Руководство пользователя
SG-16R/SG-17R

Руководство пользователя SG-16R/SG-17R

Copyright © 2007, 2008 ООО "Сигранд"

Аннотация

В данном руководстве рассмотрены вопросы настройки и эксплуатации маршрутизаторов ООО "Сигранд" 16-й и 17-й серии (SG-16R и SG-17R соответственно).

Приводится краткое описание характеристик и возможностей маршрутизатора, условий его эксплуатации, параметров сетевых интерфейсов, а так же описание поддерживаемых модулей.

Поясняются процедуры настройки сетевых интерфейсов и сервисов, а так же различных режимов работы маршрутизатора: мультиплексирование, бриджирование, объединение каналов (бондинг), VLAN, QoS, VoIP и другие.

Все торговые марки, знаки и зарегистрированные права на именования, упомянутые в настоящем документе, принадлежат соответствующим правообладателям.

Содержание

1. Описание маршрутизатора SG-16R/SG-17R 1
2. Комплектация поставки 3
    SG-16R 3
    SG-17R 3
3. Техническое описание 4
    Характеристики и параметры устройства 4
        Общие параметры 4
        Параметры линейного интерфейса SHDSL 4
        Параметры интерфейса E1 4
        Параметры интерфейса RS-232C 5
        Условия эксплуатации 5
    Характеристики SHDSL 5
        Дальность связи и скорость соединения 5
        Совместимость оборудования по интерфейсу SHDSL 7
        Подключение линии связи 7
    Внешний вид, назначение индикаторов и разъёмов SG-16R 8
    Внешний вид, назначение индикаторов и разъёмов SG-17R 10
    Сменные интерфейсы 12
        Модули SHDSL 12
        Модули E1 14
        Установка сменных интерфейсов 14
4. Начало работы с маршрутизатором 16
    Подготовка к первому включению 16
    Загрузчик 16
    Обновление прошивки маршрутизатора 17
    Установка программ 20
    MAC-адреса сетевых интерфейсов 21
5. Управление маршрутизатором 22
    Настройка маршрутизатора 22
        Настройка с помощью Веб-интерфейса 22
        Настройка через консольный интерфейс 24
        Сводная информация 24
    Логирование событий 24
    Настройка встроенного Ethernet коммутатора 25
    Установление зависимостей SHDSL — Ethernet 26
    Мониторинг SHDSL каналов 27
        Мониторинг через веб-интерфейс 27
        Мониторинг через консоль 29
        Правила приоритетов параметров производительности SHDSL канала 30
    Сохранение/восстановление конфигурации 30
6. Настройка сетевых интерфейсов 32
    Общие параметры 32
        Вкладка Status 32
        Вкладка General 33
        Вкладка Method 34
        Вкладка Options 35
        Вкладка Specific 36
    Настройка интерфейса SHDSL 36
        Настройка параметров интерфейса 36
        Настройка через демон EOCd 42
        Настройка сетевых параметров 44
    Настройка интерфейса E1 44
        Настройка параметров интерфейса 44
        Диагностирование соединения E1 47

Настройка сетевых параметров 48
Динамические интерфейсы 49
Работа с динамическими интерфейсами 49
Настройка режима Bonding 50
Настройка моста 52
Настройка соединения PPtP 55
Настройка соединения PPPoE 57
Настройка интерфейсов VLAN 58
Принцип хранения настроек для модулей 59
7. Настройка сетевых служб 60
DHCP-сервер 60
PPTP-сервер 61
Сервер DNS 64
8. Управление трафиком 69
Добавление сетевых маршрутов 69
Управление межсетевым экраном 71
NAT 73
Качество обслуживания 77
Бесклассовая дисциплина pfifo_fast 77
Бесклассовые дисциплины FIFO with bytes buffer (bfifo) и FIFO with packets buffer (pfifo) 77
Бесклассовая дисциплина SFQ 77
Бесклассовая дисциплина ESFQ 78
Бесклассовая дисциплина TBF 78
Классовая дисциплина HTB 79
IPSec 83
Введение 83
Контекст безопасности 84
Политика безопасности 86
Пример конфигурации 88
9. Мультиплексирование 95
Конфигурирование 95
Примеры конфигурации 97
10. VoIP 101
Основные сведения 101
Настройка основных параметров 102
Настройки взаимодействия с SIP-сервер 103
Маршрутизация звонков 103
Адресная книга 104
Режим Hotline 105
11. SNMP 107
Введение в SNMP 107
Уровень поддержки SNMP маршрутизатором 107
Настройка SNMPD 107
Взаимодействие SNMPD с EOCD 108
Пример использования 108
Поддерживаемое ПО для управления по SNMP 109
The Dude 109
MIB Browser 111
OpenNMS 112
12. Примеры конфигурации 114
VLAN 114
Организация независимых каналов между Ethernet-интерфейсами 114
Распределение трафика по Ethernet-портам в зависимости от VLAN ID 115
Ограничение доступа к управлению устройством с помощью VLAN 118
Организация управления устройством через интерфейс, входящий в состав моста или бондинга 120

VoIP 122
Обычные телефоны работают как два IP-телефона 122
Организация телефонного соединения через VoIP-шлюз 124
Организация связи через АТС 126
Организация связи через АТС с использованием двух маршрутизаторов 127
13. Гарантия и обязательства 130
14. Приложение 131
Особенности применения кодировок TCPAM 131
SG-16 132
SG-17 132

Список иллюстраций

2.1. Схема переходника DB-9F — RJ-45 3
3.1. Разъём RJ-45 8
3.2. Вид передней панели маршрутизатора с одним каналом SHDSL в форм-факторе 19" 8
3.3. Вид передней панели маршрутизатора с двумя каналами SHDSL в форм-факторе 19" 9
3.4. Вид задней панели маршрутизатора с питанием 220В/50Гц в форм-факторе 19" 10
3.5. Вид задней панели маршрутизатора с питанием AC 220В/50Гц и DC 36-72В в форм-факторе 19" 10
3.6. Передняя панель без сменных модулей 10
3.7. Вид задней панели маршрутизатора с питанием 36-72В DC 11
3.8. Вид задней панели маршрутизатора с питанием 220В/50Гц 11
3.9. Передняя панель с установленными модулями 12
3.10. Модуль на один канал SHDSL без дистанционного питания (MR-17H1) 12
3.11. Модуль на один канал SHDSL с дистанционным питанием (MR-17H1P2) 12
3.12. Модуль на два канала SHDSL без дистанционного питания (MR-17H2) 13
3.13. Модуль на два канала SHDSL с дистанционным питанием (MR-17H2P2) 13
3.14. Модуль на один канал E1 (MR-17G) 14
3.15. Модуль на два канала E1 (MR-17G2) 14
3.16. Передняя панель без сменных модулей 14
5.1. Смена пароля 22
5.2. Смена имени маршрутизатора 23
5.3. Синхронизация времени 23
5.4. Настройка DNS 23
5.5. Логирование 25
5.6. Настройка коммутатора 26
5.7. Общая статистика соединения 27
5.8. Таблица state 28
5.9. Таблица relative counters 29
5.10. Таблица current intervals 29
5.11. Таблица 15-ти минутных интервалов для CustSide 29
5.12. Таблица дневных интервалов для CustSide 29
5.13. Сохранение конфигурации 30
5.14. Восстановление конфигурации 30
6.1. Сетевые параметры 32
6.2. Сетевые маршруты 32
6.3. Таблица ARP 33
6.4. Встроенный коммутатор 33
6.5. Шейпер трафика 33
6.6. Управлени интерфейсом 33
6.7. Вкладка General 34
6.8. Вкладка Method 35
6.9. Вкладка Options 35
6.10. Вкладка Specific 36
6.11. Настройка SHDSL (MR16H) 37
6.12. Настройка SHDSL (MR17H) 39
6.13. Информация о состоянии соединения SHDSL (MR16H) 40
6.14. Информация о неустановленном соединении SHDSL (MR17H) 41
6.15. Информация об установленном соединении SHDSL (MR17H) 42
6.16. Создание и редактирование профилей соединения 43
6.17. Применение профиля соединения 43
6.18. Выбор протокола 44
6.19. Настройка протокола CISCO-HDLC 45
6.20. Unframed mode 47

6.21. E1: локальная петля 47
6.22. E1: удалённая петля 48
6.23. Назначение Point-to-Point адресов 48
6.24. Активация интерфейса E1 49
6.25. Создание динамического интерфейса 49
6.26. Динамический интерфейс в списке сетевых интерфейсов 49
6.27. Удаление динамического интерфейса 50
6.28. Настройка физического интерфейса 50
6.29. Создание динамического интерфейса 51
6.30. Привязка к физическим интерфейсам 51
6.31. Настройка динамического интерфейса 51
6.32. Пример моста 52
6.33. Пример моста с объединением интерфейсов 53
6.34. Настройка физического интерфейса 53
6.35. Создание интерфейса 53
6.36. Привязка к физическим интерфейсам 54
6.37. Настройка динамического интерфейса 54
6.38. Добавления интерфейса PPtP 55
6.39. Вкладка Specific 56
6.40. Вкладка General 56
6.41. Добавление интерфейса PPPoE 57
6.42. Вкладка Specific 57
6.43. Вкладка General 58
6.44. Добавление интерфейса VLAN 59
7.1. Настройка DHCP-сервера 60
7.2. Форма привязки IP к MAC 61
7.3. Обновленный список IP-адресов 61
7.4. Настройка PPTP-сервера 62
7.5. Пользователи VPN-сервера 63
7.6. Добавление нового пользователя 64
7.7. Настройка сервера DNS 64
7.8. Зоны сервера DNS 65
7.9. Добавление зоны 66
7.10. Добавление записи в зону 67
7.11. Таблица записей для зоны 68
8.1. Пример: структура сети 69
8.2. Пустой список маршрутов 70
8.3. Добавление маршрута 70
8.4. Список маршрутов 70
8.5. Активация межсетевого экрана 71
8.6. Политики цепочек 71
8.7. Цепочка FORWARD 72
8.8. Цепочка INPUT 72
8.9. Цепочка OUTPUT 72
8.10. Добавление правила 73
8.11. Цепочка PREROUTING 74
8.12. Цепочка POSTROUTING 74
8.13. Политики цепочек 75
8.14. Добавление правила 76
8.15. Конфигурирование ESFQ 78
8.16. Конфигурирования TBF 79
8.17. Класс по-умолчанию 80
8.18. Классы трафика 80
8.19. Фильтры, направляющие трафик в классы 80
8.20. Пример сети 81
8.21. Добавление класса 81
8.22. Добавление фильтра 82
8.23. Режимы работы IPSec 84

8.24. Создание контекста безопасности 85
8.25. Random keys 86
8.26. Создание политики безопасности 87
8.27. Пример конфигурации IPSec: схема сети 88
8.28. Создание контекста безопасности №1, направление 192.168.3.101-192.168.3.100 89
8.29. Создание контекста безопасности №2, направление 192.168.3.100-192.168.3.101 90
8.30. Создание политики безопасности №1 для SG1 91
8.31. Создание политики безопасности №2 для SG1 92
8.32. Создание политики безопасности №1 для SG2 93
8.33. Создание политики безопасности №2 для SG2 94
9.1. Схема сети 95
9.2. Физическая организация мультиплексирования 96
9.3. Настройка мультиплексирования 96
9.4. Пример сети 98
9.5. Взаимодействие интерфейсов на линии 0 98
9.6. Взаимодействие интерфейсов на линии 1 99
9.7. Использование одной линии для выставления и получения данных 100
10.1. Основные настройки VoIP 102
10.2. Настройки взаимодействия с SIP-серверами 103
10.3. Маршрутизация звонков 103
10.4. Маршрутизация звонков: добавление новой записи 104
10.5. Адресная книга 104
10.6. Адресная книга: добавление новой записи 105
10.7. Таблица настройки Hotline 105
11.1. The Dude 110
11.2. The Dude: маршрутизаторы Sigrand 111
11.3. MIB Browser 112
11.4. OpenNMS 113
12.1. Схема взаимодействия устройств 114
12.2. Вкладка Specific интерфейса моста (br*) 115
12.3. Структурная схема 116
12.4. Привязка к физическим интерфейсам 117
12.5. Создание интерфейса VLAN на основе моста 118
12.6. Добавление интерфейсов в мост 119
12.7. Активация интерфейса моста 119
12.8. Установка метода назначения IP-адреса 119
12.9. Назначение IP-адреса 120
12.10. Запуск интерфейса VLAN 120
12.11. Добавление интерфейсов в мост 121
12.12. Установка метода назначения IP-адреса 121
12.13. Назначение IP-адреса 122
12.14. Запуск моста 122
12.15. Обычные телефоны работают как два IP-телефона 123
12.16. Организация телефонного соединения через VoIP-шлюз 124
12.17. Настройки для вызовов через VoIP-шлюз 125
12.18. Организация связи через АТС 126
12.19. Организация связи через АТС с использованием двух маршрутизаторов 127

Список таблиц

3.1. Таблица дальности/скорости для SG-16 6
3.2. Таблица дальности/скорости для SG-17 6
3.3. Таблица дальности/скорости для SG-17+ 7
3.4. Совместимость оборудования по интерфейсу SHDSL 7
5.1. Сводная таблица 24
12.1. Таблица маршрутизации 123
12.2. Адресная книга маршрутизатора 032 123
12.3. Адресная книга маршрутизатора 033 123
12.4. Таблица Hotline для маршрутизатора 032 124
12.5. Адресная книга 125
12.6. Таблица Hotline 126
12.7. Адресная книга 126
12.8. Таблица Hotline для маршрутизатора 127
12.9. Таблица маршрутизации 128
12.10. Адресная книга маршрутизатора 032 128
12.11. Адресная книга маршрутизатора 128
12.12. Таблица Hotline для маршрутизатора 032 129
12.13. Таблица Hotline для маршрутизатора 033 129
14.1. Допустимые значения для режима CFG=LOCAL, ANNEX A 132
14.2. Рекомендуемые значения для режима CFG=LOCAL, ANNEX A 132
14.3. Допустимые значения для режима CFG=PREACT, ANNEX F 132
14.4. Рекомендуемые значения для режима CFG=PREACT, ANNEX F 132
14.5. Допустимые значения 132
14.6. Рекомендуемые значения 132

Глава 1. Описание маршрутизатора SG-16R/SG-17R

Маршрутизаторы Sigrand SG-16R, Sigrand SG-17R предназначены для организации межсетевого взаимодействия в сетях с произвольной конфигурацией, в которых используются различные протоколы и физические канальные уровни. Маршрутизатор SG-17R имеет наращиваемую модульную архитектуру и работает с модулями E1, SHDSL и VoIP. Так же имеется возможность увеличения дальности связи при сохранении требуемой скорости при использовании совместно с маршрутизаторами SG-17R регенераторов SG-17E, при этом возможно получать информацию о канале связи со всех регенераторов, работающих на линии.

Программное обеспечение маршрутизатора разрабатывается на основе операционной системы GNU/Linux с ядром версии 2.6 и распространяется в соответствии с лицензией GNU GPL.

Ограничение ответственности

Фирма-изготовитель, по понятным соображениям, не может нести ответственность за работоспособность ПО, разработанного сторонними лицами и не прошедшего тестирования на совместимость с базовым ПО устройства в ООО «Сигранд». Также, мы не можем нести ответственность за последствия применения такого ПО, приведшего к неработоспособности или ограничению функциональности устройства.

Маршрутизаторы SG-16R и SG-17R имеют следующий функционал:

- Настройка через веб-интерфейс.
- Сохранение и восстановление конфигурации.
- Сохранение настроек сменных интерфейсов с привязкой к номеру слота.
- Логирование событий.
- Независимая настройка Ethernet-портов коммутатора.
- Дополнительные Ethernet-сервисы на основе VLAN технологий.
- Мультиплексирование синхронных каналов и/или маршрутизация IP трафика.
- В режиме мультиплексирования при использовании многопарного соединения, агрегирование остатков полос от потоков E1 в один логический канал для транспорта Ethernet.
- Бриджирование трафика и объединение физических интерфейсов для увеличения скорости передачи данных.
- Поддержка сетевых интерфейсов: SHDSL, E1, Ethernet.
- Работа с SHDSL интерфейсами: SG-17 и SG-17+, обеспечивающие скорости 5.7 и 14 Мбит/с по одной паре (для SG-17R).
- При использовании SHDSL интерфейсов, обеспечение удалённого питания для регенераторов SG-17E (для SG-17R).
- Поддержка сетевых служб: DHCP, PPTP, DNS.

- Управление трафиком: NAT, Firewall, QoS.
- Встроенный мониторинг SHDSL тракта в соответствии со стандартом G.SHDSL (G.991.2).
- Поддержка SNMP: MIB-II, HDSL2-SHDSL-LINE-MIB.
- Безопасное VPN соединение при использовании протоколов: IPSec, PPPoE, PPtP.

Глава 2. Комплектация поставки

SG-16R

- Маршрутизатор.
- Блок питания от сети 220В/50Гц (для настольной версии) или сетевой шнур для подключения к сети 220В/50Гц (для стоечного форм-фактора).
- Переходник DB-9F — RJ-45 для подключения к терминальному порту маршрутизатора.
- Компакт-диск с программным обеспечением и документацией.
- Гарантийный талон.

Схема переходника DB-9F — RJ-45 приведена на рисунке.

Рисунок 2.1. Схема переходника DB-9F — RJ-45

SG-17R

- Шасси маршрутизатора.
- При типе питания DC 36-72В — ответная часть разъёма питания; при типе питания 220В/50Гц — сетевой шнур питания.
- Терминальный провод DB-9M — DB-9F.
- Компакт-диск с программным обеспечением и документацией.
- Гарантийный талон.

Глава 3. Техническое описание

Характеристики и параметры устройства

Общие параметры

- *Процессор* — 32-разрядный MIPS процессор с ядром 4KC, производительность 227 MIPS.
- *Оперативная память* — 64 MB SDRAM.
- *Дисковая память* — 32 MB flash.
- *Интерфейсы*:
  - 4 Ethernet/Fast Ethernet, auto negotiations, auto MDI/MDI-X.
  - *RS-232C* — для управления маршрутизатором.
  - 4 интерфейсных слота для установки модулей (для SG-17R).
- *Габариты* — 438x258x43 мм.
- *Вес* — 1,2 кг.
- *Питание* — 220 В/50 Гц или 36-72 В постоянного тока (в зависимости от модели и поставки).

Параметры линейного интерфейса SHDSL

- *Тип разъема*: RJ-45 (розетка).
- *Тип интерфейса*: G.SHDSL (рекоменд. ITU-T G.991.2.bis).
- *Тип соединения*: точка-точка.
- *Количество проводов линии связи*: 2 (одна пара). Используются контакты 4 и 5.
- *Скорость передачи*:
  - *SG-16*: 6 Мбит/с
  - *SG-17*: 5.7 Мбит/с
  - *SG-17+*: 14 Мбит/с
- *Линейный код*: TCPAM.
- *Вид связи*: полный дуплекс.
- *Дистанционное питание* (для моделей с поддержкой дистанционного питания)
  - *Напряжение*: 240 В.
  - *Максимальный ток*: 70 мА.

Параметры интерфейса E1

- *Тип разъема*: RJ-45 (розетка).

- *Число проводов в линии связи*: 4 (две пары). Контакты 4, 5 используются для передачи, 1, 2 — для приёма.
- *Линейный код (ITU-T G.703)*: HDB3, AMI.
- *Скорость передачи данных*: Nx64 кбит/с, где N=1:32, для каждого из интерфейсов E1 (64:2048 кбит/с с шагом 64 кбит/с).
- *Расстояние до оборудования DTE, км*: 2,4 (для кабеля 0,5 мм), 1,6 (для кабеля 0,4 мм).
- *Цикловая структура (framing)*: G.704.
- *Сверхциклы (superframe)*: CRC4, CAS.
- *Отключение цикловой структуры (unframed mode)*: есть.

Параметры интерфейса RS-232C

- *Тип разъема*:
  - *SG-16R*: RJ-45 (розетка).
  - *SG-17R*: DB-9F.
- *Скорость передачи, бит/сек*: 115 200.
- *Протокол*: 8-N-1.
- *Управление потоком*: нет.

Условия эксплуатации

Маршрутизатор предназначен для эксплуатации в закрытом отапливаемом помещении при следующих климатических условиях:

- *Температура воздуха*: 10 .. 40 °C.
- *Относительная влажность воздуха*: до 85%.
- *Атмосферное давление*: 84 .. 107 кПа.

Характеристики SHDSL

Дальность связи и скорость соединения

Условия тестирования

Информация о дальности связи и скорости соединения приведена ниже. Результаты получены на линиях длиной, при которой коэффициент ошибок (Bit Error Rate, BER) равен или меньше 10^{-7}. Указанная дальность проверена экспериментальным путём на контрольной линии связи лаборатории компании.

Результаты, полученные при эксплуатации на реальных линиях связи, могут отличаться от приведённых значений ввиду отличий параметров этих линий от эталонной.

Разные серии маршрутизаторов и разные модули имеют различные показатели дальности/скорости.

SG-16

Таблица дальности/скорости для SHDSL версии SG-16 представлена ниже.

Таблица 3.1. Таблица дальности/скорости для SG-16

Скорость, кбит/с	Кабель сечением 0,4 мм, км	Кабель сечением 0,5 мм, км
6016	1,8	2,2
4608	2,0	2,6
3072	3,0	4,2
2304	3,8	5,4
1536	4,4	6,4
1024	5,0	7,6
512	5,8	9,0
256	6,6	10,0
128	7,4	11,4
64	7,4	11,4

SG-17

Таблица дальности/скорости для SHDSL версии SG-17 представлена ниже.

Таблица 3.2. Таблица дальности/скорости для SG-17

Скорость, кбит/с	Кабель сечением 0,5 мм, км	Кабель сечением 0,9 мм, км	Кабель сечением 1,2 мм, км
5696	2,6	5,0	8,6
4608	3,6	5,6	9,6
4096	4,0	7,4	12,4
3072	5,0	8,0	13,4
2304	5,4	11,2	19,0
2048	6,2	13,0	22,2
1536	7,0	15,8	26,6
1024	7,8	17,4	29,6
768	8,4	18,6	31,6
512	9,0	20,0	33,8
384	9,6	21,0	35,8
192	10,4	23,0	40,0

SG-17+

Таблица дальности/скорости для SHDSL версии SG-17+ представлена ниже.

Таблица 3.3. Таблица дальности/скорости для SG-17+

Скорость, кбит/с	Кабель сечением 0,5 мм, км
14080	1,2
12800	1,2
11520	1,4
10240	2,0
9216	2,2
8192	2,4
7168	3,0
6144	3,4
5696	3,6
5120	3,8
4608	4,0
4096	4,4
3072	5,0
2304	5,4
2048	6,2
1536	7,0
1024	7,8
768	8,4
512	9,0
384	9,6
192	10,4

Совместимость оборудования по интерфейсу SHDSL

Таблица совместимости оборудования по интерфейсу SHDSL приведена ниже. SG-16R относится к серии SG-16, а SG-17R — к серии SG-17.

Таблица 3.4. Совместимость оборудования по интерфейсу SHDSL

Серия/версия интерфейса	SG-16	SG-17	SG-17+
SG-16	+	-	-
SG-17	-	+	+

Подключение линии связи

Внимание

Удостоверьтесь, что предоставленная Вам линия связи не имеет посторонних источников электрического напряжения, и не подключена к какому-либо постороннему оборудованию АТС! Несоблюдение этого правила может привести к выводу из строя как маршрутизаторов, так и посторонней аппаратуры на линии связи!

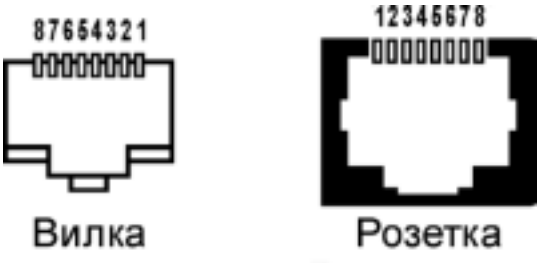
Для нормальной работы маршрутизаторов и обеспечения заданных параметров линия связи должна соответствовать следующим требованиям:

- Перед подключением линии связи удостоверьтесь, что на ней отсутствуют термопредохранители. Наличие термопредохранителей приводит к значительному снижению скоростных параметров. Так же невозможна работа на линиях, оснащённых катушками Пупина (пупинизированных линиях).
- Кабель не должен иметь замыканий жил и утечек на "землю" и на иные, в том числе и не подключённые к чему-либо, проводники. Линия связи не должна иметь ответвлений.
- В многопарном кабеле жилы должны быть взяты из одной пары.
- Параллельное включение нескольких пар (например, для уменьшения активного сопротивления) не допускается.

Отступление от указанных выше требований может привести к снижению показателей, или к полной неработоспособности линии связи.

Для подключения линии связи к маршрутизатору, установите вилку RJ-45 на кабель. Маршрутизатор использует только одну пару проводов, контакты 4 и 5, остальные контакты не задействованы.

Рисунок 3.1. Разъём RJ-45



Затем подключите кабель к разъёму SHDSL маршрутизатора.

Внешний вид, назначение индикаторов и разъёмов SG-16R

Маршрутизатор Sigrand SG-16R поставляется в настольном форм-факторе и в форм-факторе 19" для монтажа в коммуникационную стойку.

Вид передней панели маршрутизатора с одним и двумя каналами SHDSL, выполненного в форм-факторе 19", представлен ниже.

Рисунок 3.2. Вид передней панели маршрутизатора с одним каналом SHDSL в форм-факторе 19"

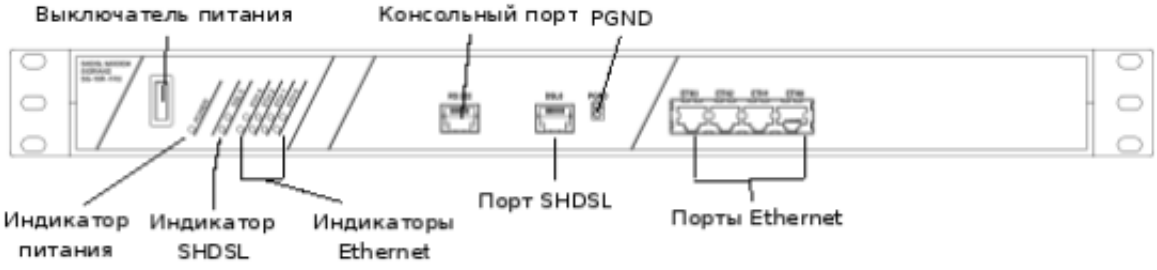
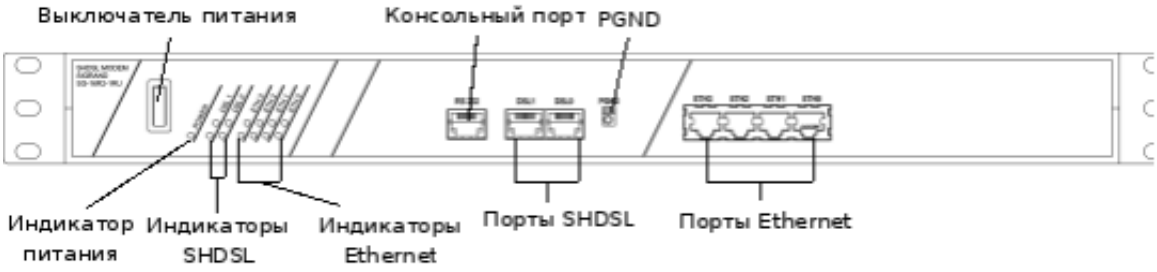


Рисунок 3.3. Вид передней панели маршрутизатора с двумя каналами SHDSL в форм-факторе 19"



- *Порты Ethernet* — RJ-45 порты для подключения по интерфейсу Ethernet.
- *Порты SHDSL* — RJ-45 порты для подключения по интерфейсу SHDSL.
- *PGND* — клемма для подключения заземления.
- *Консольный порт* — RJ-45 порт для управления маршрутизатором.
- *Индикаторы Ethernet* — каждому каналу соответствует два индикатора:
  - Верхний — *FD/C*:
    - *Горит* — полнодуплексный режим работы (Full duplex).
    - *Не горит* — полудуплексный режим работы (Half duplex).
    - *Мигает* — наличие коллизии в канале (Collision).
  - Нижний — *LINK*:
    - *Горит* — связь с удалённым устройством есть.
    - *Не горит* — связи с удалённым устройством нет.
    - *Мигает* — идёт обмен данными.
- *Индикаторы SHDSL*
  - Верхний — *ERR*:
    - *Не горит* — нет сбойных пакетов.
    - *Мигает* — получен сбойный пакет.
  - Нижний — *LINK*:
    - *Горит* — связь с удалённым устройством есть.
    - *Не горит* — связи с удалённым устройством нет.
    - *Мигает* — процесс установки связи.
- *Выключатель питания* — выключатель питания маршрутизатора.
- *Индикатор питания* — горит, когда маршрутизатор включён.

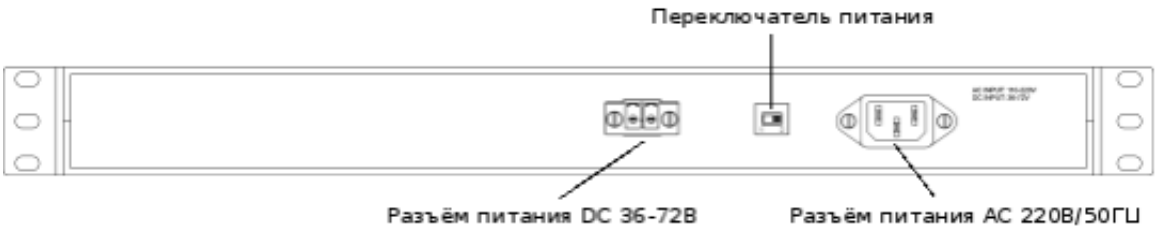
Вид задней панели маршрутизатора с питанием 220В/50Гц в форм-факторе 19" показан ниже.

Рисунок 3.4. Вид задней панели маршрутизатора с питанием 220В/50Гц в форм-факторе 19"

- *Разъём питания* — для подключения к сети 220В/50Гц.

