МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)
Кафедра информационных систем и технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
« 16 » 04 2019 г.

Инфокоммуникационные системы и сети

Методические указания по выполнению лабораторных работ для направления подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем»

Курск 2019

УДК 004

Составитель А.С. Сизов

Рецензент
Кандидат технических наук, доцент Ю.А. Халин

Инфокоммуникационные системы и сети: методические указания по выполнению лабораторных работ для направления подготовки «Математическое обеспечение и администрирование информационных систем» / Юго-Зап. гос. ун-т; сост. А.С. Сизов. Курск, 2019. 41 с.: Библиогр.: с. 41.

Методические рекомендации предназначены для студентов, обучающихся по направлению подготовки 02.03.03 «Математическое обеспечение и администрирование информационных систем»

Текст печатается в авторской редакции.

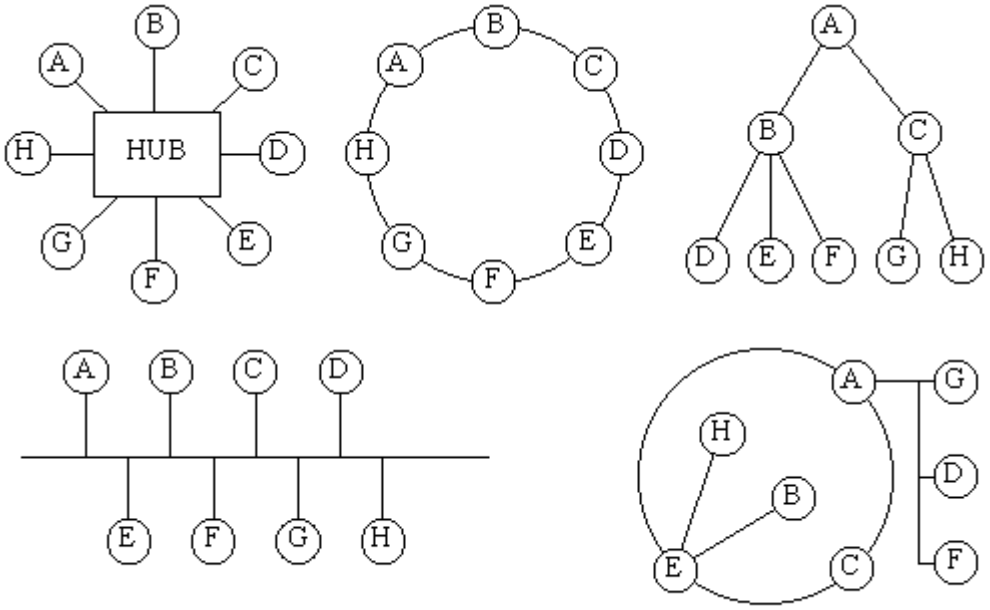
Подписано в печать 16.04.19. Формат 60x84 1/16.
Усл.печ. л. 2,4. Уч.-изд. л. 2,2. Тираж 100 экз. Заказ. 332 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94

Работа №1

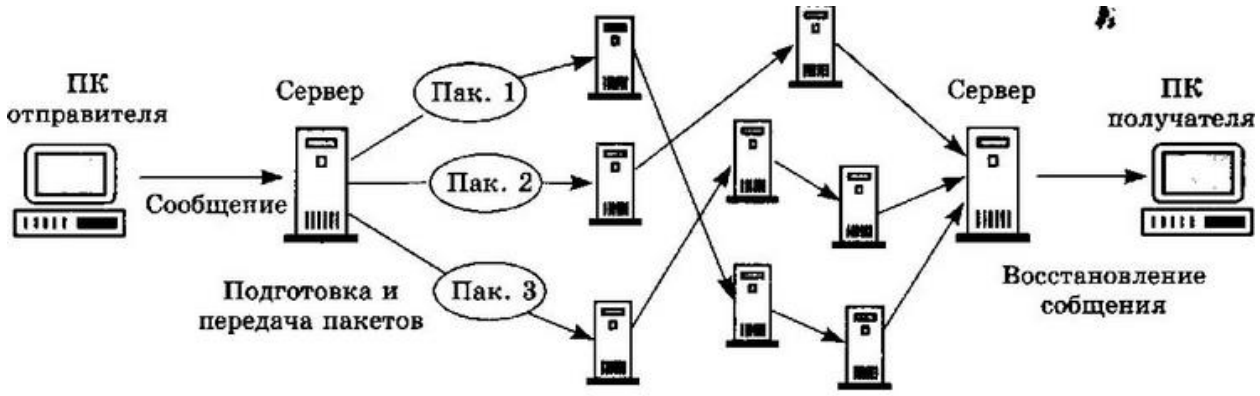
Классификация инфокоммуникационных сетей по размеру, топологии, физической среде передачи данных.

Классифицировать представленные ниже сети, указать тип каждой из сетей, описать основные характеристики.

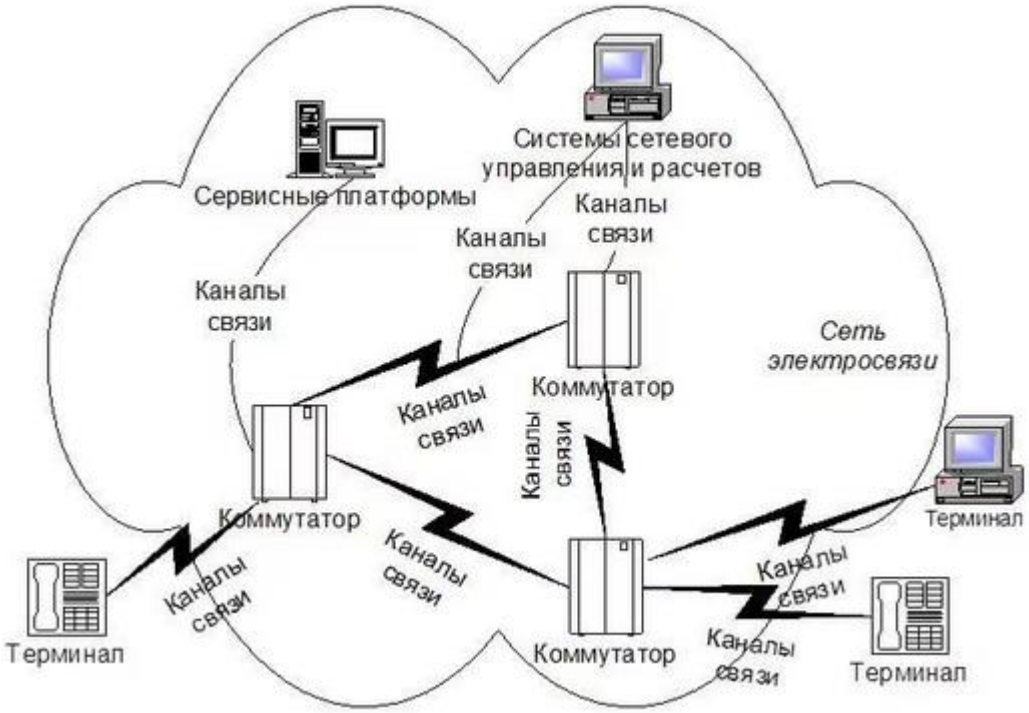
а)



б)



в)

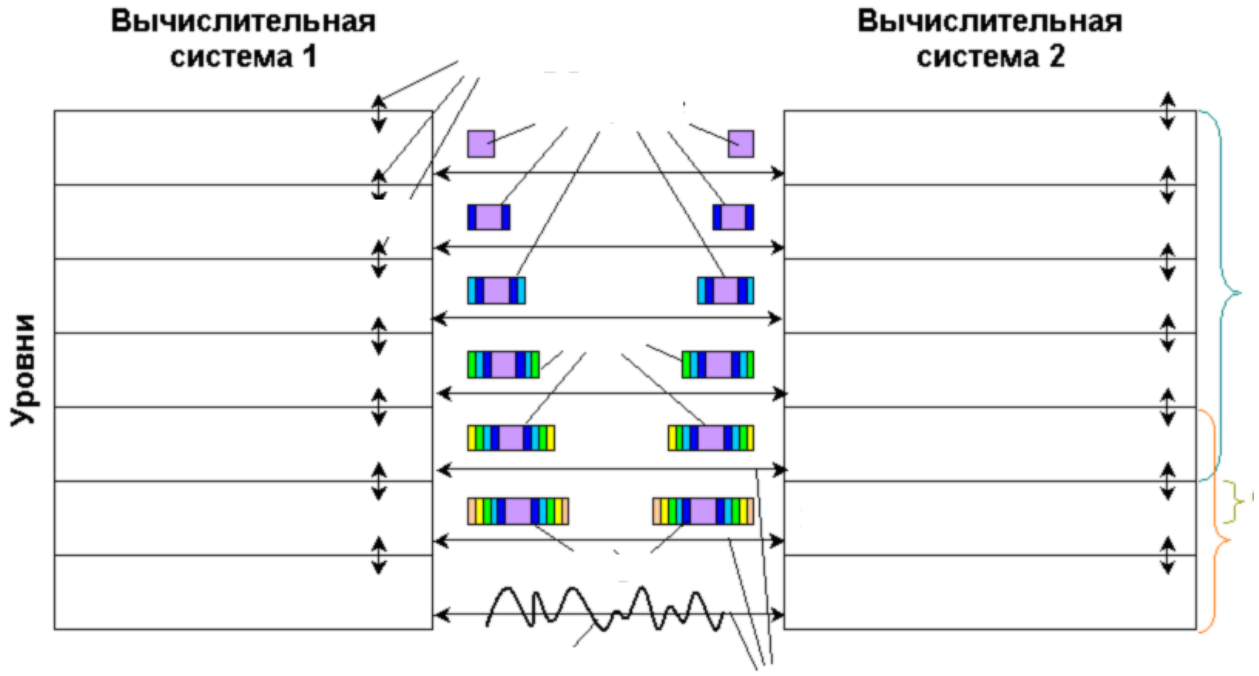


Контрольные вопросы

1. Какие классы инфокоммуникационных систем по охвату этой сети территории вы знаете?
2. Какие классы инфокоммуникационных систем по топологии вы знаете?
3. Что такое хост?
4. Что такое шлюз?

Работа №2

Уровни модели OSI и их взаимодействие. Иерархия сетей по стандарту ISO.



1. Впишите обозначения для модели OSI представленной на рисунке. Дайте краткую характеристику каждого уровня.
2. Опишите стандарт ISO.
3. Начертить следующие типы систем согласно стандарту: конечная система (ES), промежуточная система (IS), зона и автономная система (AS).

Контрольные вопросы

1. Что такое модель OSI?
2. Какие уровни модели вы знаете?
3. Опишите один из уровней модели OSI?

Работа №3

Методы выделения идентификаторов сети и узла в IP-адресе. Поля параметров IP-пакета.

