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
Сохранение/восстановление конфигурации	12
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 Е1	18
Настройка параметров интерфейса	18
Настройка сетевых параметров 2	20
Настройка работы SHDSL модемов в режиме Bonding 2	21
Настройка моста	24
4. Настройка сетевых служб 2	27
DHCP-сервер	27
5. Управление трафиком	30
Добавление сетевых маршрутов	30
Управление фаерволом	32
NAT	35

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 ДНС	. 9
2.6. Логирование	11
2.7. Конфигурация коммутатора	12
2.8. Сохранение конфигурации	12
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
36 Вклалка General	15
3.7. Вкладка Фетроа.	16
38 Виладка Method	16
30. Виладка Options	17
3.10. Создание пинамического интерфейса	17
3.11. Упаление динамического интерфейса	10
2.12. Выбол влотоково	10
	10
3.13. Конфигурация СГЗСО-ПОСС	19
3.14. Uniramed mode	20
3.15. Настроика интерфеиса	20
3.16. Настроика параметров линии связи	22
3.17. Настроика интерфеиса	22
3.18. Создание виртуального интерфеиса	23
3.19. Активация виртуального интерфеиса	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 ІР-адресов	28
4.3. Форма привязки IP к MAC	28
4.4. Обновленный список IP-адресов	29
5.1. Пример: структура сети	30
5.2. Пустой список маршрутов	31
5.3. Добавление маршрута	31
5.4. Список маршрутов	31
5.5. Удаление маршрута	32
5.6. Активация фаервола	32
5.7. Попитики цепочек	32
5.8 LIEROYKA FORWARD	33
5.9. Цепочка INPLIT	33
5 10 LIEROVKA OLITPUT	34
5.11 Побавление правила	34
5.12 Lenoura PREROLITING	35
	36
	50

Руководство по эксплуатации маршрутизатора SG-16R

5.14.	Политики цепочек	36
5.15.	Добавление правила	37

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

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:

- 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 вебинтерфейсе.

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

- ПК с СОМ-портом
- ТГТР сервер, находящийся в той же сети, что и маршрутизатор

Перед обновлением прошивки необходимо, чтобы в одной сети с маршрутизатором находился TFTP сервер, с которого будет производится обновление. После настройки TFTP сервера, 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 OC Windows или Minicom для OC 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:

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 МАС адресов (Enter new number of mac address) этот параметр следует пропустить (по умолчанию число МАС 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 addres: 00-05-5D-77-86-01
Number of mac address: 1
Enter new mac address (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:

Замечание

Приведенное выше меню соответсвует новому загрузчику, в который была добавлена возможность загрузки образов загрузчика и системы с TFTP-сервера, находящегося за маршрутизатором. Меню в старых вресиях 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 р. 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, соответсвующий 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 неправильнео 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 (OC>)) 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. маршрутизатором

Управление

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 255.255.25.0.

Конфигурация с помощью Веб-интерфейса

Конфигурация маршрутизатора выполняется через веб-интерфейс любым веббраузером, поддерживающем 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:

6	Sig	rand
System General Security Time SHDSL dsl0 dsl1 E1 hdlc0 Switch DNS Not Shi charfaces dsl0 dd1		sigrand
	System information	
	Name	sigrand1
	Version	0.2
	Platform	Linux - 2.6.16
	Hardware	ADM5120 Board
	Time	Sat Jan 1 02:16:39 MST 2000
Services	Uptime	02:16:39 up 16 min
DNS Server	CPU usage	
syslog	Memory usage	
omeng ping mtr dag tcpdump reboot Configuration backup restore Depent kdb	Webface is	s © 2005-2006 by Vladislav Meskovets. All rights reserved. [Sigrand]

Рисунок 2.1. Главная страница

Установка пароля

Важно

Настоятельно рекомендуется поменять 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

Password	
	C.48
	2462
	Set
	261
root system password	261
root system password	266

Имя маршрутизатора

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

Рисунок 2.3. Смена имени маршрутизатора

General settings		
Hostname	sigrand1	
110000101110	This is description for hostname	
	Save	

