

Руководство по эксплуатации маршрутизатора SG-16R

Руководство по эксплуатации маршрутизатора SG-16R

Copyright © 2007 Сигранд

Содержание

1. Программное обеспечение маршрутизатора	1
Загрузчик	1
Обновление прошивки маршрутизатора	2
Установка программ	6
2. Управление маршрутизатором	7
Начало работы	7
Конфигурация с помощью Веб-интерфейса	7
Конфигурация через консольный интерфейс	9
Сводная информация	10
Логирование событий	10
Настройка встроенного Ethernet коммутатора	11
Установление зависимостей SHDSL - Ethernet	12
Сохранение/восстановление конфигурации	13
3. Настройка сетевых интерфейсов	14
Общие параметры	14
Вкладка Status	14
Вкладка General	15
Вкладка Method	16
Вкладка Options	16
Вкладка Specific	17
Работа с динамическими интерфейсами	17
Конфигурация интерфейса E1	18
Настройка параметров интерфейса	18
Настройка сетевых параметров	20
Настройка работы SHDSL модемов в режиме Bonding	21
Настройка моста	24
4. Настройка сетевых служб	27
DHCP-сервер	27
PPTP-сервер	29
Сервер DNS	32
5. Управление трафиком	37
Добавление сетевых маршрутов	37
Управление фаерволом	39
NAT	42
Качество обслуживания	45

Список иллюстраций

2.1. Главная страница	7
2.2. Смена пароля	8
2.3. Смена имени маршрутизатора	8
2.4. Синхронизация времени	8
2.5. Настройка DNS	9
2.6. Логирование	11
2.7. Конфигурация коммутатора	12
2.8. Сохранение конфигурации	13
2.9. Восстановление конфигурации	13
3.1. Сетевые параметры	14
3.2. Сетевые маршруты	14
3.3. Таблица ARP	14
3.4. Встроенный коммутатор	15
3.5. Шейпер трафика	15
3.6. Вкладка General	15
3.7. Вкладка Method	16
3.8. Вкладка Options	16
3.9. Вкладка Specific	17
3.10. Создание динамического интерфейса	17
3.11. Удаление динамического интерфейса	18
3.12. Выбор протокола	18
3.13. Конфигурация CISCO-HDLC	19
3.14. Unframed mode	20
3.15. Настройка интерфейса	20
3.16. Настройка параметров линии связи	22
3.17. Настройка интерфейса	22
3.18. Создание виртуального интерфейса	23
3.19. Активация виртуального интерфейса	23
3.20. Присвоение IP-адреса	23
3.21. Привязка к физическим интерфейсам	24
3.22. Пример моста	24
3.23. Пример моста с объединением интерфейсов	24
3.24. Создание интерфейса	25
3.25. Добавленный интерфейс br0	25
3.26. Установка метода присвоения IP-адреса	25
3.27. Установка IP-адреса	26
3.28. Определение интерфейсов	26
3.29. Активация моста	26
4.1. Настройка DHCP-сервера	27
4.2. Список статических IP-адресов	28
4.3. Форма привязки IP к MAC	28
4.4. Обновленный список IP-адресов	29
4.5. Конфигурация RPTP-сервера	30
4.6. Пользователи VPN-сервера	31
4.7. Добавление нового пользователя	32
4.8. Настройка сервера DNS	32
4.9. Зоны сервера DNS	33
4.10. Добавление зоны	34
4.11. Добавление записи в зону	35
4.12. Записи зоны DNS	36
5.1. Пример: структура сети	37
5.2. Пустой список маршрутов	38
5.3. Добавление маршрута	38
5.4. Список маршрутов	38
5.5. Удаление маршрута	39

5.6. Активация фаервола	39
5.7. Политики цепочек	39
5.8. Цепочка FORWARD	40
5.9. Цепочка INPUT	40
5.10. Цепочка OUTPUT	41
5.11. Добавление правила	41
5.12. Цепочка PREROUTING	42
5.13. Цепочка POSTROUTING	43
5.14. Политики цепочек	43
5.15. Добавление правила	44
5.16. Пример сети	45

Список таблиц

2.1. Сводная таблица	10
----------------------------	----

Глава 1. Программное обеспечение маршрутизатора

Загрузчик

Меню загрузчика доступно при подключении к маршрутизатору по последовательному интерфейсу. После включения питания, на экран будет выведено предложение войти в меню загрузчика. Для этого вам необходимо 3 раза быстро нажать на клавишу пробела.

```
ADM5120 Boot:
```

```
Copyright 2007 Sigrand, Inc.  
CPU: Infineon 5120-175MHz  
SDRAM: 64MB  
Flash: NAND-32MB  
Boot System: Linux-5120  
Loader Version: 1.00.03  
Creation Date: 17.04.2007
```

```
Press <space> key tree times to enter boot menu..  
3
```

Если вы трижды нажали на пробел, то выведется меню загрузчика

```
Sigrand MR16 router:  
=====  
Bootloader Menu  
[1] Xmodem Download  
[2] TFTP Download  
[3] Print Boot Params  
[4] Set Boot Params  
[5] Check flash  
[6] Exit  
  
Please enter your number:
```

В этом меню доступны несколько действий:

- Xmodem Download - обновление загрузчика или системы через последовательный порт по протоколу Xmodem. Данный способ обновления занимает много времени.
- TFTP Download - обновление системы или загрузчика с помощью TFTP сервера.
- Print Boot Params - показывает сетевые параметры загрузчика, основные - мак адрес и IP-адрес.
- Set Boot Params - установка сетевых параметров для загрузки. Подробнее эти параметры рассмотрены в разделе "Обновление прошивки маршрутизатора".
- Check flash - проверка флэш-памяти маршрутизатора на наличие поврежденных блоков.

Чтобы проверить маршрутизатор на наличие поврежденных блоков, переходим в меню Check flash:

```
Please enter your number:5
Flash Client Menu
=====
[P]: Print existent bad blocks
[S]: Scan flash for new bad blocks
[E]: Erase flash
[X]: exit
Enter your option:
```

- Print existent bad blocks - выводит на экран информацию о выявленных в ходе предыдущих проверках поврежденных блоках.
- Scan flash for new bad blocks - сканирование флэш-памяти на предмет поврежденных блоков. В случае их обнаружения, они помечаются, как поврежденные, и не используются системой.
- Erase flash - очистка флэш-памяти. Удаляет систему с флэш-памяти.

Обновление прошивки маршрутизатора

Если маршрутизатор уже сконфигурирован, то перед прошивкой следует сохранить конфигурацию, т.к. установка новой прошивки вернет все параметры в начальное состояние. Сохранение и восстановление конфигурации выполняется в веб-интерфейсе.

Обновление прошивки выполняется через консольный интерфейс, для этого вам потребуется:

- ПК с COM-портом
- TFTP-сервер, доступный с маршрутизатора

Для обновления прошивки необходимо, чтобы маршрутизатору был доступен TFTP-сервер, на котором расположен файл образа прошивки. В старых версиях загрузчика было необходимо, чтобы этот TFTP-сервер находился в одной сети с маршрутизатором, в новой версии добавлена возможность обновления, когда сервер доступен через шлюз.

Если используется локальный TFTP-сервер, то после его настройки необходимо в каталог, являющийся для него (TFTP-сервера) корневым, скопировать файл прошивки, который можно скачать с веб-сайта www.sigrand.ru [<http://www.sigrand.ru>].

Для доступа к консольному интерфейсу маршрутизатора необходимо COM-порт компьютера (разъем DB-9F) соединить с последовательным портом (разъем RJ-45 с надписью RS232, находящийся рядом с разъемом для питания) маршрутизатора.

Для управления маршрутизатором через консольный интерфейс может использоваться любая программа управления терминалом - HyperTerminal для ОС Windows или Minicom для ОС GNU/Linux. Настройки последовательного порта следующие:

- скорость передачи: 115 200
- протокол: 8-N-1

- управление потоком: нет

После запуска программы управления терминалом и установки соответствующих настроек порта, надо включить маршрутизатор. В окне программы выведется информация о маршрутизаторе с предложением войти в меню загрузчика:

```
ADM5120 Boot:

Copyright 2005 Sigrand, Inc.
CPU: ADM5120-175MHz
SDRAM: 128MB
Flash: NAND-32MB
Boot System: Linux-5120
Loader Version: 1.00.03
Creation Date: 2004.06.04

Press <space> key tree times to enter boot menu..
2
```

Для активации меню загрузчика надо быстро нажать на клавишу пробела 3 раза. Меню загрузчика выглядит следующим образом:

```
Sigrand MR16 router:
=====
Bootloader Menu
[1] Xmodem Download
[2] TFTP Download
[3] Print Boot Params
[4] Set Boot Params
[5] Check flash
[6] Exit

Please enter your number:
```

Перед обновлением прошивки необходимо выставить сетевые параметры, которые соответствуют вашей сети. Для этого нужно перейти в пункт меню *Set Boot Params*, нажав клавишу 4. Здесь будет предложено указать:

- серийный номер маршрутизатора - (Enter new serial number) - можно пропустить
- версию аппаратной части - (Enter new hardware version) - можно пропустить
- MAC адрес сетевого интерфейса - (Enter new mac address) - можно оставить установленный MAC адрес (его значение отображено выше, Current Mac Address), или ввести новое значение.
- число MAC адресов - (Enter new number of mac address) - этот параметр следует пропустить (по умолчанию число MAC адресов равно 1)
- IP адрес - (Enter new IP address for this board) - следует ввести IP адрес, находящийся в одной сети с TFTP сервером

Пример конфигурации приведен ниже:

```
Set Boot Parameters.
```

```
=====
Enter new serial number:
Serial Number unchanged.
Enter new hardware version:
Hardware version unchanged.
Current mac address: 00-05-5D-77-86-01
Number of mac address: 1
Enter new mac address (AA-AA-AA-AA-AA-AA):
Enter new number of mac address (between 1-8):
Mac address unchanged.
IP address for this board: 10.10.10.1
Enter new IP address for this board: 10.10.10.1
IP updated successfully.
```

В приведенном примере был введен только IP адрес маршрутизатора, остальные параметры оставлены без изменений.