IP-адресация

Передача сообщений в Интернет основана на том, что каждый компьютер сети имеет индивидуальный адрес – IP-адрес. Этот адрес выражается одним 32-разрядным числом, имеющим две смысловые части. Одна часть IP-адреса определяет номер сети, вторая – номер узла(компьютера) в сети. Так как оперировать длинными двоичными числами достаточно сложно, число, определяющее IP-адрес, разбивают на 4 октета – восьмиразрядных двоичных числа,

а каждое из этих чисел представляют в десятичном виде. Октеты отделяют друг от друга точками. Таким образом, 32-разрядный IP-адрес представляется в виде: 255.255.255.255 (десятичное число может меняться от 0 до 255 – максимального значения восьмиразрядного двоичного числа). Например: 128.10.2.30 – десятичная форма представления IP-адреса,

10000000 00001010 00000010 00011110 – двоичная форма представления этого же адреса.

В сети Интернет различные глобальные сети, в зависимости от размера, делятся по классам:

Сети класса А: большие сети общего пользования, первый октет определяет номер сети, три последующие октета – номер узла; **Сети класса В:** сети среднего размера. Два первых октета определяют номер сети, два оставшихся – номер узла;

Сети класса С: сети малого размера. В этих сетях три первых октета определяют номер сети и последний октет – номер узла.

В таблице 1 представлена общая характеристика схемы Интернет-адресации

Таблица 1

Класс	**Диапазон значений первого октета**	**Общее количество сетей**	**Максимальное количество узлов в каждой сети**
A	1 – 126	126	16 777 214
B	128 – 191	16 382	65 534
C	192 – 223	2 097 150	254

Некоторые IP-адреса имеют специальное назначение, например, адрес:

- 0.0.0.0 представляет адрес шлюза по умолчанию, т.е. адрес компьютера, которому следует направлять информационные пакеты, если они не нашли адресата в локальной сети;
- 127.любое число (часто 127.0.0.1) – адрес «петли». Данные, переданные по этому адресу, поступают на вход компьютера, как полученные по сети. Такой адрес необходим при отладке сетевых программ;
- 255.255.255.255 – широковещательный адрес. Сообщения, переданные по этому адресу, получают все узлы локальной сети, содержащей компьютер-источник сообщения (в другие локальные сети оно не передается);
- Номер сети . все нули – адрес сети;
- Все нули . номер узла – узел в данной сети. Может использоваться для передачи сообщений конкретному узлу внутри локальной сети;
- Номер сети . все единицы (двоичные) – все узлы указанной сети.

В локальных сетях используются специальные, так называемые «серые» IP-адреса. Они определены документом RFC 1918 (RFC – Requests For Comments, предлагаемый проект стандарта, большинство документов, регламентирующих Интернет, описано в RFC) и приведены в табл. 2:

Таблица 2

Диапазоны IP-адресов, используемых в локальных сетях
10.0.0.0 - 10.255.255.255
172.16.0.0 - 172.31.255.255
192.168.0.0 - 192.168.255.255

В небольших по размеру локальных сетях обычно применяется последний диапазон адресов. Сетевые маршрутизаторы не передают информацию для узлов с этими адресами, поэтому она оказывается «запертой» внутри локальной сети. Такая схема позволяет в разных локальных сетях использовать одни и те же IP-адреса и не приводит к конфликтам.

Для повышения гибкости использования IP-адресов деление адреса на части с использованием классов дополняется технологией CIDR (Classless Inter-Domain Routing) – бесклассовой междоменной маршрутизации. В этом случае адрес сети формируется с помощью двух чисел: адреса и **маски**. Маска это тоже 32-разрядное двоичное число, с помощью которого из IP-адреса выделяется адрес сети. Схема формирования адреса сети с использованием маски проста, ее можно пояснить на примере, допустим, адрес представлен двоичным числом 110101, маска числом 111100. Маска накладывается на адрес, как трафарет, в котором единицы соответствуют прорезям, в которых мы «увидим» адрес сети, в нашем примере адрес сети соответствует числу 110100. Маска всегда содержит такое двоичное число, старшие разряды которого подряд единицы, а младшие – нули, единицы представляют «прозрачную» часть трафарета, а нули – «непрозрачную». Маска так же, как и адрес, записывается в виде четырех десятичных чисел, разделенных точками и представляющих двоичные октеты. Для компактной записи пары чисел: IP-адрес-маска, используется также другая форма, например: 10.0.0.8/30. Число до слеша представляет собой IP-адрес, а число после слеша – количество разрядов в IP-адресе, отводимых для адресации сети. Число 30 после слеша соответствует маске 255.255.255.252. После определения адреса сети, оставшаяся часть IP-адреса используется для адресации узлов в сети.

Символьное представление имени компьютера в сети

Каждый компьютер в сети имеет уникальный адрес. При использовании IP-адресации это IP-адрес. Однако человеку достаточно трудно оперировать длинными

наборами цифр, не несущих смысловой нагрузки, поэтому всегда применяются системы преобразования имен, ставящие в соответствие цифровому адресу компьютера его символьное имя. В глобальных сетях и сети Интернет это служба DNS (Domain Name System) — распределенная база данных, поддерживающая иерархическую систему имен для идентификации узлов в сети Интернет. Определенные части базы данных доменных имен хранятся на специальных серверах — DNS-серверах, обрабатывающих запросы любого компьютера и определяющие имя, соответствующее IP-адресу или наоборот. В каждой локальной сети, подключенной к Интернет, работает по крайней мере один DNS-сервер. База данных DNS имеет структуру дерева, называемого доменным пространством имен,

в котором каждый домен (узел дерева) имеет имя и может содержать поддомены. Имя домена идентифицирует его положение в этой базе данных по отношению к родительскому домену, а точки в имени отделяют части, соответствующие узлам домена, например, www.tusur.ru .

Для именования компьютеров в локальных сетях используются плоские (не имеющие иерархии) символьные имена, так называемые NetBIOS-имена. Протокол

NetBIOS (Network Basic Input/Output System), как расширение стандартных функций базовой системы ввода-вывода, был разработан в 1984г. компанией IBM и широко применяется в ее продуктах, а также продуктах компании Microsoft. В протоколе NetBIOS реализован механизм широковещательного разрешения имен, когда все компьютеры в локальной сети получают запрос на разрешение имени, соответствующего некоторому IP-адресу. Кроме того, компания Microsoft для своей сетевой операционной системы Windows NT разработала централизованную службу разрешения имен WINS (Windows Internet Name Service). WINS-сервер, работающий

в локальной сети, централизованно обрабатывает все запросы, касающиеся разрешения имен в сетях Windows. При большом числе компьютеров в локальной сети WINS-сервер необходим. Однако в малых сетях, содержащих менее 10 компьютеров, часто используется широковещательный механизм разрешения имен протокола NetBIOS, упрощающий административное обслуживание таких сетей. В сетях без поддержки NetBEUI/NetBIOS over TCP/IP для разрешения имѐн используют DNS-сервера.

Автоматизация процесса назначения IP-адресов узлам сети

IP-адреса могут назначаться администратором сети вручную. Это представляет для администратора достаточно сложную и длительную процедуру, если количество компьютеров в локальной сети достаточно велико. Если происходят изменения в сети, например, появляются новые компьютеры, процедуру необходимо выполнить и для них, а в некоторых случаях и выполнить коррекцию предыдущих настроек на уже работающих компьютерах. Протокол DHCP (Dynamic Host Configuration Protocol) был разработан для того, чтобы освободить администратора от этих проблем. Основным назначением DHCP является динамическое назначение IP-адресов. В локальной сети, содержащей DHCP-сервер,

каждый компьютер при включении посылает запрос этому серверу на получение IP-адреса. Способы выдачи адресов могут быть различными.

При автоматическом статическом способе выделения адреса DHCP-сервер присваивает IP-адрес (и, возможно, другие параметры конфигурации клиента) из пула (набора) наличных IP-адресов. Границы пула назначаемых адресов задает администратор при конфигурировании DHCP-сервера. Между идентификатором клиента и его IP-адресом в этом случае, как и при ручном назначении, существует постоянное соответствие.

При динамическом распределении адресов DHCP-сервер выдает адрес клиенту на ограниченное время (время подключения к сети), что дает возможность впоследствии повторно использовать этот же IP-адрес другими компьютерами (пользователями).

Адресация компьютеров на канальном уровне

Каждый компьютер, подключенный к сети, имеет сетевой адаптер (сетевую карту) с присвоенным ему адресом. Этот адрес носит название MAC-адреса, он задается при изготовлении сетевого адаптера и впоследствии не изменяется. В выпукаемых ныне сетевых адаптерах **H**ard**W**are Address возможно изменять, поскольку он хранится в электрически перепрограммируемой памяти. Длина и другие особенности MAC-адреса зависят от используемой в локальной сети технологии. В сетях Ethernet MAC-адрес имеет длину 6 байт, записанных в шестнадцатеричном формате и разделенных дефисами (например 00-AA-00-4F-2A-9C). Для определения локального адреса по IP-адресу используется протокол разрешения адреса ARP (Address Resolution Protocol). Существует также протокол, решающий обратную задачу – нахождение IP-адреса по известному локальному адресу. Он называется RARP – реверсивный ARP, и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

Необходимость в обращении к протоколу ARP возникает каждый раз, когда модуль IP передает пакет на уровень сетевых интерфейсов, например драйверу Ethernet. IP-адрес узла назначения известен модулю IP. Требуется на его основе найти MAC-адрес узла назначения. Работа протокола ARP начинается с просмотра так называемой АКР-таблицы (рис.). Каждая строка таблицы устанавливает соответствие между IP-адресом и MAC-адресом. Поле «Тип записи» может содержать одно из двух значений – «динамический» или «статический».

Статические записи создаются вручную с помощью утилиты **arp** и не имеют срока устаревания, точнее, они существуют до тех пор, пока компьютер или маршрутизатор не будут выключены. Динамические же записи создаются модулем протокола ARP, использующим широковещательные возможности локальных сетевых технологий. Динамические записи должны периодически обновляться. Если запись не обновлялась в течение определенного времени (порядка нескольких минут), то она исключается из таблицы. Таким образом, в ARP-таблице содержатся записи не обо всех узлах сети, а только о тех, которые активно участвуют в сетевых

операциях. Поскольку такой способ хранения информации называют кэшированием, ARP-таблицы иногда называют ARP-кэш. После того как модуль IP обратился к модулю ARP с запросом на разрешение адреса, происходит поиск в ARP-таблице указанного в запросе IP-адреса. Если таковой адрес в ARP-таблице отсутствует, то исходящий IP-пакет, для которого нужно было определить локальный адрес, ставится в очередь. Далее протокол ARP формирует свой запрос (ARP-запрос), вкладывает его в кадр протокола канального уровня и рассылает запрос широковещательно. Все узлы локальной сети получают ARP-запрос и сравнивают указанный там IP-адрес с собственным. В случае их совпадения узел формирует ARP-ответ, в котором указывает свой IP-адрес и свой локальный адрес, а затем отправляет его уже по адресу компьютера, сформировавшего запрос, так как в адрес отправителя указан в самом запросе.

Сетевые утилиты

В сетевых операционных системах существует большое число утилит (специальных программ), предназначенных для управления и анализа сетевых соединений, рассмотрим четыре из них: **ifconfig**, **arp**, **netstat** и **route**.

Утилита ifconfig

Позволяет просмотреть текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений, с ее помощью можно определить IP-адрес данного компьютера. Запущенная без параметров[1)] команда **ifconfig** выдает в качестве результата текущую конфигурацию адресов TCP/IP для всех установленных на данном компьютере сетевых адаптеров и коммутируемых соединений (рис. 1.1).