Вид задней панели маршрутизатора с питанием AC 220В/50Гц и DC 36-72В в форм-факторе 19" показан ниже.

Рисунок 3.5. Вид задней панели маршрутизатора с питанием AC 220В/50Гц и DC 36-72В в форм-факторе 19"

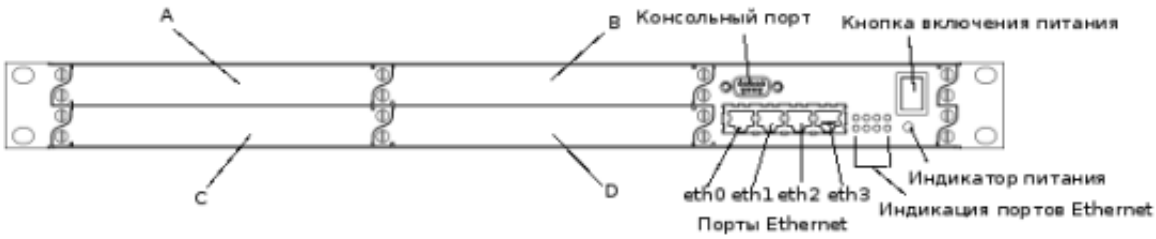


- *Разъём питания DC 36-72В* — для подключения к источнику питания постоянного тока 36-72В.
- *Разъём питания AC 220В/50Гц* — для подключения к сети 220В/50Гц.
- *Переключатель питания* — переключатель питания DC 36-72В / AC 220В/50Гц.

Внешний вид, назначение индикаторов и разъёмов SG-17R

Маршрутизатор Sigrand SG-17R поставляется в форм-факторе 19" для монтажа в коммуникационную стойку. Вид передней панели без установленных модулей представлен на рисунке.

Рисунок 3.6. Передняя панель без сменных модулей



- *A,B,C,D* — слоты для установки сменных модулей.

Важно

Слот *D* может быть использован только для установки модулей SHDSL и E1 для работы в режиме *мультиплексирования*. Соответствующий сетевой

интерфейс будет виден в системе и веб-интерфейсе и будет доступен для настройки, но он не будет иметь возможности передавать сетевой трафик (трафик, идущий не по линиям мультиплексирования). Связано это с отсутствием поддержки DMA для данного слота.

- *Консольный порт* — RS-232C порт для управления маршрутизатором.
- *Порты Ethernet* — RJ-45 порты для подключения по интерфейсу Ethernet.
- *Индикация портов Ethernet* — каждому каналу соответствует два индикатора:
  - Верхний — *FD/C*:
    - *Горит* — полнодуплексный режим работы (Full duplex).
    - *Не горит* — полудуплексный режим работы (Half duplex).
    - *Мигает* — наличие коллизии в канале (Collision).
  - Нижний — *LINK*:
    - *Горит* — связь с удалённым устройством есть.
    - *Не горит* — связи с удалённым устройством нет.
    - *Мигает* — идёт обмен данными.
- *Кнопка включения питания* — кнопка включения маршрутизатора.
- *Индикатор питания* — горит, когда маршрутизатор включён.

Вид задней панели маршрутизатора с питанием 36-72В постоянного тока (DC) показан ниже.

Рисунок 3.7. Вид задней панели маршрутизатора с питанием 36-72В DC

- *Разъём питания* — для подключения к источнику питания постоянного тока 36-72В.

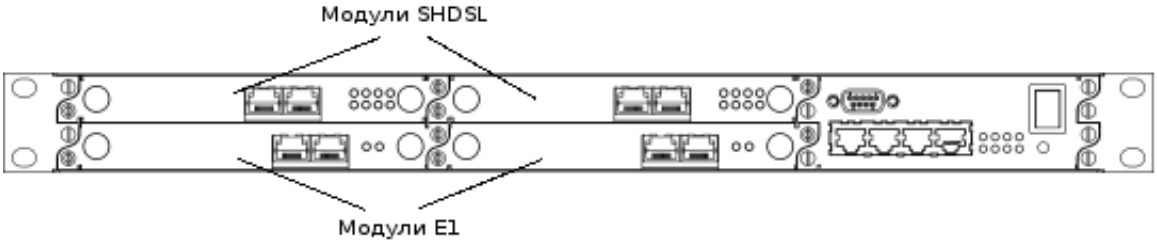
Вид задней панели маршрутизатора с питанием 220В/50Гц показан ниже.

Рисунок 3.8. Вид задней панели маршрутизатора с питанием 220В/50Гц

- *Разъём питания* — для подключения к сети 220В/50Гц.

Вид передней панели с установленными модулями SHDSL и E1 представлен ниже.

Рисунок 3.9. Передняя панель с установленными модулями



- *Модули SHDSL* — два двухканальных модуля SHDSL с дистанционным питанием.
- *Модули E1* — два двухканальных модуля E1.

Сменные интерфейсы

При использовании маршрутизатора SG-17R имеется возможность расширять его функциональные возможности за счёт использования сменных модулей — на данный момент это модули SHDSL и E1.

Модули SHDSL

Существует несколько типов модулей SHDSL:

- Один канал SHDSL без дистанционного питания (MR-17H1).
- Два канала SHDSL без дистанционного питания (MR-17H2).
- Один канал SHDSL с дистанционным питанием (MR-17H1P2).
- Два канала SHDSL с дистанционным питанием (MR-17H2P2).

Рисунок 3.10. Модуль на один канал SHDSL без дистанционного питания (MR-17H1)

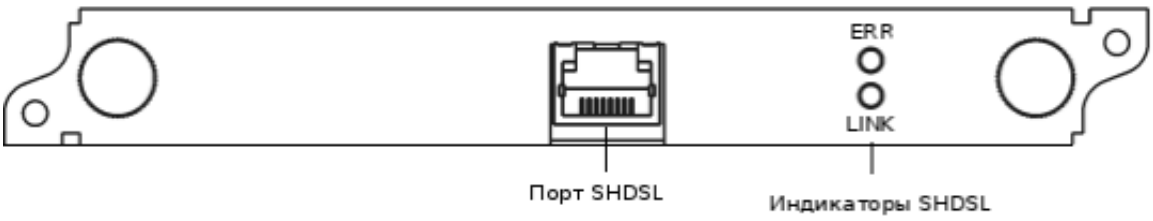


Рисунок 3.11. Модуль на один канал SHDSL с дистанционным питанием (MR-17H1P2)

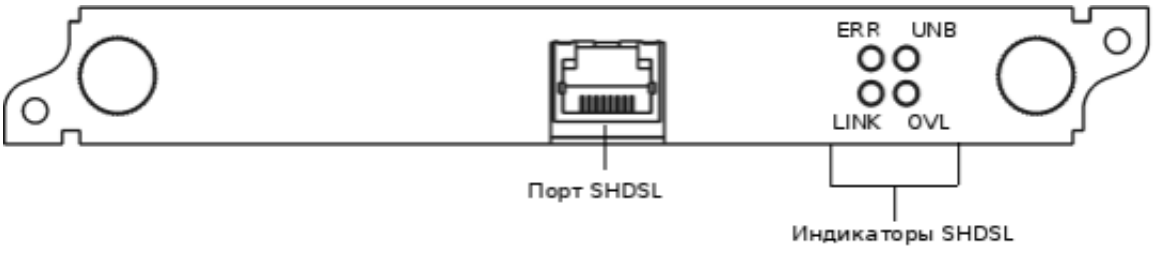


Рисунок 3.12. Модуль на два канала SHDSL без дистанционного питания (MR-17H2)

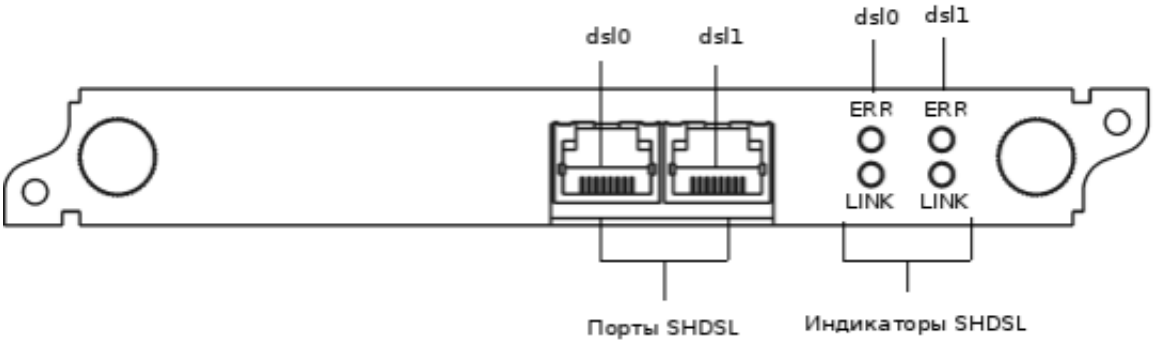
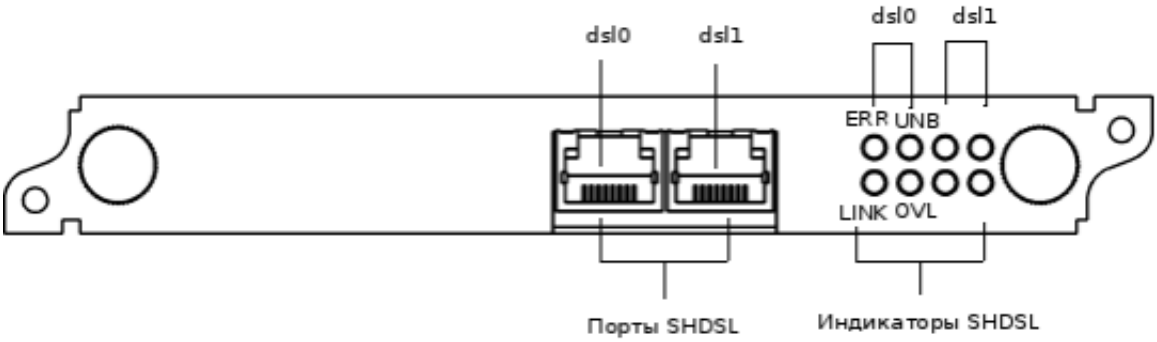


Рисунок 3.13. Модуль на два канала SHDSL с дистанционным питанием (MR-17H2P2)



- *Порты SHDSL* — RJ-45 порты для подключения по интерфейсу SHDSL.
- *Индикаторы SHDSL*
  - *ERR*:
    - *Не горит* — нет сбойных пакетов.
    - *Мигает* — получен сбойный пакет.
  - *LINK*:
    - *Горит* — связь с удалённым устройством есть.
    - *Не горит* — связи с удалённым устройством нет.
    - *Мигает* — процесс установки связи.
  - *UNB*:
    - *Горит* — нарушен баланс питания относительно земли. В норме на одном проводе +120 В, на другом — 120 В. Если перекос больше 30 В или отсутствует земля — это означает несбалансированность питания.
    - *Не горит* — баланс питания в норме.
  - *OVL*:
    - *Горит* — перегрузка питания. Это вызвано слишком большим числом (больше 4) регенераторов на линии, настроенных на питание от данного маршрутизатора.

- *Не горит* — перегрузки питания нет.

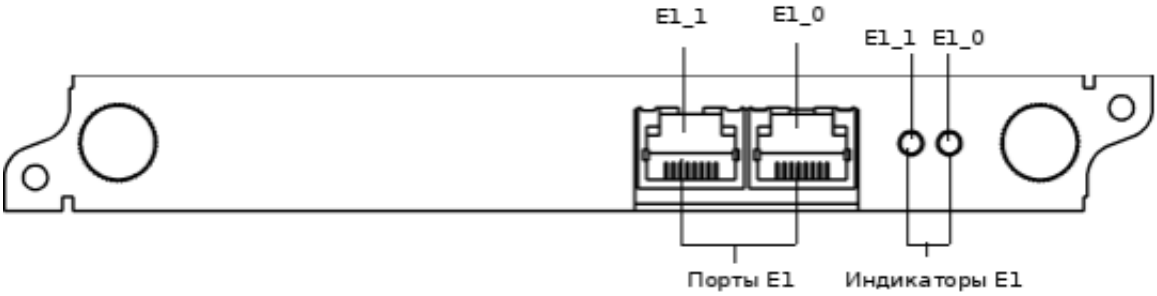
Модули E1

Существует несколько типов модулей E1:

- Один канал E1 (MR-17G).
- Два канала E1 (MR-17G2).

Рисунок 3.14. Модуль на один канал E1 (MR-17G)

Рисунок 3.15. Модуль на два канала E1 (MR-17G2)



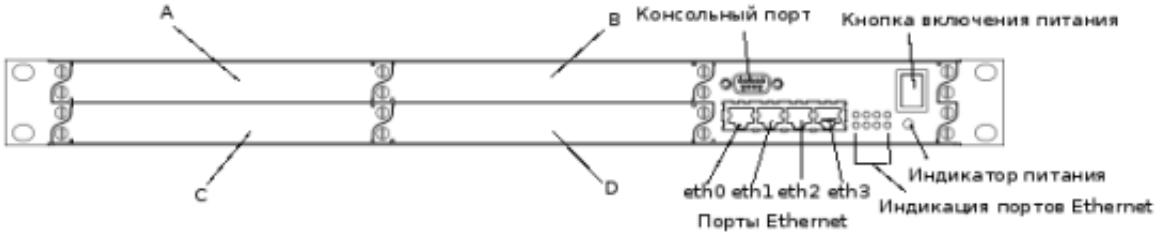
- *Порты E1* — RJ-45 порты для подключения по интерфейсу E1.
- *Индикаторы E1*
  - *Горит* — связь с удалённым устройством есть.
  - *Не горит* — связи с удалённым устройством нет.

Установка сменных интерфейсов

Важно

Для установки модулей можно использовать только слоты A, B и C маршрутизатора.

Рисунок 3.16. Передняя панель без сменных модулей



Установка модуля выполняется следующим образом:

1. Выключить питание маршрутизатора.
2. Снять с маршрутизатора заглушку, закрывающую слот.
3. Установить модуль в слот.
4. Зафиксировать его при помощи крепёжных винтов.
5. Включить питание маршрутизатора и произвести настройку установленного модуля.

Глава 4. Начало работы с маршрутизатором

Подготовка к первому включению

Важно

Удостоверьтесь в отсутствии внешних повреждений, возможно, полученных при транспортировке устройства. В случае наличия таковых, просьба немедленно связаться со службой гарантийной поддержки ООО «Сигранд».

Внимание

В случае, если устройство перевозилось или хранилось при отрицательной температуре — включение его допускается только по истечении часа нахождения при комнатной температуре!

Извлеките маршрутизатор из упаковки и расположите его на столе или иной ровной горизонтальной поверхности. Подключите соответствующее питание (220В/50Гц или DC 36-72В).

Если требуется управление маршрутизатором по консольному интерфейсу, например, для обновления прошивки маршрутизатора (см. Обновление прошивки маршрутизатора, или для диагностики процесса загрузки, соедините консольный порт маршрутизатора с последовательным портом компьютера с помощью переходника (для SG-16R) или терминального провода (для SG-17R).

Для управления маршрутизатором по консольному интерфейсу используется любая терминальная программа — HyperTerminal для ОС Windows или Minicom для ОС GNU/Linux. Настройки последовательного порта приведены выше, в разделе Параметры интерфейса RS-232C.

Для настройки маршрутизатора через веб-интерфейс соедините его интерфейс eth0 с сетевым адаптером компьютера или портом коммутатора локальной сети при помощи стандартного патч-корда.

Включение маршрутизатора производится выключателем питания, расположенным на лицевой панели.

Загрузчик

Меню загрузчика доступно при подключении к маршрутизатору по консольному 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:


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:

```
================================
Bootloader Menu
[1] Xmodem Download
[2] TFTP Download
[3] Print Boot Params
[4] Set Boot Params
[5] 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.

Обновление прошивки маршрутизатора

Важно

Перед перепрошивкой следует сохранить конфигурацию (см. раздел Сохранение/восстановление конфигурации), т.к. установка новой прошивки вернёт все параметры в исходное состояние, а так же сбросит установленные производителем MAC-адреса (см. раздел MAC-адреса сетевых интерфейсов).

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

- Компьютер с последовательным интерфейсом.
- 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]. Последняя версия прошивки находится по адресу http://sigrand.ru/temp/sigrand.

Как подготовить маршрутизатор для управления по консольному интерфейсу написано в разделе Подготовка к первому включению. 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:


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:

```
================================
Bootloader Menu
[1] Xmodem Download
[2] TFTP Download
[3] Print Boot Params
[4] Set Boot Params
[5] 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:

- *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.
========================
Current mac addres: 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 приведённом примере был введён только IP адрес маршрутизатора, остальные параметры оставлены без изменений.

После настройки сетевых параметров, следует выбрать пункт меню 2 (TFTP 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 system: openwrt

TFTP Client Menu
==============================
[S]: Update system
[P]: Set parameters
[X]: exit
Enter your option:
```

Замечание

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

Первые три 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 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 system file name : openwrt
```

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
```

PASS, соответствующий строчкам Eraseing flash и Programming flash означает, что обновление 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 загрузки новой прошивки необходимо выполнить перезагрузку маршрутизатора нажатием на кнопку RESET или включением/выключением питания.

После загрузки маршрутизатора (при обычной загрузке не требуется входить в меню загрузчика, поэтому надо подождать, пока истечёт таймер и начнётся загрузка операционной системы), 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 всё корректно, то следует проверить настройки, введённые в пункте Set Boot Params. Так же может помочь смена MAC-адреса и проверка, не блокирует ли сервер TFTP соединения с маршрутизатора.

Установка программ

Функциональность маршрутизатора может быть расширена за счёт установки дополнительного программного обеспечения, поставляемого в виде пакетов.

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-сервере 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`*).

MAC-адреса сетевых интерфейсов

MAC-адреса для сетевых интерфейсов (Ethernet, SHDSL, E1) хранятся в конфигурационном файле (kdb).

На данный момент существует два способа начального присвоения MAC-адресов:

- При *первой* после перепрошивки загрузке маршрутизатора происходит генерация случайных MAC-адресов для интерфейсов eth* и dsl0, dsl1. Такая генерация MAC-адресов не может гарантировать их уникальности для нескольких маршрутизаторов — т.е., два маршрутизатора могут сгенерировать одинаковые MAC-адреса. Чтобы свести вероятность повторения адресов к минимуму — первую загрузку следует производить, когда маршрутизатор подключён к сети ethernet, желательно с интенсивным трафиком — это увеличит случайность в генерации адресов.
- Затем запускается скрипт, реализующий второй способ присвоения MAC-адресов — получение списка MAC-адресов со специализированного сервера. Скрипт проверяет, доступен ли данный сервер — и если доступен, загружает с него список уникальных MAC-адресов, которые затем назначает сетевым интерфейсам. Данный способ доступен и используется только производителем маршрутизатора. При успешном обновлении MAC-адресов будет выдано соответствующее сообщение:

  ```
  Updating MAC addresses
  ```

  В случае, если указанный выше сервер недоступен, будет выдано соответствующее сообщение, попытки обновления MAC-адресов при последующих загрузках предприниматься не будут.