После настройки сетевых параметров, следует выбрать пункт меню 2 (TFTP Client Download) для настройки параметров обновления с помощью TFTP сервера. Содержание этого меню приведено ниже:

```
Server IP: 80.66.88.167
Gateway IP: 10.10.10.2
Remote File bootloader: bootgw
Remote File system: openwrt
```

```
TFTP Client Menu
```

```
=====
[B]: Update bootloader
[S]: Update system
[A]: Update all
[P]: Set parameters
[X]: exit
Enter your option:
```

Замечание

Приведенное выше меню соответствует новому загрузчику, в который была добавлена возможность загрузки образов загрузчика и системы с TFTP-сервера, находящегося за маршрутизатором. Меню в старых версиях загрузчика отличается отсутствием возможности установки шлюза и обновления загрузчика.

Первые четыре строчки над меню содержат информацию, установленную во время последнего обновления прошивки. Для их изменения следует выбрать пункт меню set parameters нажатием клавиши p. В ответ на это будет предложено ввести:

- IP-адрес TFTP сервера - (Please Enter TFTP Server IP) - IP адрес TFTP сервера, на котором находится файл прошивки. Можно использовать TFTP-сервер, предоставляемый компанией Сигранд - *sigrand.ru*. Вводить следует IP-адрес сервера.
- IP-адрес шлюза - (Please enter gateway IP). Установка данного параметра позволяет обновлять прошивку с TFTP-сервера, находящегося в отличной от маршрутизатора сети. Шлюз должен находиться в той же сети, что и интерфейс маршрутизатора.
- Имя файла образа загрузчика - (Enter remote bootloader file name).

- Имя файла прошивки - (Enter remote system file name) - имя файла прошивки, расположенного на TFTP сервере.

```
Please enter TFTP server IP : 80.66.88.167
Please enter gateway IP : 10.10.10.2
Enter remote bootloader file name : bootgw
Enter remote system file name : openwrt
```

После настройки необходимых параметров, можно перейти к прошивке маршрутизатора или обновлению загрузчика. Для обновления загрузчика выбираем пункт меню [B]: Update bootloader:

```
Enter your option:b
Starting the TFTP download(ESC to stop)...
PASS
File total Length: 00010DF0

Eraseing flash.....
PASS
Programming flash....
PASS
```

PASS, соответствующий строчкам Eraseing flash и Programming flash означает, что обновление загрузчика прошло успешно. FAIL говорит о возникших проблемах, как правило это неправильный IP-адрес TFTP-сервера (маршрутизатор и TFTP-сервер находятся в разных сетях) или неправильное имя файла на сервере.

Для обновления прошивки маршрутизатора переходим в пункт меню [S]: Update system:

```
Enter your option:s
Starting the TFTP download(ESC to stop).....
PASS
File total Length: 00B62808 Starting address: A0820000

Eraseing flash.....
PASS
Programming flash....
PASS
```

Если на экране присутствуют строчки

```
Eraseing flash.....
PASS
Programming flash....
PASS
```

, значит обновление прошивки прошло успешно и теперь можно загрузить новую прошивку. Для этого необходимо выполнить перезагрузку маршрутизатора нажатием на кнопку RESET (или включением/выключением питания).

Пункт меню [A]: Update all последовательно обновляет загрузчик и прошивку маршрутизатора.

После загрузки маршрутизатора (при обычной загрузке не требуется входить в меню загрузчика, поэтому надо подождать, пока истечет таймер и начнется загрузка операционной системы (ОС>)) можно перейти к настройке посредством веб-интерфейса. Доступ к консоли больше не требуется, поэтому провод и соответствующее ПО можно отключить.

В случае, если на экран была выведена строчка

```
Starting the TFTP download(ESC to stop)..FAIL
```

, значит загрузчику не удалось загрузить файл прошивки с указанного TFTP сервера. В этом случае следует проверить корректность указания IP адреса TFTP сервера и имени файла прошивки на нем. Если все корректно, то следует проверить настройки, введенные в пункте Set Boot Params. Может помочь смена MAC адреса и проверка, не блокирует ли сервер TFTP соединения с маршрутизатора.

Установка программ

Перед установкой пакета его надо загрузить на маршрутизатор. Сделать это можно несколькими способами:

- Разместить на WWW/FTP сервере и загрузить с помощью утилиты wget
- Разместить на TFTP сервер и загрузить с помощью tftp клиента

Загрузка пакета с TFTP сервера:

```
# tftp 192.168.2.1 -r libpthread_0.9.28-1_mipsel.ipk -g
```

Установка пакета:

```
# ipkg
  install
  libpthread_0.9.28-1_mipsel.ipk
Installing libpthread (0.9.28-1) to root...
Configuring libpthread
Done.
```

Если при выполнении установки пакета будет выведено сообщение `ERROR: Cannot satisfy the following dependencies for fprobe:`, следует установить указанный пакет и повторить установку текущего пакета (`fprobe`).

Глава 2. Управление маршрутизатором

Начало работы

В заводской конфигурации и после обновления прошивки на маршрутизаторе активен интерфейс eth0 (крайний правый порт) с IP-адресом 192.168.2.100, сетевая маска 255.255.255.0.

Для конфигурации маршрутизатора необходимо соединить сетевую карту компьютера и крайний правый порт Ethernet проводом витой пары. На компьютере следует выставить IP-адрес из той же сети, в которой находится маршрутизатор (192.168.2.0/24), к примеру, 192.168.2.1, с сетевой маской 255.255.255.0.

Конфигурация с помощью Веб-интерфейса

Конфигурация маршрутизатора выполняется через веб-интерфейс любым веб-браузером, поддерживающим протокол HTTPS (Internet Explorer, Opera, Safari, Mozilla Firefox). Для конфигурации необходимо в строке адреса веб-браузера ввести https://192.168.2.100, после чего будут заданы несколько вопросов касательно сертификатов шифрования, на которые следует ответить положительно. По-умолчанию, логин/пароль установлены следующие: admin/1234.

Вид главной страницы показан ниже:

Рисунок 2.1. Главная страница



Установка пароля

Важно

Настоятельно рекомендуется менять пароль для конфигурации, это выполняется на странице System/Security

Там же следует поменять и пароль для управления маршрутизатором через консольный интерфейс. Страница смены пароля приведена ниже:

Рисунок 2.2. Смена пароля

The screenshot shows two separate form sections for password management. The first section is titled 'Webface admin password' and contains a 'Password' input field followed by a 'Set' button. The second section is titled 'root system password' and also contains a 'Password' input field followed by a 'Set' button.

Имя маршрутизатора

Смена имени маршрутизатора (hostname) может быть выполнена на странице System/General, которая приведена ниже:

Рисунок 2.3. Смена имени маршрутизатора

The screenshot shows the 'General settings' page. The 'Hostname' field is highlighted and contains the text 'sigrand1'. Below the field is a small note: 'This is description for hostname'. A 'Save' button is located below the field.

Синхронизация времени

Установка сервера для синхронизации внутренних часов маршрутизатора и часового пояса выполняется на странице System/Time:

Рисунок 2.4. Синхронизация времени

The screenshot shows the 'Time settings' page. It includes three main sections: 'Use time synchronizing' with a checked checkbox and the instruction 'Check this item if you want use time synchronizing'; 'Time server' with an input field containing 'pool.ntp.org' and the instruction 'Please input hostname or ip address time server'; and 'Time zone' with a dropdown menu set to 'GMT-4'. A 'Save' button is located at the bottom.

Настройка DNS

Установка адреса DNS-сервера, к которому будет обращаться маршрутизатор с DNS запросами и имя домена, в который входит маршрутизатор, устанавливается на странице System/DNS:

Рисунок 2.5. Настройка DNS

DNS Settings ?	
Upstream server	<input type="text" value="192.168.2.1"/> Please enter ip address of upstream dns server
Domain	<input type="text" value="localnet"/> Please enter your domain

Информация о состоянии соединения SHDSL и E1 может быть получена на страницах General/SHDSL и General/E1 соответственно, конфигурация параметром линии связи для этих интерфейсов выполняется соответственно на страницах General/SHDSL/dsl* и General/E1/hdlc*, для более подробной информации о возможных настройках обратитесь к соответствующему разделу документации.

Управление интерфейсами осуществляется на страницах, указанных в меню Network. К примеру, конфигурация интерфейсов Ethernet осуществляется на страницах Network/Interfaces/eth*, SHDSL - на страницах Network/Interfaces/dsl*, а E1 - на Network/Interfaces/hdlc*. Для активация интерфейса необходимо активировать параметры Enabled и Auto на вкладке General, расположенной на странице конфигурирования выбранного сетевого интерфейса. За более подробными инструкциями обратитесь к соответствующим страницам конфигурации маршрутизатора.

В меню Tools расположены утилиты, позволяющие:

- проследить за работой маршрутизатора, просмотрев логи - страницы syslog и dmesg;
- выполнить перезагрузку с помощью reboot;
- проверить работу DNS сервера или соответствие DNS-имени IP-адресу с помощью утилиты dig;
- проверить работоспособность узла с помощью утилиты ping;
- посмотреть маршрут прохождения пакета до заданного узла в сети с помощью mtr;
- посмотреть сетевой трафик с помощью tcpdump.

Сохранение и восстановление конфигурации производится на страницах Configuration/Backup и Configuration/Restore соответственно.

Конфигурация через консольный интерфейс

Для конфигурации маршрутизатора через консольный интерфейс необходимо подключиться к маршрутизатору по протоколу SSH на порт 22. Есть несколько программ, поддерживающих работу по протоколу SSH, к примеру, Putty для OS Windows и ssh для OS GNU/Linux. В качестве логина необходимо ввести root, пароль - 1234.

После успешной аутентификации, на экран будет выведен логотип фирмы Sigrand и текущая версия прошивки маршрутизатора:

```
sigrand1 login: root
```


Рисунок 2.6. Логирование

Logging ?	
Console priority logging	0 ▼
Kernel console priority logging	3 ▼ Set the level at which logging of messages is done to the console.
Circular buffer	64k ▼ Circular buffer size
Enable remote syslog logging	<input checked="" type="checkbox"/> Check this item if you want to enable remote logging
Remote syslog server	192.168.2.1 Domain name or ip address of remote syslog server

- Circular buffer - размер буфера
- Enable remote syslog logging - включение логирования на удаленный syslog-сервер
- Remote syslog server - адрес удаленного syslog-сервера

Замечание

При включении логирования на удаленный сервер, продолжается запись событий в локальный буфер.