Синхронизация времени

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

Рисунок 2.4. Синхронизация времени

Time settings		
Use time synchronizing	Check this item if you want use time synchronizing	
Time server	pool.ntp.org Please input hostname or ip address time server	
Time zone	GMT-4	
	Save	

Настройка ДНС

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

Рисунок 2.5. Настройка ДНС

DNS Settings ?		
Upstream server	192.168.2.1 Please enter ip address of upstream dns server	
Domain	localnet Please enter your domain	
	Save	

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 ДНС 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;
- просмотреть 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 подключится 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
```

Password:

BusyBox v1.1.2 (2007.03.17-09:17+0000) Built-in shell (ash) Enter 'help' for a list of built-in commands.

Revision: r579 Builded at: 20070317 16:07

Замечание

Следует заметить, что изменения, внесенные в конфигурацию маршрутизатора через консольный интерфейс будут замены после перезагрузки параметрами, указанными в веб-интерфейсе.

Сводная информация

Параметр		Значение
IP-адрес (крайний пра	авый порт)	192.168.2.100
Сетевая маска		255.255.255.0
Веб-интерфейс		
	Протокол	HTTPS
	Логин	admin
	Пароль	1234
Консольный интерфе	ЙС	
	Протокол	SSH
	Логин	root
	Пароль	1234

Таблица 2.1. Сводная таблица

Логирование событий

Из-за особенности используемой встроенной памяти (flash-память) логи не сохраняются локально на маршрутизаторе, а пишутся в специальный буфер, доступный для просмотра через Tools/syslog. Маршрутизатор имеет несколько параметров, управляющих логированием:

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	<mark>64k</mark> ▼ Circular buffer size	
Enable remote syslog logging	X 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	
	Save	

- 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:

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 💌
	Save

Рисунок 2.7. Конфигурация коммутатора

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.

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

backup	restore	default
backup		
		Backu

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

backup	restore	default
restore ?		
Restore configuration		Restore configuration from file
Restore		

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 s	tatus
/sbin/ifc dsl0	<pre>config dsl0 Link encap:Ethernet HWaddr 00:FF:0F:E6:CB:CO 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</pre>
/usr/sbin 7: dsl0: link/ /usr/sbin 7: dsl0: link/ inet inet@ va	<pre>n/ip link show dev dsl0 mtu 1500 qdisc pfifo_fast qlen 1000 'ether 00:ff:0f:e6:cb:c0 brd ff:ff:ff:ff:ff n/ip addr show dev dsl0 mtu 1500 qdisc pfifo_fast qlen 1000 'ether 00:ff:0f:e6:cb:c0 brd ff:ff:ff:ff:ff 192.168.100.1/24 brd 192.168.100.255 scope global dsl0 5 fe80::2ff:ff:fee6:cbc0/64 scope link alid_lft forever preferred_lft forever</pre>

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 /p	cat /proc/sys/net/adm5120sw/status						
Port0	up	100M	full-duplex	enabled	vlanid=1	unit=0	
Portl	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 122212001111111
Sent 862404 bytes 1769 pkt (dropped 0, overlimits 0 requeues 0)
rate Obit Opps backlog Ob Op 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	Localinterface	
Enabled	×	
Auto	×	
Method Static address Please select method of the interface		
Save		

- 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) ір-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-adpec (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	192.168.2.100 Address (dotted quad) required	
Netmask	255.255.255.0 Netmask (dotted guad) required	
Broadcast	Broadcast (dotted quad)	
Gateway Default gateway (dotted quad)		
Save		

- 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	×	
Forwarding	×	
Proxy ARP		
RP Filter		
		Save

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) icmp-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 МАС-адреса интерфейса:

Рисунок 3.9. Вкладка Specific

Ethernet Specific parameters ?		
MAC Address	00:FF:0F:e6:cb:c2 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

Delete dynamic interface ?		
Interface	Please select interface -	
Delete		

Конфигурация интерфейса Е1

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

hdlc0 modem settings	
HDLC protocol	CISCO-HDLC
Encoding	nrz 💌
Darity	creté.ibi V

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

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