  ```
  MAC-address server is unreachable. You can update your MAC-address
  manually by running:
  /etc/init.d/updatekdb force
  ```

От изготовителя маршрутизатор поставляется с MAC-адресами, полученными со специализированного сервера, что гарантирует их уникальность для всех возможных интерфейсов маршрутизатора.

Так как MAC-адреса хранятся в конфигурационном файле — после перепрошивки они будут потеряны. Чтобы этого не произошло, перед перепрошивкой следует сохранить конфигурацию маршрутизатора (см. раздел Сохранение/восстановление конфигурации), а затем произвести её восстановление.

Глава 5. Управление маршрутизатором

Настройка маршрутизатора

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

Для настройки маршрутизатора необходимо соединить сетевую карту компьютера и Ethernet-порт eth0 патч-кордом. 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.

Настройка с помощью Веб-интерфейса

Настройка маршрутизатора выполняется через веб-интерфейс любым веб-браузером, поддерживающим протокол HTTPS и JavaScript: Internet Explorer с 6 версии, Opera, Mozilla Firefox. Для перехода к странице настройки 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.

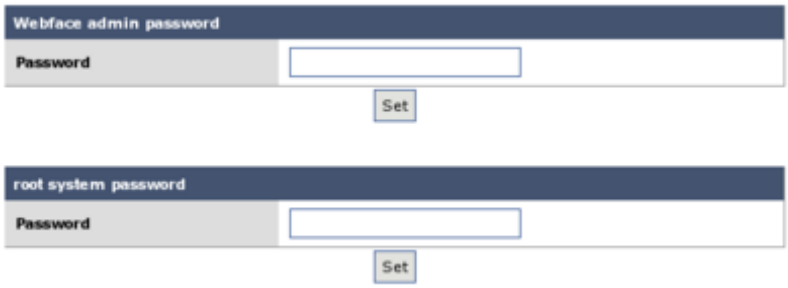
Установка пароля

Важно

Настоятельно рекомендуется поменять пароль для доступа к настройке маршрутизатора, это выполняется на странице System/Security.

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

Рисунок 5.1. Смена пароля



Имя маршрутизатора

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

Рисунок 5.2. Смена имени маршрутизатора

Синхронизация времени

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

Рисунок 5.3. Синхронизация времени

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 5.4. Настройка DNS

Информация о состоянии соединения SHDSL и E1 может быть получена на страницах General/SHDSL и General/E1 соответственно, настройка параметров линии связи для этих интерфейсов выполняется соответственно на страницах System/SHDSL/dsl* и System/E1/E1_*. Для более подробной информации о возможных настройках обратитесь к соответствующему разделу документации.

Управление интерфейсами осуществляется на страницах, указанных в меню Network. К примеру, настройка интерфейсов Ethernet осуществляется на страницах Network/Interfaces/eth*, SHDSL — на страницах Network/Interfaces/dsl*, а E1 — на Network/Interfaces/E1_*. 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 руководства.

В меню Tools расположены утилиты, позволяющие:

- Проследить за работой маршрутизатора, просмотрев логи — страницы *syslog* и *dmesg*;
- Выполнить перезагрузку с помощью *reboot*;
- Проверить работу сервера DNS 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.

Настройка через консольный интерфейс

Для настройки маршрутизатора через консольный интерфейс необходимо подключиться к нему по последовательному интерфейсу с помощью терминальной программы, либо по сети через Ethernet-порт по протоколу SSH (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.

Замечание

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

Сводная информация

Таблица 5.1. Сводная таблица

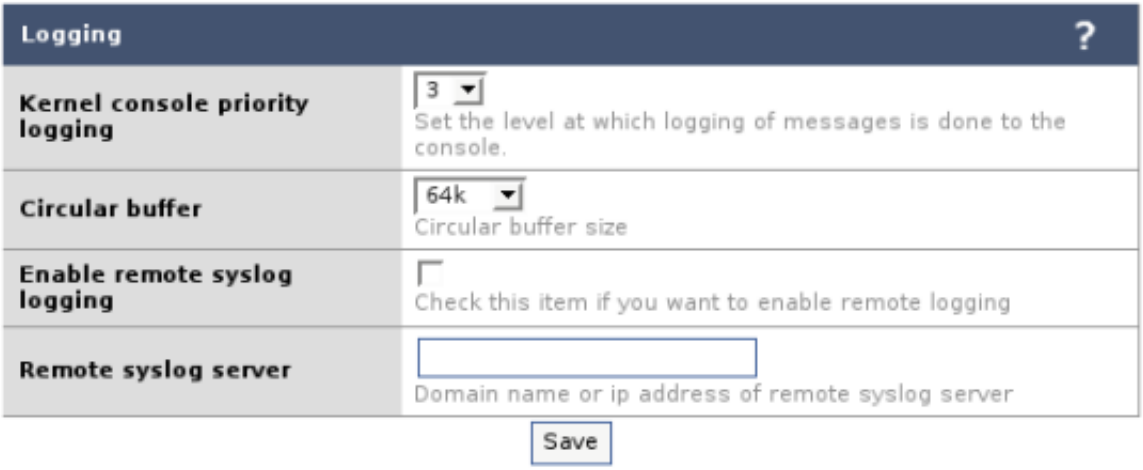
Параметр		**Значение**
IP-адрес (крайний правый порт)		192.168.2.100
Сетевая маска		255.255.255.0
Веб-интерфейс		
	Протокол	HTTPS
	Логин	admin
	Пароль	1234
Консольный интерфейс		
	Протокол	SSH
	Логин	root
	Пароль	1234

Логирование событий

Из-за особенностей используемой встроенной памяти (flash-память), системные события (логи) не сохраняются локально на маршрутизаторе, а пишутся в специальный

буфер, доступный для просмотра через Tools/syslog. Маршрутизатор имеет несколько параметров, управляющих логированием:

Рисунок 5.5. Логирование



- *Kernel console priority logging* — уровень приоритета системных сообщений, при котором они выводятся на консоль.
- *Circular buffer* — размер буфера.
- *Enable remote syslog logging* — включение логирования на удалённый syslog-сервер.
- *Remote syslog server* — адрес удаленного syslog-сервера.

Замечание

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

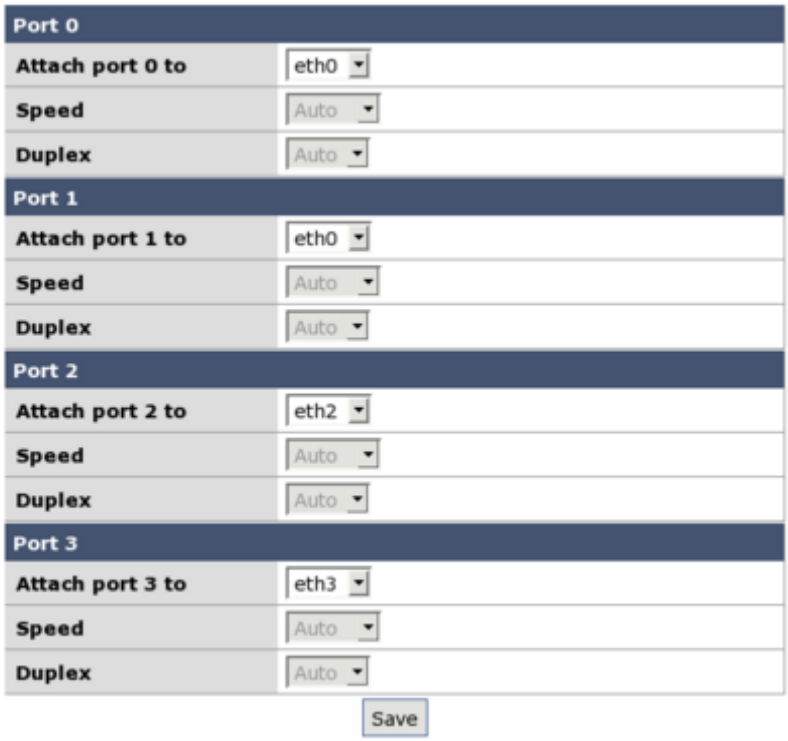
Замечание

Для того, чтобы удалённый 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 которой производится привязка физических портов коммутатора к сетевым интерфейсам. Отнесение нескольких портов к одному сетевому интерфейсу создаёт для них единую физическую среду, т.е. они начинают работать, как порты одного коммутатора. Окно настройки представлено на рисунке:

Рисунок 5.6. Настройка коммутатора



В приведённой 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.

Установление 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/dsl2eth/dsl2eth.map.

Изначально файл /etc/dsl2eth/dsl2eth.map пустой. Пример его заполнения показан в файле /etc/dsl2eth/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/dsl2eth/dsl2eth.map*

После внесения изменений в конфигурационный файл рекомендуется перезагрузить маршрутизатор.

Мониторинг SHDSL каналов

Замечание

Мониторинг поддерживают только модули MR17H.

Замечание

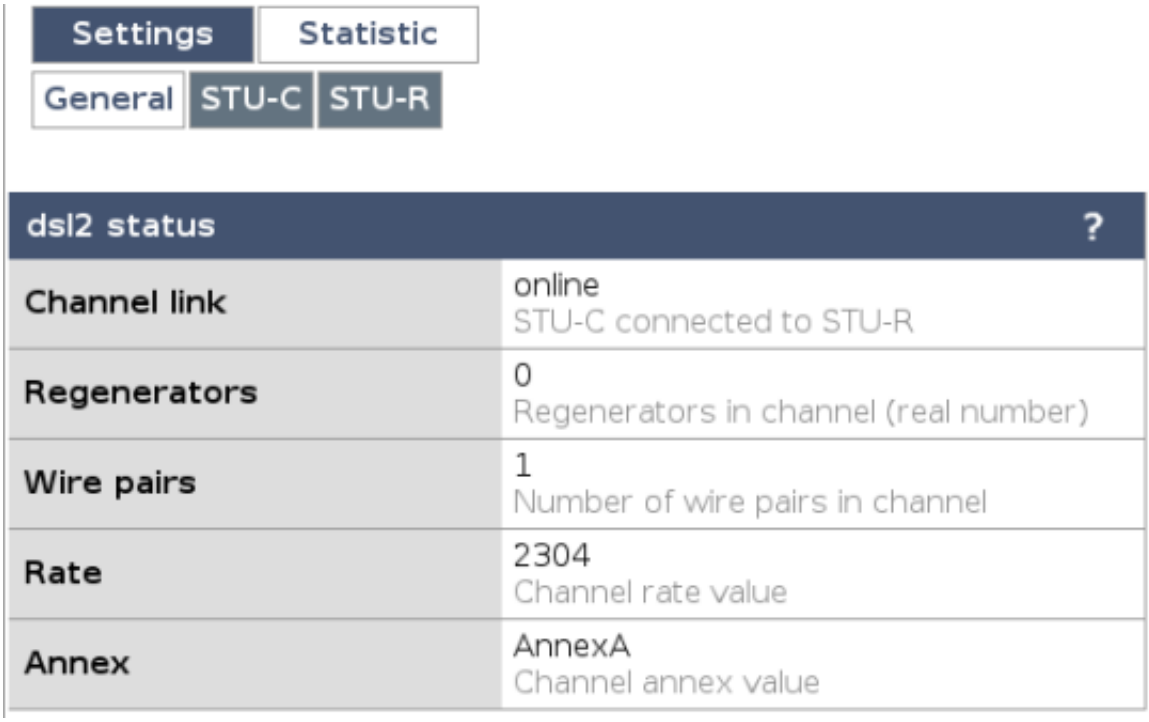
Получение статистики по каналу на данный возможно только с мастера.

Мониторинг через веб-интерфейс

Мониторинг SHDSL каналов позволяет получить информацию о различных параметрах и произошедших ошибках в линии связи. В случае, если в линии связи используются регенераторы *SG-17E*, то можно получать информацию о состоянии этих регенераторов и их количестве.

Просмотр статистики параметров канала доступен на странице System->SHDSL-EOC->имя_интерфейса, на вкладке Statistic. На вкладке General отображается общая статистика соединения.

Рисунок 5.7. Общая статистика соединения



- *Channel link* — состояние соединения между демонами EOCd. Если соединение установлено, но значение этого параметра установлено в *offline* — значит демоны EOCd не смогли установить между собой соединение. Это может быть вызвано несколькими причинами: один из демонов EOCd может быть не запущен, либо соответствующий интерфейс не управляется через EOCd.
- *Regenerators* — фактическое число регенераторов на линии.
- *Wire pairs* — число пар в канале.

- *Rate, Annex* — скорость передачи и дополнения.

Каждому юниту в канале (мастеру, слейву и регенераторам) соответствует своя вкладка, на которой отображаются параметры линии связи для данного юнита. Так, вкладки STU-C и STU-R соответствуют мастеру и слейву, а SRU1 — SRU8 — регенераторам.

Параметры производительности, характеризующие SHDSL канал:

- *Errored Second (ES)* — количество секундных интервалов, в которые была обнаружена одна или более CRC аномалий или более одного LOSW дефекта. При работе с данным параметром необходимо учитывать правила приоритетов параметров (см. правила приоритетов).

  ## Замечание

  Loss of Sync Defect (LOSW defect) – потеря синхронизации. В плезиохронном режиме дефект потери синхронизации должен обозначаться, когда не менее трех последовательно полученных кадров содержат ошибки синхронизации. Данные ошибки индицируются группой битов в кадре: Frame Sync Word, Stuff Bits и Stuff Bit Ids. Индикация LOSW очищается после получения не менее двух кадров не содержащих ошибок синхронизации, следующих друг за другом.

- *Severely Errored Second (SES)* — количество односекундных интервалов, в течение которых произошло не менее 50-ти CRC аномалий или более одного LOSW дефекта. (50 CRC аномалий в течение одной секунды соответствуют 30% некорректных кадров для стандартной длины кадра). При работе с данным параметром необходимо учитывать правила приоритетов параметров.

- *LOSW Second (LOSWS)* — количество секундных интервалов, в течение которых обнаружено более одного LOSW дефекта.

- *Unavailable Second (UAS)* — количество секундных интервалов, в течение которых SHDSL канал недоступен. Канал считается доступным после сбоя по прошествии 10 секунд, в течение которых не зарегистрировано ни одного SES. Данные 10 секунд исключаются из числа секунд, в которые канал был недоступен.

- *Code Violation (CV)* — количество CRC аномалий, обнаруженных за период, в течение которого производился мониторинг. При работе с данным параметром необходимо учитывать правила приоритетов параметров, которые будут описаны ниже.

Таблица *state* показывает текущие параметры линии (SNR и LoopAttn) и ошибки с момента начала мониторинга канала.

Рисунок 5.8. Таблица state

dsl2 state ?

Side	Pair	SNR	LoopAttn	ES	SES	CRC	LOSWS	UAS
CustSide	Pair1	22	1	0	0	0	8	0

- *Side* — сторона.

  ## Замечание

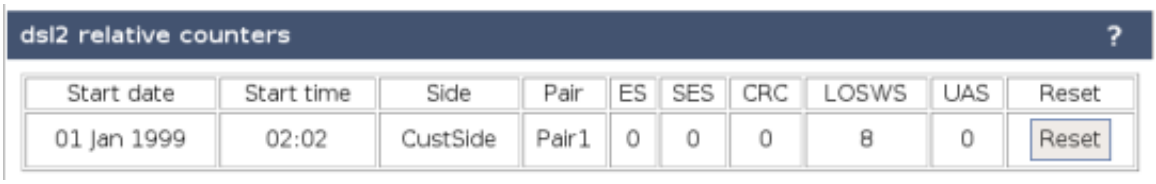
  Есть две группы, в которые входят параметры линии связи:

- *NetSide* — сторона мастера (линия связи, идущая к мастеру).
- *CustSide* — сторона клиента (линия связи, идущая к слейву).

- *Pair* — номер пары проводов.

Таблица *relative counters* содержит те же параметры, что и таблица *state*, предоставляя возможность их сбрасывания, чтобы проводить замеры в определённые промежутки времени.

Рисунок 5.9. Таблица relative counters

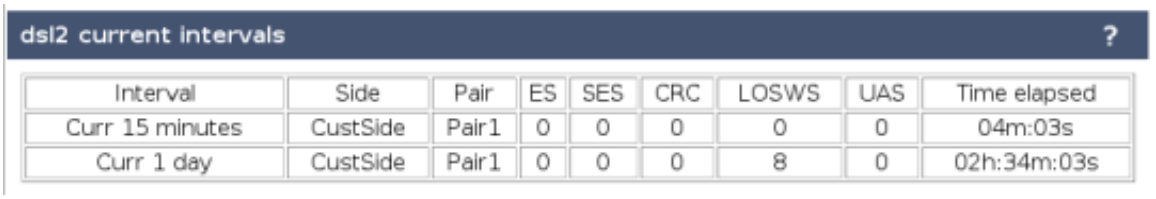


dsl2 relative counters ?

Start date	Start time	Side	Pair	ES	SES	CRC	LOSWS	UAS	Reset
01 Jan 1999	02:02	CustSide	Pair1	0	0	0	8	0	Reset

Таблица *current intervals* содержит ошибки за последние 15 минут и последний день. Значения обновляются, соответственно, каждые 15 минут и каждый день.

Рисунок 5.10. Таблица current intervals

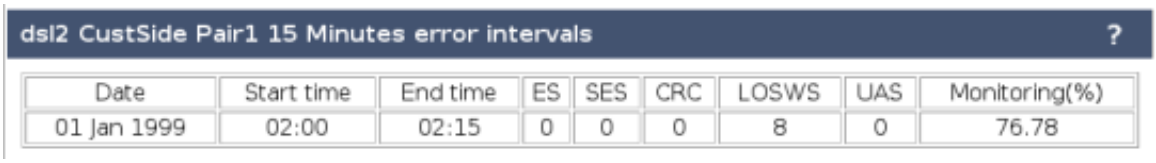


dsl2 current intervals ?

Interval	Side	Pair	ES	SES	CRC	LOSWS	UAS	Time elapsed
Curr 15 minutes	CustSide	Pair1	0	0	0	0	0	04m:03s
Curr 1 day	CustSide	Pair1	0	0	0	8	0	02h:34m:03s

Так же для каждой пары проводов и каждой стороны (NetSide и CustSide) ведутся таблицы, хранящие 15 минутные и дневные интервалы, в течении которых были ошибки. В таблицах хранится последние 96 15-ти минутных интервалов, и последние 30 — дневных.

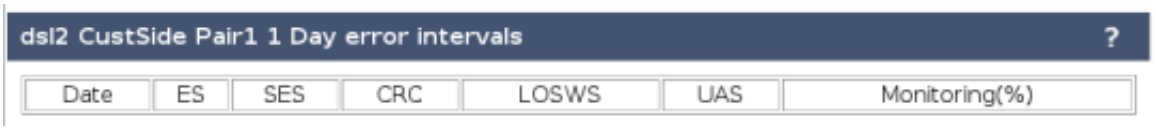
Рисунок 5.11. Таблица 15-ти минутных интервалов для CustSide



dsl2 CustSide Pair1 15 Minutes error intervals ?

Date	Start time	End time	ES	SES	CRC	LOSWS	UAS	Monitoring(%)
01 Jan 1999	02:00	02:15	0	0	0	8	0	76.78

Рисунок 5.12. Таблица дневных интервалов для CustSide



dsl2 CustSide Pair1 1 Day error intervals ?

Date	ES	SES	CRC	LOSWS	UAS	Monitoring(%)

- *Monitoring* — процент времени, в течении которого мониторился канал.

Мониторинг через консоль

Для мониторинга SHDSL канала используется утилита **eoc-info**, для получения подробной информации об её использовании используется ключ `--help`.

Для получения краткой информации о состоянии канала используется команда **eoc-info** `-s`. Она показывает состояние каждого канала: сколько регенераторов обнаружено, и установлено ли соединение со слейвом (маршрутизатор, работающий в режиме *slave*). В ее выводе *offline* показывает, что соединение со вторым маршрутизатором не установлено. В этом случае число регенераторов показывает, до какого регенератора было установлено соединение.

Для получения более детальной информации надо указать имя интерфейса: **eoc-info** `-i dsl0`. В выводе команды будет полная информация о всех юнитах в тракте — мастера, слейва и всех регенераторов. Для получения информации о конкретном юните используется опция `-u` и название юнита: STU-C, STU-R, SRU1..SRU8.

Правила приоритетов параметров производительности SHDSL канала

- На параметр *UAS* не налагается запретов.
- Параметры *ES* и *SES* запрещаются, если установлена индикация *UAS*.
- Параметр *CV* запрещается, если установлена индикация *SES*.

Сохранение/восстановление конфигурации

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

Сохранение конфигурации выполняется на странице Configuration/Backup:

Рисунок 5.13. 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 5.14. Восстановление конфигурации

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

После восстановления конфигурации, необходимо перезагрузить маршрутизатор.

Глава 6. Настройка сетевых интерфейсов

Общие параметры

В этом разделе рассматриваются общие параметры настройки для всех типов сетевых интерфейсов.

Вкладка Status

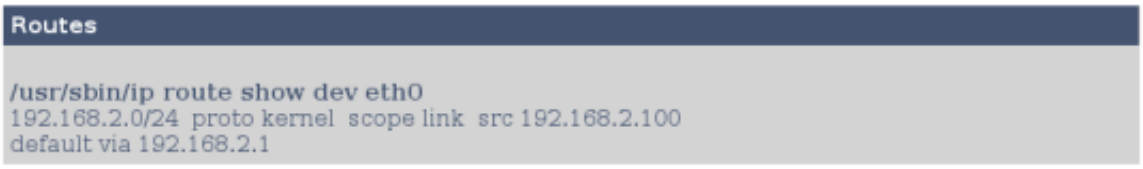
На вкладке *Status* отображается основная информация о выбранном интерфейсе, а так же предоставляется возможность останова, запуска, и перезапуска интерфейса. Информация о сетевых параметрах интерфейса:

Рисунок 6.1. Сетевые параметры

Состояние интерфейса (запущен или нет) можно определить по строке флагов. Если в ней содержится слово *UP*, то интерфейс запущен (к примеру, *UP BROADCAST MULTICAST*).

Маршруты, привязанные к интерфейсу:

Рисунок 6.2. Сетевые маршруты

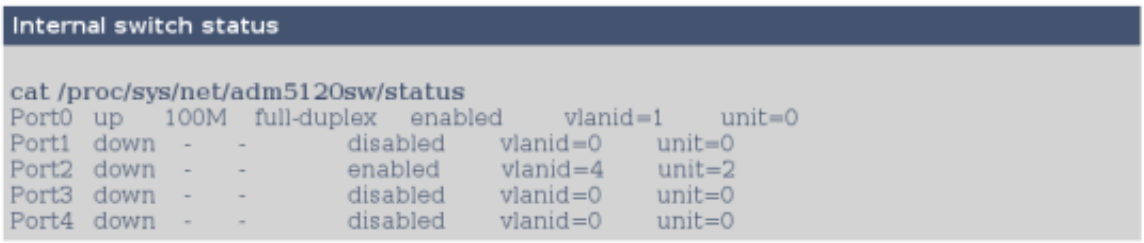


Записи в таблице ARP:

Рисунок 6.3. Таблица ARP

Информация о работе встроенного коммутатора:

Рисунок 6.4. Встроенный коммутатор



Информация о шейпере трафика, работающего на интерфейсе:

Рисунок 6.5. Шейпер трафика

Управление интерфейсом:

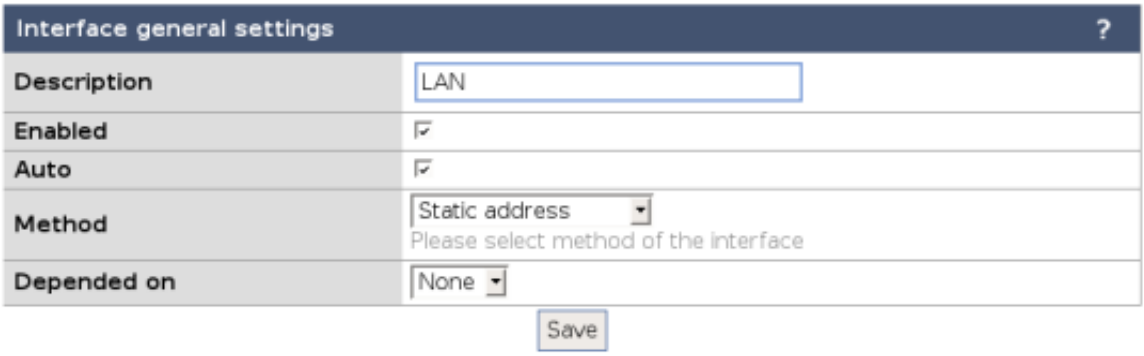
Рисунок 6.6. Управлени интерфейсом

- Кнопка *Start interface* позволяет запустить ("поднять") интерфейс, если на вкладке General установлен флажок *enabled*.
- Кнопка *Shutdown interface* останавливает интерфейс ("опускает").
- Кнопка *Restart interface* останавливает/запускает интерфейс.

Вкладка General

Опции на вкладке *General* позволяют сделать интерфейс активным, а также выбрать способ установки ip-адреса.

Рисунок 6.7. Вкладка General



- *Description* — описание интерфейса, не используется системой.
- *Enabled* — интерфейс активен. Это делает возможным запуск интерфейса другим интерфейсом (интерфейсом бондинга или моста), но интерфейс не будет запущен независимо. В частности, интерфейс можно запустить нажатием кнопки *Start interface* на вкладке *Status*.
- *Auto* — независимый запуск интерфейса. Интерфейс будет запущен при загрузке маршрутизатора, либо при сохранении настроек интерфейса.
- *Method* — метод установки IP-адреса.

Замечание

Для интерфейса E1, при выборе протоколов, отличных от ETHER-HDLC, изменение данного параметра невозможно. Метод установки IP-адреса всегда Point-to-Point, и производится на вкладке *Method*.

- *Depended on* — интерфейс, от которого зависит данный интерфейс. При запуске данного интерфейса сперва будет запущен интерфейс, от которого он зависит.

Замечание

Для интерфейса VLAN изменение данного параметра невозможно — для него здесь всегда указывается его физический интерфейс.

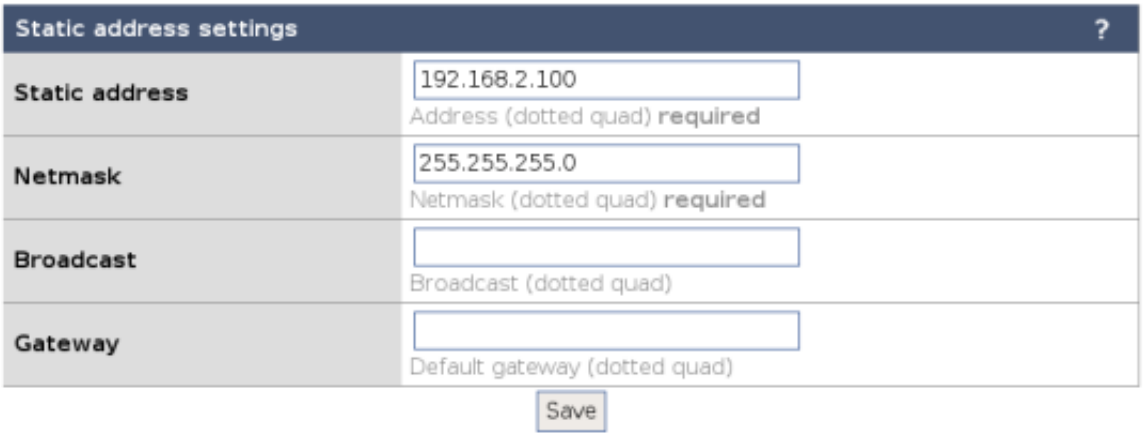
Возможно несколько методов установки IP-адреса:

- *None* — не конфигурируемый, IP-адрес не устанавливается.
- *Static address* — статический, ручной ввод пользователем. Ввод адреса производится на вкладке *Method*.
- *Zero configuration* — автоматический способ присвоения ip-адреса, позволяющий построить работающую сеть без ручного присвоения IP-адресов и без серверов DHCP. В этом случае интерфейсу будет назначен IP-адрес из диапазона 169.254.*.
- *Dynamic address* — динамический IP-адрес — адрес назначается сервером DHCP.

Вкладка Method

На вкладке *Method* осуществляется установка сетевых параметров:

Рисунок 6.8. Вкладка Method



- *Static address* — IP-адрес.
- *Netmask* — маска сети.
- *Broadcast* — широковещательный адрес.
- *Gateway* — маршрут по-умолчанию.

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 6.9. Вкладка Options

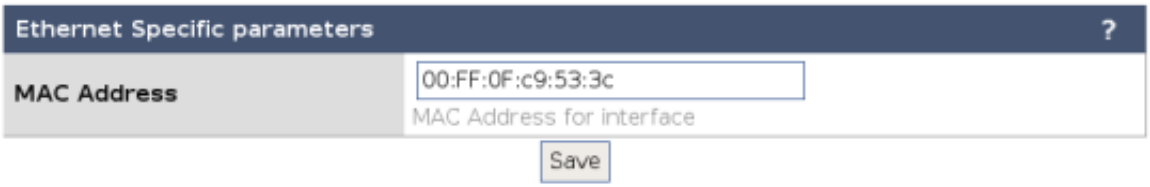
- *Accept redirects* — в активном состоянии позволяет принимать ICMP перенаправления. Например, если есть лучший маршрут до какого-либо узла чем тот, по которому был послан пакет клиентом, маршрутизатор клиенту может отправить (как правило всегда так и происходит) icmp-перенаправление с указанием, через 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 межсетевого экрана).
- *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

Данная вкладка содержит параметры, которые специфичные для данного интерфейса. Для интерфейсов Ethernet и SHDSL (и других) здесь можно установить MAC-адрес.

Рисунок 6.10. Вкладка Specific



Настройка интерфейса SHDSL

Настройка параметров интерфейса

Для соединения по SHDSL один маршрутизатор работает в режиме мастера (master), второй — в режиме слейва (slave). Настройка SHDSL соединения зависит от модели маршрутизатора и используемых модулей. Настройка интерфейса SHDSL выполняется на странице System/SHDSL/dsl*.

Маршрутизатор SG-16R

Замечание

Драйвер для SHDSL маршрутизатора SG-16R называется MR16H, его имя отображается в заголовке конфигурационного окна.

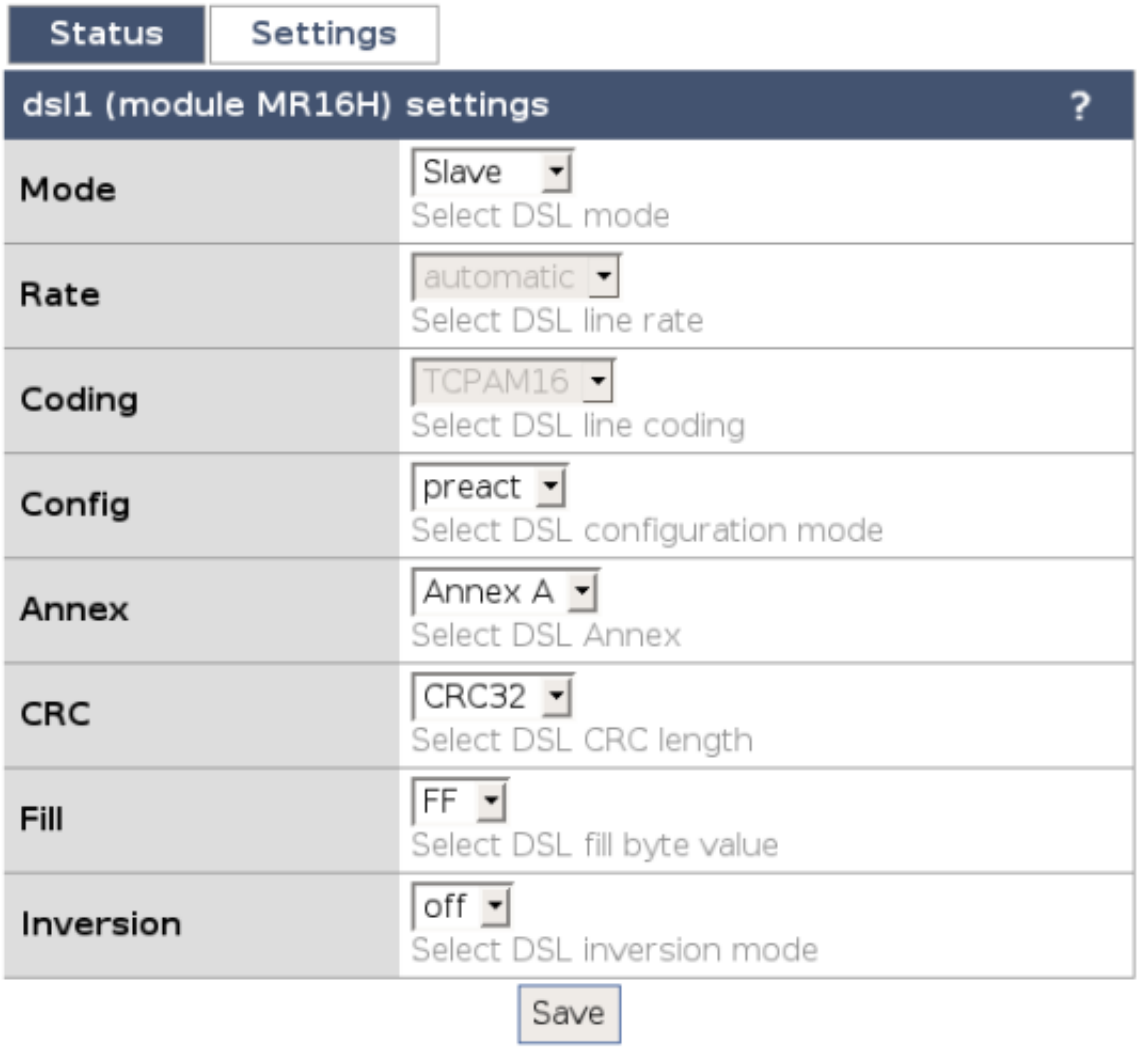
Маршрутизаторы SG-16R поддерживают два способа конфигурирования интерфейса SHDSL (MR16H) — *local* и *preact*.

- *local* — конфигурация параметров линии связи задаётся на обоих маршрутизаторах.
- *preact* — конфигурация параметров линии связи задаётся на мастере, а слейв получает настройки при установлении соединения.

Важно

Метод конфигурирования должен совпадать на обоих маршрутизаторах.

Рисунок 6.11. Настройка SHDSL (MR16H)



- *Rate* — скорость передачи, кбит/с.
- *Mode* — режим: мастер (master), слейв (slave).
- *Coding* — метод кодирования. Подробнее см. раздел Особенности применения кодировок TCPAM.
- *Config* — способ конфигурирования.
- *Annex* — выбор дополнений.

Важно

На обоих маршрутизаторах должны быть выставлены одинаковые значения параметра!

- *Annex A* — используется для совместимости с SG-16B предыдущих версий, а так же для работы на скоростях ниже 192 и выше 5696 кбит/с (с локальной настройкой). В режиме preact при использовании Annex A максимальная скорость ограничена до 2304 кбит/с.
- *Annex B* — равноценен режиму Annex A.

  - *Annex F* — используется по-умолчанию. В режиме preact максимальная скорость 5696 кбит/с, в режиме local — 6016.

- *CRC* — значение контрольной суммы пакета.

- *Fill* — выбор байта для заполнения канала, когда нет пакетов на передачу.

- *Inversion* — логическое инвертирование всего потока.

Маршрутизатор SG-17R

Замечание

Драйвер для SHDSL маршрутизатора SG-17R (и модулей MR-17H*) называется MR17H, его имя отображается в заголовке конфигурационного окна.

Важно

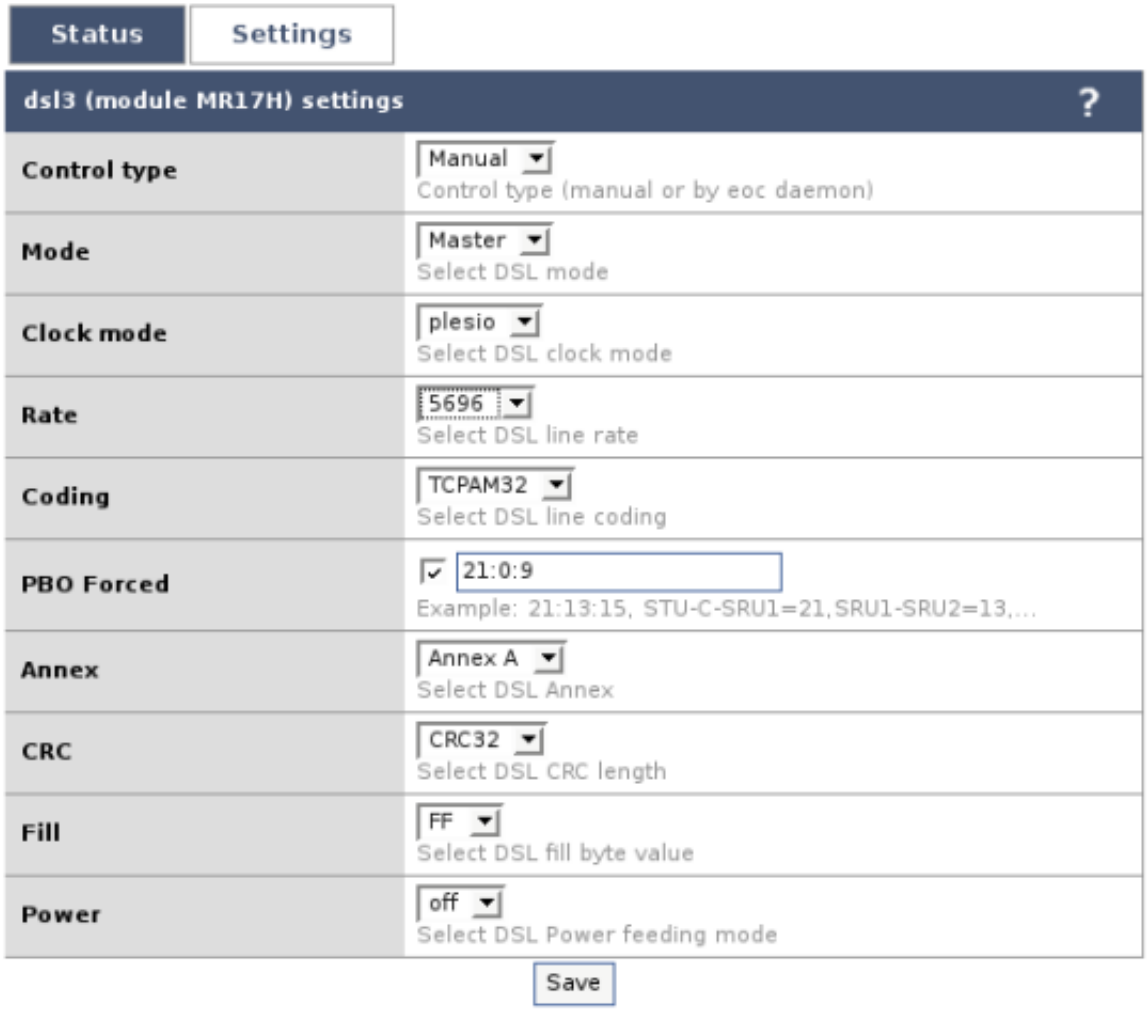
Прочтите раздел про Принцип хранения настроек для модулей.

Важно

Если данный сетевой интерфейс относится к модулю, установленному в четвёртый слот (слот *D*), то он может быть использован только для работы в режиме *мультиплексирования*. Этот сетевой интерфейс не имеет возможности передавать сетевой трафик (трафик, идущий не по линиям мультиплексирования). Связано это с отсутствием поддержки DMA для данного четвёртого слота.

Настройка скорости соединения, режима синхронизации и режима кодирования выполняется только на мастере, слейв получает эти настройки во время инициализации соединения. Окно конфигурирования показано ниже:

Рисунок 6.12. Настройка SHDSL (MR17H)



- *Control type* — режим управления интерфейсом:
  - *Manual* — задание настроек со страницы конфигурирования интерфейса (с текущей страницы).
  - *EOCd* — интерфейс управляется демоном EOCd. Это позволяет вести мониторинг SNMP параметров интерфейса, а в будущем — управлять интерфейсом по SNMP. Для получения подробной информации смотри раздел Настройка через демон EOCd.
- *Mode* — режим: мастер (master), слейв (slave).
- *Clock mode* — режим синхронизации, по-умолчанию используется режим *plesio* (плезиохронный). Перед выбором режима *sync* (синхронного) следует удостовериться, что всё оборудование, находящееся на линии связи (регенераторы, маршрутизаторы) поддерживают данный режим.
- *Rate* — скорость передачи, кбит/с. В выпадающем списке приведены не все доступные скорости — для ввода произвольной скорости следует выбрать значение *other*, что приведёт к появлению поля ввода. После сохранения, введённое значение будет округлено до ближайшего корректного значения скорости.
- *Coding* — метод кодирования. Подробнее см. раздел Особенности применения кодировок TCPAM.

- *PBO Forced* — снижение уровня выходного сигнала на указанное значение дБ. Используется для уменьшения влияния на оборудование, работающее по тому же кабелю. Данный параметр оказывает влияние на скорость/дальность соединения.

  Понижение уровня сигнала можно производить на всех сегментах линии связи — для этого значения снижения уровня сигнала указываются через двоеточие. Например, "3:0:12" снижает уровень сигнала на участке STU-C — SRU1 на 3 дБ, на участке SRU1 — SRU2 уровень сигнала не снижается, на участке SRU2 — STU-R — на 12 дБ. Если снижение задано не для всех участков, то на оставшихся понижения уровня сигнала не будет.

- *Annex* — выбор дополнений. Какие-либо рекомендации по использованию отсутствуют, оба дополнения равноценны.

- *CRC* — значение контрольной суммы пакета.

- *Fill* — выбор байта для заполнения канала, когда нет пакетов на передачу.

- *Inversion* — логическое инвертирование всего потока.

- *Power* — включить подачу питания для регенераторов, находящихся на линии.

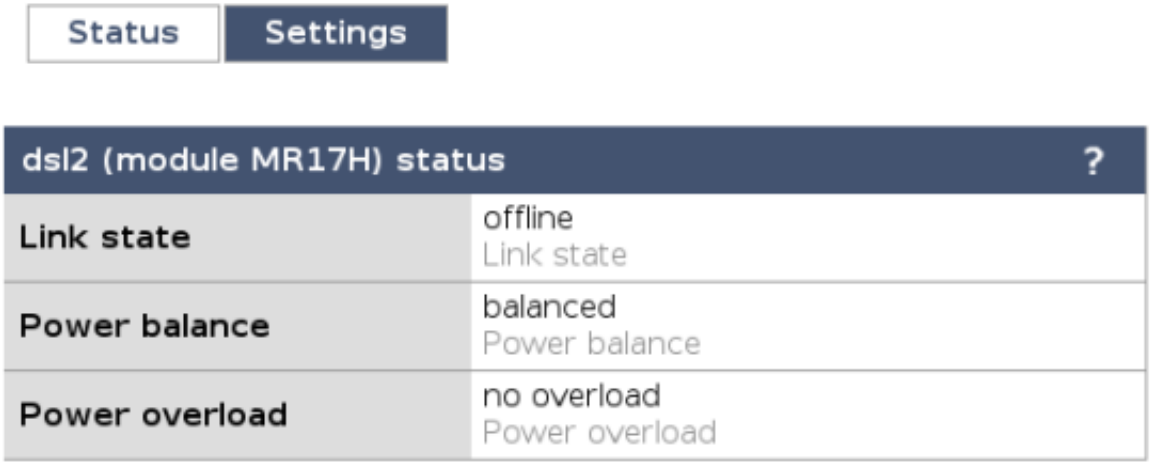
Установка и статус соединения

После сохранения настроек через некоторый промежуток времени соединение будет установлено, о чем будут сигнализировать светодиоды на лицевой панели маршрутизатора. Так же информацию о состоянии соединения можно просмотреть на вкладке статуса:

Рисунок 6.13. Информация о состоянии соединения SHDSL (MR16H)

Вкладка статуса для MR17H отображает более подробную информацию. Если соединение не установлено, выводится следующая информация:

Рисунок 6.14. Информация о неустановленном соединении SHDSL (MR17H)



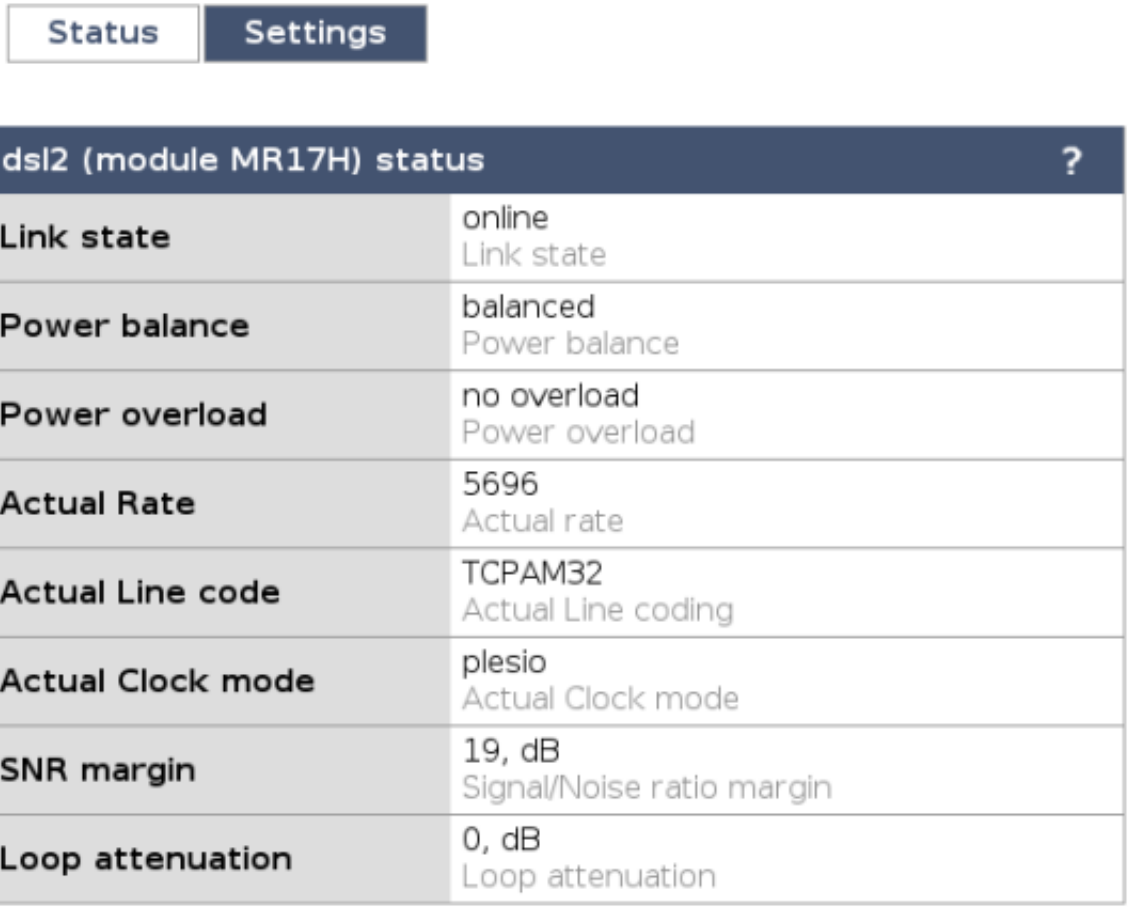
- *Link state* — состояние соединения: *offline* — соединение не установлено, *online* — соединение установлено.

- *Power balance* — баланс питания относительно земли. В норме на одном проводе +120 В, на другом — 120 В. Если перекос больше 30 В или отсутствует земля — это означает несбалансированность питания, загорается светодиод unbalanced на модуле SHDSL. Значение *balanced* этого параметра соответствует нормальной работе, *unbalanced* — несбалансированности питания.

- *Power overload* — перегрузка питания. Слишком большое число регенераторов на линии, настроенных на питание от данного маршрутизатора, вызывает перегрузку питания. На модуле SHDSL загорается светодиод overload. Значение *no overload* этого параметра соответствует нормальной работе, *overload* — перегрузке питания.

При установленном соединении добавляется следующая информация:

Рисунок 6.15. Информация об установленном соединении SHDSL (MR17H)



- *Actual rate* — скорость передачи установленного соединения, кбит/с.
- *Actual line code* — метод кодирования.
- *Actual clock mode* — режим синхронизации.
- *SNR margin* — соотношение сигнал/шум в линии связи.
- *Loop attenuation* — затухание сигнала в линии связи.

Замечание

Соединения SHDSL будет установлено, если интерфейс dsl* активен, т.е. для него настроены сетевые параметры (установлен флажок *enabled* и интерфейс активен, подробнее — см. следующий раздел).

Настройка через демон EOCd

Для управления интерфейсом через EOCd необходимо выбрать соответствующее значение параметра в настройке интерфейса (параметр *Control type*). Настройка интерфейса через демон EOCd заключается в создании профиля соединения и применения этого профиля к интерфейсу.

Создание и редактирование профиля

Создание и редактирования профиля соединения производится на странице System->SHDSL-EOC->Profiles, вид которой представлен ниже.

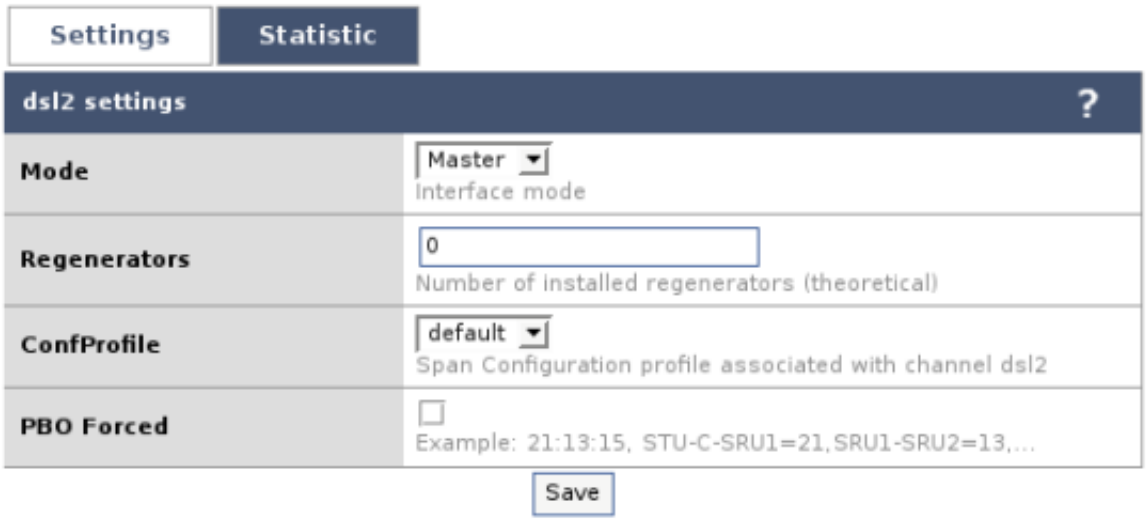
Рисунок 6.16. Создание и редактирование профилей соединения

В профиле соединения доступны не все параметры соединения, поддерживаемые модулем. Это ограничение связано со спецификой стандарта SNMP для интерфейса SHDSL. Доступные параметры — Rate, Annex, Power, Encoding — полностью соответствуют параметрам на странице настройки интерфейса (см. настройка SHDSL).

Применение профиля к интерфейсу

Применение профиля соединения к интерфейсу осуществляется на странице System->SHDSL-EOC->имя_интерфейса.

Рисунок 6.17. Применение профиля соединения



- *Mode* — режим работы интерфейса — мастер/слейв.
- *Regenerators* — справочный параметр, отражающий число регенераторов, которое должно быть на линии. Позволяет сравнить фактическое число регенераторов с тем, которое было установлено.
- *ConfProfile* — профиль соединения, который используется демоном EOCd для управления интерфейсом.
- *PBO Forced* — снижение уровня выходного сигнала на указанное значение дБ. Используется для уменьшения влияния на оборудование, работающее по тому же кабелю. Данный параметр оказывает влияние на скорость/дальность соединения.

  Понижение уровня сигнала можно производить на всех сегментах линии связи — для этого значения снижения уровня сигнала указываются через двоеточие. Например,

"3:0:12" снижает уровень сигнала на участке STU-C — SRU1 на 3 дБ, на участке SRU1 — SRU2 уровень сигнала не снижается, на участке SRU2 — STU-R — на 12 дБ. Если снижение задано не для всех участков, то на оставшихся понижения уровня сигнала не будет.

Настройка сетевых параметров

Настройка сетевых параметров аналогична настройке Ethernet соединения и выполняется на странице Network/Interfaces/dsl*.

Настройка интерфейса E1

Маршрутизатор поддерживает несколько протоколов для работы с интерфейсом E1 (для совместимости с разными видами оборудования DTE и различными прикладными протоколами): HDLC, ETHER-HDLC, CISCO-HDLC, FR, PPP, X25. Настройка интерфейса выполняется на странице System/E1/E1_*.

Важно

Прочтите раздел про Принцип хранения настроек для модулей.

Настройка параметров интерфейса

Настройка протокола CISCO-HDLC

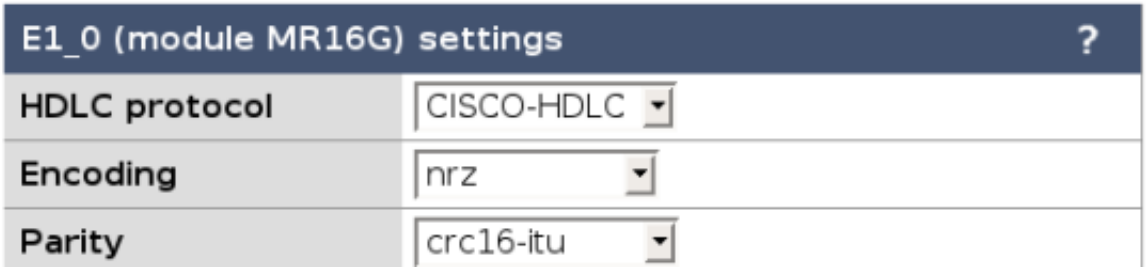
Важно

Если данный сетевой интерфейс относится к модулю, установленному в четвёртый слот (слот *D*), то он может быть использован только для работы в режиме *мультиплексирования*. Этот сетевой интерфейс не имеет возможности передавать сетевой трафик (трафик, идущий не по линиям мультиплексирования). Связано это с отсутствием поддержки DMA для данного четвёртого слота.

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.

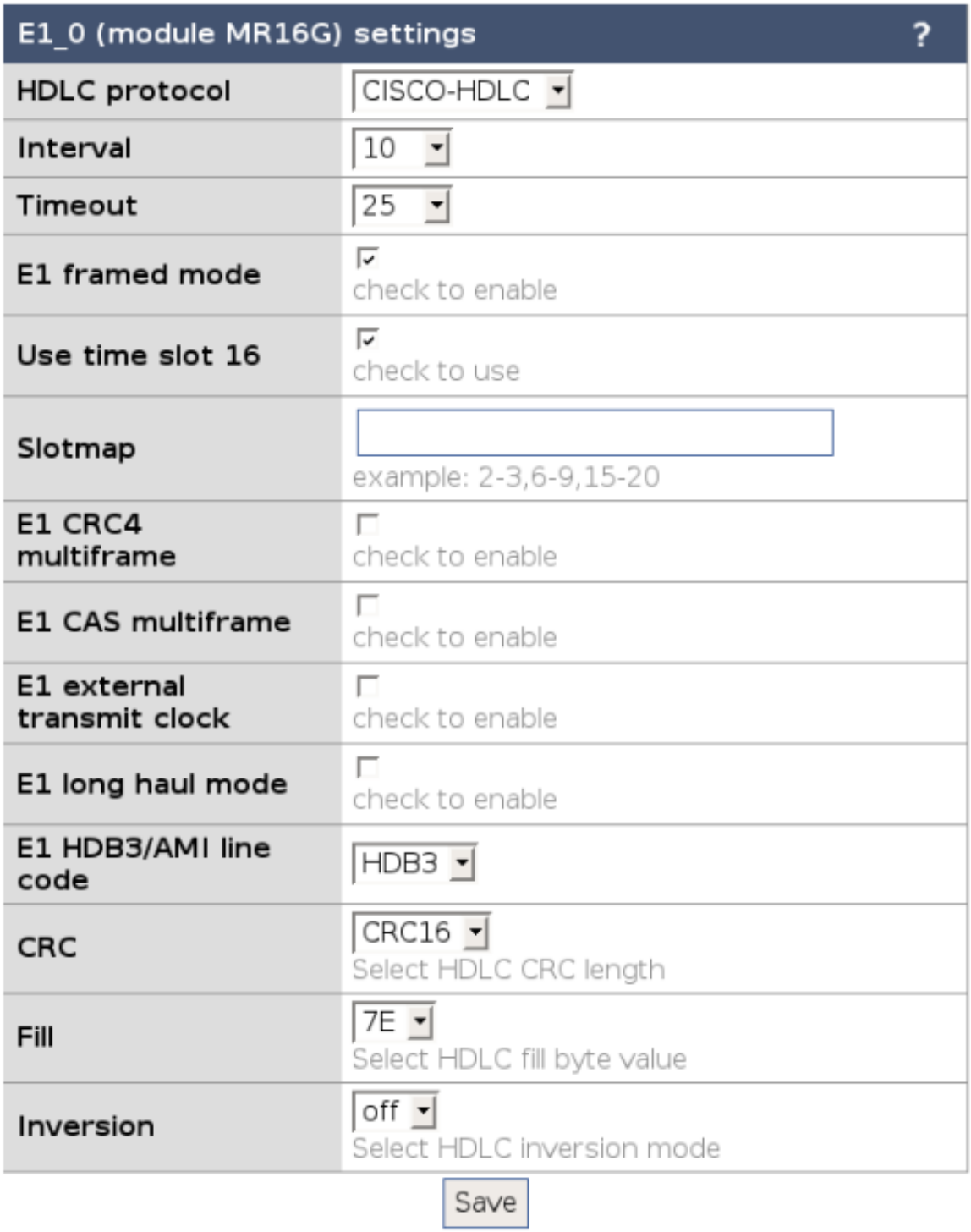
Для настройки протокола CISCO-HDLC необходимо в выпадающем списке HDLC protocol выбрать значение CISCO-HDLC:

Рисунок 6.18. Выбор протокола



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

Рисунок 6.19. Настройка протокола CISCO-HDLC



- *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 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 external transmit clock* — использовать внешний источник тактирования. По-умолчанию используется внутренний.

  ## Замечание

  Если для данного интерфейса включено мультиплексирование (MXEN=1), то используются параметры из таблицы мультиплексирования (CLKM, CLKR). Если мультиплексирование выключено, то используется данный параметр.

- *E1 long haul mode* — при включенном режиме long haul расстояние от маршрутизатора до подключённого к нему оборудования DTE может достигать 1600 метров по кабелю сечением 0,4 мм, и 2400 по кабелю сечением 0,5 мм. При отключении, эта дистанция ограничена 400 метрами.

- *E1 HDB3/AMI line code* — способ кодирования сигнала на линии связи.

  ## Важно

  Рекомендация ITU-T G.703 требует использования линейного кода HDB3!

- *CRC* — значение контрольной суммы пакета.

- *Fill* — выбор байта для заполнения канала, когда нет пакетов на передачу.

- *Inversion* — логическое инвертирование всего потока.

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

Настройка 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 external 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.

Настройка 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 6.20. Unframed mode

E1_0 (module MR16G) settings	?
HDLC protocol	CISCO-HDLC
Interval	10
Timeout	25
E1 framed mode	check to enable
E1 external transmit clock	check to enable
E1 long haul mode	check to enable
E1 HDB3/AMI line code	HDB3
CRC	CRC16 Select HDLC CRC length
Fill	7E Select HDLC fill byte value
Inversion	off Select HDLC inversion mode

Save

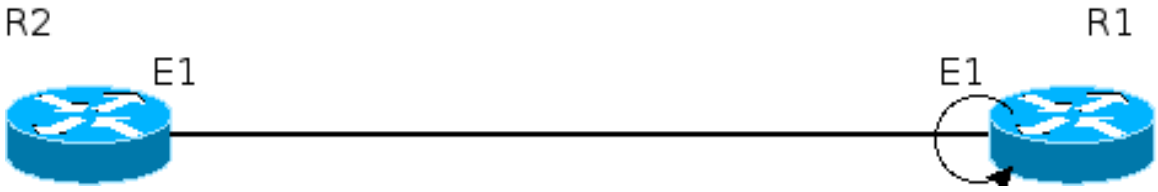
В этом режиме параметров настройки меньше, чем во framed mode, и все они сводятся к настройке линии связи.

Диагностирование соединения E1

Для диагностирования соединения можно использовать "петлю": т.е. вместо того, чтобы передавать трафик дальше, возвращать его обратно, симулируя ответ получателя трафика.

Возможно создание двух видов петель — локальной и удалённой. При создании локальной петли, модуль E1 передаёт данные в физическую линию и возвращает их сразу же отправителю, как показано ниже на схеме.

Рисунок 6.21. E1: локальная петля



Для активации этого вида петли необходимо на странице настройки интерфейса E1 активировать параметр "Local Loopback" на маршрутизаторе, на котором создаётся петля (на нашей схеме — на маршрутизаторе R1).

При использовании второго вида петли — удалённая петля — данные передаются в физическую линию, доходят до удалённого маршрутизатора, который передаёт их дальше, а так же возвращает обратно отправителю.

Рисунок 6.22. E1: удалённая петля

