебного класса.
21. Нажмите на кнопку Start/Stop Sniffer
22. Нажмите на кнопку Add to List
23. Выберите все темты (All Tests)
24. Просмотрите результаты опроса узлов сети класса. Проанализировать их. Узлы, на которых сетевые адаптеры работают в обычном (селективном) режиме, отвечают только на один запрос (M1)

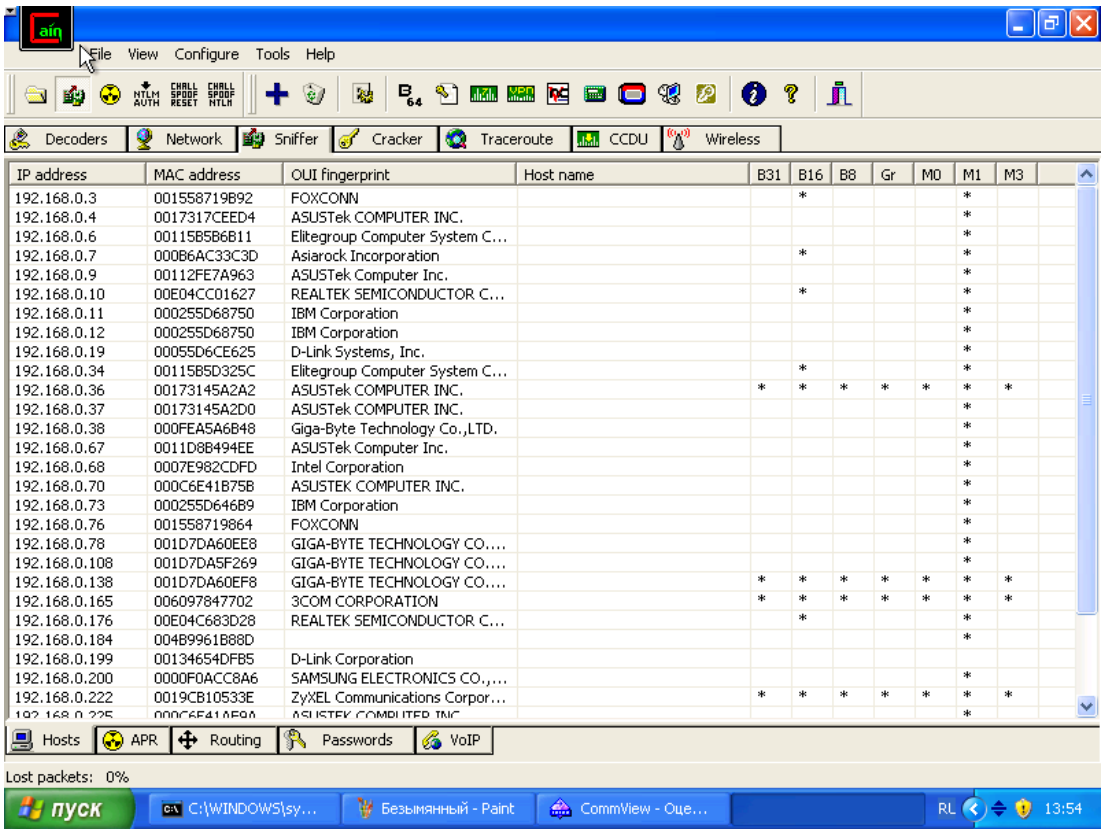


Рис 33. Реконструкция сессии с помощью программы CommView

4.4. Контрольные вопросы.

1. Какие особенности сетей Ethernet позволяют функционировать программам – «сниферам»?
2. Что такое «снифер» и каковы его функции?
3. Каким образом работает «снифер»?
4. Какие способы противодействия «сниферам» вы знаете?
5. Можно ли и как обнаружить работающий в сети «снифер»?

Лабораторная работа № 5
ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ ПРОТОКОЛА ARP

5.1. Цель работы

Изучение протокола разрешения адресов ARP и его уязвимостей.

5.2. Краткие теоретические сведения

Необходимость протокола ARP продиктована тем обстоятельством, что IP-адреса узлов сети назначаются независимо от их физических (MAC) адресов. Поэтому для доставки сообщений по сети нужен механизм, устанавливающий соответствие между физическим (MAC) адресом узла и его IP-адресом.

Функционально протокол ARP состоит из двух частей. Одна часть протокола определяет физические адреса путём посылки специальных запросов, другая - отвечает на запросы при определении физических адресов другими узлами сети. При формировании заголовка канального уровня для определения MAC-адреса получателя просматривается ARP-таблица, где

хранятся соответствия между IP-адресами и MAC- адресами узлов. Эта таблица обычно находится в оперативной памяти. Записи в таблицу добавляются динамически или вручную.

В локальных сетях протокол ARP использует широковещательные кадры канального уровня для поиска в сети узла с заданным IP-адресом. Узел, которому нужно выполнить отображение IP-адреса на MAC - адрес, формирует ARP-запрос, вкладывает его в кадр протокола канального уровня, указывая в нем известный IP-адрес, и рассылает запрос широковещательно. Все узлы локальной сети получают ARP запрос и сравнивают указанный там IP-адрес с собственным. Компьютер у которого, котором они совпадают, формирует ARP-ответ, в котором указывает свой IP-адрес, свой MAC - адрес и отправляет его уже целенаправленно, так как в ARP запросе отправитель указывает свой MAC - адрес.

ARP-запросы и ответы используют один и тот же формат пакета. На рисунке 33 показан формат пакета протокола ARP для передачи по сети Ethernet.

Тип сети	Тип протокола
Длина MAC-адреса | Длина IP адреса	Операция
MAC - адрес отправителя (байты 0-3)	
MAC - адрес отправителя (байты 4-5)	IP-адрес отправителя (байты 0-1)
IP-адрес отправителя (байты 2-3)	Искомый MAC - адрес (байты 0 -1)
Искомый MAC - адрес (байты 2-5)	
Искомый IP-адрес (байты 0-3)	

Рис.33 Формат пакета протокола ARP.

В поле типа сети для сетей Ethernet указывается значение I. Поле типа протокола позволяет использовать пакеты ARP не только для протокола IP, но и для других сетевых протоколов. Для IP значение этого поля равно 0x800.Длина MAC-адреса для протокола Ethernet равна 6 байтам, а длина IP-адреса - 4 байтам. В поле операции для ARP-запросов указывается значение I для запроса и 2 для ответа.Узел, отправляющий ARP-запрос, заполняет в пакете все поля, кроме поля искомого MAC - адреса. Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring. FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, frame relay), как правило, не поддерживающий широковещательный доступ.

Атаки на протокол ARP

1.Посылка ложного ARP-запроса

Одна из уязвимостей протокола ARP была обнаружена в Windows 9X/NT. Посылка специального ARP-пакета приводит к появлению окон с кнопкой ОК (для Windows 9X число окон равно числу посланных пакетов, Windows NT выводит только одно окно).

Обнаружить нарушителя сложно, так как MAC-адрес отправителя в пакете можно задать любым. Создать и отправить такой пакет можно с помощью любого генератора пакетов, например, SnifferPro компании Network Associated. Пользователь компьютера - жертвы будет вынужден много раз нажимать кнопку ОК или перезагружаться.

2.ARP-Spoofing

Выше была рассмотрена возможность отправки некорректного ARP-запроса Точно таким же образом можно построить и ARP-ответ. Только результатом будет добавление в ARP-таблицу узла-объекта атаки ложных записей. Большинство ОС добавляют в таблицу новую запись на основе полученного ответа даже без проверки того, был ли послан запрос именно им (исключением, например, является Solaris).

Таким образом, нарушитель может отправить ответ, в котором указан MAC - а несуществующего или неработающего в данный момент узла, что приведёт к невозможности взаимодействия узла - «жертвы» с каким-либо узлом.

3.ARP-Spoofing с использованием ARP-запроса

Для того чтобы добавить в ARP-таблицу узла ложную запись, не обязательно отправлять ARP-ответ. ARP-запрос, сформированный специальным образом, позволяет достичь такого же результата. «Побочный» эффект – появление сообщения о конфликте адресов на узле от имени которого отправляется ответ. Это происходит из-за того, что запрос широковещательный и его «слышат» все узлы сегмента. Для того, чтобы этого не происходило, можно отправить «направленный» ARP-запрос, в котором вместо широковещательного адреса получателя будет указан MAC-адрес объекта атаки.

5.3. Задание на лабораторную работу

Подготовительная часть.