Рисунок 3.13. Конфигурация CISCO-HDLC

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 могу 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 ATC 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 Кбит/с = 1088 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:

hdlc0 modem settings	
HDLC protocol	CISCO-HDLC
Interval	10
Timeout	25
E1 framed mode	Check to enable
E1 long haul mode	Check to enable
E1 HDB3/AMI line code	HDB3
CRC	CRC16
Fill	FF 💌
Inversion	off 💌
	Save

Рисунок 3.14. Unframed mode

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	Qo5	Routes
Enabled						
Auto						
Method		None	•			
Save						

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

Соединение Е1 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. Нас	тройка парамет	ров линии связи
-------------------	----------------	-----------------

dsl0 modem settings		
Rate	6016 V Select DSL line rate	0
Mode	Slave Select DSL mode	0
Coding	TCPAM32 Select DSL line coding	0
Config	Select DSL configuration mode	0
Annex	Annex A Select DSL Annex	0
CRC	CRC32 Select DSL CRC length	0
Fill	FF - Select DSL fill byte value	0
Inversion	Select DSL inversion mode	0
	Save	

- 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, парметр Enabled должен быть активным, Auto отключенным, а Method равен None:

Рисунок 3.17. Настройка интерфейса

Status	General	Method	Options	Specific	DHCP	Qo5	Routes
Enabled		×					0
Auto							Ø
Method		Nor	ie se select method	of the interface			Ø
			Save				

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

Add dynamic interfa	ce	
Protocol	Bonding	0
	Please select interface protocol	
	Add	

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

Status General	Method	Options	Specific	DHCP	QoS	Routes
Enabled	×					0
Auto	×					Ø
Method	Sta	Static address Please select method of the interface				0
Save						

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

Рисунок 3.20. При	исвоение ІР-адреса
-------------------	--------------------

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Static addres	5	19 Add	2.168.210.1 ress (dotted quad	required			Ø
Netmask		255 Net	5.255.255.0 mask (dotted quar	() required			Ø
Broadcast			adcast (dotted qu	ad)			Ø
Gateway		Def	Default gateway (dotted quad)				Ø
			Save				

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	Qo5	Routes
Bonding Spec	ific parameters						
MAC Address MAC Address for interface							0
Interfaces dsi0 dsi1 Interfaces for bonding separated by space							Ø
			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 межуд 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

Add dynamic interface		
Protocol	Bridge Please select interface protocol	?
	Add	

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

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Enabled							0
Auto							0
Method		Sta	tic address se select method	• of the interface			0
Save							

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 ІР-адреса

Status	General	Method	Options	Specific	DHCP	QoS	Routes
Static addres	s	19 Add	2.168.100.2 ress (dotted quad) required			?
Netmask		255 Netr	5.255.255.0 mask (dotted quad) required			0
Broadcast		Bro	adcast (dotted qu	ad)			0
Gateway		Defa	ault gateway (dott	ed quad)			0
			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 Specif	ic parameters						
STP Enabled		Enal	ble Spanning Tree	Protocol			0
Interfaces		eth Inter	0 dsl0 faces for l				0
Priority Forward delay		Brid	ge priority Note	npeel etho ethi asio s You can use only E laces, like ethX, dslX s interfaces should b	themet-like e enabled, but		0
			auto	should be switched o	0		
Hello time							0
Max age							0
			Save]			

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		×					0
Auto		×					0
Method		Sta	tic address se select method	▪ of the interface			0
Save							

Эту же процедуру повторяем на втором маршрутизаторе, и через пару минут, в течении которых "мост" распознает топрологию 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:

Status General Meth	od Options Specific DHCP QoS Routes					
Enable DHCP server Check this item if you want use DHCP server on your LAN						
Start IP	192.168.100.2 Start of dynamic ip range address for your LAN (dotted quad) required					
End IP	192.168.100.20 End of dynaic ip range address for your LAN (dotted quad) required					
Netmask	255.255.255.0 Netmask for your LAN (dotted quad) required					
Default router	192.168.100.3 Default router for your LAN hosts (dotted quad)					