Замечание

Для того, чтобы удаленный syslog-сервер принимал логи от маршрутизатора, его необходимо запустить с опцией "-r". Логирование производится по протоколу udp, 514 порт.

Настройка встроенного Ethernet коммутатора

Настройка коммутатора осуществляется на странице System/Switch, на который устанавливается соотношение между физическими портами коммутатора (нумерация идет справа налево, т.е. Port 0 соответствует крайнему правому разъему маршрутизатора). Отнесение нескольких портов к одному интерфейсу создает для них единую физическую среду, т.е. они начинают работать, как порты одного коммутатора. Окно конфигурации представлено на рисунке:

Рисунок 2.7. Конфигурация коммутатора

Port 0	
Attach port 0 to	eth0 ▾
Speed	Auto ▾
Duplex	Auto ▾
Port 1	
Attach port 1 to	eth0 ▾
Speed	Auto ▾
Duplex	Auto ▾
Port 2	
Attach port 2 to	eth2 ▾
Speed	Auto ▾
Duplex	Auto ▾
Port 3	
Attach port 3 to	eth3 ▾
Speed	Auto ▾
Duplex	Auto ▾

В приведенной выше конфигурации 0 и 1 порты коммутатора отнесены к сетевому интерфейсу eth0, в то время как 2 и 3 порты являются независимыми.

Замечание

После внесения изменений необходимо перезагрузить маршрутизатор.

Установка зависимостей SHDSL - Ethernet

Для создания сложных взаимосвязей между интерфейсами была добавлена возможность управления состоянием Ethernet порта в зависимости от состояния соответствующего ему SHDSL порта

На данный момент управление соответствием осуществляется через консольный интерфейс, и устанавливается в конфигурационном файле `/etc/sigrand/dsl2eth.map`.

Изначально файл `/etc/sigrand/dsl2eth.map` пустой. Пример его заполнения показан в файле `/etc/sigrand/dsl2eth.map.example` и выглядит следующим образом:

```
dsl0 eth0
dsl1 eth1
```

Это означает, что интерфейсу eth0 соответствует интерфейс dsl0, а eth1 - dsl1, и если линк на dsl0 упадет, что так же будет отключен линк на eth0. Редактировать файл можно любым текстовым редактором, к примеру следующей командой:

```
nano /etc/sigrand/dsl2eth.map
```

После внесения изменений в конфигурационный файл рекомендуется перезагрузить маршрутизатор.

Сохранение/восстановление конфигурации

Веб-интерфейс позволяет сохранять текущую, восстанавливать сохраненную или заводскую конфигурацию маршрутизатора.

Сохранение конфигурации выполняется на странице Configuration/Backup:

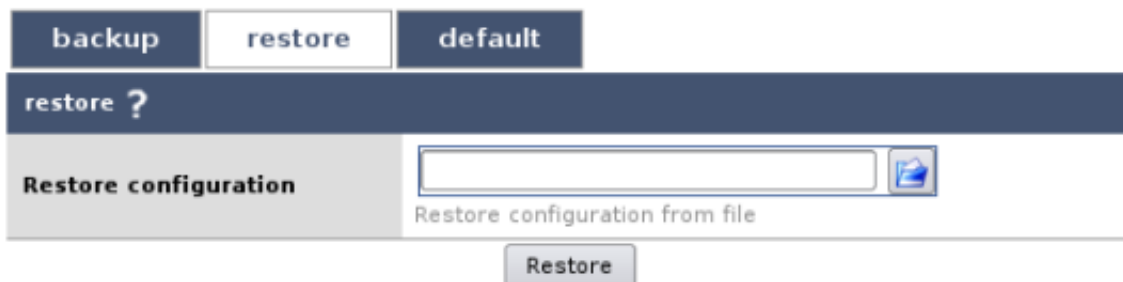
Рисунок 2.8. Сохранение конфигурации



При нажатии на кнопку Backup будет предложено сохранить файл конфигурации, который в последствии можно будет загрузить.

Восстановление конфигурации выполняется на странице Configuration/Restore:

Рисунок 2.9. Восстановление конфигурации



На вкладке default можно восстановить заводскую конфигурацию нажатием на кнопку Restore default.

После восстановления конфигурации, необходимо перезагрузить маршрутизатор.

Глава 3. Настройка сетевых интерфейсов

Общие параметры

Вкладка Status

На вкладке *Status* отображается основная информация о выбранном интерфейсе. Информация о сетевых параметрах интерфейса:

Рисунок 3.1. Сетевые параметры

```
Interface status
/sbin/ifconfig dsl0
dsl0      Link encap:Ethernet  HWaddr 00:FF:0F:E6:CB:C0
          inet addr:192.168.100.1  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::2ff:fff:fee6:cbc0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6 errors:4 dropped:0 overruns:0 frame:4
          TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:468 (468.0 B)  TX bytes:468 (468.0 B)
          Interrupt:6 Memory:11400000-11400fff

/usr/sbin/ip link show dev dsl0
7: dsl0:  mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:ff:0f:e6:cb:c0 brd ff:ff:ff:ff:ff:ff
/usr/sbin/ip addr show dev dsl0
7: dsl0:  mtu 1500 qdisc pfifo_fast qlen 1000
   link/ether 00:ff:0f:e6:cb:c0 brd ff:ff:ff:ff:ff:ff
   inet 192.168.100.1/24 brd 192.168.100.255 scope global dsl0
   inet6 fe80::2ff:fff:fee6:cbc0/64 scope link
   valid_lft forever preferred_lft forever
```

Маршруты, привязанные к интерфейсу:

Рисунок 3.2. Сетевые маршруты

```
Routes
/usr/sbin/ip route show dev dsl0
192.168.100.0/24 proto kernel scope link src 192.168.100.1
```

Записи в таблице ARP:

Рисунок 3.3. Таблица ARP

```
ARP
/usr/sbin/ip neigh show dev dsl0
```

Информация о работе встроенного коммутатора:

Рисунок 3.4. Встроенный коммутатор

```
Internal switch status ?
cat /proc/sys/net/adm5120sw/status
Port0 up 100M full-duplex enabled vlanid=1 unit=0
Port1 down - - disabled vlanid=2 unit=1
Port2 down - - enabled vlanid=4 unit=2
Port3 down - - disabled vlanid=0 unit=0
Port4 down - - disabled vlanid=0 unit=0
```

Информация о шейпере трафика, работающего на интерфейсе:

Рисунок 3.5. Шейпер трафика

```
Traffic Control
/usr/sbin/tc -s qdisc ls dev eth0
qdisc pfifo_fast 0: bands 3 priomap 1 2 2 2 1 2 0 0 1 1 1 1 1 1 1
Sent 862404 bytes 1769 pkt (dropped 0, overlimits 0 requeues 0)
rate 0bit Opps backlog 0b 0p requeues 0
```

Вкладка General

Опции на вкладке *General* позволяют включить/выключить интерфейс, а также выбрать способ установки ip-адреса:

Рисунок 3.6. Вкладка General

Interface general settings ?	
Description	<input type="text" value="Localinterface"/>
Enabled	<input checked="" type="checkbox"/>
Auto	<input checked="" type="checkbox"/>
Method	<input type="button" value="Static address"/> <small>Please select method of the interface</small>

- Description - описание интерфейса, не используется системой
- Enabled - интерфейс активен
- Auto - активация интерфейса при загрузке
- Method - метод установки IP-адреса

Возможно несколько методов установки IP-адреса:

- не конфигурируемый (none) - ip-адрес не устанавливается
- статический (static address) - ручной ввод пользователем
- Zero configuration - автоматический способ присвоения ip-адреса, позволяющий построить работающую сеть без ручного присвоения ip-адресов и без серверов DNS/DHCP
- Динамический ip-адрес (dynamic address) - адрес назначается сетевыми сервисами: DHCP/PPTP/...

Замечание

При выборе статического адреса необходимо ввести соответствующую информацию на вкладке *Method*.

При конфигурации сети с помощью Zeroconf интерфейсу будет назначен ip-адрес из диапазона 169.254.*.

При выборе динамического ip-адреса, адрес и необходимые сетевые настройки будут получены от DHCP сервера.

Вкладка Method

На вкладке *Method* осуществляется установка сетевых параметров:

Рисунок 3.7. Вкладка Method

Static address settings ?	
Static address	<input type="text" value="192.168.2.100"/> Address (dotted quad) required
Netmask	<input type="text" value="255.255.255.0"/> Netmask (dotted quad) required
Broadcast	<input type="text"/> Broadcast (dotted quad)
Gateway	<input type="text"/> Default gateway (dotted quad)

- IP-адрес (static address)
- маска сети (netmask)
- широковещательный адрес (broadcast)
- маршрут по-умолчанию (gateway)

Замечание

Обязательными для заполнения являются только первые два поля, при не заполнении поля широковещательного адреса, он будет высчитан автоматически.

Вкладка Options

Переключатели на вкладке *Options* управляют поведением интерфейса:

Рисунок 3.8. Вкладка Options

Interface options ?	
Accept redirects	<input checked="" type="checkbox"/>
Forwarding	<input checked="" type="checkbox"/>
Proxy ARP	<input type="checkbox"/>
RP Filter	<input type="checkbox"/>

Accept redirects - в активном состоянии позволяет принимать ICMP перенаправления. Например, если есть лучший маршрут до какого-либо узла чем тот, по которому был послан пакет клиентом, маршрутизатор клиенту может отправить (как правило всегда так и происходит) истр-перенаправление с указанием, через какой маршрутизатор лучше в следующий раз отправлять пакеты.

Forwarding - при активном состоянии включает режим маршрутизатора - пересылку пакеты с интерфейса на интерфейс (в соответствии с правилами фаервола).

Proxy ARP - включение режима Proxy ARP, что предоставляет третий способ соединения сетей (помимо моста и стандартной IP-маршрутизации).

RP Filter - управляет возможностью проверки пути к отправителю (reversed path) в соответствии с RFC 1812. Активное состояние включает такую проверку и рекомендуется для хостов с одним сетевым интерфейсом и маршрутизаторов тупиковых сетей.

Вкладка Specific

На вкладке *Specific* производится установка MAC-адреса интерфейса:

Рисунок 3.9. Вкладка Specific



Ethernet Specific parameters ?