1. Работа выполняется в парах. По завершению работы участникам следуют поменятся ролями. Для начала работы необходимо загрузить виртуальную машину с ОС Windows XP на своем компьютере и компьютере соседа. Прверить соединение между виртуальными машинами и локальной сетью класса.
2. Определить и записать MAC-адрес своей виртуальной машины Windows XP.
3. Определить и записать MAC-адрес соседней виртуальной машины, используя команды ping, arp и nbtstat.
4. Очистить ARP-таблицу на виртуальной машине Windows XP

Посылка ARP-запроса от чужого имени (IP-адреса)

Для проведения атаки необходимо находиться в одной подсети с объектом атаки, и знать его IP-адрес. В качестве узла злоумышленника выступает основная машина. С помощью CommView с неё отправляется ARP-запрос от имени узла - объекта атаки, в качестве которого выступает виртуальная машина с ОС Windows XP.

1. На основной машине настроить программу CommView на перехват ARP-пакетов (достаточно задать правило в разделе протоколы и направление - ARP, при этом должны быть отключены остальные правила).
2. Запустить процесс перехвата пакетов.
3. Дождаться прохождения ARP-запроса (можно не дожидаться такого пакета, а инициировать его посылку, очистив кэш ARP, и выполнив команду Ping <Соседняя виртуальная машина WinXP>).
4. Остановить процесс перехвата и открыть содержимое ARP-пакета.
5. В перехваченном ARP-запросе найти поле Sender IP address. Именно в нём указывается IP-адрес инициатора запроса. Если в этом поле поменять IP-адрес, можно послать запрос от имени любого узла.
6. Щёлкнуть правой кнопкой мыши в поле на перехваченном пакете и в меню в ыбрать пункт Отправить пакет (ы) > Выбранный.
7. В открывшемся окне отредактировать пакет, подставив в поле Sender IP address IP-адрес объекта атаки (в качестве объекта атаки указывается адрес соседней виртулъной машины с ОС Windows XP).

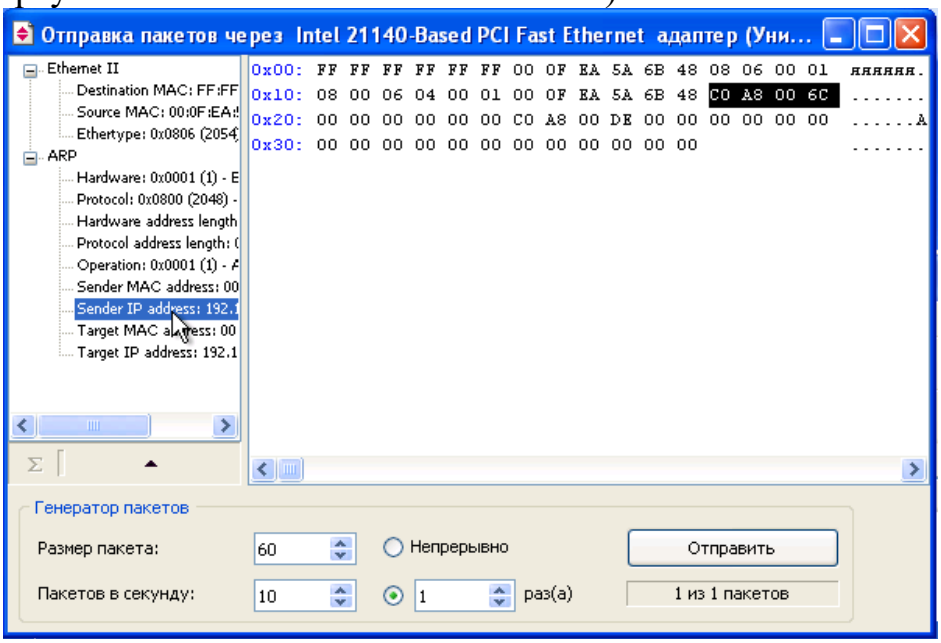


Рис.34 Формат пакета протокола ARP.

Внимание: IP-адрес необходимо задавать в шестнадцатиричном виде.
8. Нажать кнопку Отправить, чтобы отправить пакет в сеть.
9. Убедиться, что на соседнем виртуальном узле появилось сообщение об ошибке (всплывающее сообщение в правом нижнем углу - конфликт адресов IP). Просмотреть системный журнал виртуального узла, обратить внимание на указанные в нём адреса.

Удалённое изменение ARP-таблицы с помощью ARP-ответа

При определении соответствия IP-адреса и MAC-адреса используется кэш ARP. Воспользовавшись программой CommView (генератором пакетов), атакующий может посылать объекту атаки ложные ARP-ответы, добавляя в его кэш неправильные записи. Для этого необходимо перехватить

любой ответ на ARP-запрос, скорректировать его и отправить в сеть. Для реализации потребуется знать IP и MAC адреса объекта атаки. В качестве узла нарушителя выступает основная машина (как и в предыдущей части работы), Атакуемый узел - виртуальная Windows XP.

1. Определить IP и MAC адреса объекта атаки.

   IP-адрес объекта атаки (виртуальная машина Windows XP):

   MAC-адрес объекта атаки (виртуальная машина Windows XP):

2. Выбрать узел в классе, связь с которым будет нарушаться (узел X):
3. Запустить на виртуальной машине проверку связи с узлом X ping -t <узел X> (должно работать)
4. На основной машине запустить CommView, настроить фильтр на перехвата пакетов и перехватить любой ARP-ответ (или воспользоваться уже перехваченными пакетами).
5. Остановить сбор трафика
6. Открыть ARP-ответ в окне генератора пакетов и скорректировать поля ответ; следующим образом:

   a. Destination MAC - вписать MAC-адрес объекта атаки (виртуальное машины Windows XP)

   b. Source MAC - вписать несуществующий MAC-адрес (например. 22-22-22-22-22)

   c. ARP: Sender MAC address - вписать несуществующий MAC-адрес (например, 00-22-22-22-22-22)

   d. ARP: Sender IP address - вписать IP-адрес узла, от имени которого посылается ответ (в данном случае узел X - 200.x.x.200)

   e. ARP: Target MAC address - вписать MAC-адрес объекта атаки (виртуальной машины Windows XP)

   f. ARP: Target IP address - вписать IP-адрес объекта атаки (виртуальной машины Windows XP)

   g. Запустить сбор трафика Отправить пакет в сеть (можно один или несколько).

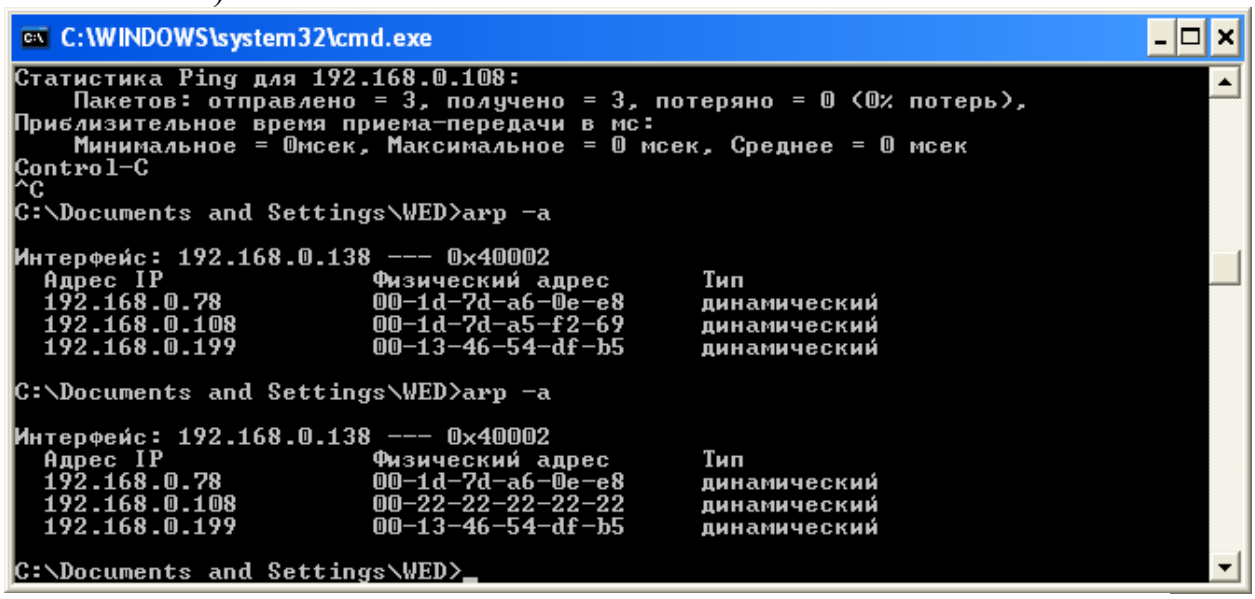


Рис.35. Результат взлома протокола ARP

9. На атакуемом узле проверить связь с узлом X, а также проверить содержимое таблицы arp (arp -a). Возможно, потребуется очистить таблицу arp командой arp -d. ping <узел X> (не должно работать)
10. Восстановить связь (очистить ARP-таблицу на виртуальной машине Windows XP)

Таким образом, в ходе атаки удалённо была изменена ARP-таблица узла - объекта атаки и нарушена связь с выбранным узлом (X).