Команду ifconfig следует первой использовать для диагностирования возможных проблем с соединением TCP/IP. С ее помощью можно определить, был ли вообще назначен IP-адрес сетевому адаптеру, а также узнать адрес шлюза.

1)

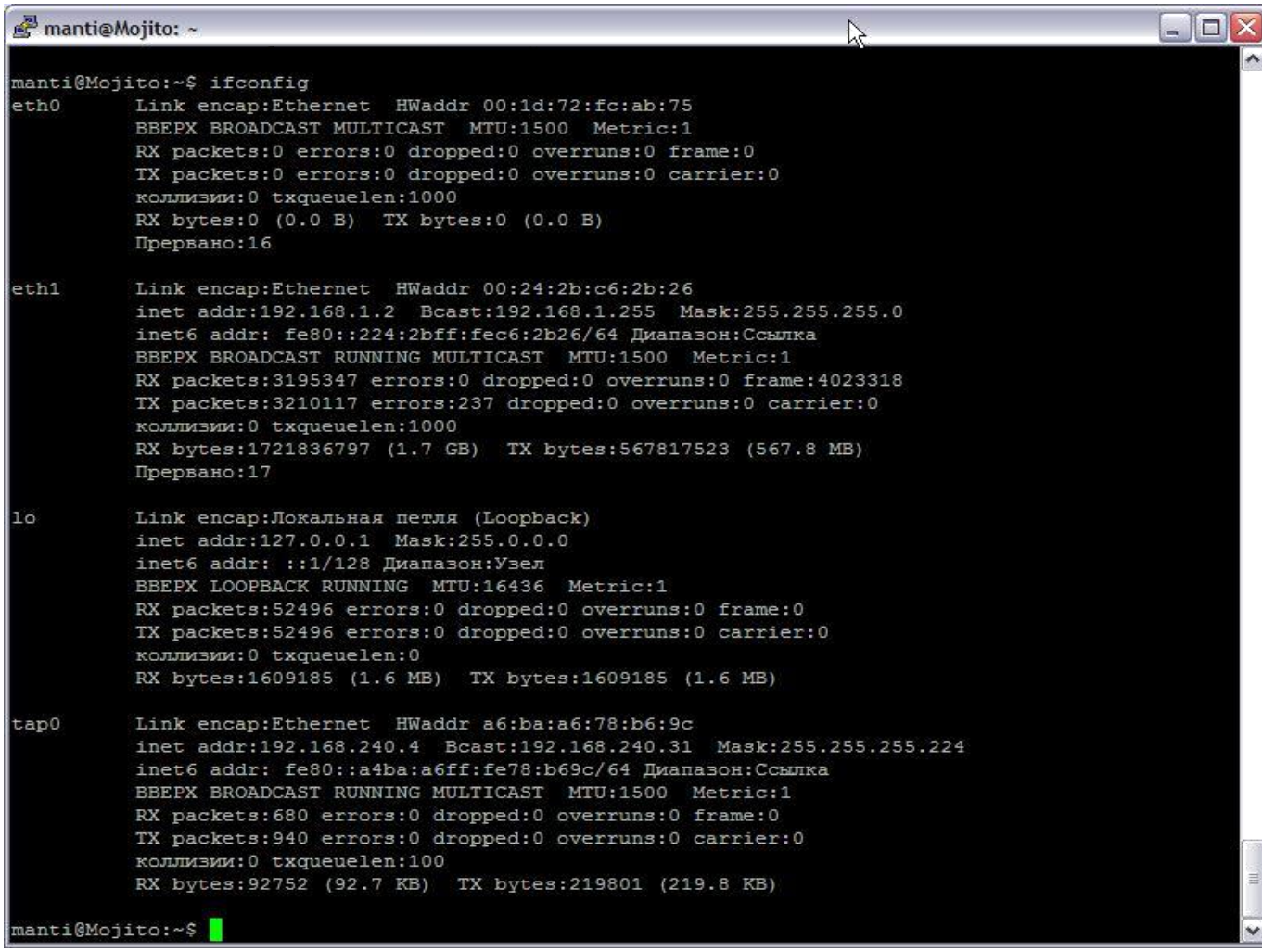


Рис. 1.1. Вывод актуальной сетевой конфигурации с помощью команды ifconfig.

Утилита route

Команда позволяет получить подробную информацию о текущей таблице маршрутизации и изменять эту таблицу.

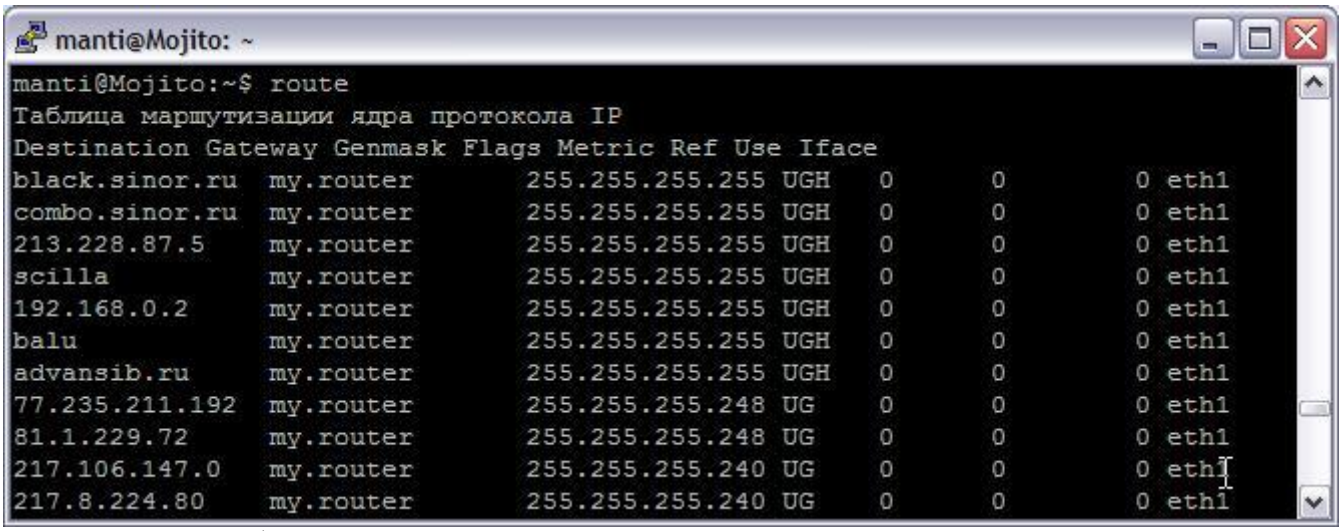


Рис. 1.2. Вывод таблицы маршрутизации с помощью команды route

Утилита netstat

Команда позволяет получить подробную информацию о соединениях, активных в настоящее время. Дополнительные ключи позволяют также получить информацию о сетевых портах, об IP-адресах компьютеров, участвующих в подключении, а также о других сетевых параметрах.

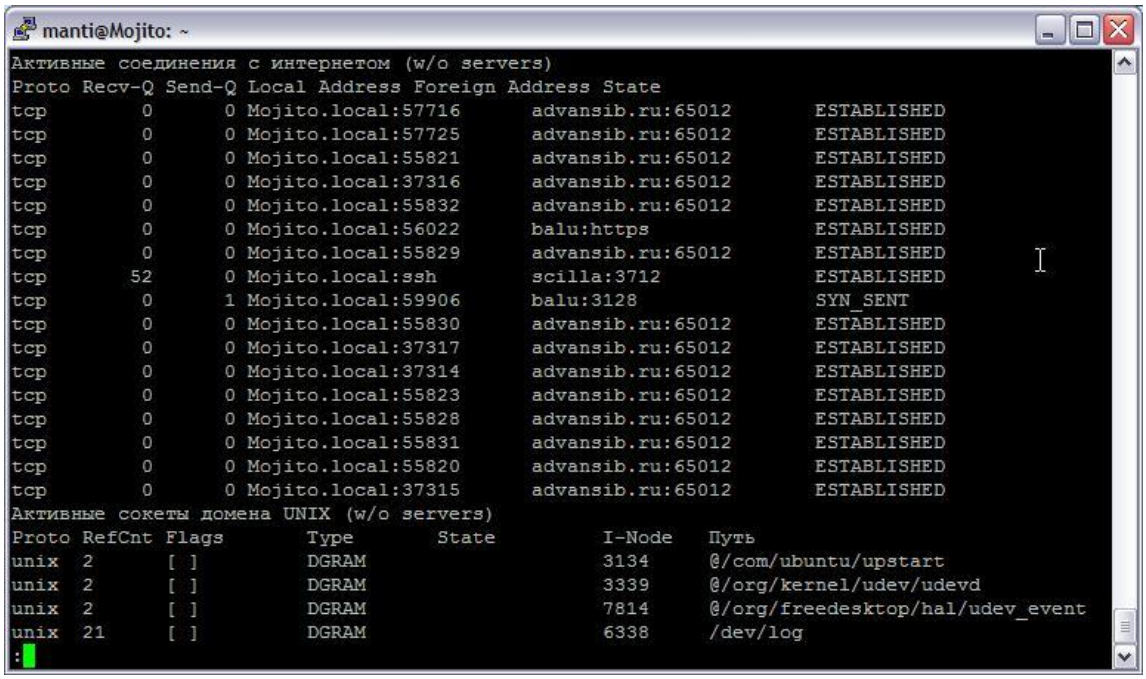


Рис. 1.3. Вывод активных подключений с помощью команды netstat.