Для активации этого вида петли необходимо на странице настройки интерфейса E1 активировать параметр "Remote Loopback" на маршрутизаторе, на котором создаётся петля (на нашей схеме — на маршрутизаторе R2).

Таким образом, при использовании обоих видов петель данные продолжают передаваться в физическую линию, но одновременно с этим возвращаются обратно, что позволяет проверять корректность конфигурации независимо от состояния линии связи.

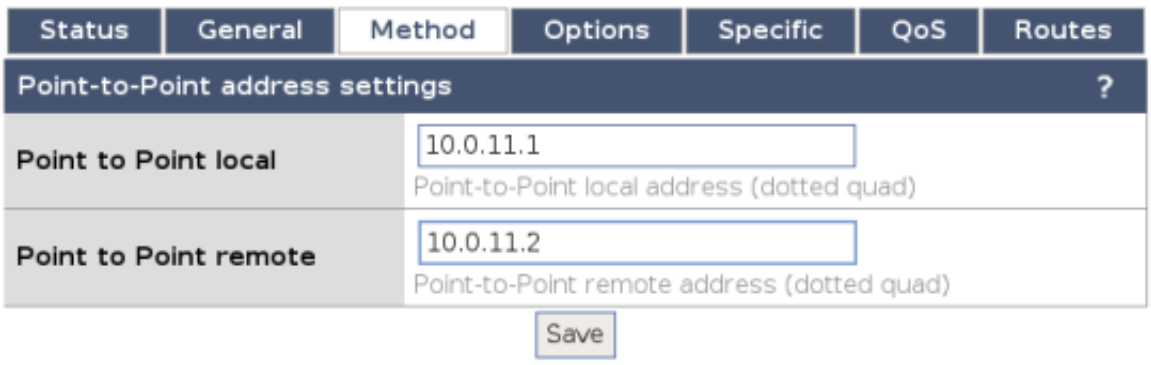
Настройка сетевых параметров

Настройка сетевых параметров интерфейса зависит от выбранного протокола. При выборе *ETHER-HDLC* выполняется обычная настройка интерфейса: доступен любой метод задания IP-адреса, как при настройке интерфейсов Ethernet или SHDSL.

При выборе любого другого протокола тип соединения становится *Point-to-Point*, т.е. маршрутизатор связывается непосредственно с другом устройством. Соответственно, меняется и способ установки IP-адреса. Рассмотрим конфигурацию P-t-P соединения подробнее.

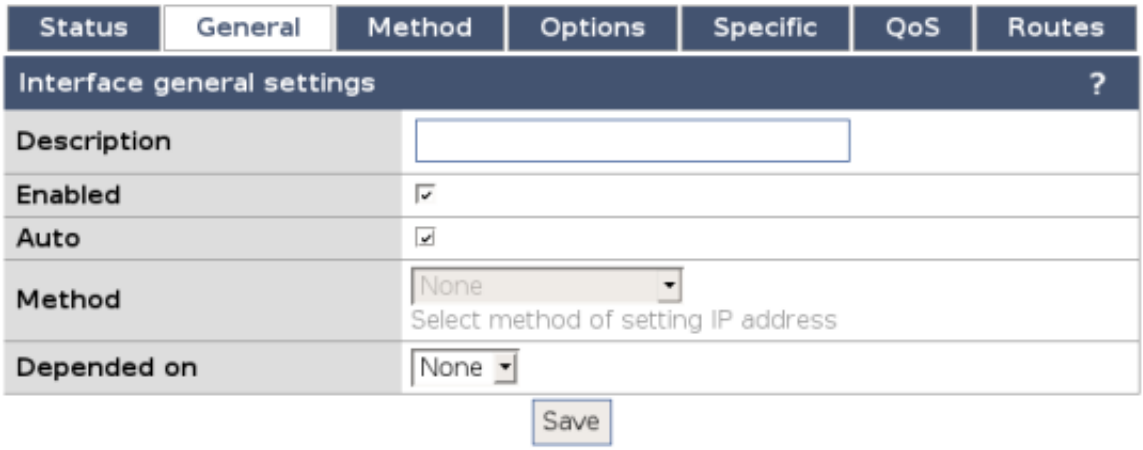
Перейдём на страницу Network/Interfaces/E1_*, вкладку Method. Введём IP-адреса Point-to-Point соединения: локальный и удалённый адреса.

Рисунок 6.23. Назначение Point-to-Point адресов



Следующим шагом настройки является активация интерфейса на вкладке General.

Рисунок 6.24. Активация интерфейса E1



Динамические интерфейсы

Работа с динамическими интерфейсами

На странице Network/Interfaces возможно добавить или удалить динамические интерфейсы, которые не являются физическими интерфейсами, а предназначены для работы поверх них. На данный момент существуют следующие динамические интерфейсы:

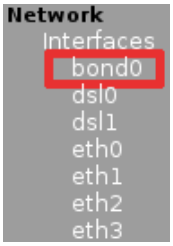
- *Bridge* — динамический интерфейс для создания моста.
- *PPPoE* — PPP over Ethernet.
- *PPtP* — Point-to-Point Tunneling Protocol.
- *Bonding* — объединение интерфейсов.

Для создания нового динамического интерфейса необходимо выбрать его тип и нажать кнопку *Add*.

Рисунок 6.25. Создание динамического интерфейса

Добавленный динамический интерфейс отобразится в списке сетевых интерфейсов:

Рисунок 6.26. Динамический интерфейс в списке сетевых интерфейсов



Чтобы удалить динамический интерфейс выберите его имя в списке интерфейсов и нажмите кнопку *Delete*.

Рисунок 6.27. Удаление динамического интерфейса

Настройка режима Bonding

Режим Bonding позволяет объединять несколько физических соединений в одно логическое (с помощью создания динамического интерфейса *bond*). К примеру, два SHDSL канала можно объединить в один, увеличив пропускную способность соединения.

Важно

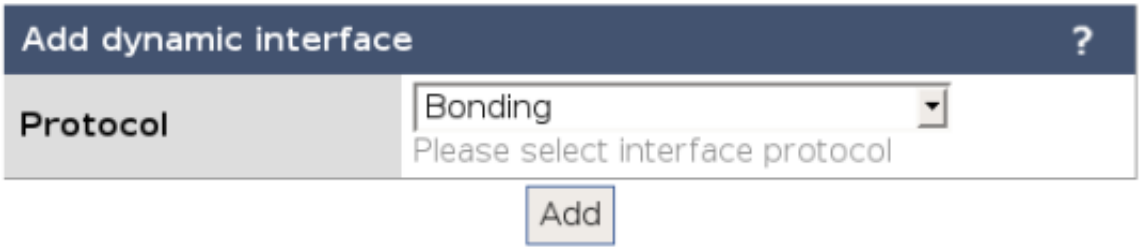
В режиме Bonding поддерживается объединение только ethernet интерфейсов. В системе все интерфейсы являются ethernet, за исключением *E1*, который только при использовании протокола *ETHER-HDLC* является ethernet интерфейсом. При использовании других протоколов (HDLC, CISCO-HDLC, ...) E1 является *hdlc* интерфейсом.

Для настройки режима Bonding в первую очередь необходимо настроить физические интерфейсы (к примеру, SHDSL или Ethernet). Интерфейсы, которые будут входить в Bonding, должны быть активны и запущены (см. настройку сетевых интерфейсов). Для интерфейса должен быть установлен флажок *enabled*, т.е. его конфигурация должна иметь следующий вид:

Рисунок 6.28. Настройка физического интерфейса

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

Рисунок 6.29. Создание динамического интерфейса



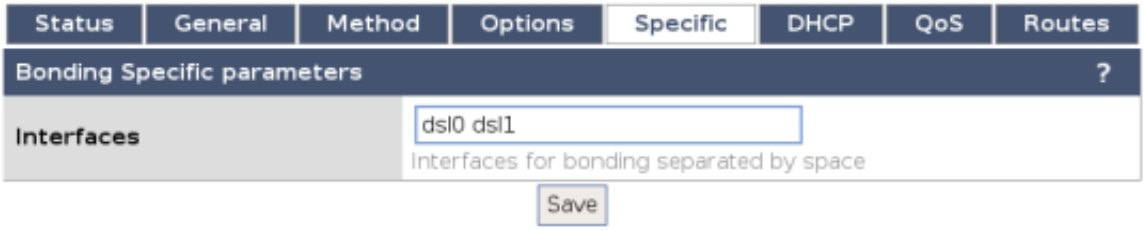
После нажатия кнопки *Add* созданный интерфейс отобразится в списке сетевых интерфейсов.

Замечание

Если вы хотите сконфигурировать несколько bonding-интерфейсов, следует добавить сразу необходимое количество динамических интерфейсов, перед их запуском. Это связано с тем, что после запуска первого bonding-интерфейса, запуск новых bonding-интерфейсов будет возможен только после перезагрузки.

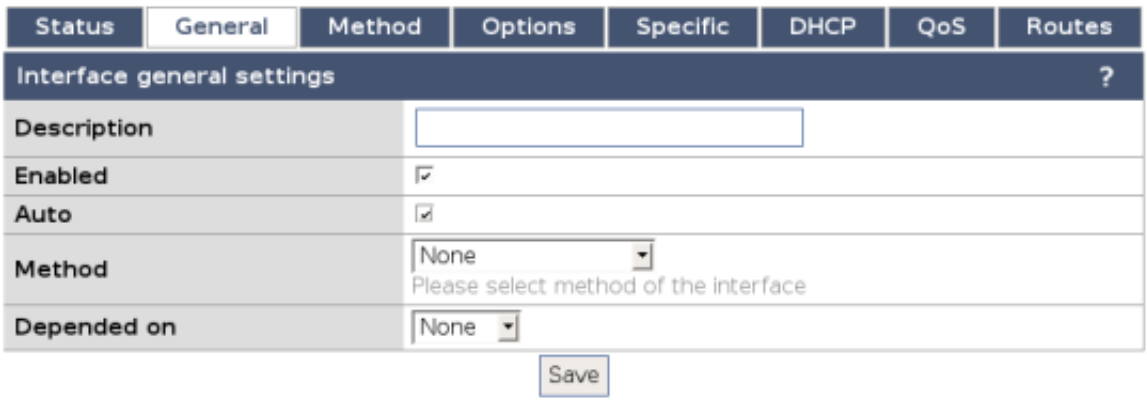
Для настройки интерфейса необходимо перейти на страницу Network/Interfaces/bond*, вкладку Specific, где указать, какие физические интерфейсы будут использоваться этим динамическим интерфейсом для передачи данных. К примеру, при настройке SHDSL Bonding, можно ввести dsl0 и dsl1:

Рисунок 6.30. Привязка к физическим интерфейсам



После сохранения настроек переходим на вкладку General. Здесь необходимо выставить флажки *enabled* и *auto*, чтобы интерфейс автоматически запускался при загрузке маршрутизатора. Если для динамического интерфейса необходимо назначить IP-адрес, то в параметре *Method* надо выбрать необходимый метод установки IP-адреса и произвести его настройку (в случае статического IP-адреса — прописать адрес на вкладке *Method*).

Рисунок 6.31. Настройка динамического интерфейса



После сохранения настроек на вкладке General, динамический интерфейс будет автоматически запущен. При этом IP-адреса реальных интерфейсов, если они были установлены, будут сброшены. Для всех интерфейсов (динамического и входящих в него физических) будет установлен один MAC-адрес, который будет соответствовать MAC-адресу одного из физических интерфейсов.

Замечание

Аналогичные настройки необходимо произвести на втором маршрутизаторе.

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 создаётся специальный сетевой динамический интерфейс с именем *br*, с которым ассоциируются сетевые интерфейсы, между которыми будет передаваться трафик.

Важно

Мост поддерживает передачу трафика только между ethernet-интерфейсами. В системе все интерфейсы являются ethernet, за исключением *E1*, который только при использовании протокола *ETHER-HDLC* является ethernet интерфейсом. При использовании других протоколов (HDLC, CISCO-HDLC, ...) E1 является *hdlc* интерфейсом.

Рисунок 6.32. 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.

Замечание

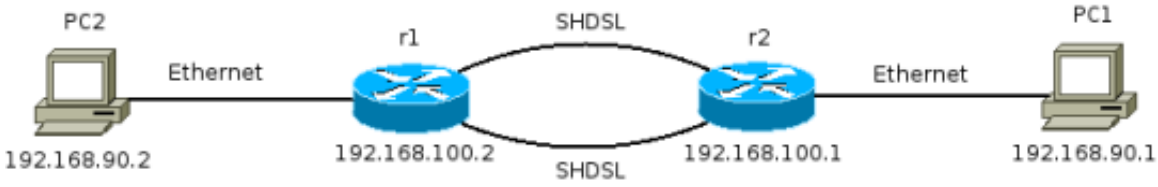
Следует заметить, что маршрутизатор, работающий в режиме моста и сети, между которыми он передаёт трафик, не обязательно должны находиться в одном адресном пространстве, как это требуется при настройке маршрутизации трафика.

Более того, у такого маршрутизатора вообще может не быть IP-адреса. Однако, если необходимо управление маршрутизатором, то ему необходимо назначить IP-адрес, входящий в ту же сеть, что и компьютер, с которого будет производиться управление. В нашем примере, маршрутизаторам можно назначить IP-адреса 192.168.90.10 и 192.168.90.11.

На следующем рисунке изображена сеть, аналогичная предыдущей, 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 6.33. Пример моста с объединением интерфейсов



Так же, как и для настройки режима Bonding, в первую очередь необходимо настроить физические интерфейсы, которые будут входить в мост: они должны быть активны (см. настройку сетевых интерфейсов). Для интерфейсов должен быть установлен флажок *enabled*, т.е. их конфигурация должна иметь следующий вид:

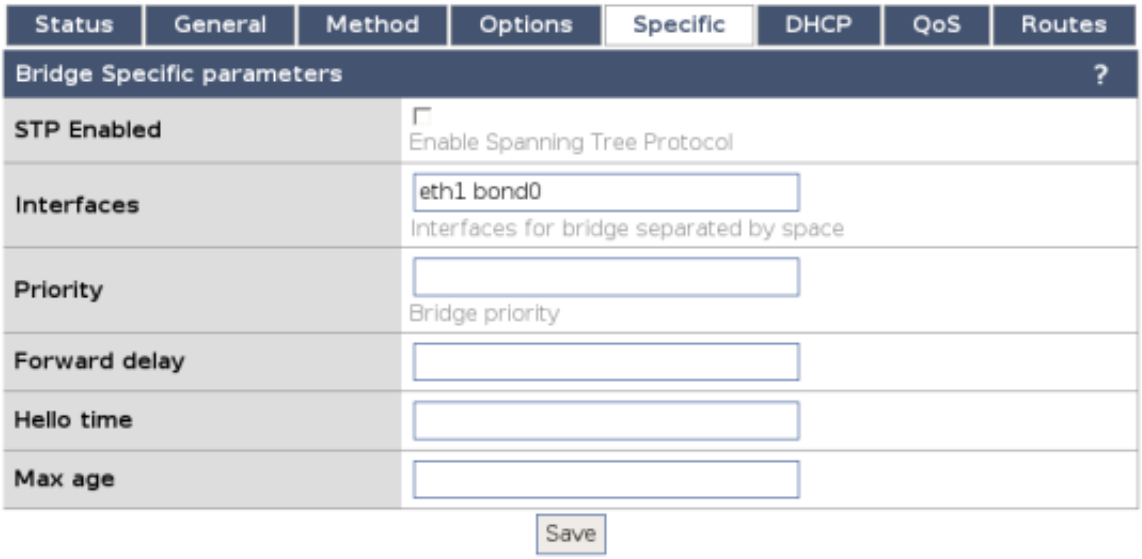
Рисунок 6.34. Настройка физического интерфейса

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

Рисунок 6.35. Создание интерфейса

После добавления динамического интерфейса он появится в списке сетевых интерфейсов. Для его настройки перейдём на страницу Network/Interfaces/br* и выберем вкладку Specific, на которой определим список интерфейсов, входящих в мост. Для этого в поле Interfaces укажем имена сетевых интерфейсов:

Рисунок 6.36. Привязка к физическим интерфейсам



Замечание

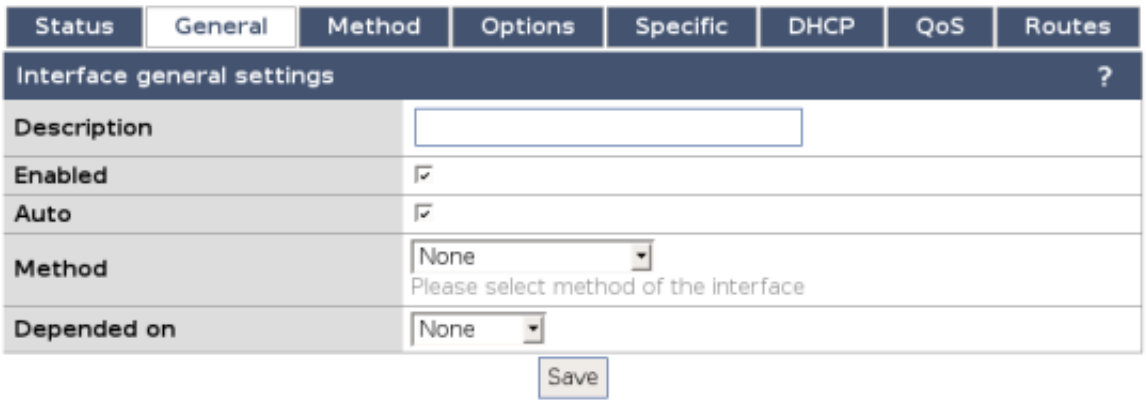
Количество интерфейсов в мосту может быть больше двух.

Важно

Физический интерфейс может быть добавлен только в *один* интерфейс моста! К примеру, нельзя создать интерфейсы br0 (eth0, dsl0) и br1 (eth1, dsl0), т.к. dsl0 может быть добавлен только в один интерфейс моста. Для преодоления этого ограничения воспользуйтесь технологией VLAN (см. соответствующий раздел и примеры использования).

После сохранения настроек перейдём на вкладку General, на которой установим флажки *enabled* и *auto* для автоматического запуска интерфейса во время загрузки маршрутизатора:

Рисунок 6.37. Настройка динамического интерфейса



Важно

Начиная с версии прошивки 879 больше нет необходимости указывать зависимый интерфейс в поле Depended on — интерфейс моста автоматически запускает интерфейсы, из которых он состоит.

Замечание

Если для динамического интерфейса необходимо назначить IP-адрес, то в параметре *Method* надо выбрать необходимый метод установки IP-адреса и произвести его настройку (в случае статического IP-адреса — прописать адрес на вкладке *Method*).

Важно

Запуск интерфейса *br** приводит к сбросу IP-адресов с физических интерфейсов, которые в него входят. Таким образом, если настройка осуществляется через физический интерфейс, который входит в мост, управление над маршрутизатором может быть потеряно. Чтобы этого избежать, необходимо назначить динамическому интерфейсу *br** IP-адрес.

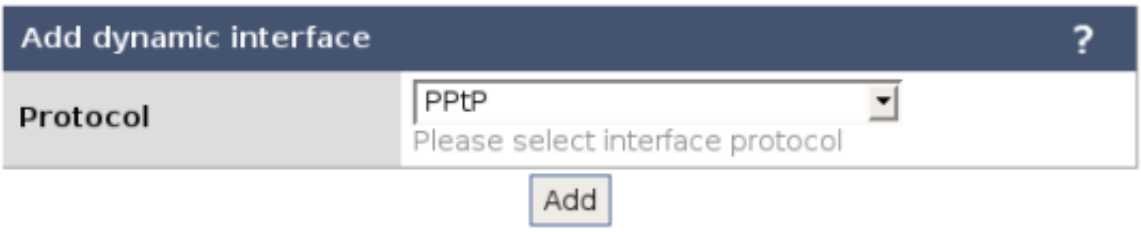
Эту же процедуру повторяем на втором маршрутизаторе, и через пару минут, в течении которых "мост" распознает топологию сети и проведёт небольшой этап самообучения, начнется передача пакетов между интерфейсами.

Настройка соединения PPtP

PPtP — Point-to-point tunneling protocol — туннельный протокол типа точка-точка, позволяющий создать виртуальную частную сеть (VPN) поверх физической сети.

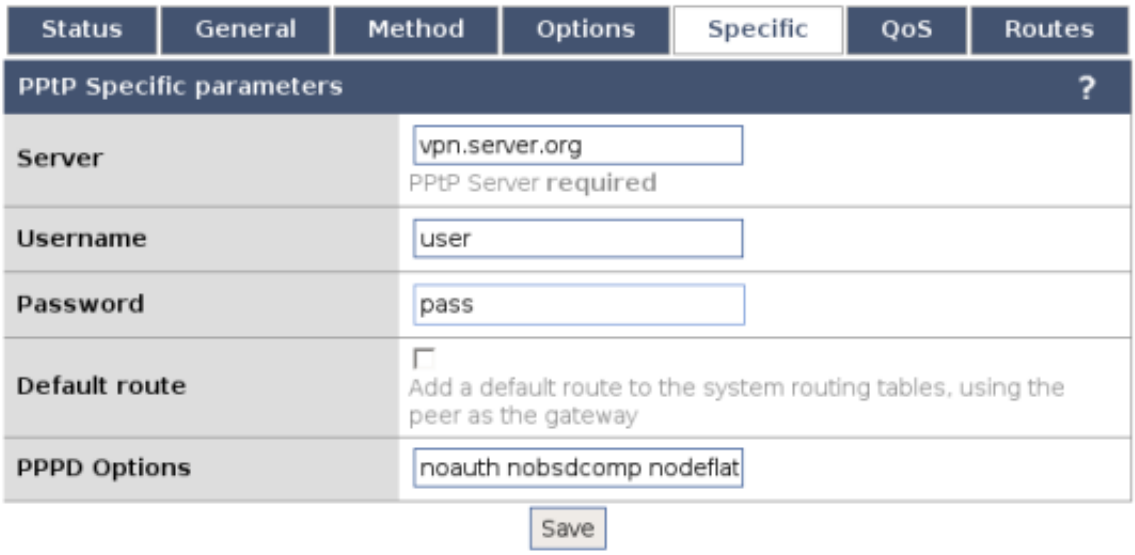
Для создания соединения необходимо добавить динамический интерфейс PPtP. Это выполняется на странице Network/Interfaces:

Рисунок 6.38. Добавления интерфейса PPtP



После добавления, следует снова перейти на страницу Network/Interfaces, чтобы обновить список доступных интерфейсов. Настройка интерфейса выполняется на странице Network/Interfaces/pptp*. Рассмотрим специфичные для данного интерфейса параметры:

Рисунок 6.39. Вкладка Specific



- *Server* — имя или IP-адрес сервера PPtP, к которому будет выполняться подключение.
- *Username* — имя пользователя.
- *Password* — пароль.
- *Default route* — является ли это соединение маршрутом по-умолчанию.
- *PPPD Options* — параметры, которые будет переданы демону PPPD при подключении.

Важно

После создания и первого редактирования настроек соединение будет инициализировано, независимо от параметров на вкладке General.

Активировать соединение и включить его автоматическую инициализацию после загрузки маршрутизатора можно на вкладке General:

Рисунок 6.40. Вкладка General

Замечание

При данном виде сетевого подключения параметр Method игнорируется и может принимать любые значения.

Замечание

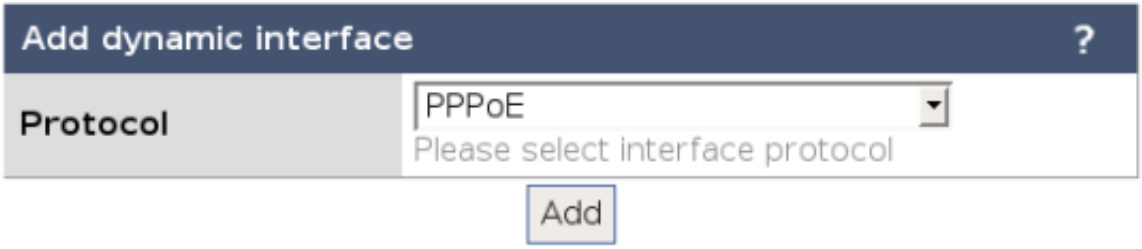
На данный момент подключение по PPtP с использованием шифрования MPPE невозможно.

Настройка соединения PPPoE

PPPoE — Point-to-point protocol over Ethernet — сетевой протокол передачи кадров PPP через Ethernet. Так же, как *PPtP* это туннелирующий протокол, но работающий непосредственно поверх Ethernet, создающий соединение типа точка-точка. Использование PPP предоставляет возможности аутентификации, сжатия трафика и его шифрования.

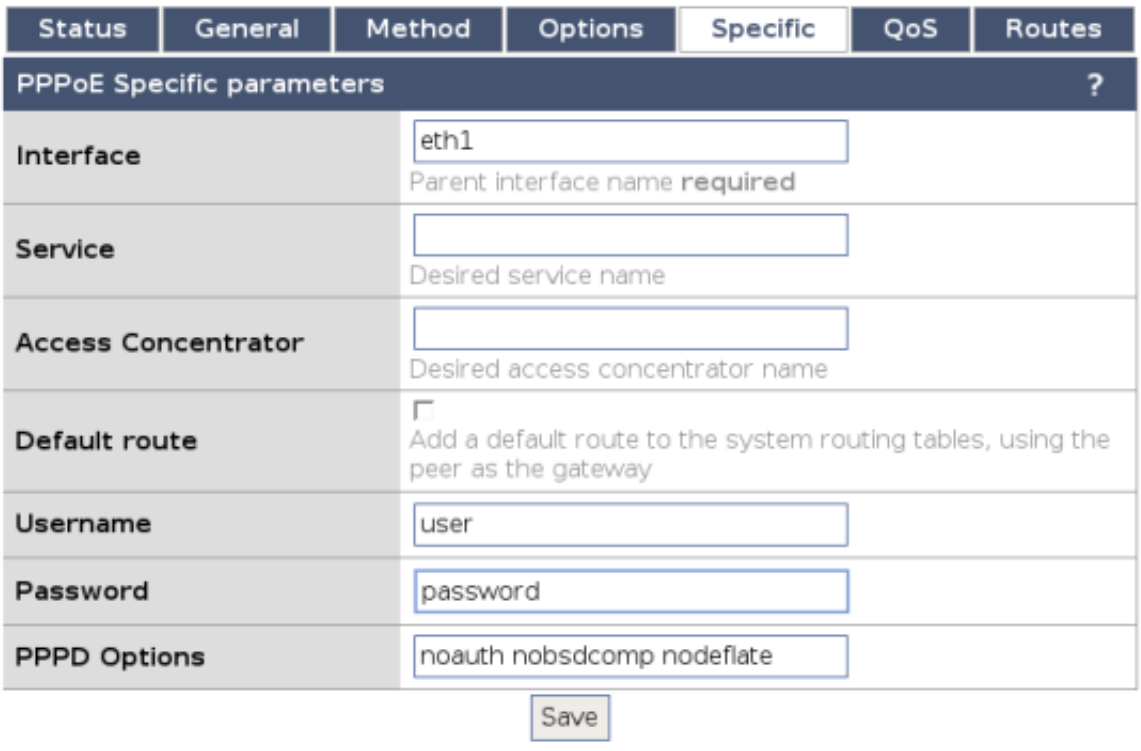
Для создания соединения необходимо добавить динамический интерфейс PPPoE на странице Network/Interfaces:

Рисунок 6.41. Добавление интерфейса PPPoE



После добавления, следует снова перейти на страницу Network/Interfaces, чтобы обновить список доступных интерфейсов. Настройка интерфейса выполняется на странице Network/Interfaces/pppoe*. Рассмотрим специфичные для данного интерфейса параметры:

Рисунок 6.42. Вкладка Specific



- *Interface* — физический интерфейс, в сети которого находится PPPoE сервер (eth0, eth1, ...).

- *Service* — маршрутизатор будет устанавливать соединение с теми серверами PPPoE, которые предоставляют данный сервис. В большинстве случаев этот параметр не используется.

- *Access Concentrator* — маршрутизатор будет устанавливать соединение только с указанным концентратором. Используется в случае наличия нескольких серверов PPPoE.

- *Default route* — является ли это соединение маршрутом по-умолчанию.

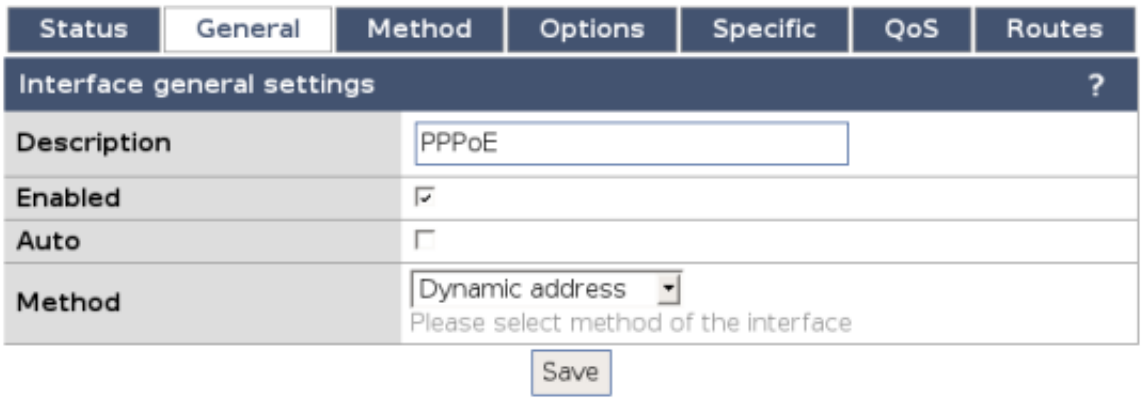
- *Username* — имя пользователя.

- *Password* — пароль.

- *PPPD Options* — параметры, которые будет переданы демону PPPD при подключении.

Активировать соединение и включить его автоматическую инициализацию после загрузки маршрутизатора можно на вкладке General:

Рисунок 6.43. Вкладка General

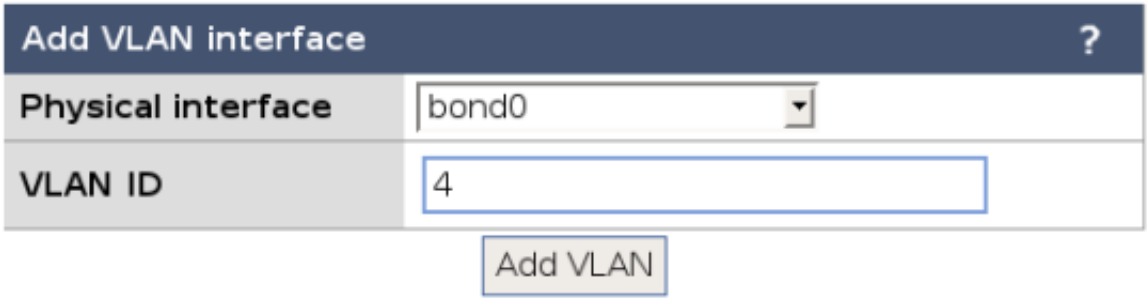


Настройка интерфейсов VLAN

Использование технологии VLAN позволяет разделить трафик пользователей в единой физической среде передачи данных. Для это в каждый Ethernet-кадр добавляет заголовок, относящий данный кадр к тому или иному VLAN. Каждый VLAN идентифицируется своим номером — *VLAN ID*, в диапазоне от 0 до 4094. Для работы с сетями VLAN на основе физического интерфейса создаётся интерфейс VLAN, с определённым VLAN ID.

Для создания интерфейса VLAN необходимо создать динамический интерфейс VLAN на странице Network/Interfaces. Для этого в форме "Add VLAN interface" выбираем интерфейс, поверх которого будет работать интерфейс VLAN, и вводим номер VLAN — VLAN ID.

Рисунок 6.44. Добавление интерфейса VLAN



Подсказка

Интерфейс VLAN может работать как поверх физических интерфейсов (SHDSL, Ethernet), так и поверх динамических (Bonding, Bridge).

После добавления, интерфейс VLAN будет показан в списке интерфейсов в виде "ИНТЕРФЕЙСvНОМЕР_ВЛАН", т.е. если интерфейс VLAN создаётся для интерфейса bond0 и VLAN ID 4, то имя интерфейса VLAN будет *bond0v4*. В системе интерфейс отображается как *bond0.4*.

Теперь над интерфейсом можно выполнять стандартные действия: назначать IP-адрес, добавлять его в бондинг или бридж.

Принцип хранения настроек для модулей

До версии прошивки *890* настройки интерфейсов привязывались к имени интерфейса, что вызывало проблемы при работе с модулями, т.к. при добавлении нового модуля имена интерфейсов могли изменяться, и настройки применялись не к тому модулю.

С версии *890* аппаратные настройки привязываются к PCI-слоту, а сетевые, в случае изменения имени интерфейса, копируются. Т.е., если при добавлении нового модуля, имя интерфейса старого модуля изменилось с *dsl0* на *dsl1*, то сетевые настройки будут скопированы с dsl0 на dsl1.

Основное отличие хранения между аппаратными и сетевыми настройками в том, что если модуль временно извлечь и включить маршрутизатор, сетевые настройки *удалятся*, а аппаратные *останутся*. Таким образом, при последующем возвращении модуля и включении маршрутизатора, модуль будет сконфигурирован по-старому, но без сетевых настроек.