Default lease time	10 minutes 💌					
DNS server	192.164.300.20 DNS server for your LNN hosts (dotted quad)					
Domain	Allows DHCP hosts to have fully qualified domain names					
NTP server	NTP server for your LAN hosts (dotted quad)					
WINS server	WINS server for your LAN hosts (dotted quad)					
	Party.					

Рисунок 4.1. Настройка DHCP-сервера

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 МАС адреса сетевой карты. Форма для привязки IP адреса к МАС адресу находится внизу страницы конфигурации и представлена на рисунке:

Рисунок 4.2. Список статических IP-адресов

DHCP Static leases					
No	Name	IP Address	MAC Address	0	

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 МАС

DHCP Host settings	1			
Host name	pc1 Host name			
IP Address	192.168.150.15 IP Address for host			
MAC Address	A0:43:08:52:09:41 MAC Address for host			
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.

DHCP S	DHCP Static leases						
No	Name	IP Address	MAC Address	0			
0	pc11	192.168.150.15	A0:43:08:52:09:41	00			
1	pc12	192.168.150.16	A0:43:98:82:c4:39	00			

Рисунок 4.4. Обновленный список IP-адресов

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

0

X

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 производится 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/Interfsces/eth0), где выбираем вкладку Routes:

Рисунок 5.2. Пустой список маршрутов

Status	General	Method	Options	Specific	DHCP	QoS	Routes
No Network					Mask	Gateway	⊙
Note: You should restart interface to apply settings							

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	192.168.30.0 O Network or host (dotted quad) required				
Netmask	255.255.255.0 Netmask (dotted quad) required				
Gateway	192.168.90.20 ⑦ Gateway for route (dotted quad) required				
Save					

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

Рисунок 5.4. Список маршрутов

Status	General	Method	Options	Specific	DHCP	QoS	Routes
No	Netwo	rk		Mask		Gateway	\odot
0	192.168	20.0		255.255.25	5.0	192.168.90.10	(e) 😣
1	192.168	30.0		255.255.25	5.252	192.168.90.20	Θ×
2	192.168	.40.0		255.255.25	5.0	192.168.90.20	<u> </u>
Note: You shoul	d restart interface	e to apply settings				_	<u>_</u>
				редакти удалени	ировани Ие	e	

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

Рисунок 5.6. Активация фаервола

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 Netwokr/Firewall:

Firewall settings Enable Firewall Check this item if you want use firewall on your router Save

Работа фаервола основана на прохождением 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 -	0
Default policy for INPUT	ACCEPT -	0
Default policy for OUTPUT	ACCEPT -	0

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:

- АССЕРТ 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

FORV	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	@ Ø

В цепочку INPUT попадают пакеты, предназначающиеся маршрутизатору:

Рисунок 5.9. Цепочка INPUT

IN	РИТ								
N	0	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	08
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

OUTP	оитрит							
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	blockhost ⑦ Name of rule			
Enable	Check this item to enable rule			
Source	10.20.30.0/24 O			
Destination	0.0.0/0 Oestination address specification			
Protocol	ALL The protocol of the rule or of the packet to check 			
Source port	any 🕜 Source port or port range specification.			
Destination port	any ⑦ Destination port or port range specification.			
Action	DROP V			
	Save			

- 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.

НАТ 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.

PRER	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	៙⊗

Рисунок 5.12. Цепочка PREROUTING

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

POS	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, предназначающиеся 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	mail Name of rule			
Enable	X Check this item to enable rule			
Source	0.0.0/0 Source address specification			
Destination	0.0.0/0 Destination address specification			
Protocol	TCP - The protocol of the rule or of the packet to check			
Source port	any Source port or port range specification.			
Destination port	25 Destination port or port range specification.			
Nat to address	11.11.11.11 Do Source NAT or Destination NAT to address			
Action	DNAT -			
	Save			

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 "е" и "х", расположенных рядом с правилом.

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