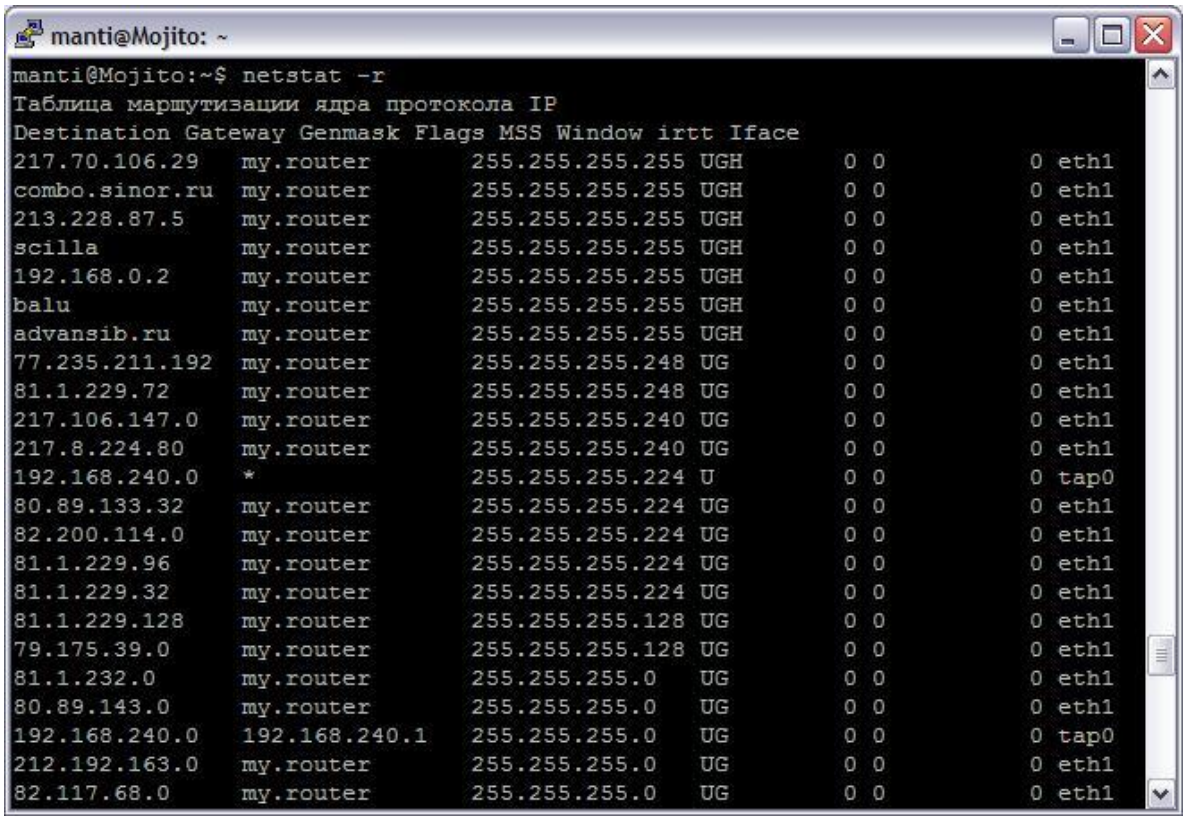
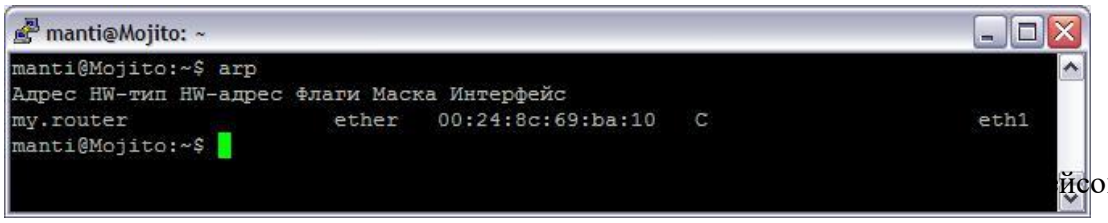


Рис. 1.4. Вывод таблицы маршрутизации с помощью команды netstat.

Утилита ARP

Служит для вывода и изменения записей кэша протокола ARP, который содержит одну или несколько таблиц, использующихся для хранения IP-адресов и соответствующих им физических адресов Ethernet или Token Ring. Для каждого сетевого адаптера Ethernet или Token Ring, установленного в компьютере, используется отдельная таблица.



йсов

Выполнение

Работа выполняется индивидуально. С помощью утилит **ifconfig**, **arp**, **netstat** необходимо получить информацию для заполнения таблиц 3-5.

Таблица 3

Символьное имя компью-тера	Адрес локаль-ной сети	IP-адрес компьютера	MAC-адрес Компьютера	Используемая в локальной сети техноло-гия

Таблица 4

Таблица маршрутизации. Активные маршруты:				
Сетевой адрес	Маска подсети	Адрес шлюза	Интерфейс	Метрика

Таблица 5

Таблица ARP-кэша:		
IP-адрес	MAC-адрес	Тип

Создайте IP-калькулятор в табличном процессоре для облегчения формирования маски подсети.

1. Откройте табличный процессор и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1		1-й октет								2-й октет								3-й октет								4-й октет								
2	биты	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
3		ID-сети																													ID-узла		
4	IP-адрес	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
5		192								0								1								255							
6	Маска подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
7		255								255								255								248							

2. Далее необходимо ввести в ячейки **B5, J5, R5, Z5** формулы для перевода двоичного представления IP-адреса в точечную десятичную нотацию по октетам.

1. Введите в ячейку B5 формулу для преобразования 1-го октета IP-адреса в десятичную систему счисления:

```
=I4*2^I2+H4*2^H2+G4*2^G2+F4*2^F2+E4*2^E2+D4*2^D2+C4*2^C2+B4*2^B2
```

2. Скопируйте введенную формулу в остальные ячейки (**J5, R5, Z5**).

3. Самостоятельно введите в ячейки **B5, J5, R5, Z5** формулы для преобразования маски подсети из двоичного представления в точечную десятичную нотацию.

4. Сохраните файл в своей папке с именем **ipcalc**.

Кроме этого, необходимо определить используются ли в локальной сети серверы DNS, WINS, DHCP и если используются, указать их IP-адреса.

Контрольные вопросы

1. Что такое IP-адрес?
2. Структура IP-адреса?
3. Какие сетевые утилиты существуют?

Работа №4

Использование сетевых калькуляторов для расчета необходимого размера маски подсети и максимального количества сетевых устройств.

Создайте IP-калькулятор в табличном процессоре для облегчения формирования маски подсети.

2. Откройте табличный процессор и сформируйте таблицу по следующему шаблону:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1		1-й октет								2-й октет								3-й октет								4-й октет							
2	биты	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
3		ID-сети																													ID-узла		
4	IP-адрес	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1
5		192								0								1								255							
6	Маска подсети	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0
7		255								255								255								248							

3. Далее необходимо ввести в ячейки **B5, J5, R5, Z5** формулы для перевода двоичного представления IP-адреса в точечную десятичную нотацию по октетам.

2. Введите в ячейку B5 формулу для преобразования 1-го октета IP-адреса в десятичную систему счисления:

=I4*2^I2+H4*2^H2+G4*2^G2+F4*2^F2+E4*2^E2+D4*2^D2+C4*2^C2+B4*2^B2

5. Скопируйте введенную формулу в остальные ячейки (**J5, R5, Z5**).

6. Самостоятельно введите в ячейки **B5, J5, R5, Z5** формулы для преобразования маски подсети из двоичного представления в точечную десятичную нотацию.

7. Сохраните файл в своей папке с именем **ipcalc**.

Контрольные вопросы?

1. Что такое маска подсети?
2. Структура маски подсети?
3. Какие сетевые калькуляторы вы знаете?

Работа №5

Ограничение работы сервисов IP при прохождении пакетов через NAT. Принцип работы firewall'а и фильтрации пакетов.

Фильтры предназначены для блокирования/пропускания IP-пакетов в зависимости от протокола, параметров протокола и адресата пакета. Назначаются для адресов зарегистрированных в окне **Сетевые фильтры** . Однако если дополнительно не выполнять настройки фильтров, то Ваш компьютер будет защищен программой ViPNet Personal Firewall в рамках заданных по умолчанию режимов безопасности.

Для того, чтобы правильно выполнить настройки правил фильтрации, необходимо знать основные принципы осуществления фильтрации IP-пакетов в ViPNet:

- Правила фильтрации IP-трафика являются результатом действия выбранного режима безопасности и заданных пользователем списка фильтров для конкретных IP-адресов, протоколов и портов.

- Список сетевых фильтров задается пользователем в виде древовидной структуры в окне **Сетевые фильтры**. Это дерево фильтров позволяет задавать фильтры, как на отдельный IP-адрес, так и на диапазон IP-адресов (первый уровень); далее могут быть определены фильтры на типы протоколов, направление установления соединения (прохождения IP-пакетов) и номера портов (второй уровень).

- Настройку правил фильтрации IP-трафика (в окне **Сетевые фильтры**) всегда следует начинать с выбора режима безопасности, а затем при необходимости уточнять его заданием сетевых фильтров.

- Существуют автоматически создаваемые сетевые фильтры, которые можно модифицировать, но нельзя удалять: главные и широковещательные фильтры для окна **Сетевые фильтры** (определение фильтров см. ниже).

- **Применение (выполнение) фильтра** – параметры пакета анализируются на соответствие параметрам фильтра, при соответствии выполняется заданное фильтром правило: блокировать или пропускать, при несоответствии фильтр не оказывает никакого влияния на данный пакет. Фильтры применяются (выполняются) друг за другом в определенном порядке и результат их работы (блокировать или

пропускать) зависит от конкретного фильтра в конкретном месте его применения.

Ряд фильтров в ПО ViPNet Personal Firewall определен по умолчанию. Эти фильтры нельзя удалять, но можно менять: инвертировать, добавлять, удалять и модифицировать фильтры протоколов.

1. Широковещательный фильтр в окне **Сетевые фильтры** с именем **Широковещательные IP-пакеты** - определяет правило фильтрации для всех широковещательных пакетов. Широковещательные фильтры разрешают те широковещательные сообщения, которые необходимы для функционирования следующих служб:
    - Широковещательные пакеты nbname (порт 137) и nbdatagram (порт 138) предназначены для организации работы службы имен NETBIOS – определения имен компьютеров, входящих в Microsoft Network.
    - Широковещательные пакеты bootp (порты 67 и 68) предназначены для организации работы службы DHCP – получения компьютером IP-адреса при его загрузке.
    - Работа фильтров для широковещательных пакетов не зависит от настроек других фильтров.
2. Главный фильтр в окне **Сетевые фильтры** с именем **Все незарегистрированные IP-адреса** – определяет общее правило фильтрации для всех IP-пакетов, незарегистрированных в окне **Сетевые фильтры**. Смысл этого фильтра – установить общую настройку для незарегистрированных IP-адресов, **то есть u1086 отсутствующих в окне Сетевые фильтры**.
3. Индивидуальный фильтр - это фильтр для конкретных адреса или диапазона адресов в **Сетевые фильтры**.
4. Фильтр протоколов – определяет правило фильтрации пакетов в зависимости от протокола, параметров протокола, адресата пакета и направления прохождения IP-пакета, может быть настроен для широковещательного, главного и индивидуального фильтров. Фильтр протоколов всегда подчинен какому-либо фильтру из указанных выше.

Сетевые фильтры можно условно разделить на два уровня (Рис.1):

1. **Фильтры первого уровня** – к ним можно отнести фильтры под номерами 1, 2, 3. Каждый из таких фильтров может либо разрешать, либо запрещать прохождение IP-пакетов.

2. **Фильтры второго уровня** (добавленные фильтры)– к ним можно отнести фильтры протоколов под номером 4. Каждый из таких фильтров может быть включенным или выключенным (со значком).

Сетевые фильтры отображаются в виде древовидной структуры (Рис. 1). Фильтры второго уровня всегда подчинены фильтрам первого уровня.

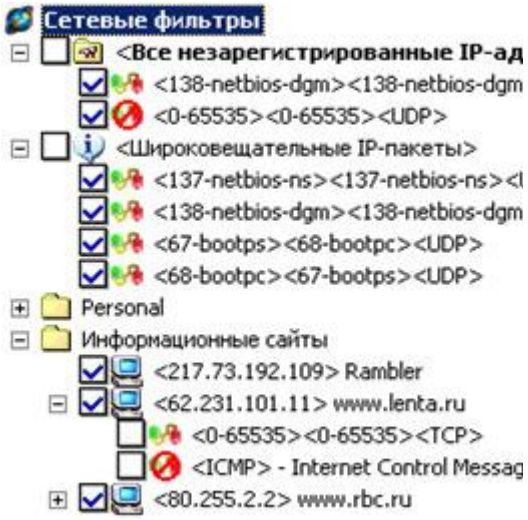


Рис. 1.