Так же поддерживается применение настроек для совместимых модулей: к примеру, если использовался одноканальный модуль, и он заменён на двухканальный, то настройки будут применены к первому каналу нового модуля.

Если же использовался двухканальный модуль, и вместо него включается одноканальный, то настройки (сетевые и аппаратные) будут применены к новому модулю, аппаратные настройки второго канала сохранятся, а сетевые — *удалятся*. Таким образом, при возвращении двухканального модуля он получит свои аппаратные настройки (и сетевые для первого канала).

Различие между аппаратными и сетевыми настройками сделано из-за технических ограничений.

Глава 7. Настройка сетевых служб

DHCP-сервер

Настройка DHCP-сервера выполняется независимо для каждого сетевого интерфейса и производится на странице Network/сетевой интерфейс, вкладка DHCP, либо Services/DHCP Server.

Важно

Перед активацией DHCP-сервера необходимо запустить интерфейс (активировать флажки *Enabled* и *Auto*), на котором он будет работать, а так же назначить интерфейсу IP-адрес.

Ниже представлена страница настройки DHCP-сервера.

Рисунок 7.1. Настройка DHCP-сервера

- *Enable DHCP Server* — активировать DHCP-сервер для данного интерфейса.
- *Start IP*, *End IP* — начало и конец диапазона IP-адресов для выдачи клиентам DHCP.
- *Netmask* — сетевая маска сети, для которой выдаются IP-адреса.
- *Default router* — маршрут по-умолчанию.

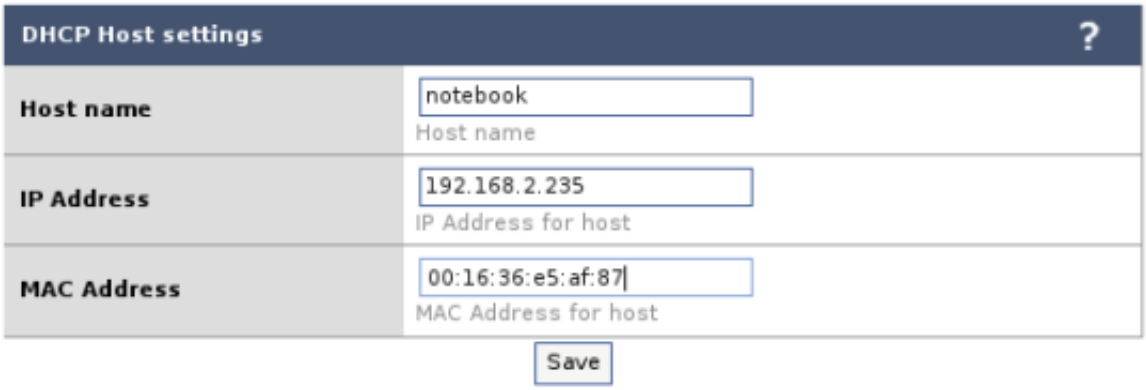
- *Default lease time* — время, на которое выдаётся IP-адрес. По истечении этого времени клиент должен снова обратиться к DHCP-серверу для подтверждения использования выданного ранее адреса или получения нового.
- *DNS server* — IP-адрес DNS-сервера, к которому будет обращаться клиент для разрешения доменных имен.
- *Domain* — домен, в который будет входить клиент DHCP-сервера.
- *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 определённым машинам статические IP-адреса. Идентификация машин производится по значению MAC-адреса сетевой карты. Форма для привязки IP-адреса к MAC-адресу находится внизу страницы настройки и представлена на рисунке:

Рисунок 7.2. Форма привязки IP к MAC



- *Host name* — задаёт имя машины, для которой выполняется привязка адреса. Это значение носит справочный характер и используется только в правиле, может не соответствовать фактическому имени машины.
- *IP Address* — IP-адрес, который будет присвоен данной машине.
- *MAC Address* — MAC-адрес сетевой карты машины, по которому будет производиться привязка IP-адреса.

После сохранения изменений в таблице статических адресов появится новая запись.

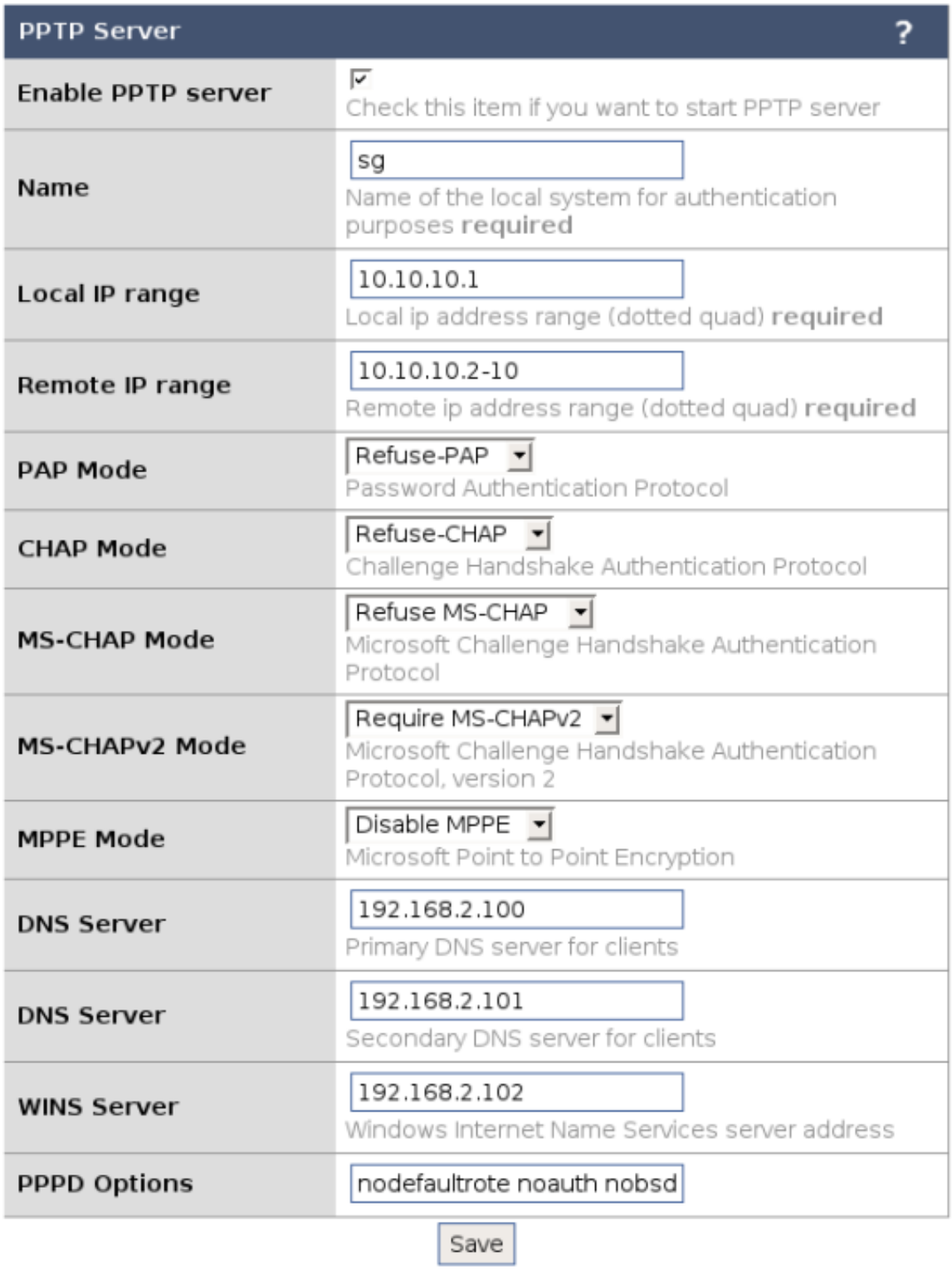
Рисунок 7.3. Обновленный список IP-адресов

PPTP-сервер

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

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

Рисунок 7.4. Настройка PPTP-сервера



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

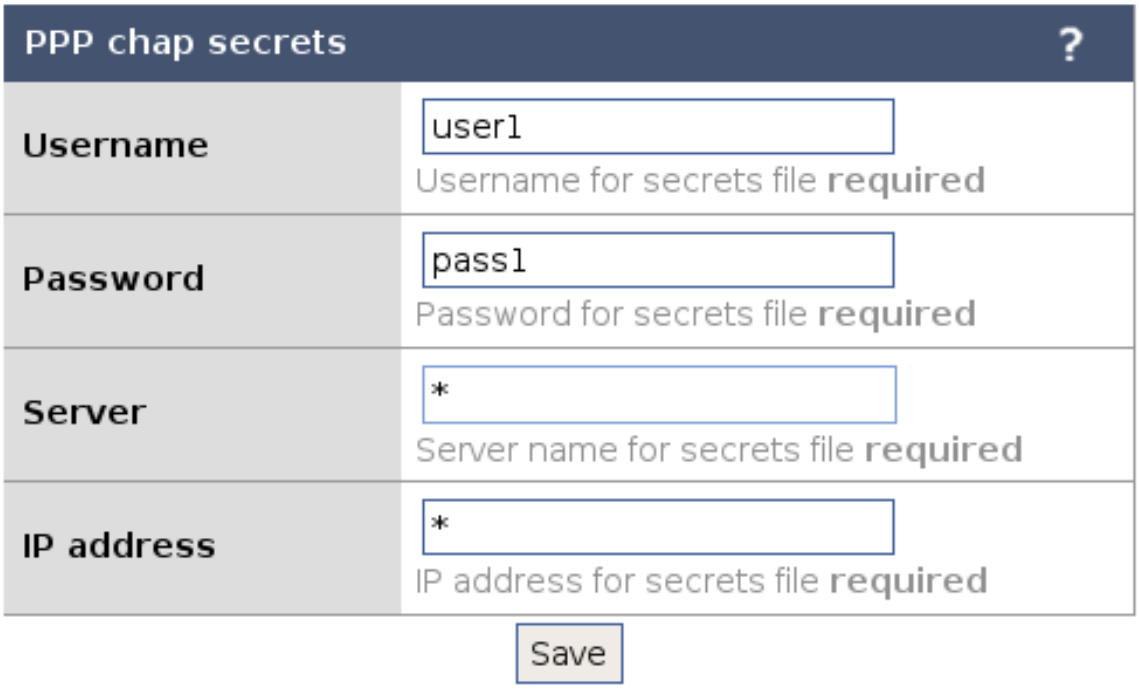
- *Name* — имя VPN-сервера. Используется при аутентификации. У пользователя в *-secret файле значение имени сервера должно совпадать с этим, либо там должна стоять "звездочка".
- *Local IP range* — диапазон IP-адресов, которые будут присвоены соединению на стороне сервера.
- *Remote IP range* — диапазон IP-адресов, которые будут присвоены соединению на стороне клиента.
- Механизмы аутентификации. Имеют три значения — *none* — не определено, *require* — обязателен, *refuse* — запрещён 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 VPN-сервера, перейдем на страницу System/Security/PPP secrets:

Рисунок 7.5. Пользователи VPN-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 7.6. Добавление нового пользователя



- *Username* — имя пользователя.
- *Password* — пароль пользователя.
- *Server* — имя сервера VPN, "*" — любой.
- *IP address* — IP-адрес, выдаваемый клиенту. "*" — любой.

Сервер DNS

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

Рисунок 7.7. Настройка сервера DNS

- *Enable DNS server* — активировать сервер DNS.
- *Forwarder DNS 1* — сервер DNS №1, к которому следует перенаправлять запросы в случае, если локальный сервер DNS не может дать ответ.

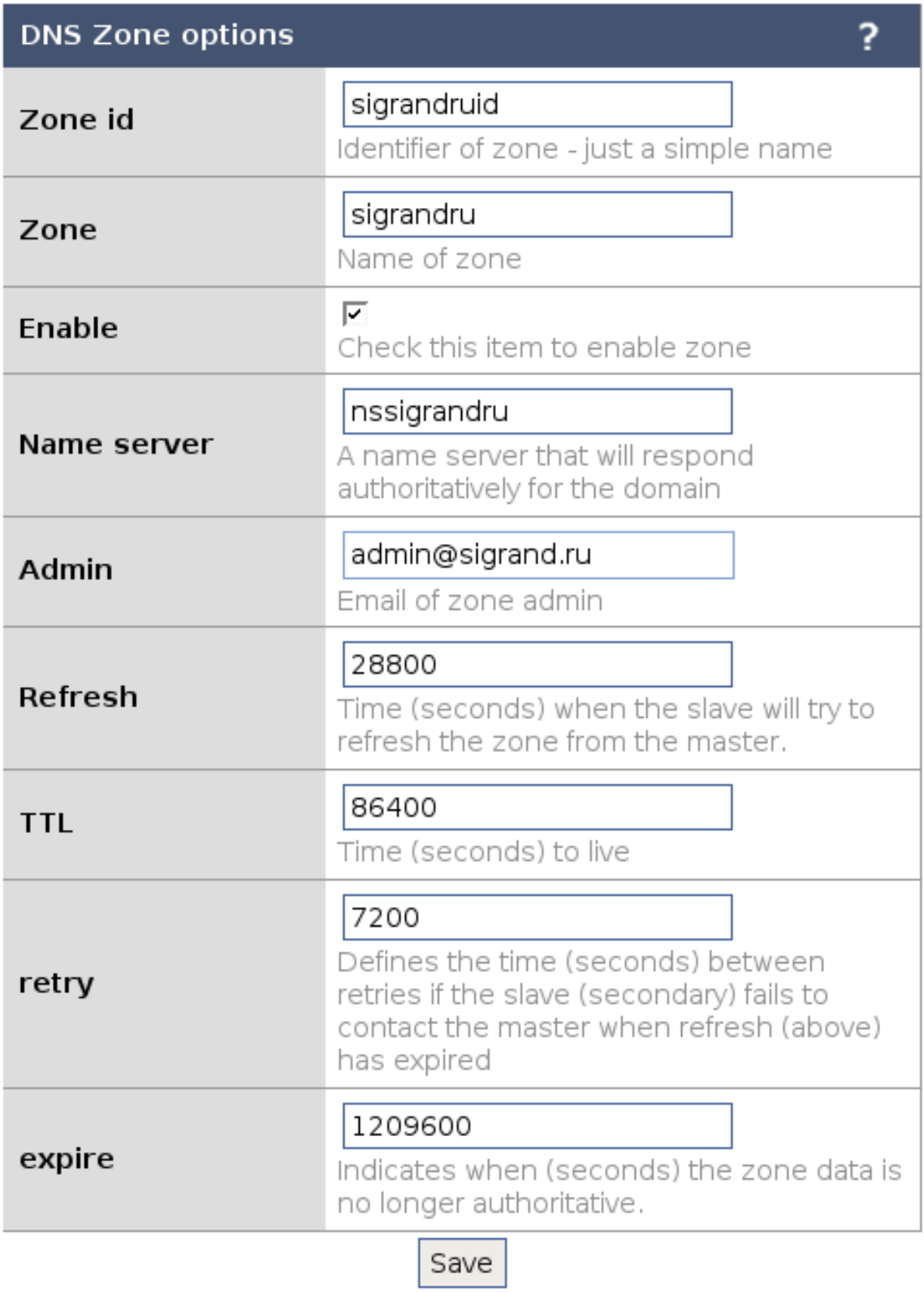
- *Forwarder DNS 2* — сервер DNS №2, к которому следует перенаправлять запросы в случае, если локальный сервер DNS не может дать ответ.

Данный сервер DNS может выступать в роли авторитетного сервера для домена, т.е. хранить информацию о записях (NS, A, CNAME, ...) домена. Для этого необходимо создать файл зоны, в котором хранится информация о домене и его записях. Список зон сервера DNS отображается в форме Zones.

Рисунок 7.8. Зоны сервера DNS

Создание и редактирование файла зоны выполняется в форме Zones по нажатию соответствующей кнопки.

Рисунок 7.9. Добавление зоны



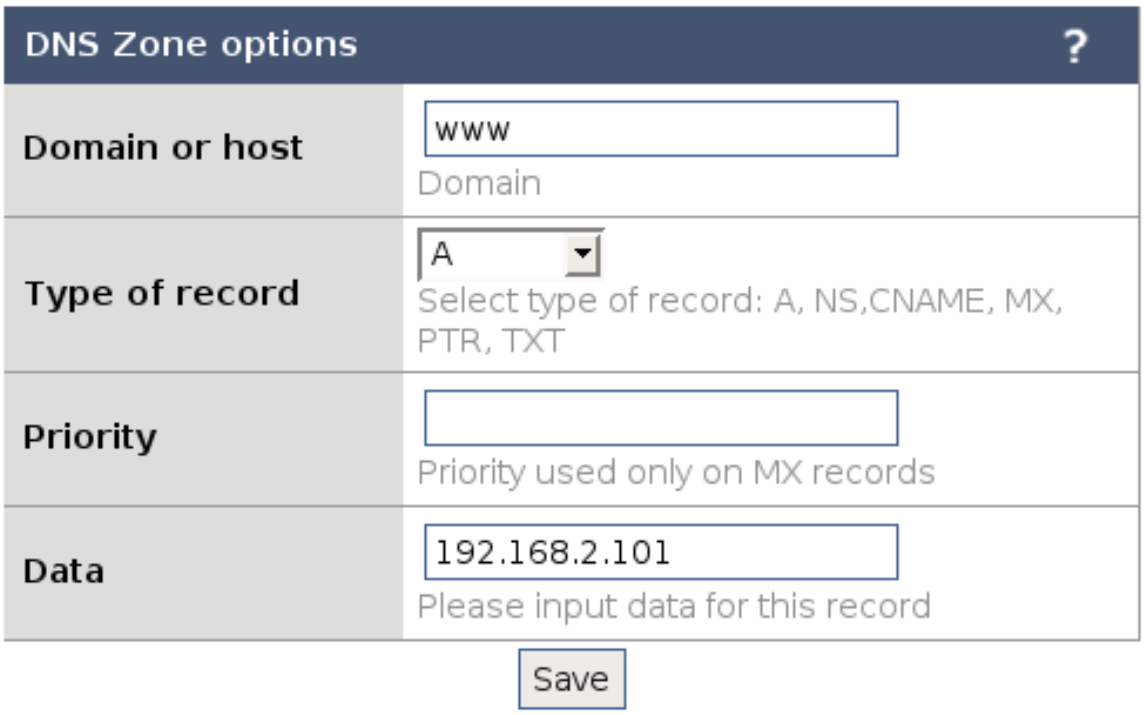
- *Zone id* — идентификатор зоны (этим идентификатором называется файл, в котором хранится зона).
- *Zone* — имя зоны (доменное имя, для которого создаётся зона).
- *Enable* — активна ли зона.

- *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 зоны соответствующая запись появится в таблице зон.

Переход на страницу добавления записей в зону осуществляется щелчком мыши по идентификатору или имени зоны. В результате откроется страница с таблицей, содержащей записи для данной зоны. Форма добавления новой записи представлена ниже.

Рисунок 7.10. Добавление записи в зону

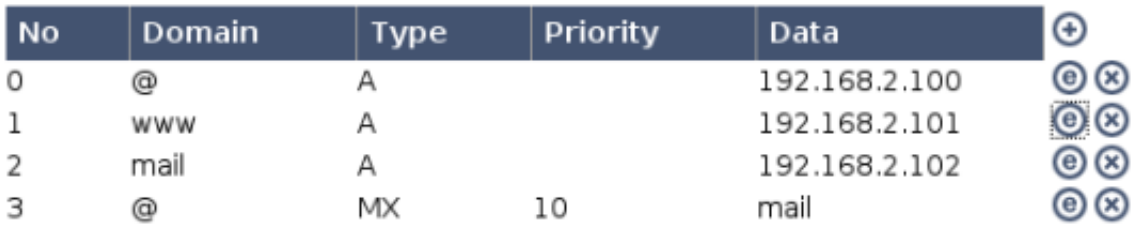


- *Domain or host* — имя (или IP-адрес, если зона обратная).
- *Type of record* — тип записи. Возможны следующие значения:
  - *A* — указывает IP-адрес, соответствующий имени.
  - *CNAME* — синоним другого имени. В этом случае в качестве DATA указывается соответствующее имя.
  - *MX* — имя почтового сервера для данного домена.
  - *NS* — указывает авторитетный сервер DNS для домена (по сути — делегирование домена).

  - *PTR* — указывает имя для данного IP-адреса. Используется в обратной зоне.
  - *TXT* — дополнительная текстовая информация.
- *Priority* — приоритет для записи MX.
- *Data* — данные записи — доменное имя или IP-адрес, либо какая-то текстовая информация.

После сохранения в таблице будет показана новая запись для зоны.

Рисунок 7.11. Таблица записей для зоны



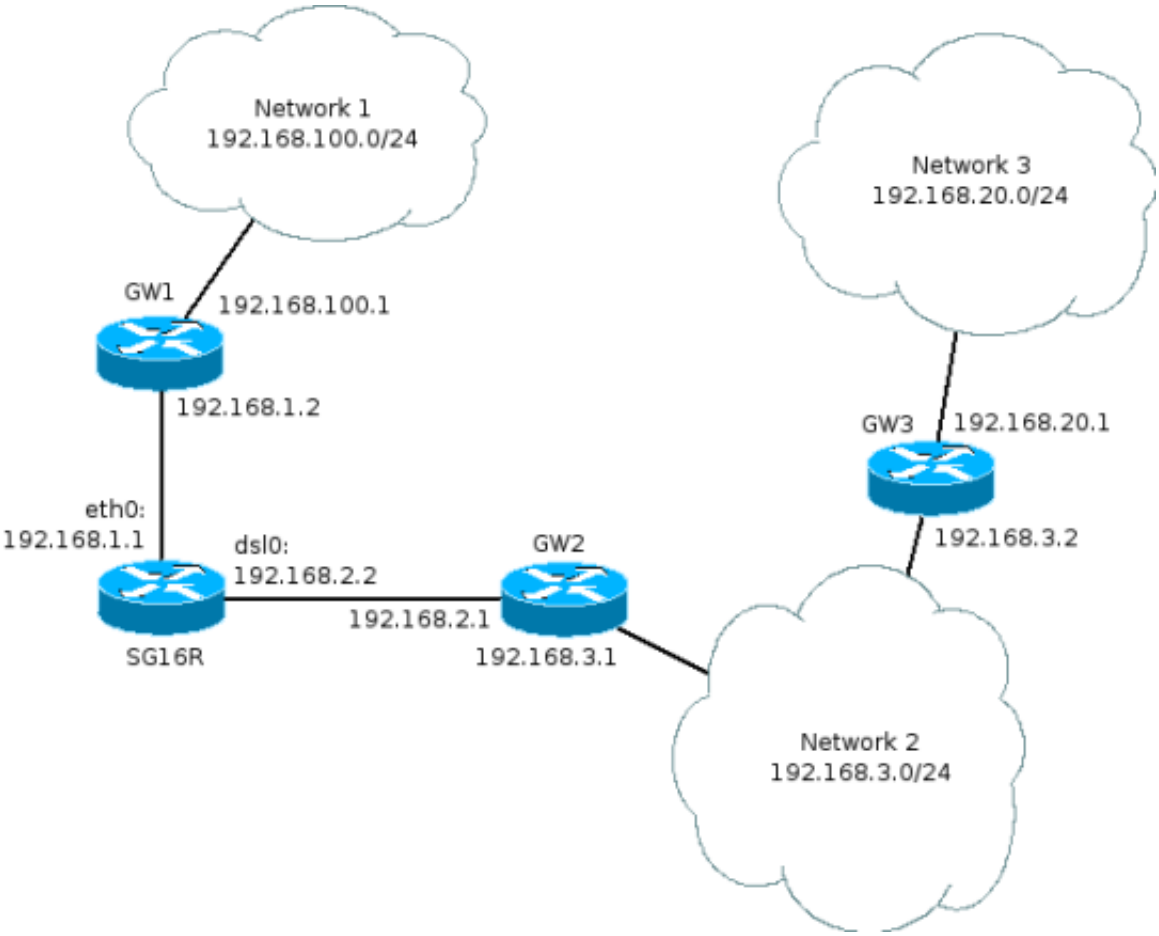
No	Domain	Type	Priority	Data
0	@	A		192.168.2.100
1	www	A		192.168.2.101
2	mail	A		192.168.2.102
3	@	MX	10	mail

Глава 8. 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 8.1. 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

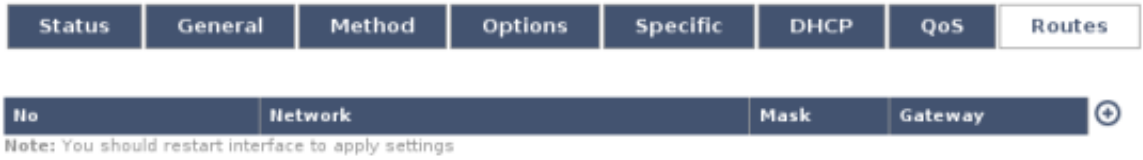
Проанализировав маршруты, приходим к выводу, что маршрут на первую сеть относится к интерфейсу eth0, а на вторую и третью — к dsl0. Поэтому и добавление маршрутов через веб-интерфейс будет производится на страницах соответствующих интерфейсов.

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.

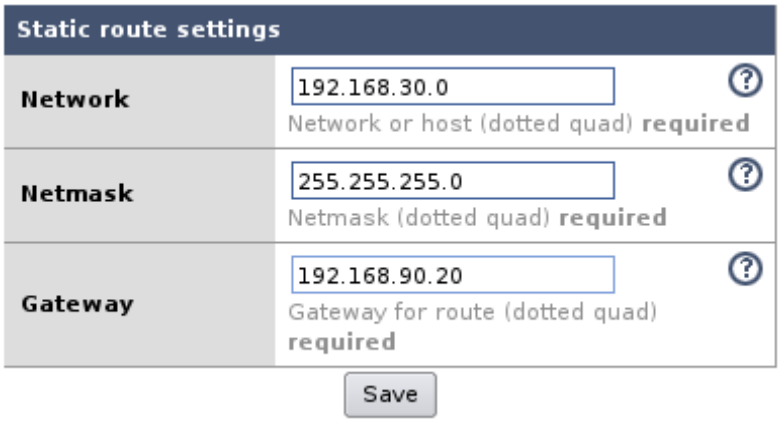
Для добавления маршрута переходим на страницу настройки соответствующего маршруту интерфейса (к примеру, Network/Interfaces/eth0), где выбираем вкладку Routes:

Рисунок 8.2. Пустой список маршрутов



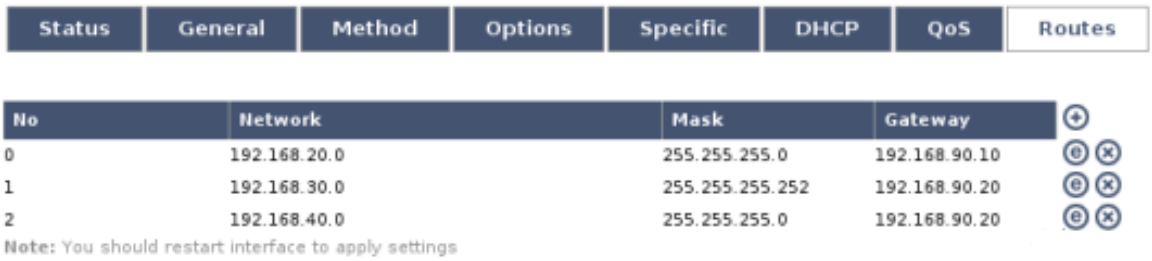
Изначально список пустой. Для добавления нового маршрута, нажимаем на кнопку со значком "+" и заполняем поля в новом окне:

Рисунок 8.3. Добавление маршрута



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

Рисунок 8.4. Список маршрутов



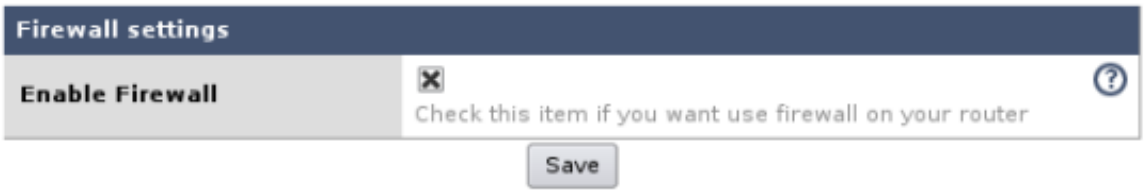
Чтобы внесённые изменения вступили в силу, необходимо "перезагрузить" интерфейс, т.е. на вкладке Status нажать на кнопку *Restart interface*.

Управление межсетевым экраном

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

Активация межсетевого экрана осуществляется на странице Network/Firewall:

Рисунок 8.5. Активация межсетевого экрана



Работа межсетевого экрана основана на прохождении пакетом цепочек правил, где каждое правило определяет одно из действий: приём 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 8.6. Политики цепочек

Замечание

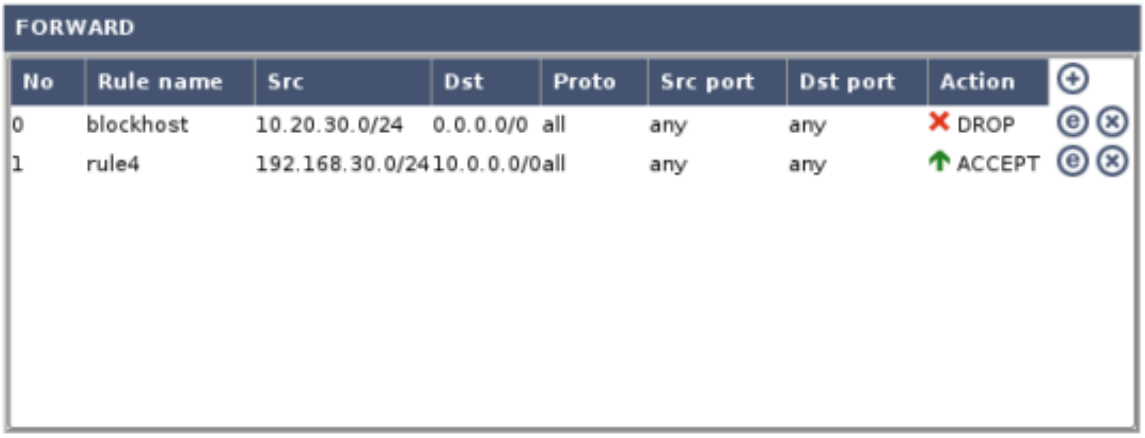
При установлении политики в значение DROP для цепочки INPUT или OUTPUT, удостоверьтесь, что в этих цепочках есть разрешающие правила, иначе управление маршрутизатором может быть потеряно.

Для правила определены следующие действия:

- *ACCEPT* — приём пакета.
- *DROP* — отброс пакета без отправки уведомления источнику пакета.
- *REJECT* — отброс пакета с отправкой уведомления.

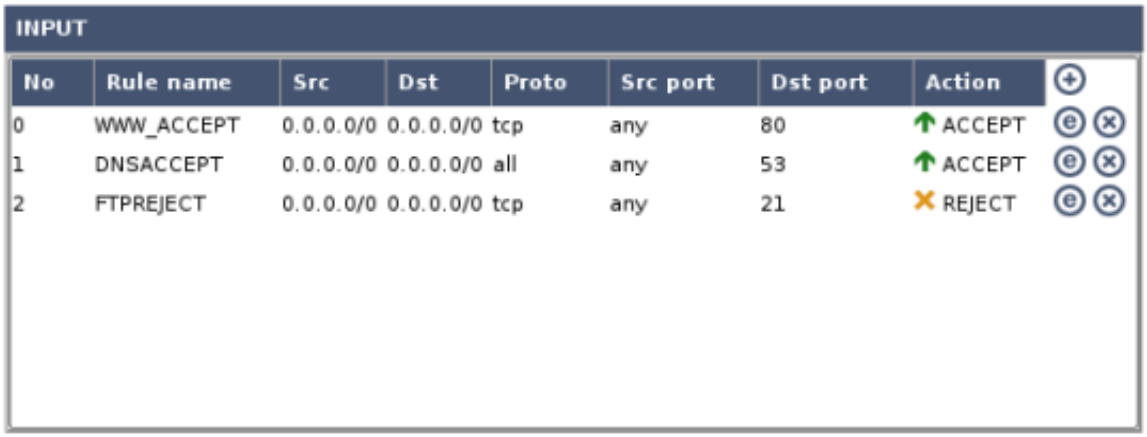
Цепочку FORWARD проходят пакеты, являющиеся транзитными, т.е. идущие с одного интерфейса маршрутизатора на другой:

Рисунок 8.7. Цепочка FORWARD



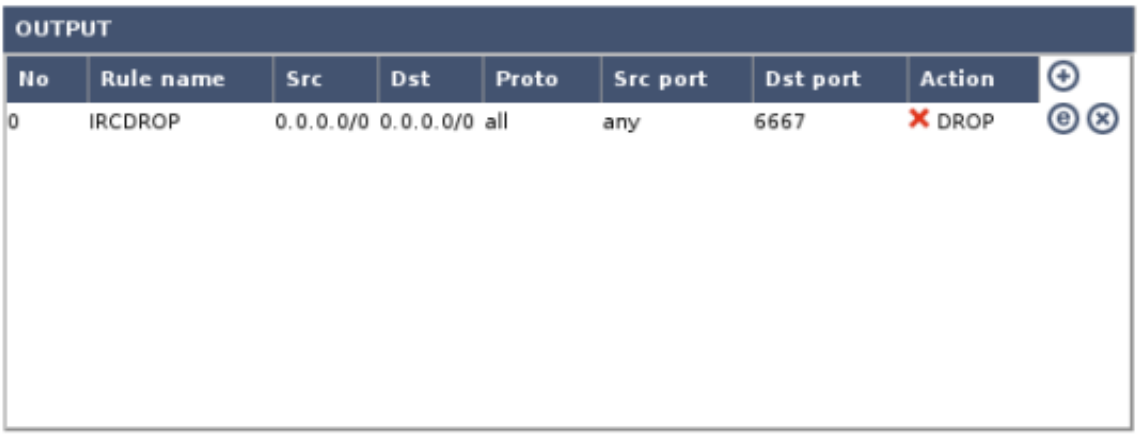
В цепочку INPUT попадают пакеты, предназначающиеся маршрутизатору:

Рисунок 8.8. Цепочка INPUT



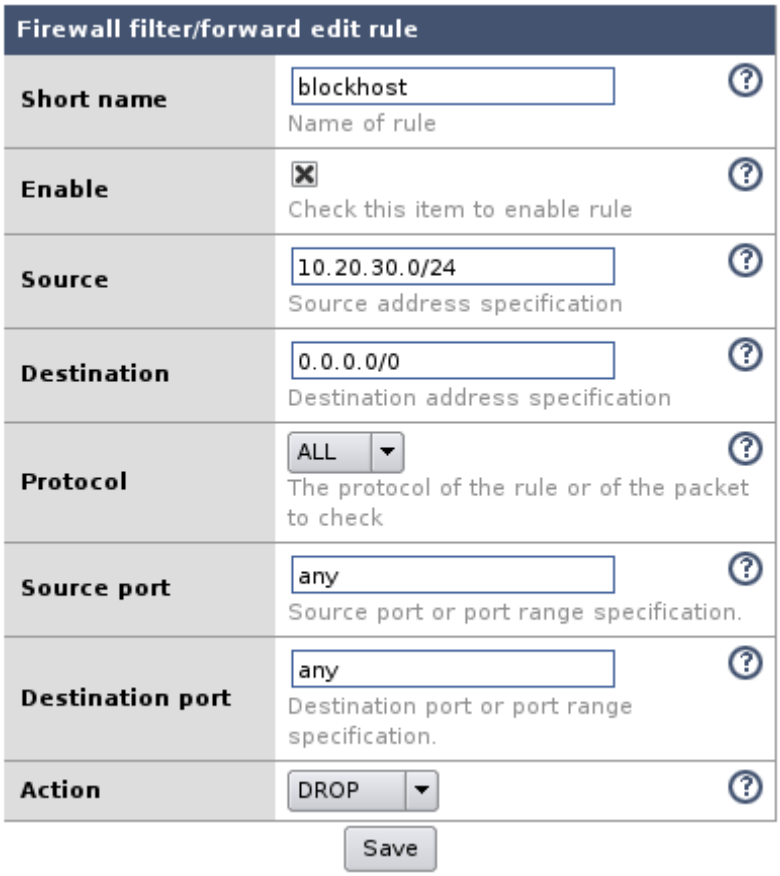
В цепочку OUTPUT попадают пакеты, источником которых является маршрутизатор:

Рисунок 8.9. Цепочка OUTPUT



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

Рисунок 8.10. Добавление правила



- *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

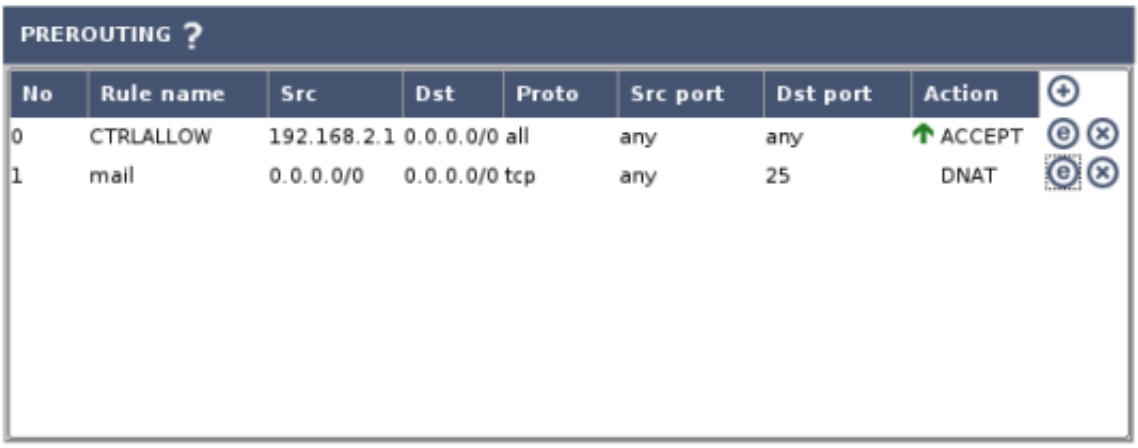
Если внесённые вами изменения не вступают в силу, проверьте, что вы активировали межсетевой экран на странице Network/Firewall.

NAT

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

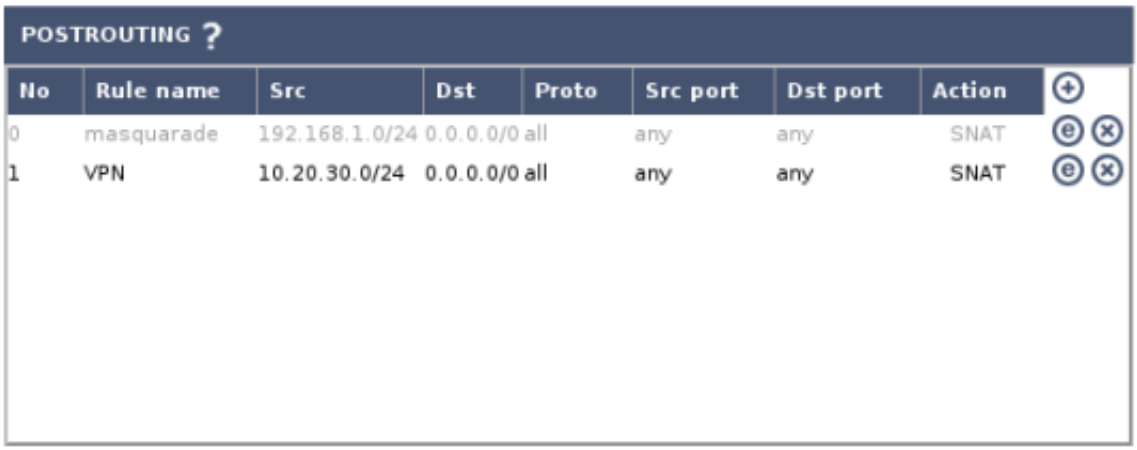
NAT является частью межсетевого экрана, поэтому схема управления остаётся той же, меняется только действие. Все сетевые пакеты, являются ли они транзитными или предназначаются маршрутизатору, попадают сперва в цепочку PREROUTING, где над ними может быть выполнено несколько действий. В этой цепочке не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

Рисунок 8.11. 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 8.12. Цепочка POSTROUTING



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

Рисунок 8.13. Политики цепочек

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 8.14. Добавление правила

Добавление правила и поля аналогично добавлению правила в межсетевом экране (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 НАТа необходимо активировать межсетевой экран на странице Network/Firewall.

Качество обслуживания

Качество обслуживания (QoS — quality of service) позволяет изменить очередность прохождения трафика на интерфейсе. Разные дисциплины обслуживания предоставляют разные возможности по управлению трафиком и его классификации.

Бесклассовая дисциплина pfifo_fast

Стандартная дисциплина обслуживания трафика, реализующая простой механизм First In First Out. Состоит из трех полос — 0, 1 и 2. Полоса 0 обслуживается до тех пор, пока в ней есть пакеты, ожидающие передачи. Затем аналогичным образом обслуживаются полосы 1 и 2.

Распределять трафик по полосам можно с помощью установки битов ToS — Type of Service, которая производится средствами межсетевого экрана. Существует четыре бита ToS, в каждый момент времени может быть установлен только один:

- *Minimum Delay* — минимальная задержка.
- *Maximum Throughput* — максимальная пропускная способность.
- *Maximum Reliability* — максимальная надежность.
- *Minimum Cost* — минимальная стоимость канала.

Важно

В текущей версии веб-интерфейса маршрутизатора отсутствует возможность установки битов ToS. Для этого можно воспользоваться консольным интерфейсом маршрутизатора.

Бесклассовые дисциплины FIFO with bytes buffer (bfifo) и FIFO with packets buffer (pfifo)

Самые простые дисциплины обслуживания. Не содержат внутренних полос, весь трафик равнозначен. Позволяют получать некоторую статистику по их работе.

- *limit* — длина очереди, для bfifo — в байтах, для pfifo — в пакетах.

Бесклассовая дисциплина SFQ

SFQ — Stochastic Fairness Queueing — дисциплина честного планирования. Она оперирует таким понятием, как "поток" — сессия TCP или поток данных UDP, для каждого из которого создаётся своя псевдо-очередь в рамках этой дисциплины. Дисциплина поочередно (round robin) переключается между псевдо-очередями, не позволяя какому-либо потоку использовать весь канал монопольно.

Для распределения сессий по псевдо-очередям используются хэши, которые для повышения эффективности работы дисциплины требуется реконфигурировать. Дисциплина конфигурируется несколькими параметрами.

- *perturb* — интервал времени в секундах, через который выполняется реконфигурация хэша. Рекомендуемое значение — 10.
- *quantum* — число байт, которое изымается из очереди за один "ход" (перед тем, как переключиться на другую очередь). По-умолчанию равно максимальному размеру пакета (MTU), и не должно его превышать!

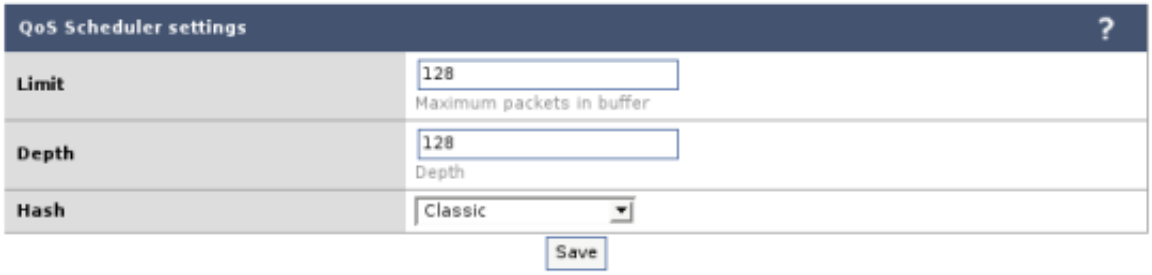
- *limit* — число пакетов, которое может быть помещено в очередь. При превышении этого значения пакеты будут сбрасываться.

При установке дисциплины SFQ в веб-интерфейсе приведённые выше параметры устанавливаются автоматически в рекомендуемые значения.

Бесклассовая дисциплина ESFQ

ESFQ — Enhanced Stochastic Fairness Queueing — улучшенная дисциплина SFQ. Она предоставляет больше возможностей по своей настройке, что позволяет достичь более равномерного распределения полосы пропускания. К примеру, если пользователь использует программы, работающие в несколько потоков, то обычная SFQ становится неэффективной, т.к. она не может разделить канал между пользователями. Дисциплина ESFQ позволяет выбрать другой алгоритм хэширования, например, по IP-адресу отправителя или получателя пакета, что позволяет разнести разных пользователей по разным псевдо-очередям независимо от числа сессий каждого пользователя.

Рисунок 8.15. Конфигурирование ESFQ



- *Limit* — число пакетов, которое может быть помещено в очередь. При превышении этого значения пакеты будут сбрасываться.
- *Depth* — максимально возможное количество псевдо-очередей (в SFQ жёстко задано значение 1024).
- *Hash* — тип хэша.
  - *Classic* — аналогичный используемому в SFQ.
  - *Source address* — по адресу источника.
  - *Destination address* — по адресу получателя.
- *perturb* — интервал времени в секундах, через который выполняется реконфигурация хэша. Рекомендуемое значение — 10 (при установке дисциплины через веб-интерфейс автоматически используется рекомендуемое значение).

Бесклассовая дисциплина TBF

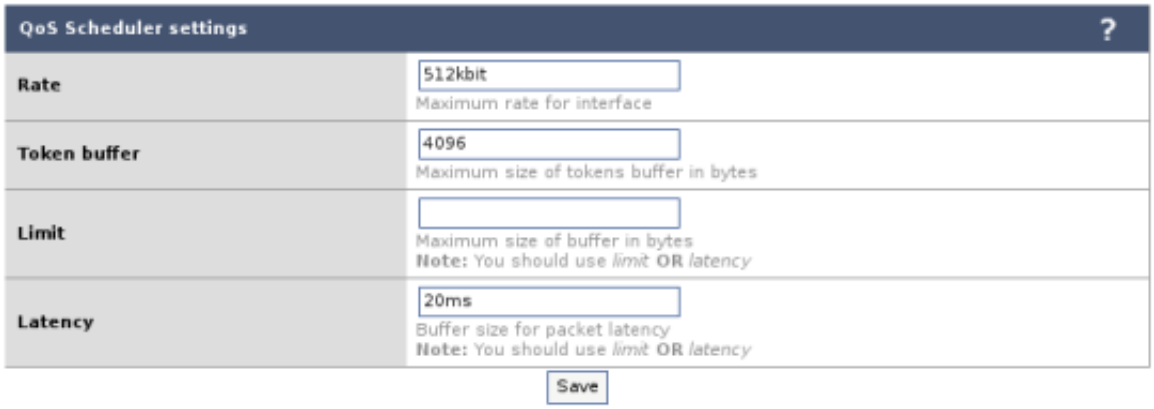
Token Bucket Filter (TBF) — простая бесклассовая дисциплина, пропускающая поступающие пакеты со скоростью, не превышающей заданной. Эта дисциплина относится весьма бережливо к ресурсам системы, поэтому в случае, если надо просто ограничить скорость исходящего трафика — это лучший выбор.