Удалённое изменение ARP-таблицы с помощью ARP-запроса

1. На соседней виртуальной машине Windows XP проверить связь с любым узлом в классе (узел X)
2. Просмотреть arp-таблицу соседней виртуальной машине Windows XP. В таблице должны присутствовать IP и MAC адрес узла X
3. На основной машине запустить CommView, настроить фильтр на перехват ARP-пакетов и перехватить любой ARP-запрос (или воспользоваться уже перехваченными пакетами).
4. Остановить сбор трафика
5. Открыть ARP-запрос в окне генератора пакетов и скорректировать поля следующим образом:
    a. Destination MAC - оставить широковещательный адрес (FF-FF FF-FF)
    b. Source MAC - вписать несуществующий MAC-адрес (напriver 22-22-22-22-22)
    c. ARP: Sender MAC address-вписать несуществующий MAC- (например, 00-22-22-22-22-22)
    d. ARP: Sender IP address - вписать IP-адрес узла, от имени которого посылается ответ (в данном случае узел X)
    e. ARP: Target MAC address - оставить без изменений
    f. ARP: Target IP address - вписать IP-адрес объекта атаки (соседней виртуальной машины Windows XP)
    6. Запустить сбор трафика
7. Проверить, что на виртуальной машине Windows XP запись в arp-таблице осталась. В противном случае вновь выполнить команду ping <адрес узла X>
8. Отправить пакет в сеть (можно один или несколько).
9. На атакуемом узле (виртуальной машине Windows XP) просмотреть содер arp-таблицы. Убедиться, что запись с «неправильным» MAC-адресом (в данном случае - 00-22-22-22-22-22) добавилась в таблицу.

Обнаружение атак, использующих уязвимости протоколов ARP

1. Запустите на виртуальной машине WinXP программу XArp.
2. Дождитесь, пока программа соберет статистику. Убедитесь в том, что в списке присутствует адрес вашей виртуальной машины, виртуальной машины соседа, а также компьютера в классе, с которым будет нарушаться связь.

3. Последовательно выполнить описанные ранее атаки на соседнюю виртуальную машину, обращаяя внимание на реакцию программы XArp.

5.4. Контрольные вопросы.

1. Что такое протокол ARP и каково его назначение?
2. Каков формат ARP пакета?
3. Чем различаются ARP запросы и ARP пакеты?
4. Какие особенности протокола ARP использует атака, основанная на отправке ложного ARP-запроса? Каковы последствия такой атаки?
5. Что такое ARP- spoofing?
6. Какие способы противодействия ARP атакам вы знаете?

Лабораторная работа № 6
СЕТЕВОЕ СКАНИРОВАНИЕ УЯЗВИМОСТЕЙ

6.1. Цель работы

Изучение возможностей сканера безопасности на примере программы nmap.

6.2. Краткие теоретические сведения

В большом числе реальных практических задач перед администраторами безопасности возникает задача проверки соответствия используемых механизмов защиты принятой в организации политике безопасности. И такая задача периодически возникает при изменении, обновлении компонент информационной системы. Однако администраторы часто не имеют достаточно времени на проведение такого рода проверок для всех узлов корпоративной сети. Следовательно, специалисты отделов защиты информации и управлений автоматизации нуждаются в средствах, облегчающих анализ эффективности используемых механизмов обеспечения информационной безопасности. Автоматизировать этот процесс могут средства анализа защищенности, называемые также сканерами безопасности или сканерами уязвимостей. Использование этих средств поможет определить уязвимости узлов корпоративной сети и устранить их до того, как ими воспользуются злоумышленники.

Системы анализа защищенности можно поделить на две категории с точки зрения их расположения по отношению к объекту сканирования: Локальные и Дистанционные. Системы первой категории устанавливаются на сканируемой узле и выполняют анализ «изнутри». Иногда такие сканеры имеют возможности по автоматическому устранению найденных уязвимостей. Системы второй категории выполняют дистанционные проверки. Такие сканеры устанавливаются на выделенные для этой цели узел и могут параллельно сканировать несколько узлов сети, осуществлять сбор информации и т.п.

К наиболее известным программным продуктам для выполнения анализа защищенности относятся: Nessus Security Scanner, Internet Scanner, XSpider, LANguard, Nmap и пр.

Сетевые сканеры могут быть использованы для решения следующих задач:

1. Инвентаризация ресурсов сети
2. Тестирование сети на устойчивость к взлому
3. Аудит безопасности сети или отдельных ее частей на соответствии заданным требованиям

В рамках настоящей работы исследуются функции и возможности одного из сканеров безопасности – программы nmap. Достоинством этой программы является простота использования, возможность встраивания в сторонние программы, бесплатное распространение.

Утилита Nmap предназначена для сканирования сетей, использующих протокол TCP с целью определения состояния объектов сканируемой сети, а также портов и соответствующих им служб.

Основные возможности программы:

- Определение доступности узла (включен/выключен)
- Определение состояния заданного порта (TCP/UDP)
- Идентификация ОС сканируемого узла
- Поддержка различных методов сканирования
- Гибкая настройка

В большинстве случаев схема работы утилиты следующая:

1. Посылка на сканируемый узел запроса ICMP Echo Request.
2. Посылка на сканируемый узел TCP-пакета с установленным флагом ACK и портом получателя 80.
3. Сканирование портов из заданного диапазона заданным методом.

Формат команды:

nmap [тип сканирования] [опции] <узел или сеть>

Далее указаны основные типы сканирования, поддерживаемые утилитой:

-sT (TCP connect scan) Наиболее простой тип сканирования, предполагающий установление соединения с портами из диапазона сканирования. Используется по умолчанию.

-sS (TCP SYN scan) Сканирование с установлением полусоединения TCP. На сканируемый узел посылается пакет с флагом SYN, после получения подтверждения (SYN/ACK) посылается пакет с флагом RST и TCP-соединение не устанавливается.

-sP (Ping Scan) Используется для определения доступности узла. При этом применяется следующая технология. Обычно доступность узла устанавливается посылкой ICMP пакета с запросом (команда ping). Однако некоторые узлы игнорируют ICMP-пакеты. В этом случае посылается пакет с флагом ACK на 80-й порт, если в ответ приходит пакет с флагом RST, то узел доступен.

-sU (UDP scan) Используется для определения открытых UDP портов. При этом на заданный порт посылается UDP-датаграмма нулевой длины. Порт считается недоступным в случае получения в ответ сообщения Destination unreachable.

-sA (scan ACK) ACK-сканирование

-sF, -sX, -sN (scan FIN, scan Xmas, scan NULL) Эти методы используются в случае, если SYN-сканирование по каким-либо причинам оказалось неработоспособным или нежелательно.

Далее приведены некоторые полезные опции, предлагаемые утилитой:

-P0 (Ping 0) Не производить ping-опрос узлов перед их сканированием, т. е. не выполнять шаг 1 в приведённой выше схеме работы утилиты. Эта опция позволяет сканировать узлы, блокирующие обработку ICMP-пакетов.

-PI Производить проверку доступности узла только с помощью ping-

опроса, т. е. не выполнять шаг 2 в приведённой выше схеме работы утилиты. Эта опция противоположна предыдущей.

-PT (Ping TCP) Использовать вместо посылки запроса ICMP отправку TCP ACK-пакета на сканируемый узел (шаг 2). Для указания номера порта используется формат -PT <номер_порта>. По умолчанию используется 80-й порт.

-O Определение ОС сканируемого узла. Дополнительно выводится оценка случайности генерации начального значения TCP-последовательности (Sequence Number).

-D <ложный_адрес1,[ложный_адрес2],...> (Decoy-режим)

Интересный режим работы утилиты, в котором Nmap искусственно создает ложные узлы, адреса которых указаны в качестве аргументов. При этом на стороне сканируемого узла создается видимость, что производится одновременное сканирование с различных узлов (обладающих разными IP-адресами), что затрудняет обнаружение реального IP-адреса сканирующего. Адреса разделяются запятой, можно указать свой IP-адрес в качестве одного из узлов. Если он явно не указан, Nmap поместит его на случайную позицию. Лучше, если узлы, указанные в качестве ложных, реально существуют, в противном случае это может облегчить обнаружение узла, производящего сканирование.