Наличие значка у какой-либо записи означает "пропускать пакеты". Наличие значка у какой-либо записи означает "блокировать пакеты".

Если фильтр первого уровня не содержит фильтров второго уровня, то наличие "галочки" напротив данного фильтра говорит о том, что фильтр пропускающий. Если "галочки" нет, то фильтр блокирующий.

Если фильтр первого уровня содержит фильтры второго уровня - фильтры протоколов, то наличие "галочки" напротив фильтра первого уровня говорит о том, что фильтр пропускает все IP-Фильтры второго уровня.

Фильтры первого уровня пакеты, удовлетворяющие фильтру первого уровня, кроме пакетов, явно указанных в фильтрах второго уровня (напротив фильтров протоколов второго уровня "галочки" отсутствуют). Если "галочка" напротив фильтра первого уровня отсутствует, то это означает, что фильтр блокирует все IP-пакеты, удовлетворяющие фильтру первого уровня, кроме пакетов, явно указанных в фильтрах

второго уровня (напротив фильтров протоколов второго уровня - присутствуют "галочки").

Чтобы изменить тип фильтра, например, с разрешающего (Рис. 2) на запрещающий (Рис. 3), необходимо щелкнуть левой кнопкой мыши на значке перед фильтром первого уровня (Рис. 2), и положительно ответить на заданный вопрос.

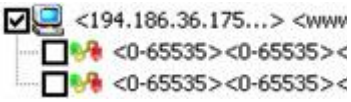


Рис. 2.

После этого значок перед фильтром первого уровня изменится на (Рис. 3). При этом автоматически инвертируется и установленный тип фильтров второго уровня (фильтров протоколов). Т.е. состояние аналогичного значка напротив фильтра второго уровня изменится на противоположное - (Рис. 3).

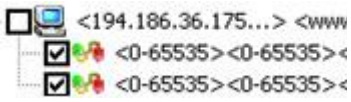


Рис. 3.

Исключение из описанных выше правил может возникнуть при регистрации фильтров из окна Блокированные пакеты. В этом случае возможно создание разрешающего фильтра второго уровня для разрешающего фильтра первого уровня либо запрещающего фильтра второго уровня для запрещающего фильтра первого уровня.

Если фильтр имеет два уровня, то сначала применяются подчиненные фильтры протоколов, а потом фильтр первого уровня (если пакет не соответствует условиям ни одного из подчиненных фильтров).

Фильтры протоколов, подчиненные одному и тому же фильтру первого уровня, всегда имеют один тип: либо пропускающий, либо блокирующий (всегда противоположный типу соответствующего фильтра первого уровня). Поэтому порядок их применения значения не имеет.

Любой фильтр протоколов может быть отключен. В этом случае в обработке пакетов он участвовать не будет, но запись об этом фильтре сохранится.

Работа фильтров настроенных в окне **Сетевые фильтры** зависит от установленного режима работы:

1. Если установлен 5-й режим, то пропускаются все пакеты вне зависимости от каких-либо установок фильтров.
2. Если установлен 1-й режим, то все пакеты блокируются.
3. Если установлен 4-й режим, то все пакеты пропускаются.
4. Если установлен 2-й или 3-й режим, то для широковещательных пакетов применяется **широковещательный фильтр** в окне ***Сетевые фильтры***, в результате применения которого пакет может быть либо заблокирован (событие 20), либо пропущен. Для не широковещательных пакетов фильтры в окне ***Сетевые фильтры*** применяются в порядке, **противоположном** их порядку расположения в этом окне:

- Самым первым работает индивидуальный фильтр для конкретного IP-адреса (если таковой для данного адреса настроен), от которого из сети поступил пакет, или по которому пакет ушел в сеть. В результате применения этого фильтра пакет может быть либо **заблокирован** (событие 20)**,** либо **пропущен**.
    - 1 Фильтр на этом рисунке означает: Все пакеты от и для этих адресов для всех протоколов, кроме протоколов казанных в добавленных фильтрах будут пропускаться.
    - 2 Фильтр на этом рисунке означает: Все пакеты от и для этих адресов для всех протоколов, кроме протоколов, указанных в добавленных фильтрах, будут блокироваться.
- Если пакет прошел вышеуказанный фильтр и по нему не было принято решения, то затем работает главный фильтр для всех незарегистрированных в окне ***Сетевые фильтры*** IP-адресов (фильтр ***Все незарегистрированные IP-адреса***). В результате применения этого фильтра пакет может быть **пропущен**.
- Затем, если установлен 2-й режим, то все остальные пакеты, по которым не было принято решение, блокируются (событие 21).
- Если установлен 3-й режим, то работает механизм бумеранга:

Все исходящие пакеты, по которым не было принято решение предыдущими фильтрами, пропускаются, при этом регистрируются протокол, адреса, время отправки пакета, а для "жёсткого бумеранга" – ещё и

параметры протоколов: для UDP и TCP – номера портов отправителя и получателя, для ICMP – тип сообщения.

Входящие пакеты, если пакет не был блокирован или пропущен предыдущими фильтрами, пропускаются только в случае, если выполняются следующие условия:

Было установлено специальное соединение (бумеранговое) с этим узлом. Установка этого соединения зависит от режима бумеранга:

Если бумеранг установлен в "мягкий" режим: входящие пакеты пропускаются в случае, если ранее на адрес источника прошел исходящий пакет этого же протокола.

Если бумеранг установлен в "жесткий" режим: входящие пакеты протоколов TCP и UDP пропускаются в случае, если ранее на адрес и конкретный порт источника от конкретного порта получателя прошел исходящий пакет этого же типа. Входящие пакеты протокола ICMP пропускаются, если они являются ответами на ранее отосланные ICMP-запросы на этот адрес.

Пары поддерживаемых ICMP- запросов и ответов следующие: echo – echo reply, timestamp – timestamp reply, information request – information reply.

С момента отправки соответствующего *исходящего* пакета или пропуска соответствующего *входящего* пакета от этого же адреса прошло не более 60 секунд.

Во всех остальных случаях пакет блокируется.

окне **Режимы** (Рис. 4).

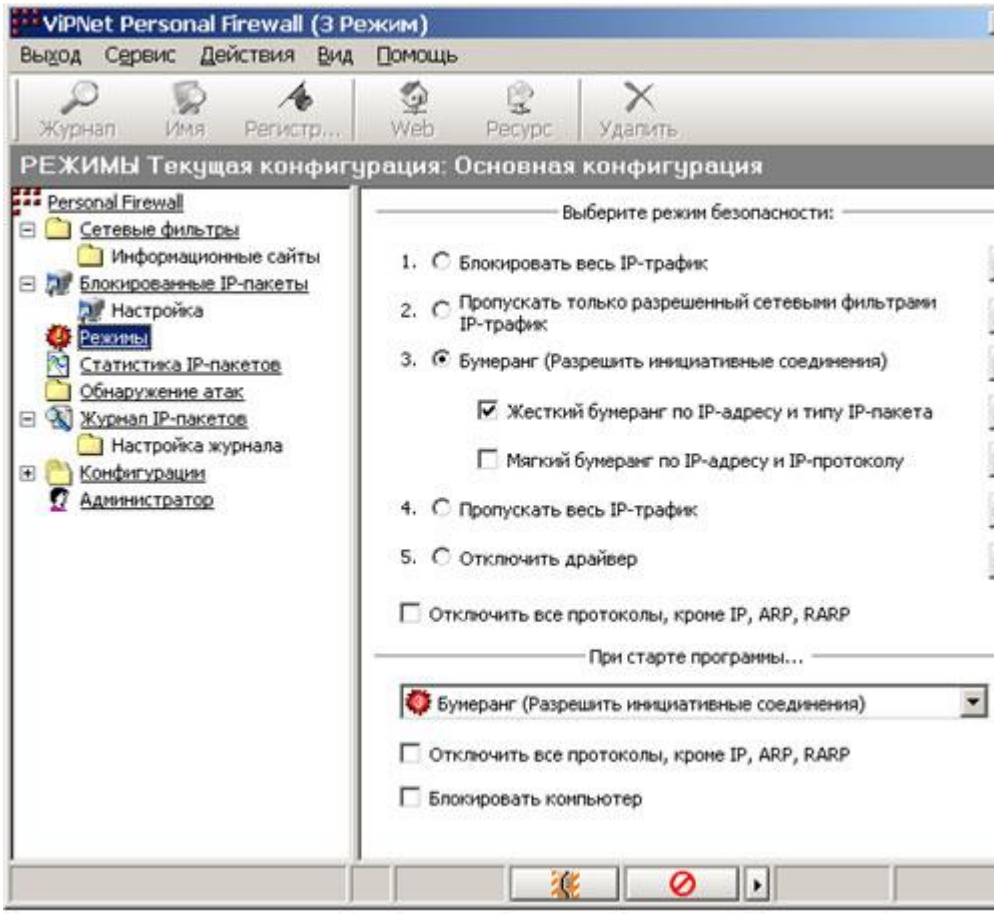


Рис. 4.

Для выбора режима, необходимо установить переключатель напротив нужного режима, а также выбрать этот режим из списка в разделе *При старте программы…* (Рис. 4). Изменения настроек вступают в силу немедленно.

Замечание: Если на Вашем компьютере установлена ОС Windows XP (SP 2 и выше), то при включении 4 или 5 режима Windows Security Center3 (если не отключены настройки оповещения) сообщит об отключении ViPNet Firewall (т.е. защиты Вашего компьютера программным обеспечением ViPNet).

Во всех режимах (кроме последнего – ***Режим №5***) ViPNet Personal Firewall осуществляет мониторинг и выявляет все попытки осуществления несанкционированных соединений, а также санкционированные соединения (определяется настройками), с отражением этой информации в соответствующих журналах IP-пакетов.

Режим работы программы можно также изменить с помощью меню, которое вызывается щелчком правой кнопки мыши на значке программы в области уведомлений на панели задач.

Сверху полужирным шрифтом будет выделен текущий режим. Чтобы его изменить следует поставить "галочку" напротив нужного.

Помимо задания режима безопасности в окне ***Режимы*** (Рис. 4) можно произвести ряд дополнительных настроек:

- ***Отключить все протоколы, кроме IP, ARP, RARP*** – по умолчанию опция выключена. При включении этой опции будут отключены сетевые протоколы IPX/SPX, NetBEUI из стека протоколов Microsoft, если они установлены в системе.
    - Можно произвести ряд настроек в разделе ***При старте программы*** ... (Рис. 4) , которые будут определять параметры работы программы ViPNet Personal Firewall сразу после ее старта:
- ***Отключить все протоколы, кроме IP, ARP, RARP*** - позволяет определить состояние одноименной опции (описана выше) после старта программы.
- ***Блокировать компьютер*** - позволяет блокировать доступ к рабочему столу компьютера после старта программы. Разблокировать доступ можно, введя пароль. По умолчанию опция выключена.

ViPNet Personal Firewall может быть установлен в один из нижеперечисленных режимов безопасности:

Рассмотрим основные режимы безопасности.

1 режим – Блокировать весь IP-трафик

Это режим абсолютной защиты Вашего компьютера и эквивалентен отключению компьютера от внешней сети и работе его в автономном режиме. Работайте в этом режиме, если Вам не требуется сеть. В этом режиме весь IP-трафик (входящий и исходящий), независимо от настроек в окне ***Сетевые фильтры,*** полностью блокируется. Никакие атаки на Ваш компьютер невозможны. Доступ к ресурсам Локальной сети и Интернет, а также доступ к Вашему компьютеру с их стороны также невозможны.