MAC Address
MAC Address for interface

Save

Работа с динамическими интерфейсами

На странице Network/Interfaces возможно добавить или удалить динамический интерфейс. На данный момент существуют следующие динамические интерфейсы:

- Bridge - создание моста
- PPPoE - PPP over Ethernet
- PPTP - Point-to-Point Tunneling Protocol
- Bonding - объединение интерфейсов

Для создания нового интерфейса его тип выбирается из выпадающего списка, нажимается кнопка Add:

Рисунок 3.10. Создание динамического интерфейса



Add dynamic interface ?

Protocol
Please select interface protocol

Add

После добавления надо перезагрузить страницу, щелкнув в меню по ссылке Network/Interfaces, чтобы добавленный интерфейс отобразился в списке сетевых интерфейсов.

Для удаления интерфейса его имя выбирается в выпадающем списке, нажимается кнопка Delete:

Рисунок 3.11. Удаление динамического интерфейса



Конфигурация интерфейса E1

Маршрутизатор поддерживает несколько протоколов для работы с интерфейсом E1: HDLC, ETHER-HDLC, CISCO-HDLC, FR, PPP, X25. Конфигурация интерфейса выполняется на странице System/E1/hdlc*.

Настройка параметров интерфейса

Настройка протокола CISCO-HDLC

Настройка некоторых параметров устанавливается в "два этапа": т.е. сперва выбирается значение параметра, затем внесенные изменения сохраняются, и после перезагрузки страницы добавляются опции, относящиеся к выбранному параметру.

Для настройки протокола CISCO-HDLC необходимо в выпадающем списке HDLC protocol выбрать значение CISCO-HDLC:

Рисунок 3.12. Выбор протокола



Для активации страницы с настройками, относящимся к выбранному протоколу, необходимо сохранить внесенные изменения. После перезагрузки страница примет следующий вид:

Рисунок 3.13. Конфигурация CISCO-HDLC

hdlc0 modem settings	
HDLC protocol	CISCO-HDLC
Interval	10
Timeout	25
E1 framed mode	<input checked="" type="checkbox"/> check to enable
Use time slot 16	<input type="checkbox"/> check to use
Slotmap	1-15,17-31 example: 2-3,6-9,15-20
E1 internal transmit clock	<input type="checkbox"/> check to enable
E1 CRC4 multiframe	<input type="checkbox"/> check to enable
E1 CAS multiframe	<input type="checkbox"/> check to enable
E1 long haul mode	<input type="checkbox"/> check to enable
E1 HDB3/AMI line code	HDB3
CRC	CRC16
Fill	FF
Inversion	off

Описание параметров конфигурации:

- Interval - время в секундах между пакетами поддержания соединения (keepalive packets)
- Timeout - время в секундах после последнего полученного пакета поддержания соединения, по истечению которого соединение считается разорванным.
- E1 framed mode - структурированный режим, при котором канал разбивается на таймслоты. В этом режиме для соединения задается карта таймслотов, которая должна совпадать с картой на другом конце соединения.
- Use time slot 16 - по умолчанию в интерфейсе E1 зарезервированы 0 и 16 слоты, которые могут быть использованы для служебной информации. Активация этого параметра позволяет использовать таймслот 16 для передачи данных.
- Slotmap - карта таймслотов. После сохранения из карты будут удалены служебные таймслоты.
- E1 internal transmit clock - использовать внутренний генератор частоты. Как правило, в соединении должно быть хотя бы одно устройство с внутренним генератором частоты.
- E1 CRC4 multiframe - включение режима CRC4.
- E1 CAS multiframe - включение режима CAS, используемого, как правило, при работе с АТС оборудованием. В этом режиме таймслот 16 зарезервирован для служебного использования.
- E1 HDB3/AMI line code - способ кодирования сигнала на линии связи.
- CRC - способ контроля ошибок.

Пропускная способность одного таймслота составляет 64 Кбит/с, т.о. максимальная пропускная способность интерфейса E1 в unframed mode составляет 2 Мбит/с.

Конфигурация framed mode

Для работы интерфейса в framed mode необходимо активировать параметр E1 framed mode и ввести карту таймслотов, например "2-9,17-27 (именно в таком формате, без пробела между диапазонами)". На другом конце соединения должна быть установлена такая же карта слотов. Строго говоря, все параметры, за исключением E1 internal transmit clock, должны быть согласованы с двух сторон.

При такой конфигурации карты таймслотов, максимальная пропускная способность канала составит $17 * 64 \text{ Кбит/с} = 1088 \text{ Кбит/с}$, что подтверждается тестами.

Конфигурация unframed mode

Для настройки интерфейса на режим работы unframed mode, параметр E1 framed mode должен быть неактивным. После внесения изменений (деактивация параметра) и сохранения, будут доступны следующие параметры настройки:

Рисунок 3.14. Unframed mode

hdlc0 modem settings	
HDLC protocol	CISCO-HDLC
Interval	10
Timeout	25
E1 framed mode	<input type="checkbox"/> check to enable
E1 long haul mode	<input type="checkbox"/> check to enable
E1 HDB3/AMI line code	HDB3
CRC	CRC16
Fill	FF
Inversion	off

В этом режиме параметров конфигурации меньше, чем во framed mode и все они сводятся к настройке линии связи.

Настройка сетевых параметров

В данной версии ПО, установленного на маршрутизаторе, нет возможности задавать сетевые параметры через веб-интерфейс настройки, поэтому эту часть конфигурации требуется выполнить вручную. В первую очередь, необходимо убедиться, что на странице настройки сетевого интерфейса Network/Interfaces/hdlc*/General параметры Enabled и Auto неактивны:

Рисунок 3.15. Настройка интерфейса

Status	General	Method	Options	Specific	QoS	Routes
Enabled	<input type="checkbox"/>					
Auto	<input type="checkbox"/>					
Method		None				

После внесения необходимых изменений, необходимо активировать консоль маршрутизатора: либо подключившись к нему по последовательному порту, либо по сети по протоколу SSH.

Соединение E1 имеет тип точка-точка. Для активация соединения необходимо выполнить следующую команду:

```
# ifconfig hdlc0 192.168.200.1 pointopoint 192.168.200.2
```

- hdlc0 - сетевой интерфейс
- 192.168.200.1 - IP-адрес соединения на стороне маршрутизатора

Если соединение не установилось, то надо деактивировать/активировать сетевой интерфейс:

```
# ifconfig hdlc0 down
```

```
# ifconfig hdlc0 up
```

Для активация соединения после загрузки маршрутизатора, необходимо выполнить следующие команды:

```
# echo "ifconfig hdlc0 192.168.200.1 pointopoint 192.168.200.2" >> /  
etc/init.d/S90my_hdlc
```

```
# echo "ifconfig hdlc0 down" >> /etc/init.d/S90my_hdlc
```

```
# echo "ifconfig hdlc0 up" >> /etc/init.d/S90my_hdlc
```

Созданный файл необходимо сделать исполняемым:

```
# chmod +x /etc/init.d/S90my_hdlc
```

Настройка работы SHDSL модемов в режиме Bonding

Режим Bonding позволяет объединять несколько физических соединений в одно логическое. К примеру, два SHDSL канала можно объединить в один, увеличив пропускную способность соединения.

Для настройки режима Bonding в первую очередь необходимо настроить физическое соединение. Для этого на странице System/SHDSL/dsl* надо выставить параметры, пригодные для вашей линии связи:

Рисунок 3.16. Настройка параметров линии связи

dsl0 modem settings	
Rate	6016 <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL line rate	
Mode	Slave <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL mode	
Coding	TCPAM32 <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL line coding	
Config	local <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL configuration mode	
Annex	Annex A <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL Annex	
CRC	CRC32 <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL CRC length	
Fill	FF <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL fill byte value	
Inversion	on <input type="button" value="v"/> <input type="button" value="i"/>
Select DSL inversion mode	

- Rate - пропускная способность линии связи, Кбит/с. Зависит от качества линии связи, если на выбранной вами скорости соединение не устанавливается, уменьшите этот параметр. Значения на обоих концах соединения должны совпадать
- Mode - режим работы - ведущий/ведомый
- Coding - метод кодирования
- CRC - метод контроля ошибок

После указания необходимых параметров, внесенные изменения необходимо сохранить. После настройки параметров линии связи для обоих интерфейсов, dsl0 и dsl1, можно перейти к настройке виртуального интерфейса, который будет для передачи данных использовать объединение физических линий.

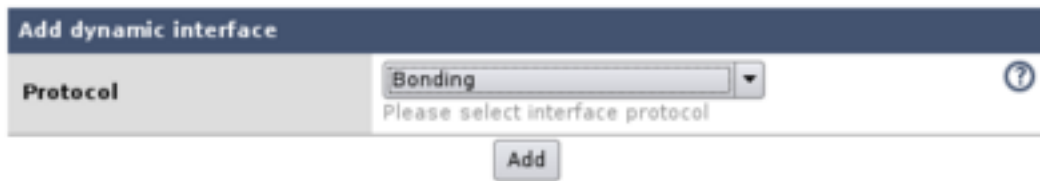
Перед конфигурацией виртуального интерфейса следует убедиться, что интерфейсы dsl0 и dsl1 активны. Выполняется это на странице Network/Interfaces/dsl*/General, параметр Enabled должен быть активным, Auto отключенным, а Method равен None:

Рисунок 3.17. Настройка интерфейса

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Enabled	<input checked="" type="checkbox"/>						<input type="button" value="i"/>
Auto	<input type="checkbox"/>						<input type="button" value="i"/>
Method	None <input type="button" value="v"/>						<input type="button" value="i"/>
		Please select method of the interface					

Виртуальный интерфейс создается на странице Network/Interfaces, на которой в разделе Add dynamic interface необходимо выбрать в качестве протокола Bonding:

Рисунок 3.18. Создание виртуального интерфейса



После создания интерфейса нажатием кнопки Add, следует щелкнуть кнопкой мыши на меню Network/Interfaces, чтобы созданный интерфейс отобразился в меню. Для его настройки необходимо перейти на страницу Network/Interfaces/bond0, на которой следует выбрать вкладку General и выставить следующие настройки:

Рисунок 3.19. Активация виртуального интерфейса



Эти настройки активирует интерфейс и настраивают его автоматическую активацию после загрузки системы, IP-адрес для него задается статически на вкладке Method:

Рисунок 3.20. Присвоение IP-адреса



Замечание

Если требуется указать маршрут по-умолчанию, адрес маршрутизатора следует ввести в поле Gateway.