6.3. Задание на лабораторную работу

1. Перейти в командную строку
2. Запустить nmap без указания параметров, посмотреть номер версии
3. Выполнить идентификацию узлов в сети учебного класса

nmap -sP 192.X.X. 1-254 –n

4. Просмотреть результаты
5. Повторить предыдущую команду, добавив опцию -v для увеличения степени подробности.

nmap -sP 192.X.X. 1-254 -n -v
6. Просмотреть результаты, обратить внимание на использованный метод идентификации узлов сети
7. Среди найденных сетевых объектов вашего учебного класса выбрать один
и выполнить идентификацию открытых TCP-портов
nmap -sS 192.X.X.X-n
8. Просмотреть результаты. Среди перечня открытых портов TCP выбрать какой-нибудь, например, 21, 25 или 80.
9. Выполнить для выбранного порта идентификацию службы приложения
nmap -A 192.X.X.X -p21 -п
10. Просмотреть результаты (правильно ли была идентифицирована служба?), обратить также внимание на результаты идентификации ОС.
11. Ещё раз выполнить идентификацию ОС выбранного узла, включив подробный вывод результатов (опция —w)
nmap -O 192.X.X.X -n -vv
12 . Просмотреть результаты, найти перечень тестов, выполняемых утилитой, обратить внимание на сложность подбора значения поля Initial Sequence Number
13 . Выполнить идентификацию ОС других узлов учебного класса. Сравнить поведение поля ISN для различных ОС
14. Запустить процесс идентификации открытых портов UDP выбранного узла:
nmap -sU 192.X.X.X -n
15. Просмотреть результаты.
16. Выбрать 3-4 узла из учебного класса и выполнить по ним полную инвентаризацию с записью результатов в xml-файл
nmap -A -sS -sU 192.X.X.1-3 -p U:l-500,T:l-500 -п -oX inventory.xml
Примечание: опция —р указывает диапазон сканируемых портов. Время сканирования зависит от заданного диапазона и в данном случае занимает около 10 минут. Для сокращения времени сканирования можно сократить диапазон сканируемых портов или отказаться от сканирования портов UDP.
17. Открыть файл с результатами сканирования с помощью Excel
18. Удалить все столбцы до поля IP-адрес

6.4. Контрольные вопросы.

1. Что представляет собой сканер безопасности и каковы его функции?
2. Какие типы сканеров безопасности вы знаете?
3. Какие программные продукты для выполнения анализа защищенности вы знаете?
4. Какие функции имеет программа nmap?
5. Каковы схема работы утилиты nmap?

Лабораторная работа № 7
ОСОБЕННОСТИ МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

7.1. Цель работы

Исследование типовой конфигурации локальных вычислительных сетей и вариантов их сопряжения.

7.2. Краткие теоретические сведения

Несмотря на обилие локальных вычислительных сетей, их конфигурация, как правило, основывается на общих принципах. Одним из таких принципов является повышенное внимание к «периметру» сети – т.е. области (компьютеру, сети, устройству и т.д.) ее сочленения с внешней сетью. Такой внешней сетью в большинстве случаев является глобальная сеть Интернет. Повышенное внимание к «периметру» сети объясняется наличием в сети Интернет значительной части потенциальных угроз безопасности. К этим угрозам можно отнести разнообразные «вирусы», нарушающие работоспособность компьютерной сети и влекущие потерю данных, программы, позволяющие установить контроль над сетью или ее частью и прочие угрозы. Для минимизации возможности реализации этих угроз в локальных вычислительных сетях применяют типовые конфигурации компьютеров и устройств. В настоящей работе рассмотрена одна из таких типовых конфигураций: две сети, состоящие из компьютеров с установленной ОС Windows и объединенные стандартными коммутаторами. Местом пересечения сетей является компьютер с установленной ОС Unux (Linux, FreeBSD и т.д.). Значительная роль ОС Unix в вопросах защиты периметра сетей определяется меньшим по сравнению с Windows количеством уязвимостей и многообразием версий. Подобная топология позволяет обеспечить приемлемый уровень защиты для отдельной сети за счет размещения на «пограничном» компьютере специализированных программ типа прокси-серверов и фильтров трафика.

7.3. Задание на лабораторную работу

1. Запустите программу Sun xVM VirtualBox (рис.). Программа эквивалентна по своим функциям Microsoft Virtual PC, но позволяет запускать в режиме эмуляции запускать операционные системы семейства Unix. Проверьте наличие в списке готовых к запуску виртуальных машин позиций Linux и Windows.
2. Убедитесь в том, что для эмулируемой системы Linux подключены два сетевых адаптера, один из которых работает в режиме «Хост-интерфейса», второй в режиме внутренней сети.

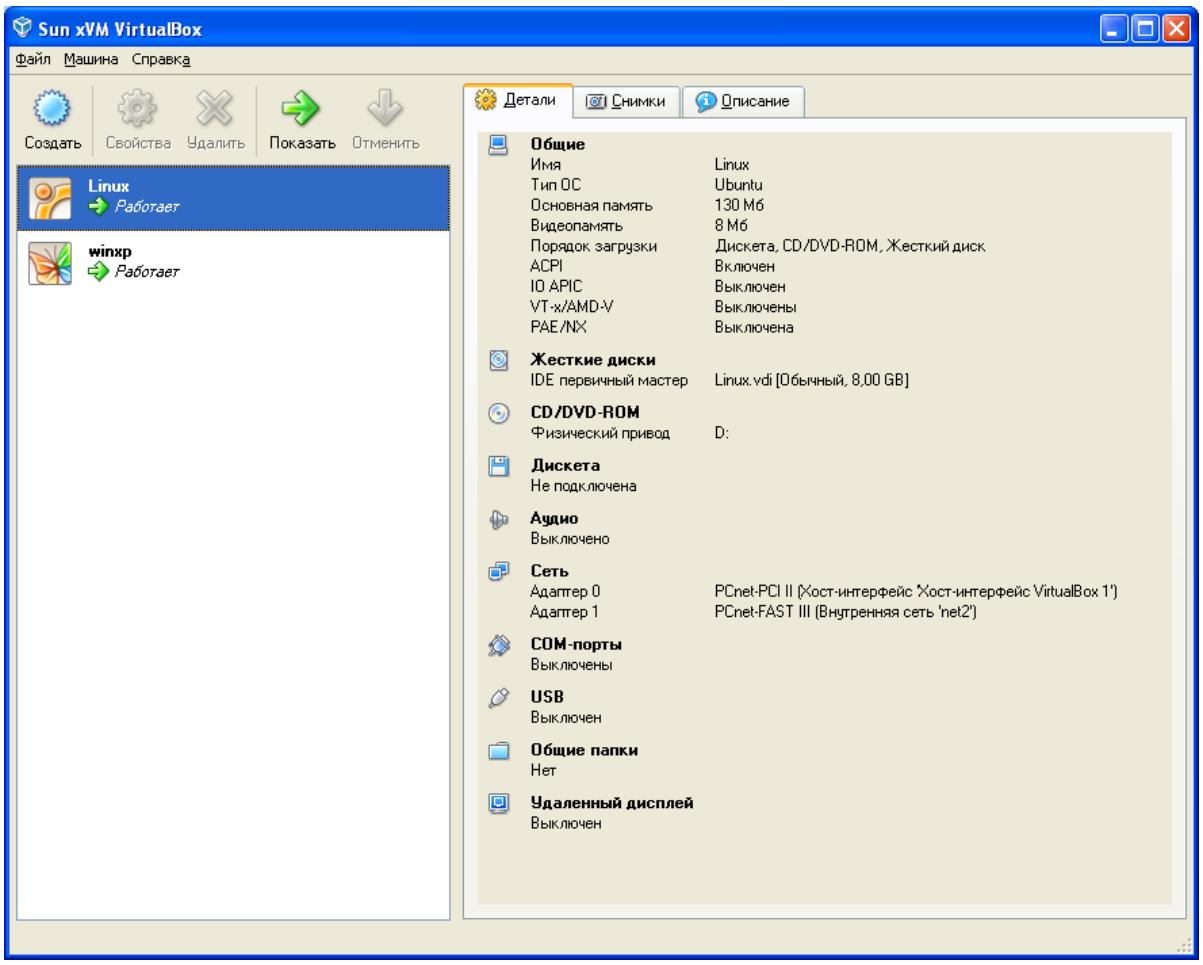


Рис.35. Внешний вид ПО Sun Virtual Box

3. Запустите виртуальные машины Linux и WinXp.