2 режим – Пропускать только разрешенный сетевыми фильтрами IP-трафик

По умолчанию в этом режиме трафик полностью блокируется, за исключением нескольких разрешенных по умолчанию протоколов для широковещательных пакетов. Рекомендуется периодически включать этот

режим для выявления несанкционированных Вами попыток компьютера установить соединения с неизвестными адресами. Если в окне ***Блокированные пакеты*** появится информация о таких исходящих пакетах, то зарегистрируйте эти адреса в режиме их блокировки. Тогда и в режиме Бумеранг работа попавших к Вам на компьютер программ, излучающих несанкционированный трафик, будет нейтрализована. В этом режиме также обеспечивается фильтрация трафика в соответствии с заданными настройками фильтров в окне ***Сетевые фильтры***. Рекомендуется также использовать этот режим, если:

На данном компьютере устанавливается какой-либо сервер, и нет необходимости устанавливать соединения по инициативе этого компьютера. В этом случае Вы должны в фильтре для ***Всех незарегистрированных IP-адресов*** добавить фильтр, разрешающий, например работу WEB-сервера на этом компьютере. Требуется ограничить перечень других компьютеров, например, WEB - серверов, с которыми Вы желаете работать. В этом случае Вы должны в окне ***Сетевые фильтры*** зарегистрировать конкретные адреса этих WEB - серверов с фильтром, разрешающим работу с WEB - серверами. Вы можете в этом режиме настраивать, при необходимости, фильтры как для незарегистрированных адресов, так и для зарегистрированных IP-адресов. При этом настройки фильтров для незарегистрированных адресов действуют только для адресов отсутствующих в окне ***Сетевые фильтры***. А для зарегистрированных адресов действуют собственные настройки фильтров.

3 режим - Бумеранг Предназначен для обеспечения работы компьютера в локальной или **(Разрешить инициативные соединения)** глобальной сети (например, Интернет) с внешними ресурсами. Бумеранг - это оптимальный режим защиты. При этом обеспечивается защита от любых видов атак, в том числе от инициализации различных "троянских коней". "Троянский конь" - это, как правило, программа-сервер, каким-либо образом попавшая на Ваш компьютер и ожидающая, когда *Злоумышленник* попытается с ней соединиться для нанесения вреда Вашему компьютеру. Но все попытки *Хакера* установить соединение с программой - "трояном" будут блокированы, и программа не сможет нанести Вам вреда.

Режим Бумеранга устанавливается по умолчанию после установки программы и является наиболее безопасным при необходимости работы с внешними ресурсами. При работе в этом режиме в локальной или глобальной сети Вы сможете получить доступ к внешним ресурсам, тогда как на Ваш

компьютер, в независимости от настроек Windows, доступ оттуда получить невозможно.

Существует два режима Бумеранга:

1. **Жесткий бумеранг по IP-адресу и типу IP-пакета**

Это режим Бумеранга (устанавливается по умолчанию), в котором анализ поступающей во время соединения информации производится по большому числу параметров (адрес, протокол, порт). Поэтому атаки на Ваш компьютер практически невозможны, даже с компьютера, с которым Вы соединились.

2. **Мягкий бумеранг по IP-адресу и IP-протоколу**

Мягкий режим – анализ поступающей во время соединения информации производится по меньшему числу параметров (адрес, протокол). Поэтому данный режим менее безопасен, и его рекомендуется включать только в случае необходимости.

4 режим – Пропускать весь IP-трафик

В этом режиме защита снята, и Ваш компьютер полностью открыт для доступа извне. Фильтрация трафика не производится. Режим предназначен только для временного включения при отладочных работах. В этом режиме ведется журнал трафика IP-пакетов.

5 режим – Отключить драйвер

Защита снята, и Ваш компьютер полностью открыт для доступа извне.

Фильтрация трафика не производится. Режим предназначен только для временного включения при отладочных работах. В этом режиме не ведется журнал трафика IP-пакетов.

В окне ***Сетевые фильтры*** Вы можете настроить правила фильтрации пакетов сразу для всех IP-адресов, (фильтр ***Все незарегистрированные IP-адреса***), правила фильтрации широковещательных пакетов для всех IP-адресов (фильтр ***Широковещательные IP-пакеты***), а также индивидуальные правила фильтрации для определенных IP-адресов.

При этом настройки фильтров для конкретных адресов имеют больший приоритет, то есть они отменяют общие настройки главного фильтра ***Все незарегистрированные IP-адреса***.

Для настройки уже имеющихся в окне ***Сетевые фильтры*** правил фильтрации, в зависимости от потребностей, можно настроить только фильтр первого уровня (разрешить, либо запретить прохождение IP-пакетов), либо добавить к нему еще фильтр(ы) второго уровня (фильтры протоколов). Настройте тип фильтра первого уровня, а затем, при необходимости добавьте фильтр второго уровня:

Настройка фильтров протоколов происходит в окне ***Фильтр протоколов***, которое вызывается по кнопке **Фильтр протоколов** из окна ***Правило доступа***, а также непосредственно из окна ***Сетевые фильтры*** по пункту **Правила доступа -> Добавить**

Фильтр протоколов при использовании меню по правой кнопке мыши, находясь на какой-либо записи из окна ***Сетевые фильтры***.

Добавлять правила фильтрации пакетов для IP-адресов в окне ***Сетевые фильтры*** можно несколькими способами:

1. Добавление правил фильтрации по сетевому имени или URL. Для этого нужно воспользоваться пунктом ***Правила доступа -> Добавить правило…*** в открывающемся меню по правой кнопке мыши, находясь на строке ***Сетевые фильтры*** в правой части окна или на строке с названием какой-либо папки. Появится окно ***Правило доступа*** (Рис. 5).

В строке ***Имя компьютера*** (Рис. 5) наберите URL (например, имя web-сайта, ftp) или сетевое имя компьютера, для которых Вы хотите создать правило доступа, и нажмите кнопку **OK** или клавишу ENTER. Откроется окно поиска и произведётся поиск IP-адресов. Если адреса определятся, то они появятся в окне ***IP-адрес***. Далее Вам необходимо выбрать, ***разрешить*** работу с этим(и) IP-адресом(ами) или ***блокировать***. Для этого установите переключатель в соответствующее положение (Рис. 5). Вы можете дать название созданному правилу в строке ***Псевдоним***.

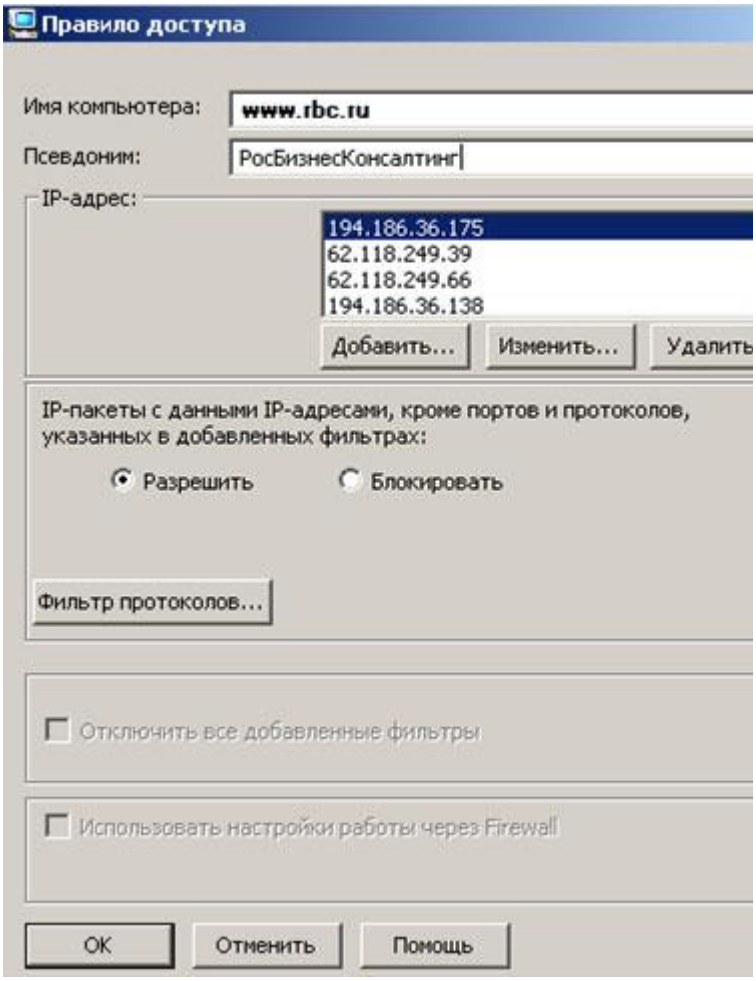


Рис. 5.

При необходимости добавьте фильтры протоколов (по кнопке **Фильтр протоколов** …). Для сохранения нажмите кнопку **OK**.

2. Добавление правил фильтрации по IP-адресу или диапазону IP-адресов. Если IP-адрес или диапазон IP-адресов, для которых Вы хотите создать правило фильтрации, известен, то в этом случае есть возможность сразу внести его в поле ***IP-адрес*** в окне ***Правило доступа***. Для этого по пункту меню ***Правила доступа -> Добавить правило…*** по правой кнопке мыши, находясь на строке ***Сетевые фильтры*** в правой части окна или на строке с названием какой-либо папки вызывается окно ***Правило доступа***. В этом окне нужно нажать на кнопку **Добавить** (Рис. 6) и в появившемся меню вручную ввести IP-адрес или диапазон адресов, после чего нажать кнопку **OK** . Далее Вам необходимо выбрать, ***разрешить*** работу с этим(и) IP-адресом(ами) или ***блокировать***. Для этого установите переключатель в соответствующее положение (Рис. 6). Вы можете дать название созданному правилу в строке ***Псевдоним***.