На вкладке Specific указывается, какие физические интерфейсы будут использоваться этим виртуальным интерфейсом для передачи данных. При настройке SHDSL Bonding, следует ввести dsl0 и dsl1:

Рисунок 3.21. Привязка к физическим интерфейсам

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Bonding Specific parameters							
MAC Address	<input type="text"/>			MAC Address for interface			
Interfaces	<input type="text" value="dsl0 dsl1"/>			Interfaces for bonding separated by space			
<input type="button" value="Save"/>							

Аналогичные настройки необходимо произвести и на втором маршрутизаторе. После соединения SHDSL модемов маршрутизатора по линиям связи, будут установлены два физических соединения, которые будут объединены в одно логическое с увеличенной пропускной способностью.

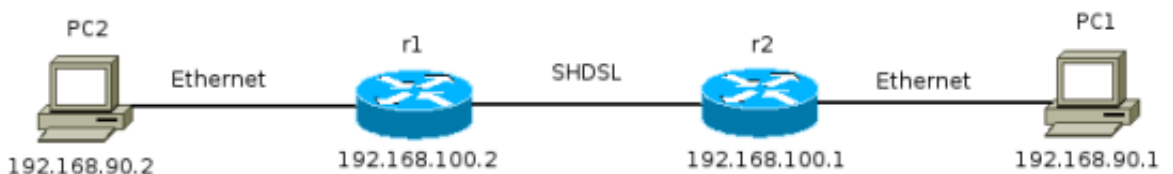
Замечание

При разрыве одного из физических соединений, трафик будет передаваться по оставшемуся соединению.

Настройка моста

Работа маршрутизатора в режиме моста (bridging) позволяет прозрачно передавать трафик между интерфейсами, имитируя работу коммутатора. Для этого создается специальный сетевой интерфейс с именем *br*, с которым ассоциируются сетевые интерфейсы между которыми будет передаваться трафик.

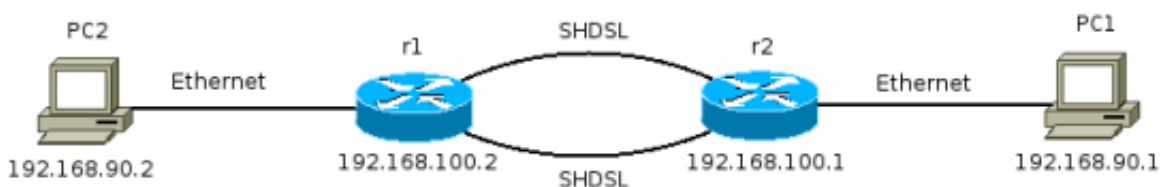
Рисунок 3.22. Пример моста



В приведенном выше рисунке мост состоит из двух интерфейсов - Ethernet-интерфейса *eth0* и SHDSL-интерфейса *dsl0* - и объединяет в одну сеть компьютеры PC1 и PC2

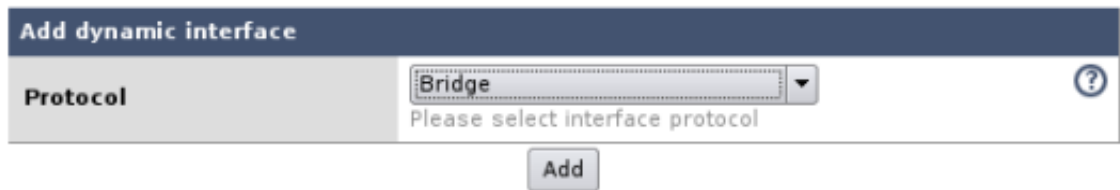
На следующем рисунке изображена сеть, аналогичная предыдущий, но с использованием технологии объединения каналов (bonding), позволяющей увеличить производительность сети. В этом случае мост состоит из Ethernet-интерфейса *eth0* и объединенных SHDSL-интерфейсов *dsl0* и *dsl1* в один интерфейс *bond0*:

Рисунок 3.23. Пример моста с объединением интерфейсов



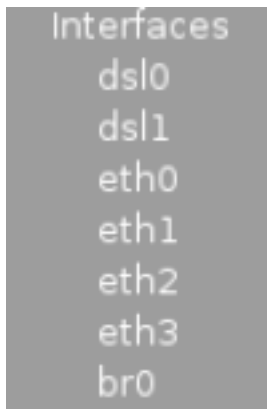
Создание интерфейса происходит на странице Network/Interfaces, на которой в меню Add dynamic interface надо выбрать в качестве протокола Bridge:

Рисунок 3.24. Создание интерфейса



После добавления интерфейса надо снова перейти по ссылке Network/Interfaces, чтобы добавленный интерфейс отобразился в меню:

Рисунок 3.25. Добавленный интерфейс br0



Новому интерфейсу надо поставить метод установки IP-адреса статическим. Для этого перейдем в настройки интерфейса (по ссылке в меню Network/Interfaces/br0) и выберем вкладку General, на которой установим необходимое значение:

Рисунок 3.26. Установка метода присвоения IP-адреса



Замечание

Установка IP-адреса нужна только для того, чтобы иметь возможность управлять маршрутизатором, если управление им возможно только через интерфейсы, включенные в мост. Вызвано это тем, что после добавления сетевого интерфейса в мост, доступ к нему становится невозможным по присвоенному ему ранее IP-адресу. Проще говоря, добавленный в мост интерфейс становится без IP-адреса.

Установим IP-адрес и сетевую маску на вкладке Method:

Рисунок 3.27. Установка IP-адреса

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Static address		<input type="text" value="192.168.100.2"/>					
		Address (dotted quad) required					
Netmask		<input type="text" value="255.255.255.0"/>					
		Netmask (dotted quad) required					
Broadcast		<input type="text"/>					
		Broadcast (dotted quad)					
Gateway		<input type="text"/>					
		Default gateway (dotted quad)					
<input type="button" value="Save"/>							

Следующим шагом настройки является определение списка интерфейсов, входящих в мост. Для этого перейдем на вкладку Specific, где в поле Interfaces укажем имена сетевых интерфейсов, из которых будет состоять мост:

Рисунок 3.28. Определение интерфейсов

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Bridge Specific parameters							
STP Enabled		<input type="checkbox"/>					
		Enable Spanning Tree Protocol					
Interfaces		<input type="text" value="eth0 dsl0"/>					
		Interfaces for bridge					
Priority		<input type="text"/>					
		Bridge priority					
Forward delay		<input type="text"/>					
Hello time		<input type="text"/>					
Max age		<input type="text"/>					
<input type="button" value="Save"/>							

Examples: eth0 eth1 dsl0
Notes: You can use only Ethernet-like interfaces, like ethX, dslX
Note: Interfaces should be enabled, but **auto** should be switched off

В завершении настройки, активируем интерфейс на вкладке General, поставив флажки напротив значений Enable и Auto:

Рисунок 3.29. Активация моста

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Enabled		<input checked="" type="checkbox"/>					
Auto		<input checked="" type="checkbox"/>					
Method		<input type="text" value="Static address"/>					
		Please select method of the interface					
<input type="button" value="Save"/>							

Эту же процедуру повторяем на втором маршрутизаторе, и через пару минут, в течении которых "мост" распознает топологию сети и проведет небольшой этап самообучения, начнется передача пакетов между интерфейсами.

Глава 4. Настройка сетевых служб

DHCP-сервер

Настройка DHCP-сервера выполняется независимо для каждого сетевого интерфейса и производится на вкладке Network/настраиваемый сетевой интерфейс/DHCP. На этой странице представлены конфигурационные параметры, управляющие работой DHCP-сервера, а так же параметры сетевой конфигурации, которые передаются клиенту.

Общий вид страницы конфигурации представлен на рисунке:

Рисунок 4.1. Настройка DHCP-сервера

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Enable DHCP server		<input checked="" type="checkbox"/> Check this item if you want use DHCP server on your LAN					
Start IP		<input type="text" value="192.168.100.2"/> Start of dynamic ip range address for your LAN (dotted quad) required					
End IP		<input type="text" value="192.168.100.20"/> End of dynamic ip range address for your LAN (dotted quad) required					
Netmask		<input type="text" value="255.255.255.0"/> Netmask for your LAN (dotted quad) required					
Default router		<input type="text" value="192.168.100.3"/> Default router for your LAN hosts (dotted quad)					
Default lease time		<input type="text" value="10 minutes"/>					
DNS server		<input type="text" value="192.168.100.20"/> DNS server for your LAN hosts (dotted quad)					
Domain		<input type="text"/> Allows DHCP hosts to have fully qualified domain names					
NTP server		<input type="text"/> NTP server for your LAN hosts (dotted quad)					
WINS server		<input type="text"/> WINS server for your LAN hosts (dotted quad)					

Настройки DHCP-сервера:

- За активацию DHCP-сервера отвечает опция Enable DHCP server
- Значения Start IP и End IP указывают диапазон IP адресов, из которого будет выбираться адрес для клиента

Сетевые настройки, которые будут переданы клиенту:

- Netmask - задает сетевую маску
- Default router - маршрут по-умолчанию
- Default lease time - время, на которое выдается IP адрес. По истечению этого времени клиент должен снова обратиться к DHCP-серверу для подтверждения использования выданного ранее адреса или получения нового
- DNS server - IP адрес DNS-сервера, к которому будет обращаться клиент для разрешения доменных имен
- Domain - домен, который будет присвоен клиенту
- NTP server - IP адрес сервера точного времени
- WINS server - IP адрес WINS сервера

Замечание

После сохранения настроек, DHCP сервер будет запущен либо перезапущен автоматически.

Существует возможность присваивать определенным машинам статические IP адреса. Идентификация машин производится по значению MAC адреса сетевой карты. Форма для привязки IP адреса к MAC адресу находится внизу страницы конфигурации и представлена на рисунке:

Рисунок 4.2. Список статических IP-адресов

No	Name	IP Address	MAC Address
+			


Изначально форма пуста. Добавление значений производится с помощью формы, вызываемой по нажатию на кнопку  справа от заголовка таблицы:

Рисунок 4.3. Форма привязки IP к MAC



DHCP Host settings	
Host name	<input type="text" value="pc1"/> Host name
IP Address	<input type="text" value="192.168.150.15"/> IP Address for host
MAC Address	<input type="text" value="A0:43:08:52:09:41"/> MAC Address for host
<input type="button" value="Save"/>	

- Host name - задает имя машины, для которой выполняется привязка адреса. Это значение носит справочный характер и используется только в правиле, и может не соответствовать фактическому имени машины
- IP Address - IP адрес, который будет присвоен данной машине
- MAC Address - MAC адрес сетевой карты машины. Именно при совпадении с этим адресом происходит присвоение указанного IP адреса

После заполнения полей, необходимо сохранить внесенные изменения. После этого, в список статических IP адресов будет добавлен новый адрес, а на экране появится новая форма для добавления следующего IP адреса. После добавления всех статических адресов, форму можно закрыть.