4. В настройках сетевых подключений для виртуальных машин Linux, WinXP, а также хост-интерфейса основной машины проверьте следующие настройки

Сетевое подключение WinXP: IP-адрес 192.168.5.1, Шлюз 192.168.5.149

Первый интерфейс (eth1) Linux: IP-адрес 192.168.5.149

Второй интерфейс (eth2) Linux: IP-адрес 192.168.1.149

Хост-интерфейс: IP-адрес 192.168.1.147, Шлюз 192.168.1.149

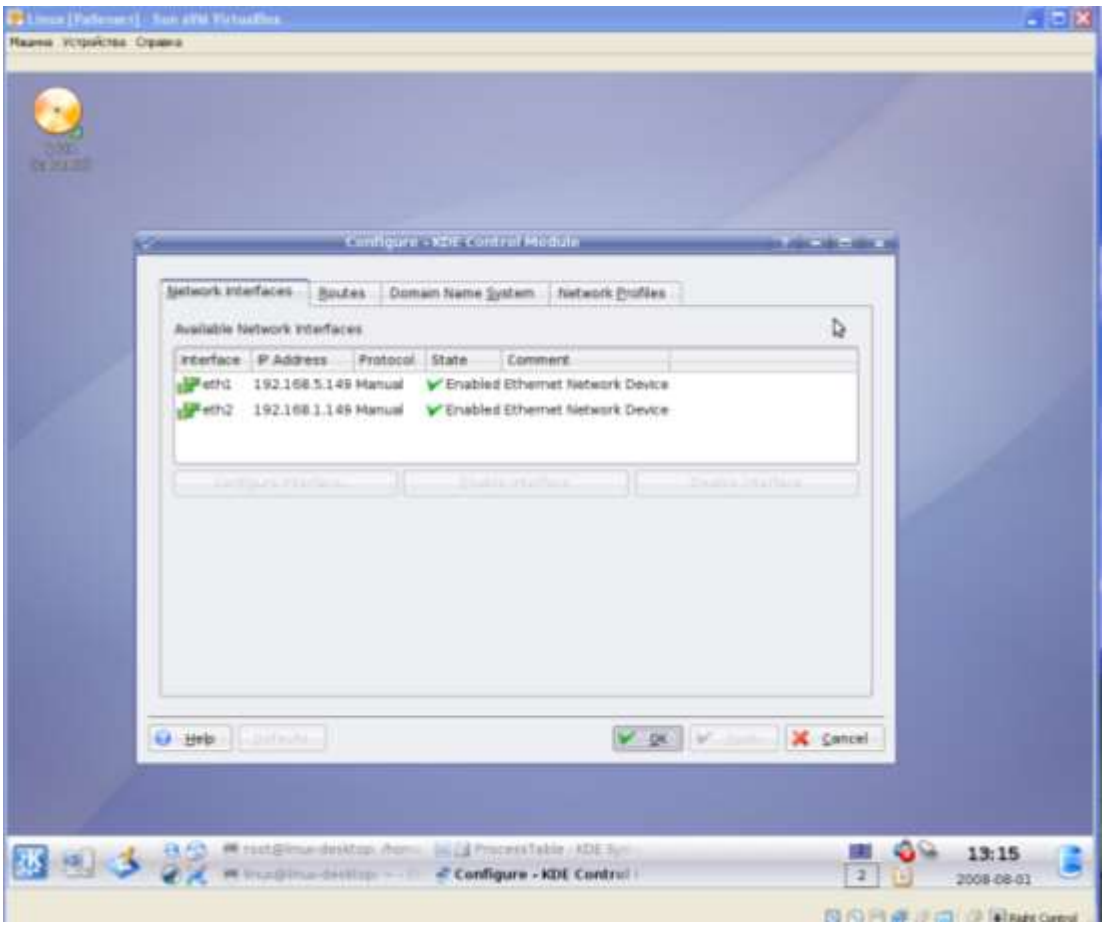


Рис.36. Конфигурация сетевых настроек в ОС Linux

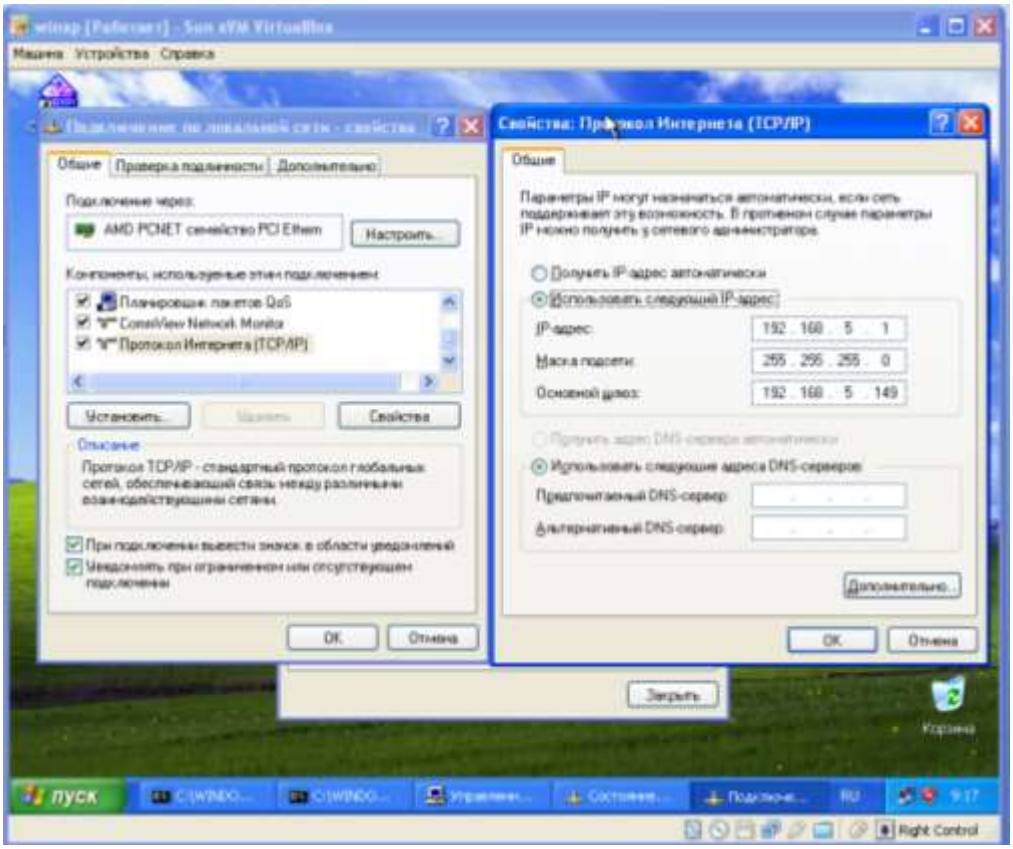
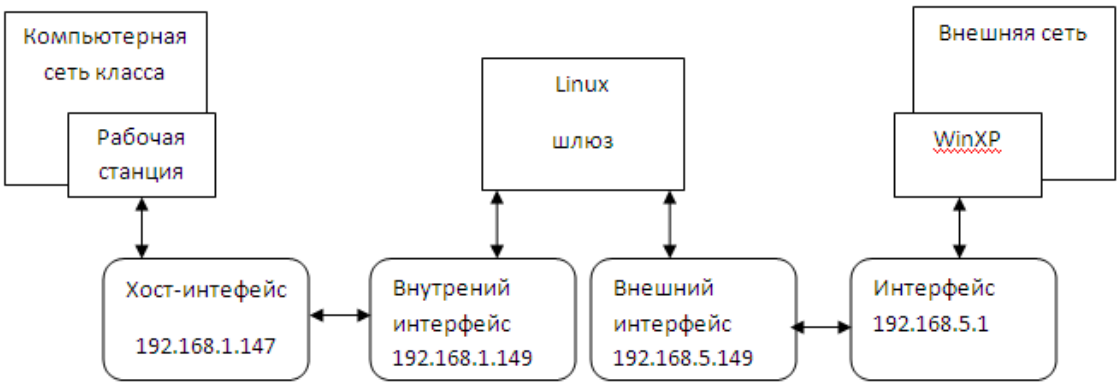


Рис.37. Конфигурация сетевых настроек в ОС Windows

Таким образом, смоделирована следующая сетевая структура:



5. На виртуальной машине Linux запустите Консоль (System/Konsole). Так как последующие действия потребуют права суперпользователя (root), вводим команду su root для переключения консоли под управление суперпользователя.