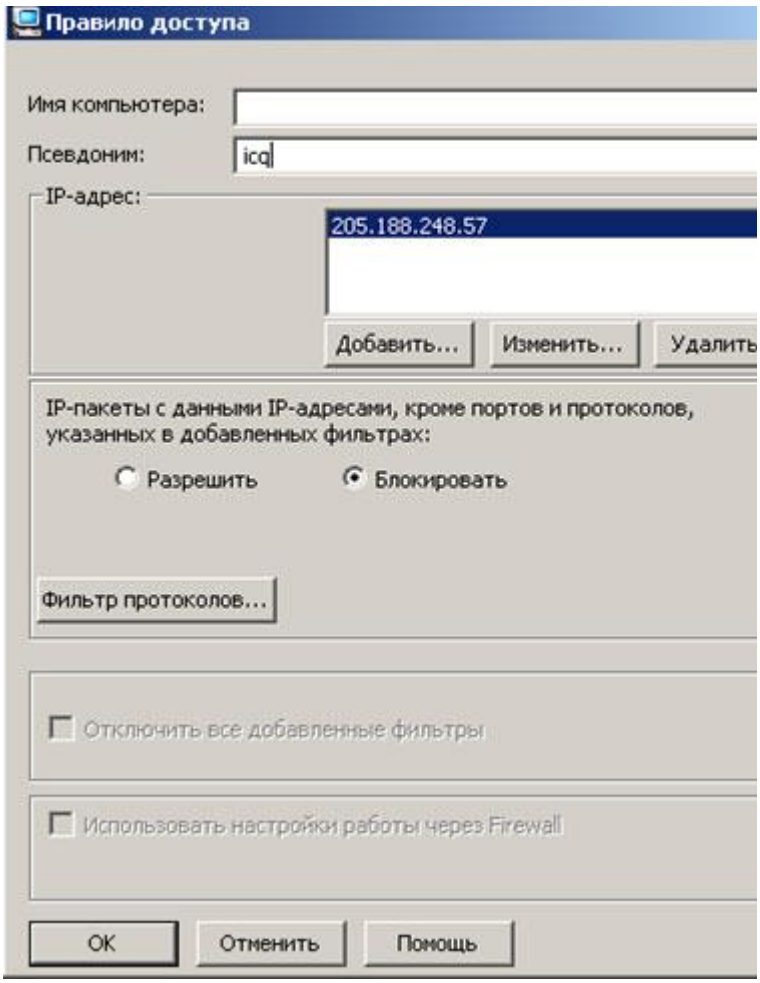


Рис. 6.

При необходимости добавьте фильтры протоколов (по кнопке **Фильтр протоколов** …). Для сохранения нажмите кнопку **OK**..

3. Добавление правил фильтрации на основе IP-адресов и параметров IP-пакетов, заблокированных программой и отображенных в окне ***Блокированные IP-пакеты***. Вся информация о правилах добавленных любым из вышеперечисленных способов, появится в окне ***Сетевые фильтры*** (Рис. 1). Вы можете настроить фильтры протоколов для каждой записи об IP-адресе, используя пункт меню ***Правила доступа -> Добавить фильтр протоколов***, открывающегося по правой кнопке мыши, находясь на строке с требуемой записью (Рис. 1).

Настройки производятся в окне **Обнаружение Атак** (Рис. 7). В этом окне можно осуществить настройки для системы обнаружения атак (intruder detection system, IDS). Это система служит для обнаружения и предотвращения таких действий со стороны злоумышленника («хакера» либо «взломщика»), которые могут привести к проникновению внутрь Вашей

операционной системы (ОС), либо совершению по отношению к ней каких-либо злоупотреблений.

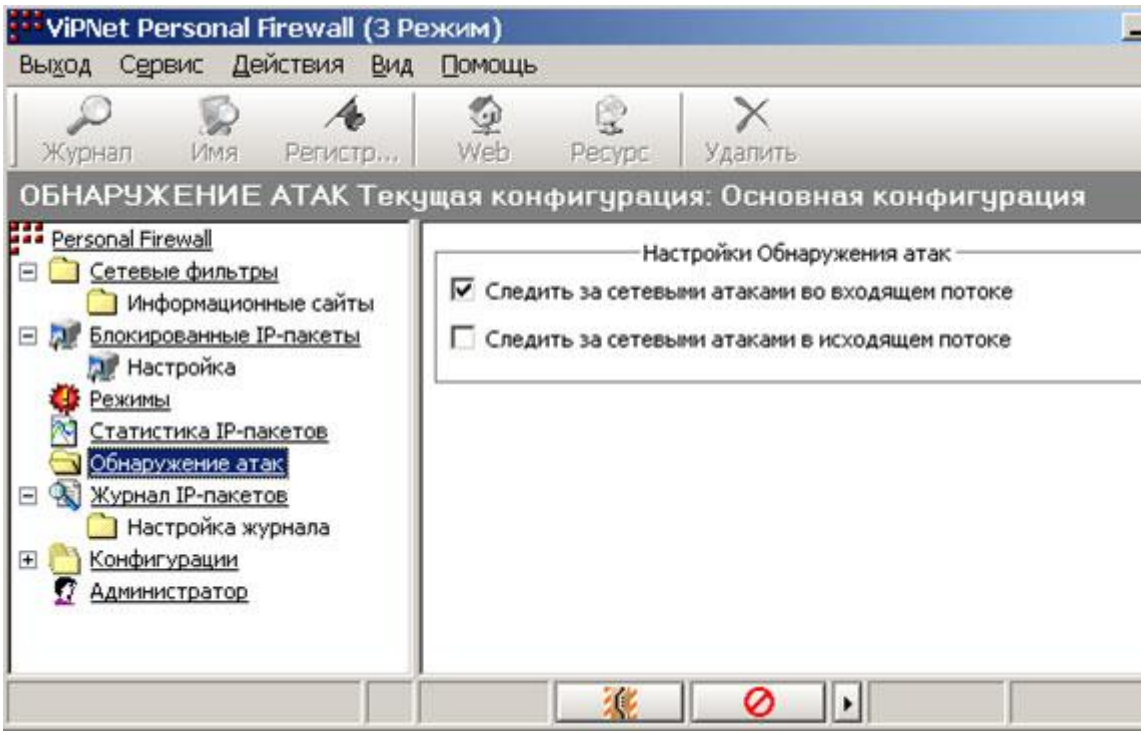


Рис. 7.

Система обнаружения атак работает на сетевом уровне, благодаря чему имеет ряд достоинств:

- Возможность обнаруживать и блокировать сетевые пакеты до обработки их стеком TCP/IP и этим защищать стек от атак на него самого (такие атаки, как WinNuke).
- Возможность блокировать на ранней стадии атаки, направленные на перегрузку ОС, приводящие к отказу от обслуживания (например, jolt2 (CAN-2000-0305)).
- В случае установки IDS на шлюз, возможность контроля сразу всех компьютеров, находящихся за этим шлюзом.

Кроме того, IDS способна обнаруживать исходящие атаки (как если бы злоумышленник находился за Вашим компьютером). Это полезно в том случае, если Ваша ОС каким-либо образом была скомпрометирована (например, с помощью программ – троянских коней) и после используется злоумышленником в качестве атаки на какую-либо третью ОС.

Настройки обнаружения атак осуществляются с помощью включения или выключения следующих опций в окне *Обнаружение атак*:

- **Следить за сетевыми атаками во входящем потоке** – по умолчанию опция включена, то есть программа проверяет на сетевые атаки весь входящий трафик Вашего компьютера. Рекомендуем не выключать эту опцию, поскольку при ее выключении программа перестает следить за сетевыми атаками во входящем потоке, и Ваш компьютер может быть атакован.

- **Следить за сетевыми атаками в исходящем потоке** – по умолчанию опция включена. При ее включении программа будет проверять также весь исходящий трафик от Вашего компьютера.

В случае если программа обнаружит пакет, отвечающий условиям одной из типовых атак, он будет заблокирован. Чтобы убедиться, что параметры блокированного пакета соответствуют признакам известных сетевых атак, нужно отобразить для него **Журнал регистрации IP-пакетов**, где в поле **Событие** будет указана причина блокировки в виде номера события и названия возможной атаки. Описание обнаруживаемых атак находится в таблице. Для просмотра журнала регистрации IP-пакетов в окне **Журнал IP-пакетов** в списке **Событие** выберите **События системы обнаружения вторжений** и нажмите **Найти**.

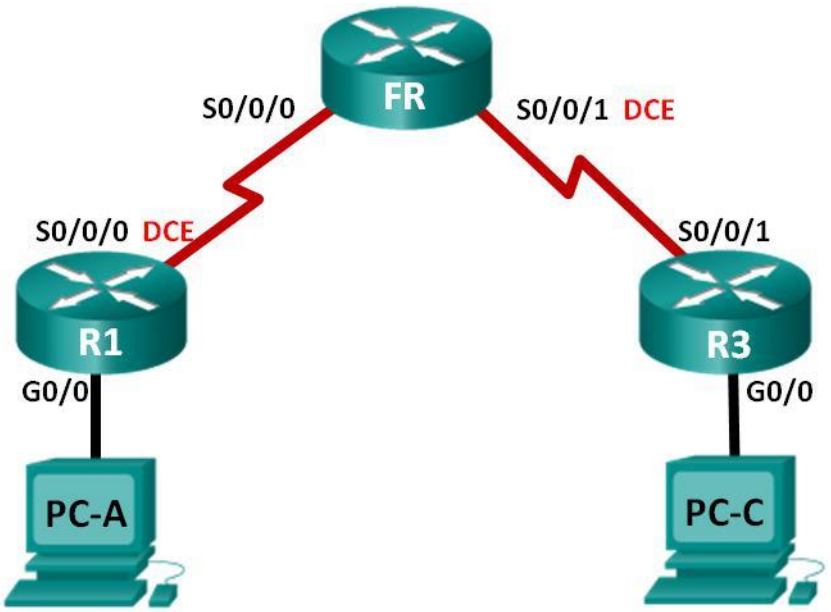
Контрольные вопросы

1. Правила фильтрации IP-трафика?
2. Список сетевых фильтров?
3. Как осуществляется выбора режима безопасности.
4. Какие автоматически создаваемые сетевые фильтры вы знаете?

Работа №6

Построение глобальных сетей передачи данных на основе протокола Frame Relay. Работа коммутаторов Frame Relay.

Топология



Задачи

1. Создание сети и настройка базовых параметров устройств

2. Настройка коммутатора Frame Relay

3. Настройка базового протокола Frame Relay Часть

4. Отладка Frame Relay

5. Настройка подынтерфейса Frame Relay

Исходные данные/сценарий

Frame Relay — это высокопроизводительный протокол глобальной сети, который работает на физическом и канальном уровнях эталонной модели OSI. В отличие от выделенных линий, для обеспечения связи по

протоколу Frame Relay между узлами , подключёнными к одному и тому же провайдеру, требуется только один канал доступа от узла к провайдеру.

Протокол Frame Relay был одним из самых широко используемых протоколов WAN. Основной причиной этого была относительно невысокая стоимость подключения по сравнению с выделенными линиям. Кроме того, в сети Frame Relay очень просто настраивается оборудование пользователя. С появлением таких услуг широкополосного доступа, как DSL и кабельный модем, GigaMAN (сервис Ethernet «точка-точка» по оптоволоконному кабелю), VPN и MPLS («Multiprotocol Label Switching», многопротокольная коммутация по меткам), технология Frame Relay стала менее приемлемым решением для доступа к глобальной сети. Однако в некоторых сельских местностях нет доступа к этим альтернативным решениям, и там для соединения с глобальной сетью по-прежнему используют Frame Relay.

1: Построение сети и базовая настройка устройств

Вам предстоит настроить топологию сети и сделать базовую настройку устройств.

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

Шаг 2: Выполните запуск и перезагрузку маршрутизаторов.

Шаг 3: Произведите базовую настройку маршрутизаторов.

a. Отключите поиск DNS.

b. Настройте имена устройств в соответствии с топологией.

c. Назначьте **class** в качестве пароля привилегированного режима.

d. Назначьте **cisco** в качестве пароля консоли и виртуального терминала VTY и включите запрос пароля при подключении.

e. Настройте **logging synchronous** на линии консоли.

f. Зашифруйте пароли.

g. Настройте баннер MOTD (сообщение дня) для предупреждения пользователей о запрете несанкционированного доступа.

h. Для всех последовательных интерфейсов DCE установите тактовую частоту **128000**.

i. Настройте для всех интерфейсов адреса IPv4 и IPv6, перечисленные в таблице адресации. На данном этапе не активируйте последовательные интерфейсы.

j. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте узлы.