Рисунок 4.4. Обновленный список IP-адресов

No	Name	IP Address	MAC Address
0	pc11	192.168.150.15	A0:43:08:52:09:41
1	pc12	192.168.150.16	A0:43:98:82:04:39

Существующие в таблице записи можно изменить с помощью кнопки  ,
находящейся справа от правила. Удаление правила осуществляется кнопкой  .

PPTP-сервер

PPTP-сервер позволяет организовать ВПН - виртуальную частную сеть - поверх обычной сети. Для этого пользователи подключаются к ВПН-серверу, и в случае успешной авторизации получают доступ к ресурсам частной сети. Функции ВПН-сервера в маршрутизаторе выполняет PPTP-сервер - point-to point tunneling protocol.

Страница конфигурации находится в Services/PPTP server и приведена ниже:

Рисунок 4.5. Конфигурация PPTP-сервера

PPTP Server ?	
Enable PPTP server	<input checked="" type="checkbox"/> Check this item if you want to start PPTP server
Name	<input type="text" value="sg"/> Name of the local system for authentication purposes required
Local IP range	<input type="text" value="10.10.10.1"/> Local ip address range (dotted quad) required
Remote IP range	<input type="text" value="10.10.10.2-10"/> Remote ip address range (dotted quad) required
PAP Mode	<input type="text" value="Refuse-PAP"/> Password Authentication Protocol
CHAP Mode	<input type="text" value="Refuse-CHAP"/> Challenge Handshake Authentication Protocol
MS-CHAP Mode	<input type="text" value="Refuse MS-CHAP"/> Microsoft Challenge Handshake Authentication Protocol
MS-CHAPv2 Mode	<input type="text" value="Require MS-CHAPv2"/> Microsoft Challenge Handshake Authentication Protocol, version 2
MPPE Mode	<input type="text" value="Disable MPPE"/> Microsoft Point to Point Encryption
DNS Server	<input type="text" value="192.168.2.100"/> Primary DNS server for clients
DNS Server	<input type="text" value="192.168.2.101"/> Secondary DNS server for clients
WINS Server	<input type="text" value="192.168.2.102"/> Windows Internet Name Services server address
PPPD Options	<input type="text" value="nodefaultrote noauth nobsd"/>

Активация VPN-сервера выполняется установкой флажка напротив параметра *Enable PPTP server*. Настройка сервера состоит из двух стадий - конфигурации самого сервера и добавления пользователей, которые могут к нему подключаться. Рассмотрим параметры конфигурации сервера:

- Name - имя ВПН-сервера. Используется при аутентификации. У пользователя в *-secret файле значение имени сервера должно совпадать с этим, либо там должна стоять "звездочка".
- Local IP range - диапазон IP-адресов, которые будут присвоены соединению на стороне сервера.
- Remote IP range - диапазон IP-адресов, которые будут присвоены соединению на стороне клиента.
- Механизмы аутентификации. Имеют три значения - *none* - не определено, *require* - обязателен, *refuse* - запрещен к использованию
 - PAP Mode - метод PAP
 - CHAP Mode - метод CHAP
 - MS CHAP Mode - метод MS CHAP
 - MS CHAPv2 Mode - метод MS CHAPv2
- MPPE Mode - использовать шифрование трафика по алгоритму MPPE (Microsoft Point-to-Point Encryption)
- DNS server - адреса первичного и вторичного сервера DNS, которые будут переданы клиенту
- WINS server - адрес WINS сервера
- PPPD options - опции, которые будут переданы серверу pptp

После внесения изменений, конфигурацию необходимо сохранить. Для добавления пользователей ВПН-сервера, перейдем на страницу System/Security/PPP secrets:

Рисунок 4.6. Пользователи ВПН-сервера



Вкладка CHAP содержит пользователей, использующих систему аутентификации CHAP (в т.ч. обе версии MS CHAP), вкладка PAP - соответственно пользователей, использующих PAP. Пример добавления нового пользователя показан ниже:

Рисунок 4.7. Добавление нового пользователя

PPP chap secrets ?	
Username	<input type="text" value="user1"/> Username for secrets file required
Password	<input type="text" value="pass1"/> Password for secrets file required
Server	<input type="text" value="*"/> Server name for secrets file required
IP address	<input type="text" value="*"/> IP address for secrets file required

- Username - имя пользователя
- Password - пароль пользователя
- Server - имя сервера ВПН, "звездочка" - любой
- IP address - IP-адрес, выдаваемый клиенту. "Звездочка" - любой.

Сервер DNS

Сервер ДНС отвечает за преобразование доменного имени в IP-адрес. Его настройка осуществляется на странице Services/DNS server:

Рисунок 4.8. Настройка сервера ДНС

DNS Settings ?	
Enable DNS server	<input checked="" type="checkbox"/> Check this item if you want use DNS server on your router

Для активации сервера ДНС необходимо поставить флажок напротив *Enable DNS server*. Добавление новой зоны осуществляется в форме Zones, в которой отображаются зоны, обслуживаемые сервером ДНС:

Рисунок 4.9. Зоны сервера DNS

Zones ?				
Zone id	Zone name	Admin	Serial	
✘ domain1	example1.com	vasya@example1.com	2006091400	⊕ ⊗
✔ domain2	example2.com	petya@example2.com	2006091601	⊕ ⊗

При добавлении новой зоны, необходимо ввести следующие параметры:

- Zone id - идентификатор зоны, можно ввести имя зоны (этим идентификатором называется файл, в котором хранится зона)
- Zone - имя зоны (доменное имя, для которого создается зона)
- Enable - активна ли зона
- Name server - авторитетный сервер DNS для домена
- Admin - адрес электронной почты администратора зоны
- Refresh - время, через которые ведомые сервера DNS (slave) будут обновлять зону
- TTL - время, которое запись зоны может храниться в кэше
- retry - время, через которое ведомый сервер в случае неудачи повторит попытку обновить зону
- expire - время, через которое информация о зоне перестает считаться действительной

После добавления соответствующая запись появится в таблице зон. Пример добавления показан ниже:

Рисунок 4.10. Добавление зоны

DNS Zone options ?	
Zone id	<input type="text" value="sigrandruid"/> Identifier of zone - just a simple name
Zone	<input type="text" value="sigrandru"/> Name of zone
Enable	<input checked="" type="checkbox"/> Check this item to enable zone
Name server	<input type="text" value="nssigrandru"/> A name server that will respond authoritatively for the domain
Admin	<input type="text" value="admin@sigrand.ru"/> Email of zone admin
Refresh	<input type="text" value="28800"/> Time (seconds) when the slave will try to refresh the zone from the master.
TTL	<input type="text" value="86400"/> Time (seconds) to live
retry	<input type="text" value="7200"/> Defines the time (seconds) between retries if the slave (secondary) fails to contact the master when refresh (above) has expired
expire	<input type="text" value="1209600"/> Indicates when (seconds) the zone data is no longer authoritative.

Переход на добавление записей в зону осуществляется щелчком мыши по идентификатору или имени зоны. При добавлении новой записи нужно ввести следующие параметры:

- Domain or host - имя (или IP-адрес, если зона реверсивная)
- Type of record - тип записи. Возможны следующие значения:
 - A - указывает IP-адрес, соответствующий имени
 - CNAME - синоним другого имени. В этом случае в качестве DATA указывается соответствующее имя
 - MX - имя почтового сервера для данного домена
 - NS - указывает авторитетный сервер ДНС для зоны (по сути - делегирование зоны)
 - PTR - указывает имя для данного IP-адреса. Используется в реверсивной зоне)
 - TXT - дополнительная текстовая информация
- Priority - приоритет текущей записи MX
- Data - данные записи - доменное имя или IP-адрес, либо какая-то текстовая информация

Пример добавления новой записи показан ниже:

Рисунок 4.11. Добавление записи в зону

DNS Zone options ?	
Domain or host	<input type="text" value="www"/> Domain
Type of record	<input type="text" value="A"/> Select type of record: A, NS,CNAME, MX, PTR, TXT
Priority	<input type="text"/> Priority used only on MX records
Data	<input type="text" value="192.168.2.101"/> Please input data for this record

Пример зоны после добавления записей:

Рисунок 4.12. Записи зоны DNS

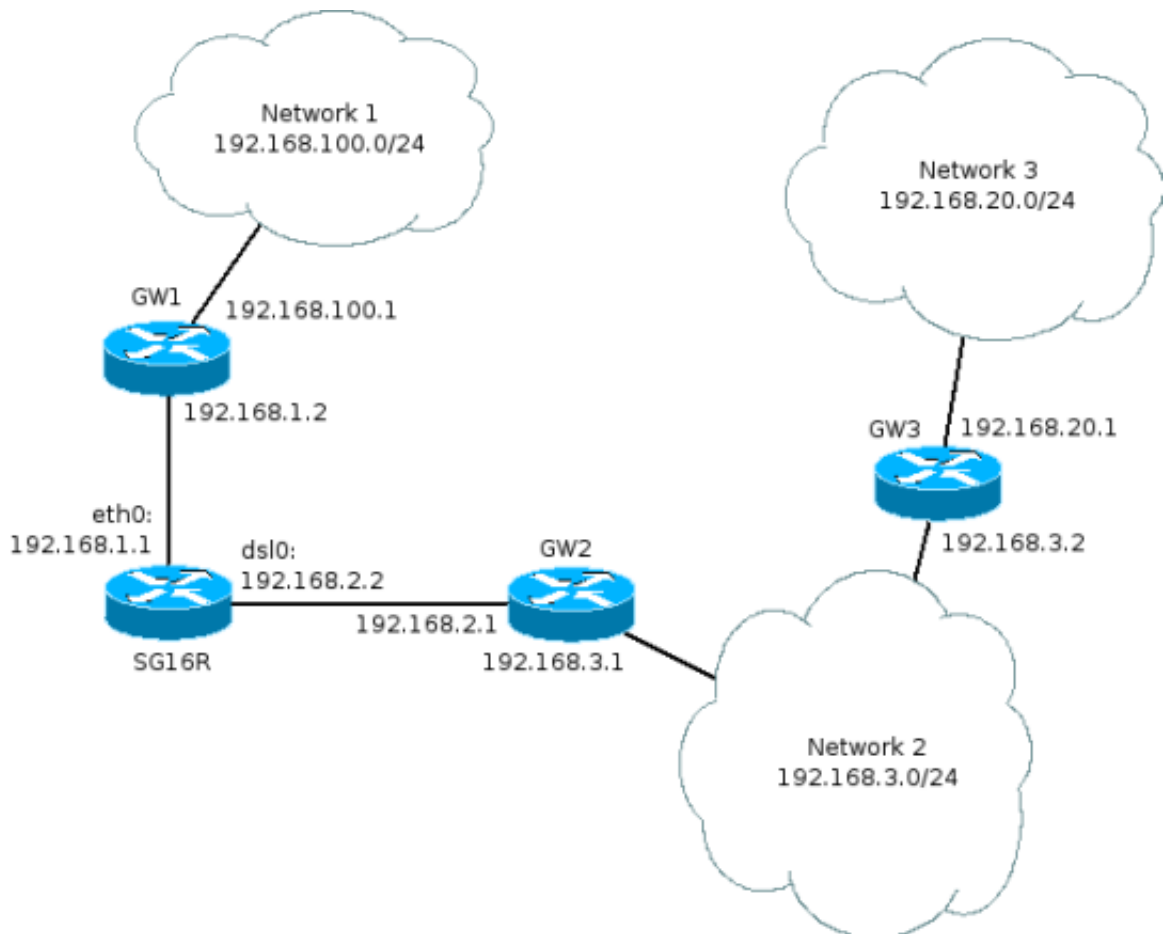
No	Domain	Type	Priority	Data	
0	@	A		192.168.2.100	⊕ ⓔ ×
1	www	A		192.168.2.101	ⓔ ×
2	mail	A		192.168.2.102	ⓔ ×
3	@	MX	10	mail	ⓔ ×

Глава 5. Управление трафиком

Добавление сетевых маршрутов

Сетевые маршруты определяют, через какие маршрутизаторы доступна та или иная сеть. Добавление маршрутов осуществляется на странице настройки того сетевого интерфейса, через который он пролегает. К примеру, сеть имеет следующую структуру:

Рисунок 5.1. Пример: структура сети



Наш маршрутизатор имеет обозначение SG16R, и подключен к двум маршрутизаторам - GW1 и GW2 через интерфейсы eth0 (Ethernet) и dsl0 (SHDSL) соответственно. Видно, что добавление маршрутов для сетей будет иметь вид:

- Network1: сеть 192.168.100./24 через маршрутизатор 192.168.1.2
- Network2: сеть 192.168.3.0/24 через маршрутизатор 192.168.2.1
- Network3: сеть 192.168.20.0/24 через маршрутизатор 192.168.2.1

Проанализировав маршруты, приходим к выводу, что маршрут на первую сеть относится к интерфейсу eth0, а на вторую и третью - к dsl0. Поэтому и добавление маршрутов через веб-интерфейс будет производиться на страницах соответствующих интерфейсов.

Замечание

Маршрут на сеть Network3 добавляется так же как и для сети Network 2 через маршрутизатор GW2 по причине того, что маршрутизатор SG16R не имеет прямого подключения к маршрутизатору GW3 и вынужден обращаться к нему через GW2.

Для добавления маршрута переходим на страницу конфигурации соответствующего маршруту интерфейса (к примеру, Network/Interfaces/eth0), где выбираем вкладку Routes:

Рисунок 5.2. Пустой список маршрутов



Изначально список пустой. Для добавления нового маршрута, нажимаем на кнопку со значком "+" и заполняем поля в новом окне:

Рисунок 5.3. Добавление маршрута

Static route settings

Network	<input type="text" value="192.168.30.0"/>	?
	Network or host (dotted quad) required	
Netmask	<input type="text" value="255.255.255.0"/>	?
	Netmask (dotted quad) required	
Gateway	<input type="text" value="192.168.90.20"/>	?
	Gateway for route (dotted quad) required	

После добавления маршрута, информация о нем появится в таблице маршрутов:

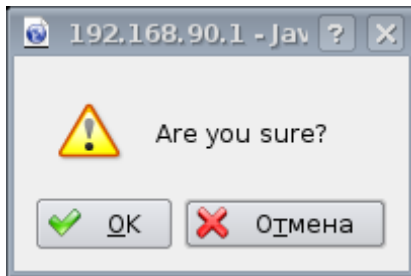
Рисунок 5.4. Список маршрутов

No	Network	Mask	Gateway	
0	192.168.20.0	255.255.255.0	192.168.90.10	⊕ ⊖ ⊗
1	192.168.30.0	255.255.255.252	192.168.90.20	⊕ ⊖ ⊗
2	192.168.40.0	255.255.255.0	192.168.90.20	⊕ ⊖ ⊗

Note: You should restart interface to apply settings

редактирование
удаление

Добавленные маршруты можно редактировать или удалять с помощью соответствующих кнопок. При удалении маршрута, потребуется подтвердить свои действия в диалоговом окне:

Рисунок 5.5. Удаление маршрута

Чтобы внесенные изменения вступили в силу, необходимо "перезагрузить" интерфейс, т.е. на вкладке General выключить/включить его. Если же через этот интерфейс осуществляется управление маршрутизатором, то необходимо перезагрузиться.

Замечание

Это будет исправлено в будущих версиях ПО для маршрутизатора: после добавления маршрута изменения будут вступать в силу автоматически без перезагрузки интерфейса.

Управление фаерволом

Фаервол используется, чтобы ограничить доступ к тем или иным сетевым ресурсам, основываясь на IP-адресах, портах отправителя и назначения, или используемого протокола.

Активация фаервола осуществляется на странице Network/Firewall:

Рисунок 5.6. Активация фаервола

Работа фаервола основана на прохождении пакетов цепочек правил, где каждое правило определяет одно из действий: прием или отброс пакета, основываясь на одном или нескольких критериях. Добавление правил осуществляется на странице Network/Firewall/Filter. Для каждой цепочки устанавливается действие по-умолчанию - политика, т.е. в случае, если пакет не попал ни под один критерий:

Рисунок 5.7. Политики цепочек

Default policy		
Default policy for FORWARD	DROP	?
Default policy for INPUT	ACCEPT	?
Default policy for OUTPUT	ACCEPT	?

Замечание

При установлении политики в значение DROP для цепочки INPUT или OUTPUT, удостоверьтесь, что в этих цепочках есть разрешающие правила, иначе управление маршрутизатором может быть потеряно.

Для правила определены следующие действия:

- ACCEPT - прием пакета
- DROP - отброс пакета без отправки уведомления источнику пакета
- REJECT - отброс пакета с отправкой уведомления

Цепочку FORWARD проходят пакеты, являющиеся транзитными, т.е. идущие с одного интерфейса маршрутизатора на другой:

Рисунок 5.8. Цепочка FORWARD

FORWARD								
No	Rule name	Src	Dst	Proto	Src port	Dst port	Action	
0	blockhost	10.20.30.0/24	0.0.0.0/0	all	any	any	✗ DROP	⊕ ⊗
1	rule4	192.168.30.0/24	10.0.0.0/0	all	any	any	↑ ACCEPT	⊕ ⊗

В цепочку INPUT попадают пакеты, предназначенные маршрутизатору:

Рисунок 5.9. Цепочка INPUT

INPUT								
No	Rule name	Src	Dst	Proto	Src port	Dst port	Action	
0	WWW_ACCEPT	0.0.0.0/0	0.0.0.0/0	tcp	any	80	↑ ACCEPT	⊕ ⊗
1	DNSACCEPT	0.0.0.0/0	0.0.0.0/0	all	any	53	↑ ACCEPT	⊕ ⊗
2	FTPREJECT	0.0.0.0/0	0.0.0.0/0	tcp	any	21	✗ REJECT	⊕ ⊗

В цепочку OUTPUT попадают пакеты, источником которых является маршрутизатор:

Рисунок 5.10. Цепочка OUTPUT

OUTPUT							
No	Rule name	Src	Dst	Proto	Src port	Dst port	Action
0	IRCDROP	0.0.0.0/0	0.0.0.0/0	all	any	6667	✗ DROP

Добавление правил осуществляется нажатием кнопки "+", и заполнением формы, открывшейся в новом окне:

Рисунок 5.11. Добавление правила

Firewall filter/forward edit rule	
Short name	<input type="text" value="blockhost"/> ? Name of rule
Enable	<input checked="" type="checkbox"/> ? Check this item to enable rule
Source	<input type="text" value="10.20.30.0/24"/> ? Source address specification
Destination	<input type="text" value="0.0.0.0/0"/> ? Destination address specification
Protocol	ALL ▾ ? The protocol of the rule or of the packet to check
Source port	<input type="text" value="any"/> ? Source port or port range specification.
Destination port	<input type="text" value="any"/> ? Destination port or port range specification.
Action	DROP ▾ ?

- Short name - имя правила. Должно включать только английские буквы и цифры
- Enable - активно ли правило
- Source - IP-адрес или сеть источника пакета
- Destination - IP-адрес или сеть получателя пакета

- Protocol - протокол
- Source port - порт источника пакета
- Destination port - порт получателя пакета
- Action - действие, выполняемое над пакетом

Удаление и редактирование правила осуществляется соответственно кнопками "x" и "e".

Замечание

Если внесенные вами изменения не вступают в силу, проверьте, что вы активировали фаервол на странице Network/Firewall.

NAT

NAT - network address translation - позволяет заменять адреса источника или отправителя пакета.

NAT является частью фаервола, поэтому схема управления остается той же, меняется только действие. Все сетевые пакеты, являются ли они транзитными или предназначаются маршрутизатору, попадают сперва в цепочку PREROUTING, где над ними может быть выполнено несколько действий. В этой цепочке не рекомендуется производить фильтрацию пакетов, для этого надо использовать цепочку FORWARD фаервола. Цепочка PREROUTING предназначена для выполнения DNAT - destination NAT, т.е. замена адреса получателя пакета.