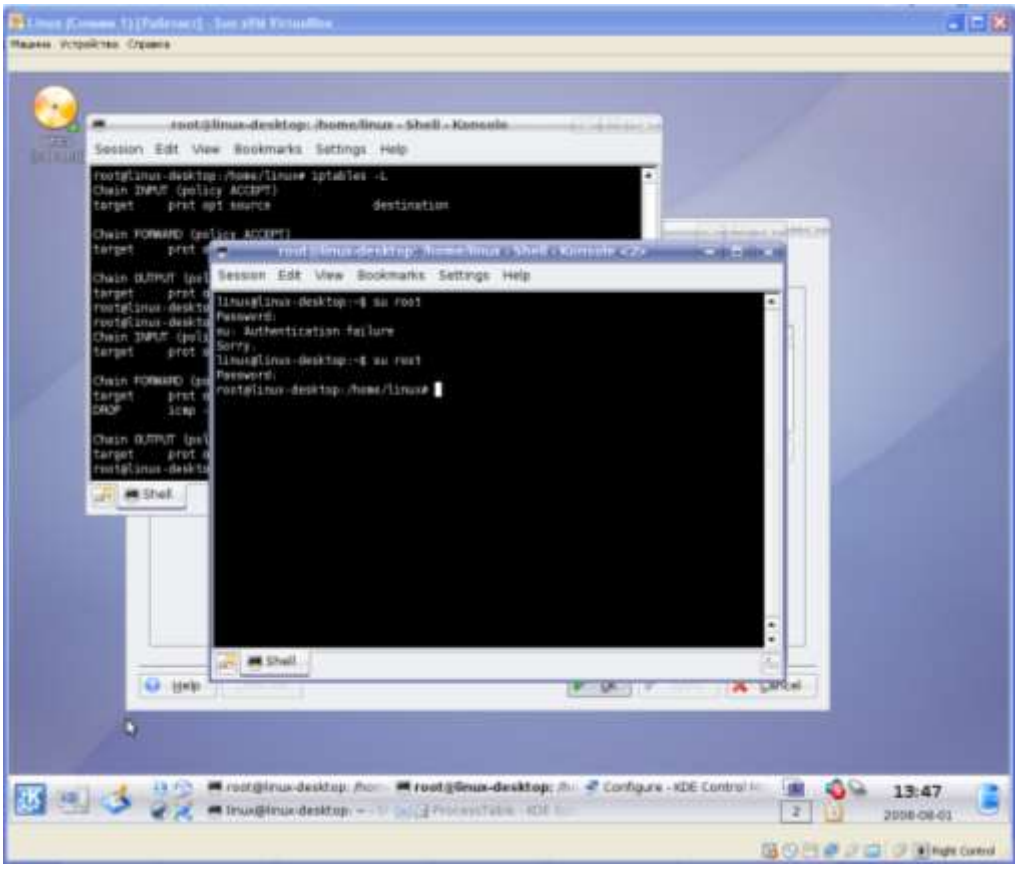


Рис.38. Конфигурация сетевых настроек в ОС Linux

6. Вводим команду echo "1" > /proc/sys/net/ipv4/ip_forward, позволяющую выполнять маршрутизацию между сетевыми интерфесами.

7. На рабочей станции и виртуальной WinXP с помощью команды route print проверяем наличие маршрутов до внешней сети. Если маршрут отсутствует, добавляем его с помощью команды route -p add 192.168.5.0 mask

255.255.255.0 192.168.1.149 (ключ –p необходим, чтобы маршрут сохранялся после перезагрузки)

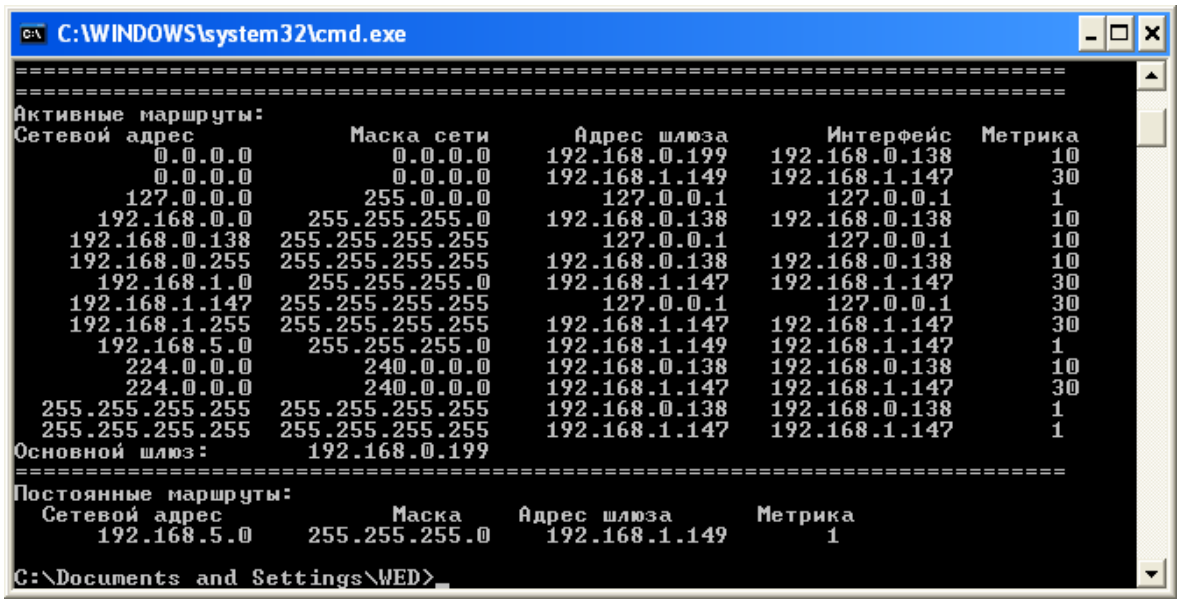


Рис.39. Установка маршрутов в ОС Windows

8. Проверяем с помощью команды ping наличие соединения с рабочей станции (192.168.1.147) до виртуальной машины winXP (192.168.5.1).

9. Проверить наличие доступа к web серверу виртуальной машины winXP (192.168.5.1) с рабочей станции (192.168.1.147). Для этого на компьютере (192.168.1.147) запустите Интернет браузер и откройте страницу http://192.168.5.1/

Таким образом, смоделирована типовая конфигурация двух локальных вычислительных сетей и способа их сопряжения.

7.4. Контрольные вопросы.

1. Какие угрозы для локальных вычислительных сетей вы знаете?
2. Что такое «периметр» сети?
3. По какой причине при проектировании сетей большое внимание уделяется их «периметру»?
4. Почему на роль операционной системы для компьютера, находящегося на «границе» сети избирают Unix?

Лабораторная работа № 8
МЕЖСЕТЕВЫЕ ЭКРАНЫ И СПОСОБЫ ИХ НАСТРОЙКИ

8.1. Цель работы

Изучение типовой конфигурации локальных вычислительных сетей и вариантов их сопряжения.

8.2. Краткие теоретические сведения

Интуитивно понятно, что корпоративная сеть имеет какие-то границы, своего рода «забор», скрывающий её «от посторонних глаз». Разумеется, должны быть и «двери», через которые возможно «взаимодействие» со всем остальным миром. До недавнего времени роль таких дверей в корпоративной сети играла «точка» подключения к Internet, а также выделенные каналы, соединяющие центральный офис с филиалами. Соответственно, периметр такой сети (представляющий собой границы и двери) «выглядел» достаточно чётко.

Сейчас периметр сети становится всё более «размытым». Возможными точками взаимодействия с «окружающим миром» могут быть:

- Беспроводные сегменты, делающие весьма вероятной возможность нарушения границ сети на физическом и канальном уровнях.
- Клиентские приложения, часто имеющие постоянное соединение с ресурсами, расположенными в недоверенных сетях.
- Сегменты, обеспечивающие удалённый доступ к сети, включая доступ посредством виртуальных частных сетей (Virtual Private Network, VPN).
- Выделенные каналы, соединяющие филиалы друг с другом или обеспечивающие взаимодействие с сетями партнёров
- Точка подключения к Internet

Межсетевые экраны (МЭ) занимают важное место в комплексе средств обеспечения безопасности корпоративной сети. Иногда используются термины «брандмауэр» или «firewall».

На практике, МЭ - это специализированное программное или аппаратное обеспечение. позволяющее разделить сеть на две или более частей и реализовать набор правил определяющих условия прохождения сетевых пакетов из одной части в другую. Прежде всего основным назначением МЭ является воплощение политики безопасности, принятой в организации в вопросах обмена информацией с внешним миром.