Адреса ПК можно посмотреть в таблице адресации.

Шаг 5: Проверьте связь.

На этом этапе ПК не могут отправлять друг другу эхо-запросы, но должны успешно отправлять эхо-запросы на свои шлюзы по умолчанию. Проверьте оба протокола, IPv4 и IPv6. При неудачном выполнении эхо-запросов выполните поиск и устранение неполадок.

2: Настройка коммутатора Frame Relay

Вам предстоит настроить коммутатор Frame Relay. Вы создадите постоянные виртуальные каналы (PVC) и назначите идентификаторы DLCI (Data Link Connection Identifier — идентификатор соединения канального уровня). В процессе этой настройки создаётся два канала PVC: один от R1 к R3 (DLCI 103) и один от R3 к R1 (DLCI 301).

Шаг 1: Настройте маршрутизатор FR в качестве коммутатора Frame Relay.

Команда **frame-relay switching** глобально активирует коммутацию Frame Relay на маршрутизаторе, что позволяет ему перенаправлять кадры на основе DLCI входящего канала, а не на основе IP-адреса.

FR(config)# **frame-relay switching**

Шаг 2: Измените инкапсуляцию на интерфейсе S0/0/0.

Измените тип инкапсуляции интерфейса на Frame Relay. Подобно HDLC и PPP, Frame Relay является протоколом канального уровня, который определяет формирование кадров для трафика уровня 2.

FR(config)# **interface s0/0/0**

FR(config-if)# **encapsulation frame-relay**

Шаг 3: Измените тип интерфейса на DCE.

Изменение типа интерфейса на DCE означает, что маршрутизатор должен отправлять сообщения LMI keepalive и что разрешено применять команды route протокола Frame Relay.

Примечание. Не требуется, чтобы типы интерфейсов Frame Relay соответствовали типу используемого физического интерфейса. Физический последовательный интерфейс DTE может выступать в качестве интерфейса DCE Frame Relay, а физический интерфейс DCE может выступать в качестве логического интерфейса DTE Frame Relay.

FR(config)# **interface s0/0/0**

FR(config-if)# **frame-relay intf-type dce**

Шаг 4: Настройте DLCI.

Настройте маршрутизатор для перенаправления трафика, входящего по интерфейсу S0/0/0

с идентификатором DLCI 103, на интерфейс S0/0/1 по исходящему каналу с идентификатором DLCI 301.

FR(config-if)# **frame-relay route 103 interface s0/0/1 301** FR(config-if)# **no shutdown**

Шаг 5: Настройте Frame Relay на интерфейсе S0/0/1.

FR(config)# **interface s0/0/1**

FR(config-if)# **encapsulation frame-relay**

```
FR(config-if)# frame-relay intf-type dce

FR(config-if)# frame-relay route 301 interface s0/0/0 103

FR(config-if)# no shutdown
```

Шаг 6: Проверьте настройку Frame Relay.

a. Для проверки правильности настройки Frame Relay используйте команду **show frame-relay pvc**.

FR# **show frame-relay pvc**

PVC Statistics for interface Serial0/0/0 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	0	1	0	0
Unused	0	0	0	0

DLCI = 103, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/0

input pkts 0 output pkts 0 in bytes 0

out bytes 0 dropped pkts 0 in pkts dropped 0

out pkts dropped 0 out bytes dropped 0

in FECN pkts 0 in BECN pkts 0 out FECN pkts 0

out BECN pkts 0 in DE pkts 0 out DE pkts 0

out bcast pkts 0 out bcast bytes 0

30 second input rate 0 bits/sec, 0 packets/sec

30 second output rate 0 bits/sec, 0 packets/sec

switched pkts 0

Detailed packet drop counters:

no out intf 0 out intf down 0 no out PVC 0

in PVC down 0 out PVC down 0 pkt too big 0

shaping Q full 0 pkt above DE 0 policing drop 0

connected to interface Serial0/0/1 301

pvc create time 00:00:53, last time pvc status changed 00:00:53

PVC Statistics for interface Serial0/0/1 (Frame Relay DCE)

	Active	Inactive	Deleted	Static
Local	0	0	0	0
Switched	0	1	0	0
Unused	0	0	0	0

DLCI = 301, DLCI USAGE = SWITCHED, PVC STATUS = INACTIVE, INTERFACE = Serial0/0/1

input pkts 0 output pkts 0 in bytes 0

out bytes 0 dropped pkts 0 in pkts dropped 0

out pkts dropped 0 out bytes dropped 0

in FECN pkts 0 in BECN pkts 0 out FECN pkts 0

```
out BECN pkts 0          in DE pkts 0            out DE pkts 0

out bcast pkts 0         out bcast bytes 0

30 second input rate 0 bits/sec, 0 packets/sec

30 second output rate 0 bits/sec, 0 packets/sec

switched pkts 0

Detailed packet drop counters:

no out intf 0            out intf down 0         no out PVC 0

in PVC down 0            out PVC down 0          pkt too big 0

shaping Q full 0         pkt above DE 0          policing drop 0

connected to interface Serial0/0/0 103


pvc create time 00:00:16, last time pvc status changed 00:00:16
```

b. Выполните команду **show frame-relay route**. Это маршрут уровня 2, по которому трафик Frame Relay проходит через сеть. (Не следует его путать с IP-маршрутизацией уровня 3.)

```
FR# show frame-relay route


Input Intf      Input Dlci      Output Intf     Output Dlci     Status

Serial0/0/0     103             Serial0/0/1     301             inactive

Serial0/0/1     301             Serial0/0/0     103             inactive
```

Контрольные вопросы

1. Что такое протокол Frame Relay?
2. Недостатки и преимущества данного протокола?
3. Основные шаги построения сети по данному протоколу?

Работа №7

Возможности обеспечить приоретизацию трафика на физическом, канальном, сетевом и прикладном уровнях в сетевых устройствах.

Понятие качества обслуживания трафика Quality of Service (QoS).

Принципы передачи мультимедийной информации в инфокоммуникационных сетях. Механизмы реализации QoS.

Обеспечение приоретизации трафика на физическом, канальном, сетевом и прикладном уровнях в сетевых устройствах

Понятие качества обслуживания трафика Quality of Service (QoS).

В настоящее время вместе с планомерным увеличением скоростей передачи данных в инфокоммуникациях увеличивается доля интерактивного трафика, крайне чувствительного к параметрам среды транспортировки. Поэтому задача обеспечения качества обслуживания (*Quality of Service - QoS*) становится все более актуальной.

Качество – совокупность характеристик объекта, которые имеют отношение к его возможности удовлетворять установленные и предполагаемые потребности.

Примечание. Характеристики должны поддаваться экспериментальной оценке и/или измерению. Когда характеристики определены, они становятся параметрами и выражаются метриками.

Обслуживание – это набор функций, предоставляемых пользователю организацией.

Качество обслуживания (***Quality of Service - QoS***) – способность сети обеспечить необходимый сервис заданному трафику в определенных технологических рамках (пределах).

Примечание 1. Конфигурация, показанная выше, относится к обычному обслуживанию при наличии пользователей на каждом конце соединения. Однако принцип этой конфигурации может применяться в случае предоставления услуг, когда поставщик услуг находится на одном конце, а пользователь(и) – на другом конце.

Примечание 2. – Оконечное оборудование: различное качество оконечного оборудования может оказывать влияние на сквозное QoS.

Примечание 3. – Сеть доступа: влияние сети доступа на сквозное QoS зависит от сочетания среды доступа и технологии (например, беспроводной, кабельной, АЦАЛ и др.), используемой для предоставления конкретной услуги.

Примечание 4. – Базовая сеть: базовая сеть может принадлежать одному оператору или быть соединением сетей различных операторов. Влияние QoS базовой сети на сквозное качество будет определяться влиянием отдельных сетевых компонентов (принадлежащих одному или нескольким операторам); используемой технологии (цифровое мультиплексирование, IP и пр.); среды передачи (эфир, оптический или медный кабель) и другими факторами.

Задача: обеспечить заданное качество обслуживания в сквозном соединении (end-to-end) для различных видов трафика.

Условие: заданное качество обслуживания должны поддерживать все сетевые устройства на всем сквозном соединении

Для определения конечного QoS необходимо указать заданные *условия работы*, при которых обеспечивается предоставление услуги после установления связи (без установления соединения или ориентированного на соединение). При заданном наборе определенных условий работы качество обслуживания QoS может также изменяться под влиянием условий среды, таких как трафик и маршрутизация.

Качество обслуживания QoS включает показатели работы сети (ПРС) и показатели, не относящиеся к работе сети. Примерами ПРС являются *коэффициент ошибок по битам*, *запаздывание* и др., а примерами показателей, не относящихся к работе сети, – время предоставления, длительность ремонта, диапазон тарифов и время разрешения жалоб. Список критериев QoS для конкретной услуги будет зависеть от услуги, и их значение может изменяться в зависимости от сегментов совокупности абонентов.

Меры по обеспечению QoS

— Увеличение полосы пропускания

— Задание приоритетов данных

— Организация очередей

— Предотвращение перегрузок

— Формирование трафика

Архитектура QoS

— Средства QoS узла сети , выполняющие обработку поступающего в узел трафика в соответствии с требованиями качества обслуживания

— Протоколы QoS- сигнализации для координации работы сетевых элементов по поддержке качества обслуживания «из-конца-в-конец»

— Централизованные функции политики управления и учета QoS, позволяющие администраторам сети централизованно воздействовать на сетевые элементы для разделения ресурсов сети между различными видами трафика с требуемым уровнем QoS

Задания

1. Отразить на рисунке сквозное QoS, определяемое вкладами компонентов.

2. Обеспечить заданное качество обслуживания в сквозном соединении (end-to-end) для различных видов трафика. Условие: заданное качество обслуживания должны поддерживать все сетевые устройства на всем сквозном соединении.

Контрольные вопросы

1. Что такое качество обслуживания трафика?
2. Меры обеспечения качества QoS?
3. Архитектура QoS?

Библиографический список

1. Моделирование систем [Текст] : учебное пособие / И. А. Елизаров [и др.]. - Старый Оскол : ТНТ, 2013. – 136 с.

2. Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы [Текст] : учебное пособие / Е. А. Богданова [и др.]. - М. : Национальный Открытый Университет "ИНТУИТ", 2013. – 743 с.

1. Технологии коммутации и маршрутизации в локальных компьютерных сетях [Текст] : учебное пособие / под общ.ред. А. В. Пролетарского. - Москва : Изд - во МГТУ им. Н. Э. Баумана, 2013. - 389, [3] с.

2. Отечественные телекоммуникационные системы [Текст] : учебное пособие для вузов / Ю. К. Шарипов, В. К. Кобляков. - 3-е изд., перераб. и доп. - М. : Логос, 2005. – 832 с.

3. Системы и сети передачи информации [Электронный ресурс] : учебное пособие / Ю. Ю. Громов, И. Г. Карпов, Г. Н. Нурутдинов. - Тамбов : Издательство ФГБОУ ВПО «ТГТУ», 2012. - 128 с. – Режим доступа: biblioclub.ru