Рисунок 5.12. Цепочка PREROUTING

PREROUTING ?							
No	Rule name	Src	Dst	Proto	Src port	Dst port	Action
0	CTRLALLOW	192.168.2.1	0.0.0.0/0	all	any	any	ACCEPT
1	mail	0.0.0.0/0	0.0.0.0/0	tcp	any	25	DNAT

В цепочку POSTROUTING идут пакеты, выходящие с маршрутизатора, транзитные или сгенерированные на маршрутизаторе. В этой цепочке можно выполнить SNAT - source NAT - замену адреса отправителя, с указанием адреса, либо MASQUERADE - смысл тот же, только адрес замена будет выбираться автоматически (удобно при работе с динамическими интерфейсами и IP-адресами).

Рисунок 5.13. Цепочка POSTROUTING

POSTROUTING ?							
No	Rule name	Src	Dst	Proto	Src port	Dst port	Action
0	masquarade	192.168.1.0/24	0.0.0.0/0	all	any	any	SNAT
1	VPN	10.20.30.0/24	0.0.0.0/0	all	any	any	SNAT

Для этих цепочек так же выставляются политики, т.е. действия для пакетов, не попавшие ни под одно правило:

Рисунок 5.14. Политики цепочек

Default policy ?	
Default policy for PREROUTING	DROP
Default policy for POSTROUTING	ACCEPT

Замечание

Т.к. в цепочку PREROUTING попадают пакеты, предназначенные самому маршрутизатору, перед выставлением политики DROP убедитесь, что в цепочке есть правило, разрешающее прохождение пакетов для управления маршрутизатором.

Добавление правил осуществляется нажатием кнопки "+", расположенной рядом с заголовком соответствующей таблицы:

Рисунок 5.15. Добавление правила

Firewall nat/prerouting edit rule ?	
Short name	<input type="text" value="mail"/> Name of rule
Enable	<input checked="" type="checkbox"/> Check this item to enable rule
Source	<input type="text" value="0.0.0.0/0"/> Source address specification
Destination	<input type="text" value="0.0.0.0/0"/> Destination address specification
Protocol	TCP ▾ The protocol of the rule or of the packet to check
Source port	<input type="text" value="any"/> Source port or port range specification.
Destination port	<input type="text" value="25"/> Destination port or port range specification.
Nat to address	<input type="text" value="11.11.11.11"/> Do Source NAT or Destination NAT to address
Action	DNAT ▾

Добавление правила и поля аналогично добавлению правила в фаерволе (Network/Firewall/Filter), добавляется только одно новое поле:

- Nat to address - IP-адрес, которым будет заменяться адрес отправителя или получателя, в зависимости от действия. При выполнении действий, отличных от SNAT и DNAT, заполнение поля необязательно.

Редактирование и удаление правил осуществляется с помощью кнопок "e" и "x", расположенных рядом с правилом.

Для работы NATа необходимо активировать фаервол на странице Network/Firewall.

Качество обслуживания

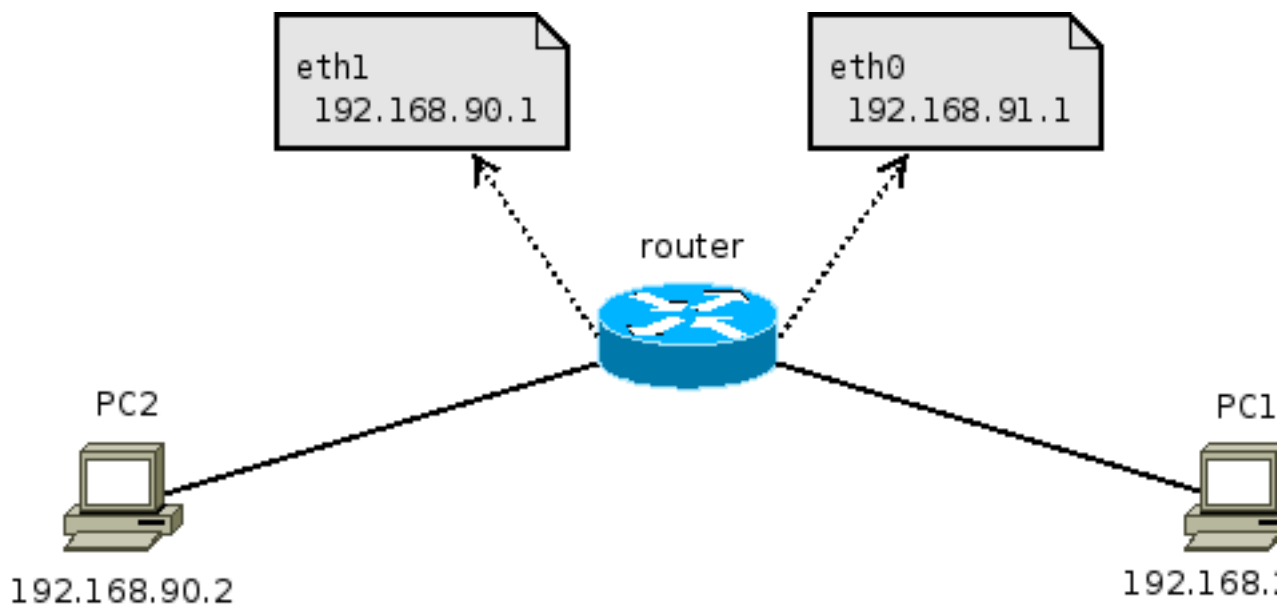
Качество обслуживания (QoS - quality of service) позволяет отдать предпочтение определенным пользователям или типам трафика, определяя их на основании IP-адресов или портов отправителя/получателя в разные классы трафика.

На данный момент управление качеством обслуживания возможно только через консольный интерфейс с помощью программы `tc`, позволяющей создавать классы, фильтры, а так же назначить дисциплину обслуживания.

Целью этой главы не является полное описание возможностей шейпинга трафика в ОС Linux (на которой базируется ПО маршрутизатора), а лишь рассмотрение основных моментов его использования.

В первую очередь следует отметить, что управлять скоростью можно только исходящего трафика (что, в общем, вполне разумно), поэтому при написании правил шейпинга необходимо определить интерфейс, на котором этот трафик будет исходящим. Рассмотрим в качестве примера простую сеть, схема которой представлена ниже:

Рисунок 5.16. Пример сети



К примеру, если мы хотим ограничить пропускную способность канала для входящего трафика к хосту PC2, то нам необходимо работать с интерфейсом `eth1` маршрутизатора, поскольку через него проходит исходящий трафик к хосту PC2. В качестве примера ограничим весь трафик, поступающий на PC2, для этого нам необходимо выполнить следующие команды:

```
# tc qdisc add dev eth1 root handle 1: htb
# tc class add dev eth1 parent 1: classid 1:1 htb rate 200kbps
# tc filter add dev eth1 parent 1: prio 1 protocol ip u32 match ip dst 192.168.90.2
```

Первая команда указывает, что для интерфейса `eth1` будет использоваться HTB - пакетный шедюлер, непосредственно и занимающийся шейпингом трафика (к примеру, еще есть CBQ). Вторая команда создает класс, являющимся дочерним первого

(параметр `parent 1:`), назначает ему идентификатор `1:1` (`classid 1:1`), и максимальную скорость в 200kbps - кбайт в секунду. Последняя команда создает фильтр с приоритетом 1 (`prio 1`), назначающийся корневому классу (`parent 1:`) и направляющий весь трафик, удовлетворяющий критерию, что IP-адрес получателя пакета равен 192.168.90.2 (`protocol ip u32 match ip dst 192.168.90.2`), в класс `1:1` (`flowid 1:1`).

Чтобы избежать путаницы, заранее рассмотрим принятые сокращения, описывающие скорость:

- `mbps` = 1024 kbps = 1024 * 1024 bps => byte/s => 1024 килобайт в секунду
- `mbit` = 1024 kbit => kilo bit/s => 1024 килобит в секунду

Шедулер НТВ построен следующим образом: к интерфейсу подключается сам шедулер НТВ. Классы, определяющие скорость трафика, могут добавляться как в корень, так и в другие подклассы, образуя иерархию классов. Фильтры добавляются в корень иерархии.

Подсказка

Особенность подклассов в том, что скорость одного подкласса может быть увеличена (в пределах скорости родительского класса) за счет *неиспользуемой* скорости другого подкласса.

В приведенном выше примере мы ограничили входящую скорость для хоста PC2. Но исходящая осталась неограниченной. Чтобы исправить положение, необходимо определить, какой интерфейс является исходящим для трафика с PC2. Это зависит от того, кто запрашивает трафик с PC2, в нашем случае это может быть только PC1, следовательно интерфейс, через который пойдет трафик к PC1, будет `eth0`. Создадим для этого интерфейса следующие правила:

```
tc qdisc add dev eth0 root handle 1: htb
tc class add dev eth0 parent 1: classid 1:1 htb rate 100kbps
tc filter add dev eth0 parent 1: prio 1 protocol ip u32 match ip src 192.168.
```

Этими правилами мы ограничили исходящую скорость с хоста PC2 100 килобайтами в секунду. В фильтре было изменено условие - теперь смотрится адрес отправителя пакета на совпадение с IP-адресом PC2.

Система шейпинга трафика в ОС Linux позволяет разделять трафик на различные классы, руководствуясь не только IP-адресами источников или приемников пакетов, но и используемыми портами. К примеру, чтобы ограничить трафик с порта SSH (22), выполним следующую команду:

```
tc filter add dev eth0 parent 1: prio 1 protocol ip u32 match ip sport 22 0xffff flowid 1:1
```

Так же можно использовать несколько критериев в одном фильтре:

```
# tc filter add dev eth1 parent 1: protocol ip prio 1 u32 \
  match ip dst 192.168.90.3 \
  match ip sport 22 0xffff flowid 1:1
```

Этим фильтром трафик, идущий к хосту с IP-адресом 192.168.90.3 с порта 22, направляется в класс `1:1`

На самом деле НТВ предоставляет еще более широкие возможности по управлению трафиком, о которых можно почитать на английском здесь [<http://lartc.org/howto/>], или перевод [<http://gazette.linux.ru.net/rus/articles/lartc/index.html>].