МЭ используются для решения следующих задач:

- Фильтрация трафика
- Противодействие атакам
- Анализ содержимого трафика
- Защита от спама
- Антивирусная защита

Существует несколько критериев, по которым можно классифицировать МЭ. Например, с точки зрения реализации различают МЭ:

- Программные
- Аппаратные
- Программно-аппаратные

С точки зрения защищаемых ресурсов МЭ могут быть:

- Пери метровые (защищающие целую сеть)
- Персональные (контролирующие трафик отдельного узла)

Удобно классифицировать МЭ по уровням модели OSI. В этом случае принадлежность МЭ к тому или иному типу определяется уровнем модели OSI, на котором осуществляется перехват и анализ сетевых пакетов. Соглас-

но такой классификации различают следующие типы МЭ:
Мосты (мостовые МЭ)
Пакетные фильтры
Посредники (шлюзы) уровня соединения
Посредники (шлюзы) прикладного уровня

Мостовые МЭ

Мостовые МЭ выполняют анализ фреймов канального уровня и перенаправляют их нужный сетевой интерфейс. Они подключаются как бы «в разрыв кабеля» и не требуют изменения сетевых настроек (на уровне IP).
Хотя «единицей работы» для мостовых МЭ является фрейм, анализироваться может информация с различных уровней.
Достоинства мостовых **МЭ:**

- **Производительность.** Задержка при прохождении пакетов через мостовой МЭ минимальна. Дополнительные ресурсы требуются для более тщательного анализа данных.
- **Прозрачность.** Мостовой МЭ просто пересылает фреймы после их анализа между сетевыми интерфейсами. А это означает, что нет необходимости в изменении существующих сетевых настроек и маршрутизации.
- **Защищённость от атак.** Сетевые интерфейсы мостового МЭ не имеют IP-адреса. Без IP-адресов он невидим для окружающего мира.

Пакетные фильтры

Пакетный фильтр - маршрутизатор, перенаправляющий сетевые пакеты в соответствии с заданной на нём политикой безопасности.
Пакетный фильтр работает на сетевом уровне модели OSI, но может анализировать заголовки протоколов вышележащего уровня (TCP, UDP, ICMP). Взаимодействие между внутренней и внешней сетью является прозрачным, просто маршрутизируются не все IP-пакеты (датаграммы), а только те, которые удовлетворяют заданным правилам фильтрации.
Главный недостаток пакетного фильтра — отсутствие контроля соединения (статичность). Статичность означает, что пакетный фильтр манипулирует отдельными пакетами, не учитывая при этом принадлежности пакета к какому-либо соединению, ни, тем более, сопоставляя данные нескольких (взаимосвязанных между собой) соединений.

Технология «stateful inspection»

Очевидно, недостаточно только лишь просматривать отдельные пакеты. Информация о состоянии, извлеченная из имевших место ранее соединений и других приложений используется для принятия окончательного решения о пропуске или запрете очередного анализируемого пакета. В зависимости от типа проверяемого пакета; при принятии решения важными могут быть как текущее состояние соединения, к которому он принадлежит (полученное из его истории), так и состояние приложения, его использующего.
Технология «stateful inspection» обеспечивает сбор информации из пакетов, классификация и накопление ее в специальных контекстных таблицах, которые динамически обновляются.

Таким образом, обработка нового соединения происходит с записью параметров соединения в так называемую таблицу соединений.

Шлюзы уровня соединения

Этот и следующий тип МЭ основан на использовании так называемого принципа посредничества, т. е. запрос принимается МЭ, анализируется и только потом перенаправляется реальному серверу.

Посредник уровня соединения (circuit-level proxy) - это посредник, определяющий, какой трафик должен быть перенаправлен, только на основе информации не выше сеансового уровня (например, номера портов). Он просто копирует данные между участниками соединения, работая на сеансовом уровне сетевой модели.

Когда клиент (из внутренней сети) запрашивает соединение с сервером (из внешней сети), шлюз принимает запрос и проверяет его на соответствие критериям фильтра. После того, как шлюз проверил допустимость данного сеанса, он устанавливает соединение с требуемым сервером. Таким образом, реально устанавливается два соединения и. начиная с этого момента, шлюз просто ретранслирует пакеты в обе стороны, контролируя процесс обмена данными между клиентом и сервером. При этом на шлюзе должна поддерживаться таблица установленных соединений.

Для шлюзов уровня соединения, как правило, требуется установка на клиенте специального программного обеспечения, но это не всегда так. Главная особенность посредников уровня соединения - статичность, т. е. они устанавливают соединение, основываясь исключительно на правилах политики безопасности, а не на особенностях конкретной службы. Например, если правила фильтрации разрешают ftp-соединение, то такой посредник всегда будет ретранслировать трафик на порт 20 (ftp-data), даже если отсутствует управляющее соединение (порт 20, ftp-control).

Большинство сетевых ОС имеют возможности фильтрации пакетов. Это достигается либо средствами самой ОС, либо установкой дополнительных модулей. Ярким примером, наглядно демонстрирующим такие возможности, является ОС Linux. Ядро этой ОС имеет встроенные возможности фильтрации пакетов, а утилита, облегчающая процесс настройки, называется iptables.

Устройство пакетного фильтра iptables

Архитектура пакетного фильтра iptables изображена на следующем рисунке:

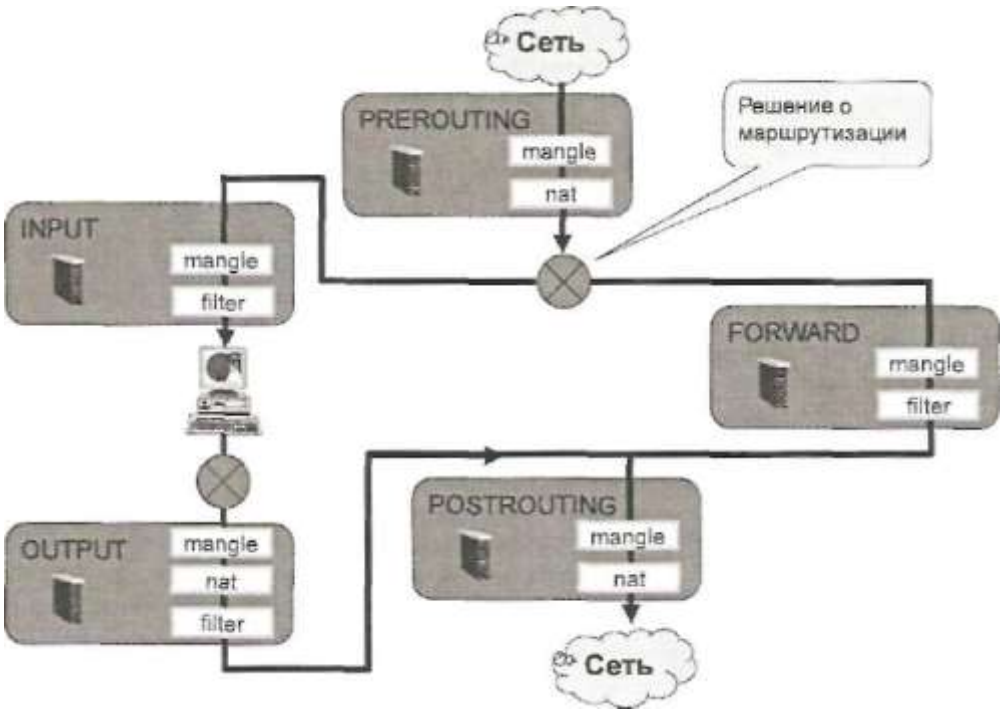


Рис. 40. Архитектура пакетного фильтра iptables

При прохождении пакета через пакетный фильтр срабатывает одна или несколько цепочек. Цепочка - это список правил. Правила просматриваются подряд, одно за другим. Если ни одно из правил цепочки не удовлетворяет параметрам заголовка пакета, пакет пропускается или уничтожается в зависимости от политики цепочки, которая может либо запрещать все остальные пакеты, либо разрешать. Правила фильтрации, входящие в цепочки, хранятся во внутренних таблицах ядра системы.

Функции цепочек фильтрации:

• цепочка INPUT занимается фильтрацией пакетов, адресованных данному узлу.

• цепочка OUTPUT занимается фильтрацией пакетов, сгенерированных данным узлом.

• цепочка FORWARD занимается фильтрацией пакетов, проходящих транзитом.

Кроме этого, до и после маршрутизации присутствуют цепочки трансляции адресов. При маршрутизации срабатывает цепочка PREROUTING, а после маршрутизации -POSTROUTING. Краткое описание каждой цепочки приведено в таблице:

PREROUTING	Пакет фильтруется на этой цепочке до того, как будет принято решение о его маршрутизации. Это самое удачное место для размещения проверок пакета на правильность.
INPUT	На этой цепочке фильтруются пакеты, прошедшие маршрутизацию и предназначенные данному узлу.
FORWARD	На этой цепочке фильтруются пакеты, прошедшие маршрутизации и предназначенные для передачи в следую-

OUTPUT	Через эту цепочку проходят пакеты, сгенерированные на данном узле, до того, как будет принято решение об их
POSTROUTING	Пакет фильтруется на этой цепочке после того, как он прошел маршрутизацию, и непосредственно перед тем, как он будет отправлен в сеть. В этой цепочке необходимо размещать правила преобразования адресов отправителя.

8.3. Задание на лабораторную работу

Часть 1. Проверка конфигурации

1. Загрузить ОС Linux и Windows XP в виртуальных машинах.
2. В ОС Linux проверить:

- Адреса сетевых адаптеров (команда ifconfig)
- Связь с хост-интерфейсом рабочей станции.
- Связь с виртуальной машиной WinXP

3. Включить маршрутизацию

echo "1" > /proc/sys/net/ipv4/ip_forward

4. С рабочей станции проверить связь с виртуальной машиной Windows XP.
5. Перейти в ОС Linux
6. Вывести версию утилиты *iptables:* **iptables —version**

Можно также попробовать вариант **iptables -V**

7. Просмотреть содержимое цепочек правил **iptables -L**

Должно быть пусто. Если присутствуют какие-либо правила, сбросьте их. выполнив команду ***iptables*** *-F*

8. Просмотреть содержимое отдельной цепочки (например, входной) **iptables -L INPUT**

(Должно быть пусто)

Часть 2. Простейшие приёмы работы с iptables

В текущей конфигурации через пакетный фильтр разрешено прохождение любого трафика. В качестве примера далее рассматривается запрет прохождения через пакетный фильтр трафика UDP или ICMP.

1. На рабочей станции перейти в командную строку. **Start > Program > Accessories > Command Prompt**
2. Запросить список зарегистрированных имён NetBIOS на узле виртуальной машины (должно работать, эта команда использует протокол UDP, который пока разрешён)
3. На виртуальной машине с ОС Linux для цепочки FORWARD задать правило, запрещающее UDP-трафик:

iptabies -A FORWARD -p UDP -j DROP

4. Просмотреть список правил для цепочки **FORWARD iptabies -L FORWARD**

Убедиться, что правило добавилось к цепочке.

5. Вновь запросить с Windows XP список зарегистрированных имён NetBIOS на
узле виртуальной машины, используя командную строку:
6. Удалить добавленное правило
iptabies -D FORWARD -p UDP -j DROP
7. Вновь запросить с Windows XP список зарегистрированных имён NetBIOS на
узле виртуальной машины:
nbtstat -a <узел виртуальной машины > (должно работать)
8. Вывести содержимое цепочки **FORWARD: iptabies -L FORWARD**
Убедиться, что правило удалено
9. Отправить с внутреннего узла (Windows XP) ICMP-запрос на узел виртуальной машины
ping <узел виртуальной машины > (должно работать)
10. Задать правило, запрещающее прохождение ICMP-пакетов для цепочки **FORWARD iptabies -A FORWARD -p ICMP -j DROP**
11. Просмотреть список правил для цепочки **FORWARD iptabies -L FORWARD**
Убедиться, что правило добавилось к цепочке
12 . Снова отправить ICMP-запрос с внутреннего узла на узел виртуальной машины **ping <узел виртуальной машины >** (не должно работать)
13 . Удалить добавленное правило
iptabies -D FORWARD -p ICMP -j DROP
14. Ещё раз отправить ICMP-запрос с внутреннего узла на узел преподавателя (должно работать)
15. Вывести содержимое цепочки **FORWARD: iptabies -L FORWARD**
Убедиться, что правило удалено
Часть 3. Построение заданной конфигурации на основе iptabies, изучение stateful inspection
Допустим, требуется построить следующую конфигурацию.
1. Разрешить обращение к узлу виртуальной машины по протоколу SMTP
2 . Разрешить обращение к узлу виртуальной машины по протоколу HTTP
3. Разрешить обращение к узлу виртуальной машины по протоколу FTP (при этом долже работать активный и пассивный вариант)
Для этого необходимо выполнить следующие действия:
1. В ОС Linux убедиться что все правила сброшены, на всякий случай выполнить команду **iptables -F**
2 . Сменить политику цепочки **FORWARD: iptables -P FORWARD DROP**
С этого момента через МЭ запрещено прохождение любого транзитного трафика
3. Разрешить обращение к внешним ресурсам по протоколу SMTP. Для этого
необходимо добавить два правила:
iptables -A FORWARD -p TCP -s 192.N.N.0/24 -dport 25 -j ACCEPT

iptables -A FORWARD -p TCP -d 192.N.N.0/24 -sport 25 -tcp-flags ACK ACK -j ACCEPT

Первое правило разрешает прохождение пакетов TCP от узлов внутреней сети, при этом порт получателя = 25, что соответствует протоколу SMTP. Второе правило разрешает прохождение ответов (в этом правиле задано требование - наличие флага АСК).

Примечание: Если вы добавили ошибочное правило, его можно удалить, указав

его номер, например:

iptables -D FORWARD 2 (удаление правила с номером 2)

4. Проверить работу правила, обратившись с внутреннего узла (Windows XP) к

SMTP-серверу виртуальной машины

telnet 200.X.X.200 25 (должно работать)

5.Проверить, что другие протоколы запрещены, например: **telnet 200.X.X.200 80** (не должно работать)

Итак, построен простейший пакетный фильтр, в котором не задействована технология stateful. Прежде чем переходить к добавлению других правил фильтрации, проверьте, как «выглядит» построенный пакетный фильтр снаружи. Для этого далее в качестве внешнего узла используется ваша основная машина.

6. На базовой ОС перейти в командную строку
7. Добавить маршрут к сети за вашим МЭ

route add 192.N.N.0 mask 255.255.255.0 200.X.X.200+N

8. Проверить, что снаружи доступа нет. Для этого попытаться подключиться к

некоторым службам, например:

telnet 192.N.N.100+N 80 (не должно работать)

9. Перейти в каталог с утилитой nmap

cd \nmap-4.01

10. Выполнить сканирование портов на целевом узле **nmap -P0 192.N.N.100+N --system-dns -p20-200**

Все порты должны иметь статус filtered

11. Зная, что изнутри можно обращаться на порт 25, попытаться выполнить сканирование путём отправки пакетов с флагом АСК и портом источника 25:

nmap -P0 -sA 192.N.N.100+N --system-dns -p20-200-g25 Все порты должны иметь статус Unfiltered

Таким образом, пакетный фильтр пропустил все отправленные пакеты. Чтобы этого избежать, необходимо включить режим stateful.

12. Удалить последнее правило **iptables -D FORWARD 2**
13. Проверить, что осталось только одно правило, разрешающее прохождение пакетов на порт 25.

8.4. Контрольные вопросы.

1. Что такое межсетевой экран?

2. Какие типы межсетевых экранов Вы знаете?
3. Что такое технология State full Inspection?
4. Что такое пакетный фильтр?
5. В чем разница при использовании цепочек фильтрации INPUT и OUTPUT?
5. В чем разница при использовании цепочек фильтрации PREROUTING и POSTROUTING?

СПИСОК ЛИТЕРАТУРЫ

1. Мельников, Владимир Павлович. Защита информации: учебник / Мельников В. П., Куприянов А. И., Схиртладзе А. Г.; под ред. В. П. Мельникова. - Москва: Академия, 2014. - (Высшее образование. Информационная безопасность). - 296 с.: рис. - Библиогр.: с. 291-293 (56 назв.). - ISBN 978-5-4468-0332-3, Гриф: УМО
2. Олифер, Виктор Григорьевич. Компьютерные сети. Принципы, технологии, протоколы: учебное пособие для вузов / Олифер В. Г., Олифер Н. А. - 3-е изд. - Санкт-Петербург [и др.]: Питер, 2008. - 957 с.: ил. - ISBN 978-5-469-00504-9 Гриф: МО и науки РФ
3. Гладких А.А., Дементьев В.Е. Базовые принципы информационной безопасности вычислительных систем //Ульяновск: УлГТУ, 2009. – 167 с.
4. Сергеева Ю. С. Защита информации: конспект лекций / Сергеева Ю. С.; . - Москва: А-Приор, 2011. - (Серия: Конспект лекций. В помощь студенту). - 128 с. - ISBN 978-5-384-00397-7