Смысл работы данной дисциплины заключается в следующем. Поступающие для передачи пакеты записываются в буфер дисциплины, откуда они с заданной скоростью поступают на исходящий интерфейс. Возможно три ситуации:

- Пакеты поступают со скоростью, равной скорости передачи их на исходящий интерфейс. В этом случае пакеты проходят через интерфейс без задержек.
- Пакеты поступают со скоростью, меньшей скорости передачи их на исходящий интерфейс. В этом случае при кратковременном возрастании скорости входящего трафика — он будет накоплен во входящей очереди и передан с заданной скоростью.
- Пакеты поступают со скоростью, превышающей скорость передачи их на исходящий интерфейс. В этом случае через некоторое время пакеты начнут сбрасываться.

Дисциплина имеет несколько параметров, позволяющих управлять её работой:

Рисунок 8.16. Конфигурирования TBF



- *Rate* — скорость, с которой поступающий трафик передается на исходящий интерфейс.
- *Token Buffer* — число байт, передаваемых в момент времени на исходящий интерфейс.
- *Limit* — размер буфера в байтах, в который записываются поступающие пакеты, если скорость их поступления превышает скорость их передачи на исходящий интерфейс. При превышении этого параметра пакеты будут сбрасываться.
- *Latency* — время, которое пакет может находиться, ожидая передачи на исходящий интерфейс. По истечении этого времени, пакет будет сброшен.

Важно

Одновременно можно выставлять либо *Limit*, либо *Latency.*

Классовая дисциплина HTB

Дисциплина HTB позволяет выделить разную пропускную способность канала под разные виды трафика. Осуществляется это путём направления трафика в разные классы, которым назначена необходимая пропускная способность. Классифицировать трафик по классам можно на основе IP-адреса или портов отправителя/получателя пакета. Такая обработка трафика (ограничение его по скорости) называется *шейпингом*.

В первую очередь следует отметить, что управлять можно только скоростью исходящего трафика (что, в общем, вполне разумно), поэтому при добавлении правил шейпинга необходимо определить интерфейс, на котором этот трафик будет исходящим.

Реализация QoS на основе классовой дисциплины HTB состоит из двух этапов — создания класса и распределения трафика по классам в соответствии с определенными критериями с помощью фильтров. 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 счёт *неиспользуемой* скорости другого подкласса.

Для дисциплины может быть назначен класс, в который будет направляться весь трафик, не подходящий ни под один фильтр.

Рисунок 8.17. Класс по-умолчанию

Ниже приведена таблица, содержащая информацию о классах. Опционально для каждого класса может быть добавлена своя бесклассовая дисциплина обслуживания, которые описаны выше.

Рисунок 8.18. Классы трафика

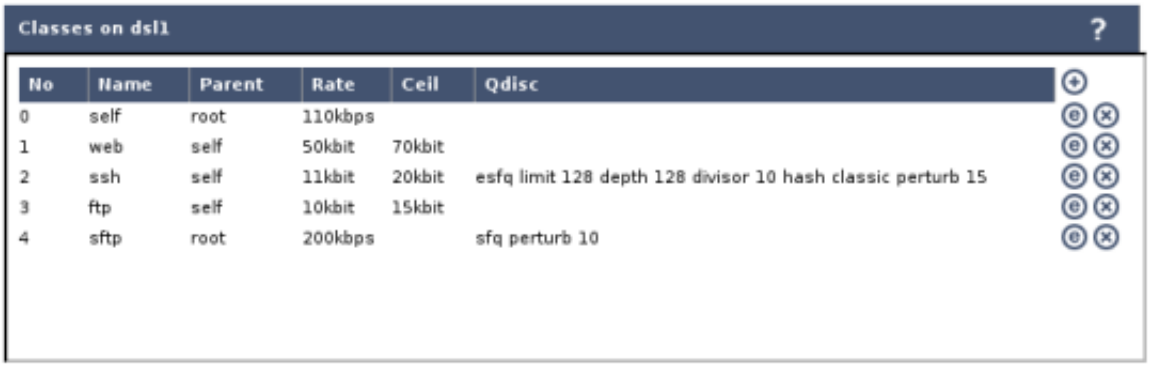
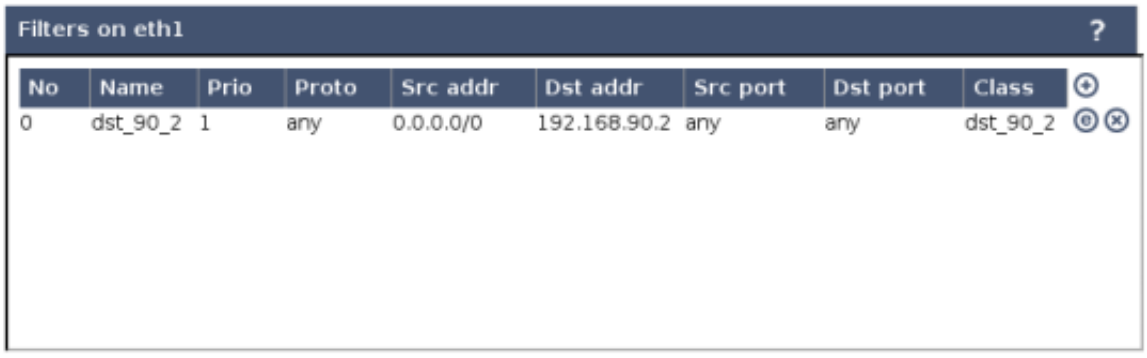


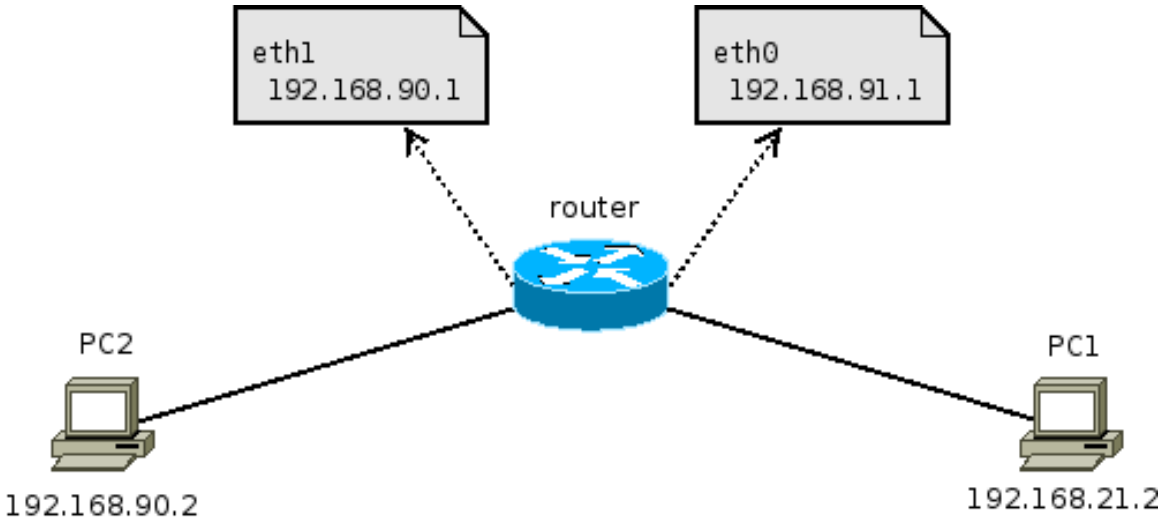
Таблица фильтров, по тем или иным критериям направляющих трафик в классы.

Рисунок 8.19. Фильтры, направляющие трафик в классы



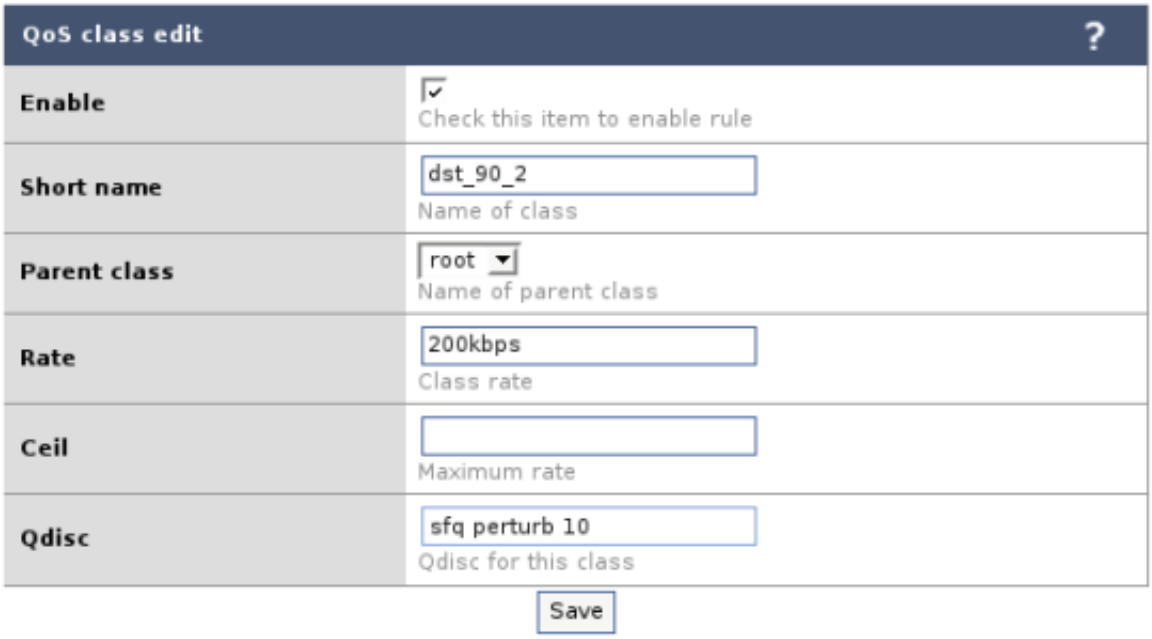
Рассмотрим в качестве примера простую сеть, схема которой представлена ниже:

Рисунок 8.20. 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 создать класс, в который будет поступать трафик, идущий к хосту PC2:

Рисунок 8.21. Добавление класса



- *Enable* — активен ли класс.
- *Short name* — имя добавляемого класса. Используется при классификации трафика в фильтре.
- *Parent class* — родительский класс. root — корневой класс. При добавлении класса в некорневой класс — добавляемый класс будет *подклассом*.

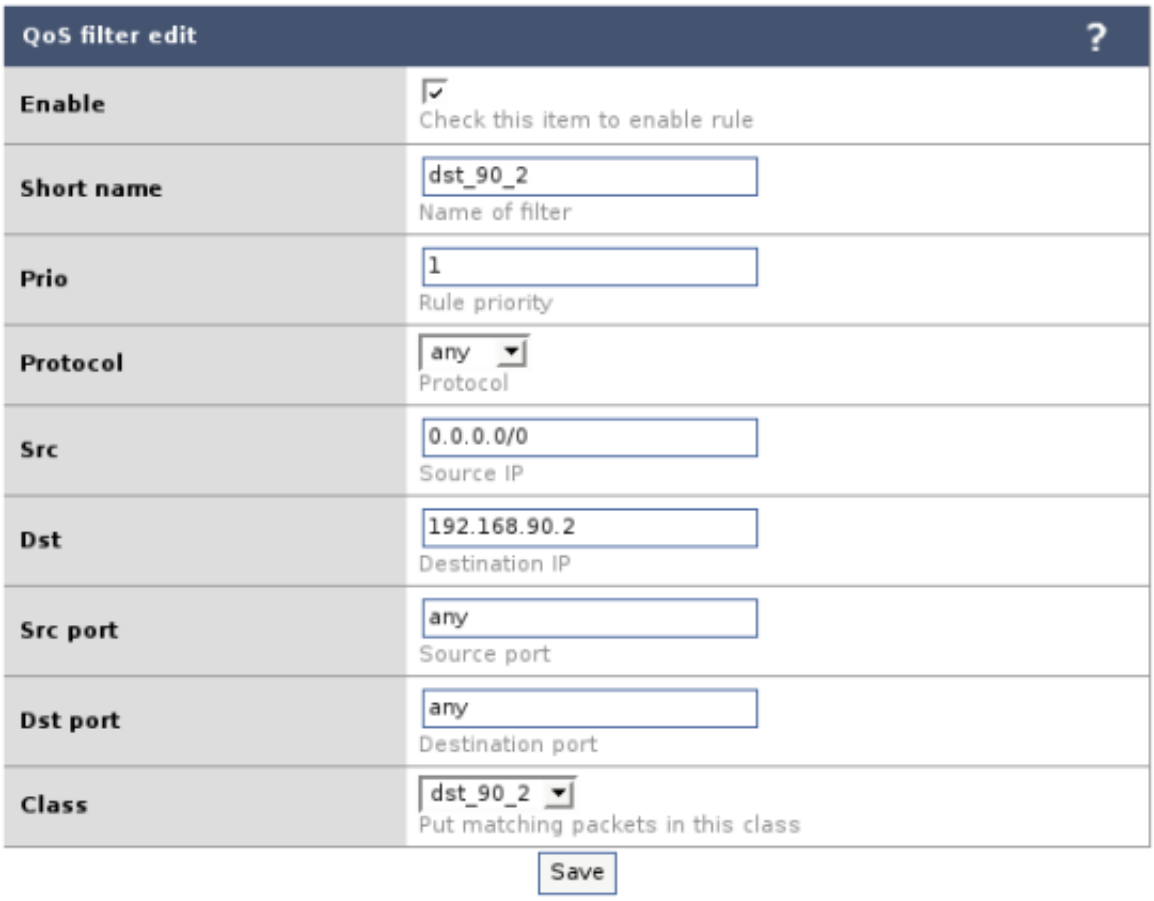
- *Rate* — пропускная способность, выделяемая классу.
- *Ceil* — максимальная пропускная способность подкласса (в случае, если другой подкласс этого же класса использует не всю предоставленную ему пропускную способность). Не должна превышать скорость родительского класса!
- *Qdisc* — опциональная бесклассовая дисциплина обслуживания для класса. Здесь можно указать название дисциплины обслуживания и её параметры, например: **esfq limit 128 depth 128 divisor 10 hash classic perturb 15** или **sfq perturb 10**, и т.д. Подробнее о бесклассовых дисциплинах и их параметрах написано выше.

Чтобы избежать путаницы, заранее рассмотрим принятые в QoS 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.

Теперь нам необходимо классифицировать трафик, идущий к хосту PC2. Для этого нам необходимо создать фильтр:

Рисунок 8.22. Добавление фильтра



- *Enable* — активен ли фильтр.
- *Short name* — имя фильтра.
- *Prio* — приоритет фильтра. Чем меньше значение приоритета — тем он выше.
- *Protocol* — классификация трафика по используемому протоколу.

- *Src* — классификация трафика по адресу отправителя пакета.
- *Dst* — классификация трафика по адресу получателя пакета.
- *Src port* — классификация трафика по номеру порта отправителя пакета.
- *Dst port* — классификация трафика по номеру порта получателя пакета.
- *Class* — в какой класс направить пакет.

В приведённом выше примере мы ограничили входящую скорость для хоста PC2. Но исходящая осталась неограниченной. Чтобы исправить положение, необходимо определить, какой интерфейс является исходящем 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. Поэтому для ограничения исходящего трафика необходимо создать класс с требуемой скоростью и добавить фильтр, который будет отправлять трафик, идущий от хоста PC2 (src 192.168.90.2) направлять в нужный класс.

IPSec

Введение

IPSec является расширением протокола *IP*, предоставляет средства аутентификации и шифрования трафика. Данная реализация IPSec выполнена на основе KAME. Настройка IPSec выполняется на странице Network/IPSec.

В IPSec предусмотрено два протокола — *AH* для аутентификации и *ESP* для шифрования трафика. Однако, протокол *ESP* имеет встроенные средства для проверки аутентичности пакета. Таким образом, есть несколько способов передачи трафика с разной степенью защиты:

- Передача трафика только с проверкой аутентификации. В этом случае задействован протокол *AH*, трафик передаётся в открытом виде, гарантируется только подлинность отправителя пакета. Это наименее ресурсоёмкий способ защиты трафика.
- Передача трафика с его шифрованием. В этом случае используется протокол *ESP*, проверка подлинности отправителя не выполняется. Это гораздо более ресурсоёмкий способ защиты трафика.
- Передача трафика с аутентификацией и шифрованием, с использованием протоколов *AH* и *ESP*. Этот режим называется *nested ESP in AH*. Каждый протокол выполняет свою функцию. Это наиболее ресурсоёмкий режим.
- Передача трафика с аутентификацией и шифрованием, используя только протокол *ESP*. Этот режим называется *authenticated ESP*, он менее ресурсоёмок режима *nested ESP in AH*.

Протокол *AH* используется для аутентификации и проверки целостности пакета. Для этого он выполняет расчёт хэша пакета (HMAC) на основе секретного ключа, полезного содержимого пакета и его неизменяемой части — IP-адреса. Так как в расчёте HMAC участвует IP-адрес, протокол AH не допускает трансляцию адресов (NAT). Получатель пакета повторяет расчёт HMAC и сверяет его с переданным вместе с пакетом, если они отличаются — нарушена целостность пакета либо его аутентичность.

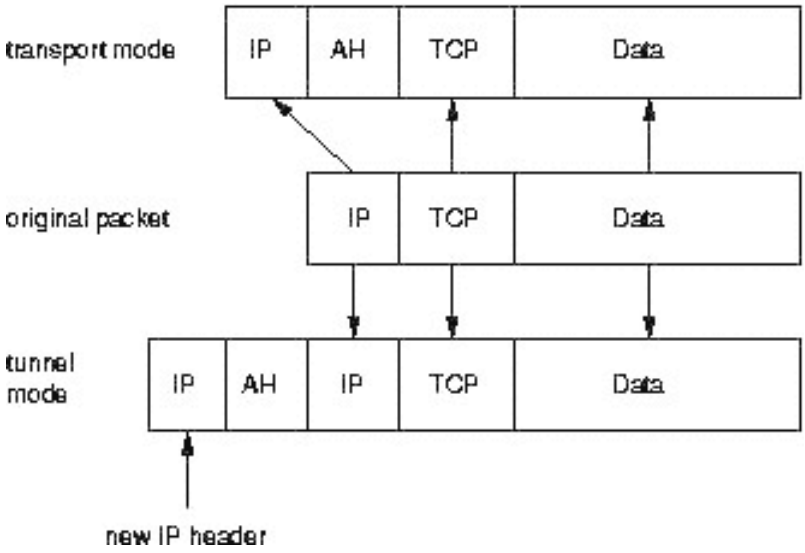
Протокол *ESP* может быть использован как для шифровании пакета, так и для проверки его целостности и аутентичности. Шифрование производится блочными алгоритмами с

использованием секретного ключа, аутентификация выполняется так же, как в *AH*. При использовании аутентификации, получатель пакета сперва проверяет корректность HMAC, и лишь затем дешифрует пакет.

Есть два режима работы IPSec:

- *Транспортный режим* — защищается только полезная нагрузка пакета — заголовок IPSec вставляется между заголовком IP и заголовком протокола верхнего уровня. Таким образом, видны адреса отправителя и получателя пакета.
- *Туннельный режим* — оригинальный пакет инкапсулируется в новый пакет IPSec, таким образом полностью защищается исходный пакет, скрываются оригинальные адреса отправителя и получателя пакета.

Рисунок 8.23. Режимы работы IPSec



Настройка IPSec заключается в создании защищённых виртуальных каналов (*SA*, security association, контекст безопасности) и политик безопасности (*SP*, security policy). Их настройка описывается в соответствующих разделах.

Контекст безопасности

Создание и редактирование контекстов безопасности выполняется на вкладке Security Association. Каждый контекст безопасности определяет, как защищать передаваемый трафик, и характеризуется следующими параметрами:

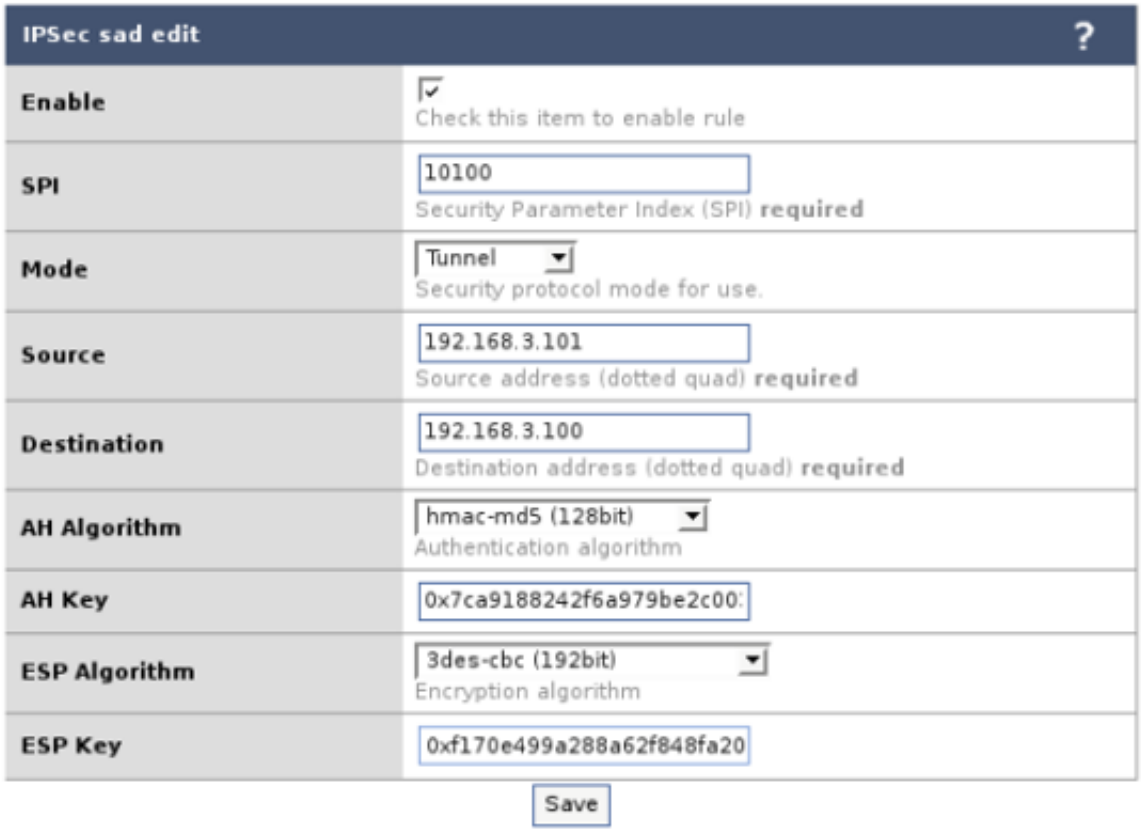
- IP-адреса отправителя и получателя IPSec пакета (узлов, которые защищают трафик).
- Протокол IPSec: AH или ESP.
- Алгоритм и секретный ключ, используемый IPSec протоколом.
- Индекс контекста безопасности, SPI (Security Parameter Index).
- Режим IPSec (транспортный или туннельный).

Так как в контексте безопасности указываются IP-адреса получателя и отправителя пакета, то один контекст безопасности способен передавать трафик только в одном направлении. Чтобы организовать полнодуплексную передачу, необходимо создать

два контекста, по одному для каждого направления. Если используется оба протокола — AH и ESP — то необходимо создать 4 контекста безопасности — по каждому на каждый протокол и каждое направление.

Пример создания контекста безопасности показан на рисунке.

Рисунок 8.24. Создание контекста безопасности



- *SPI* — Security Parameter Index — индекс контекста безопасности, произвольное 32-х битное целое число (кроме значений от 0 до 255).
- *Mode* — режим работы: транспортный или туннельный.
- *Source* — IP-адрес источника пакета IPSec.
- *Destination* — IP-адрес получателя пакета IPSec.

Замечание

Source, *Destination* — IP-адреса узлов, генерирующих IPSec пакеты, т.е. обеспечивающие безопасность соединения. Это не всегда IP-адреса узлов, являющиеся источниками незащищённого трафика.

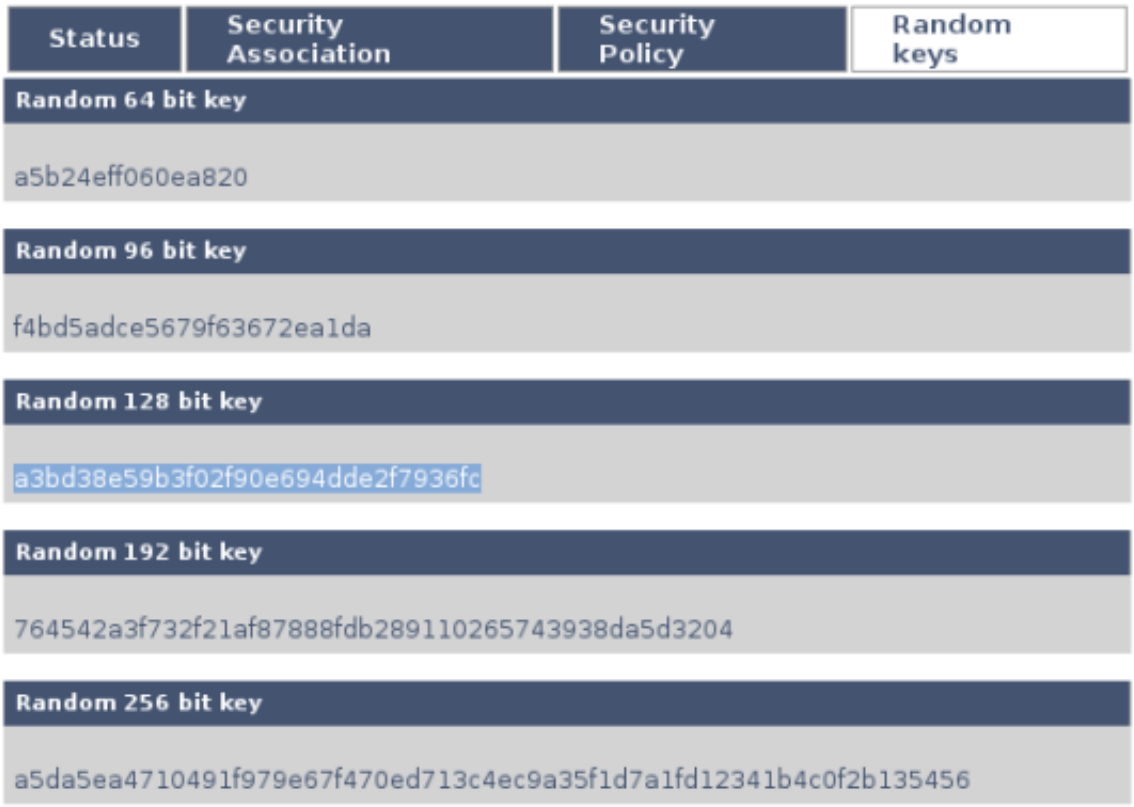
- *AH Algorithm* — алгоритм для проверки аутентичности пакета.
- *AH Key* — секретный ключ, используемый алгоритмом AH для вычисления хэша HMAC.
- *ESP Algorithm* — алгоритм для шифрования пакета.
- *ESP Key* — секретный ключ, используемый алгоритмом ESP для шифрования пакета.

Немного подробнее об алгоритмах AH и ESP:

- Если выбран только алгоритм AH (ESP — none) — то протокол контекста безопасности будет установлен в AH.
- Если выбран только алгоритм ESP (AH — none) — то протокол контекста безопасности будет установлен в ESP.
- Если выбраны оба алгоритма (AH и ESP) — то протокол контекста безопасности будет установлен в ESP, и для пакета будет рассчитываться хэш HMAC (authenticated ESP).

Рядом с названием алгоритма указана необходимая длина ключа. Ключи различной длины генерируются на вкладке Random keys, содержимое которой обновляется при каждой перезагрузке страницы.

Рисунок 8.25. Random keys



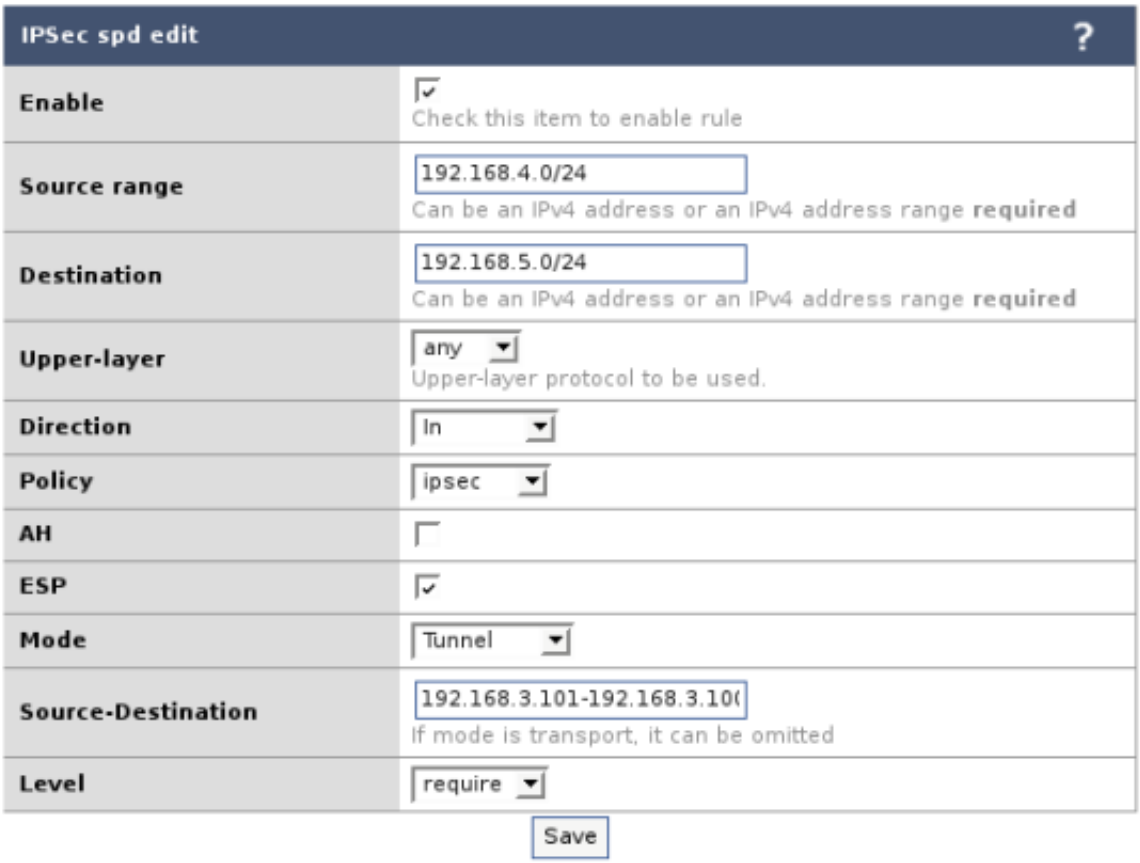
Политика безопасности

Политика безопасности определяет, какой трафик следует защищать, т.е. использовать для него контекст безопасности. Настройка политики безопасности выполняется на вкладке Security Policy и характеризуется следующими основными параметрами:

- IP-адреса источника и получателя пакетов, которые следует защищать. В транспортном режиме это те же адреса, что и в контексте безопасности, в туннельном могут отличаться.
- Вышележащий протокол, подлежащий защите (tcp, udp, ...).
- Режим IPSec (транспортный или туннельный).

Так же как и в контексте безопасности, политика безопасности определяет только одно направление трафика, поэтому для полнодуплексного обмена необходимо создать две политики безопасности. Ниже приведён пример создания политики безопасности.

Рисунок 8.26. Создание политики безопасности



- *Source range* — IP-адрес или сеть отправителя пакета, для которого надо применить контекст безопасности.
- *Destination* — IP-адрес или сеть получателя пакета, для которого надо применить контекст безопасности.
- *Upper-layer* — вышележащий протокол, для которого надо применить контекст безопасности.
- *Direction* — направление трафика:
  - *In* — входящий трафик.
  - *Out* — исходящий трафик.
  - *Fwd* — транзитный трафик.
- *Policy* — политика, применяемая к пакету, попавшему под критерии:
  - *ipsec* — применять для пакета операции IPSec.
  - *none* — не применять для пакета операции IPSec.
  - *discard* — сбросить пакет.
- *AH* — использовать контекст безопасности с протоколом AH.

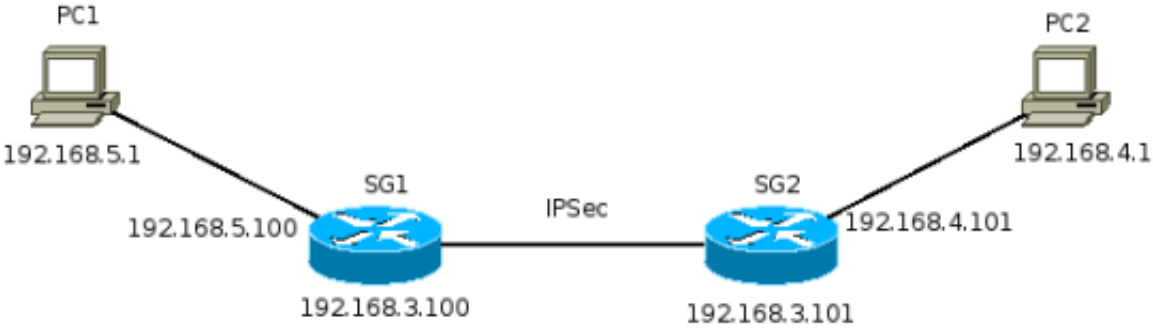
- *ESP* — использовать контекст безопасности с протоколом ESP.
- *Mode* — транспортный или туннельный режим.
- *Source-Destination* — IP-адрес отправителя-получателя пакета в контексте безопасности.
- *Level* — правило обработки пакета:
  - *default* — использовать системные настройки для выбранного протокола, например значение переменной sysctl *esp_trans_deflev*.
  - *use* — использовать, если возможно, контекст безопасности, иначе обрабатывать пакет в обычном режиме (как обычный IP пакет).
  - *require* — всегда использовать контекст безопасности, если он не доступен — сбрасывать пакет.
  - *unique* — не используется.

Пример конфигурации

В качестве примера рассмотрим настройку наиболее типичной конфигурации — authenticated ESP, т.е. передачи шифрованного трафика с помощью протокола ESP с проверкой аутентичности пакета. IPSec будет работать в туннельном режиме.

В нашем примере есть две сети, соединённые маршрутизаторами, образующими между собой третью сеть. Стоит задача защиты трафика, передаваемого между узлами PC1 и PC2 на участке SG1-SG2, т.е. между маршрутизаторами. Пример сети представлен ниже.

Рисунок 8.27. Пример конфигурации IPSec: схема сети



Прежде всего необходимо настроить маршрутизацию, в общем виде следует выполнить следующие действия:

- *PC1* — добавить маршрут к сети 192.168.4.0/24 через маршрутизатор 192.168.5.100.
- *PC2* — добавить маршрут к сети 192.168.5.0/24 через маршрутизатор 192.168.4.101.
- *SG1* — добавить маршрут к сети 192.168.4.0/24 через маршрутизатор 192.168.3.101.
- *SG2* — добавить маршрут к сети 192.168.5.0/24 через маршрутизатор 192.168.3.100.

Как прописывать статические маршруты для маршрутизатора см. раздел Добавление сетевых маршрутов.

Без использования IPSec трафик на интерфейсе eth1 (192.168.3.100) маршрутизатора SG1 имеет следующий вид:

```
03:11:37.423594 IP 192.168.4.1 > 192.168.5.1:
 ICMP echo request, id 9596, seq 5, length 64
03:11:37.424282 IP 192.168.5.1 > 192.168.4.1:
 ICMP echo reply, id 9596, seq 5, length 64
03:11:38.421283 IP 192.168.4.1 > 192.168.5.1:
 ICMP echo request, id 9596, seq 6, length 64
03:11:38.421947 IP 192.168.5.1 > 192.168.4.1:
 ICMP echo reply, id 9596, seq 6, length 64
```

Из вывода *tcpdump* видно, что по каналу идёт нешифрованный трафик — пинг от 192.168.4.1 к 192.168.5.1.

Для настройки IPSec необходимо создать два контекста безопасности (по одному на каждое направление трафика), одинаковых для обоих маршрутизаторов.

Рисунок 8.28. Создание контекста безопасности №1, направление 192.168.3.101-192.168.3.100

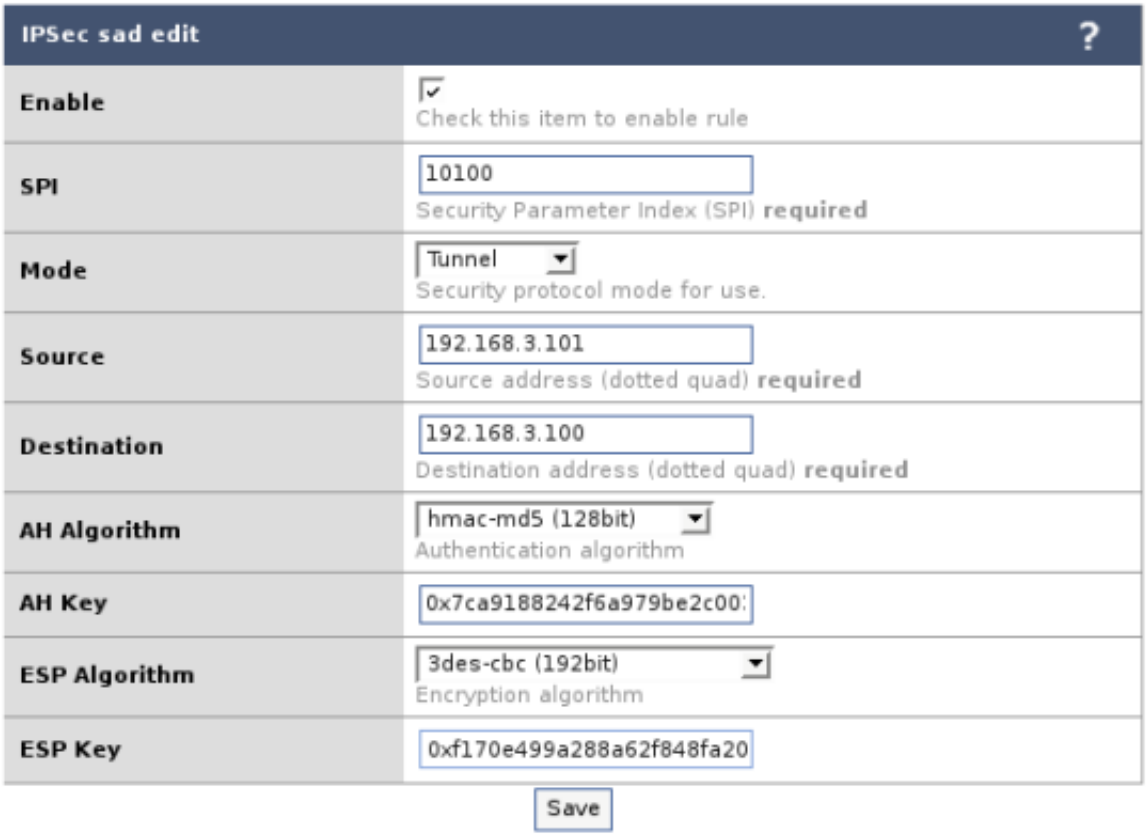
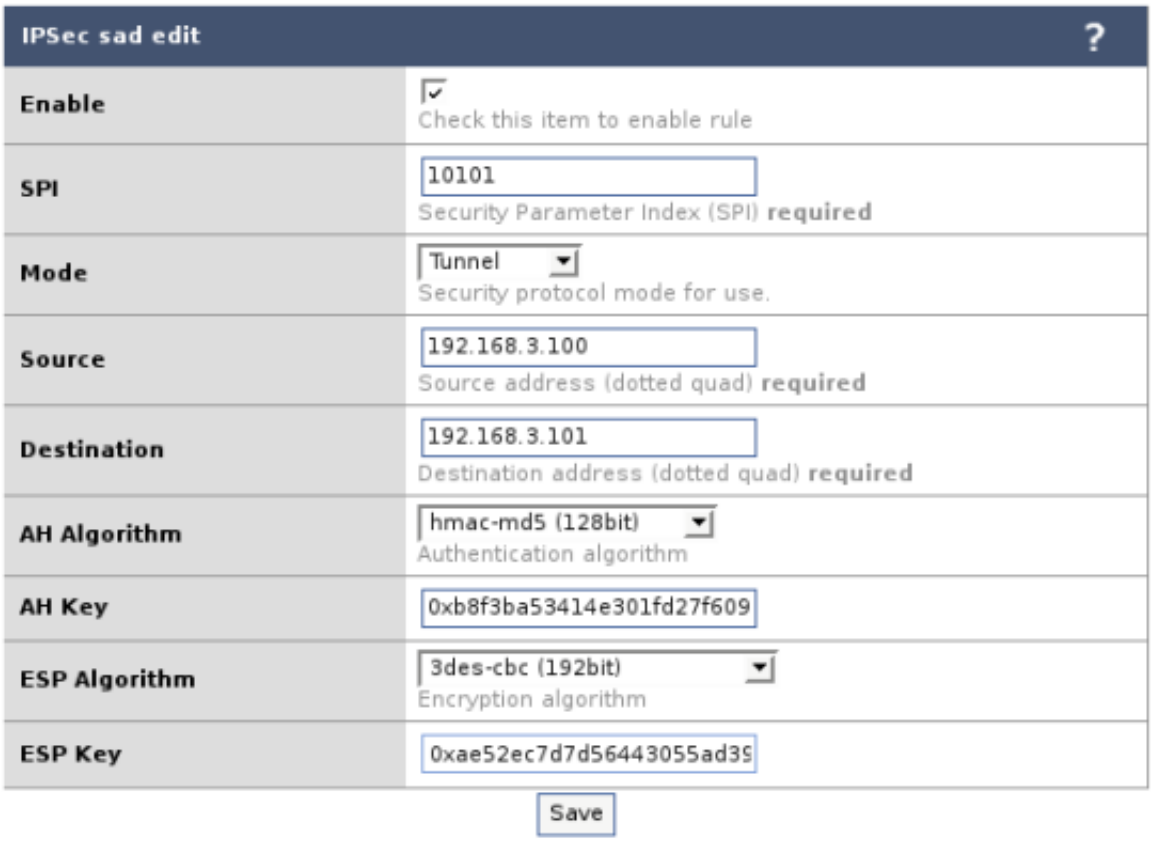


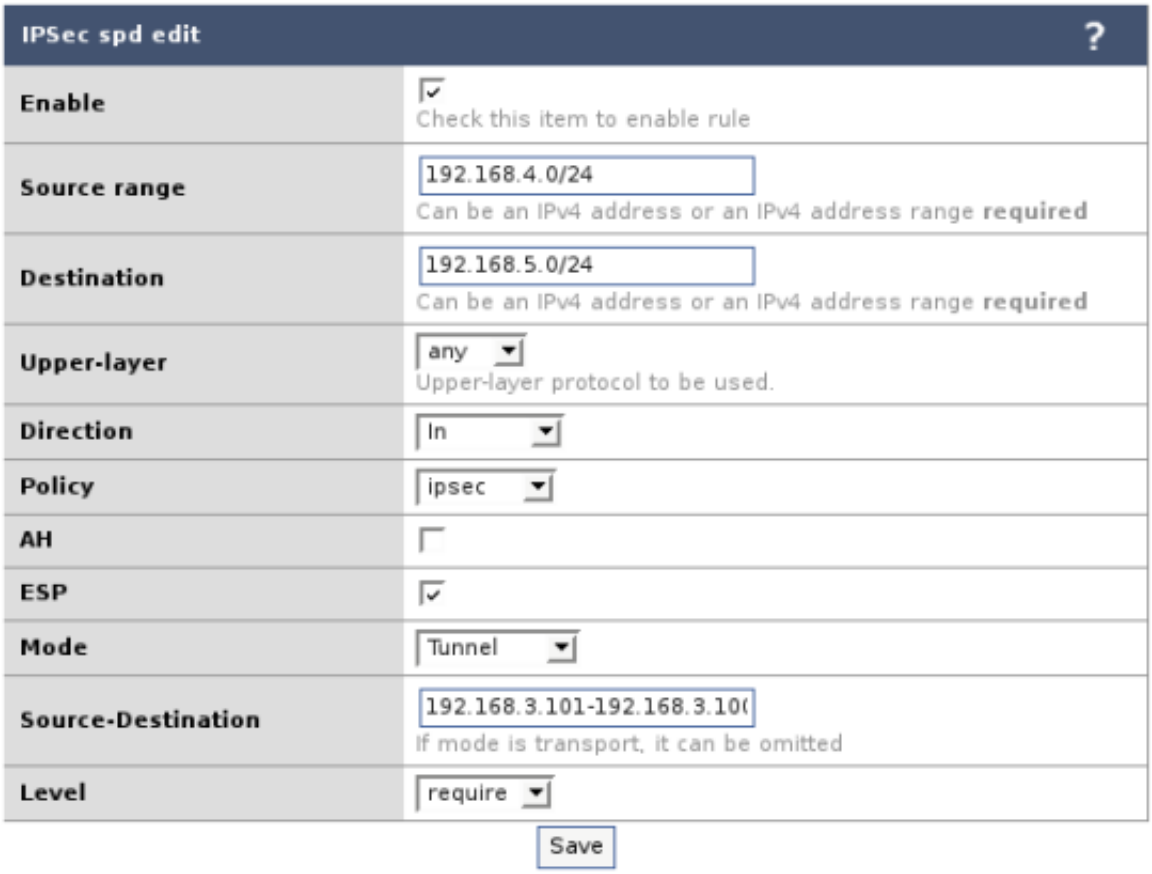
Рисунок 8.29. Создание контекста безопасности №2, направление 192.168.3.100-192.168.3.101



В контексте безопасности мы установили туннельный режим, задали алгоритмы AH и ESP, что означает authenticated ESP, и ввели номер SPI.

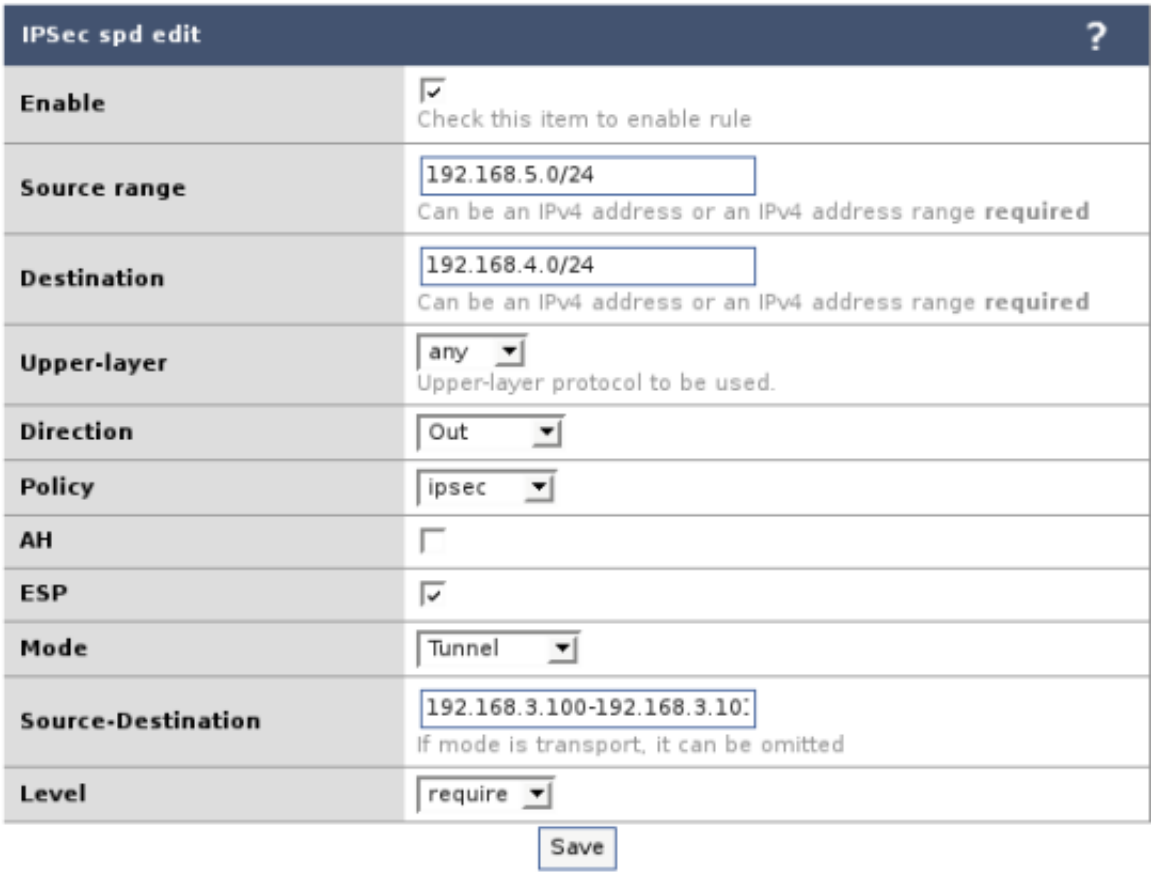
Так же необходимо создать по две политики безопасности на каждом маршрутизаторе, отличающихся направлением трафика. Так, для маршрутизатора SG1 передача трафика 192.168.3.101-192.168.3.100 имеет направление *IN*, т.к. для него это входящий трафик, а для маршрутизатора SG2 — *OUT*, т.к. для него это исходящий трафик.

Рисунок 8.30. Создание политики безопасности №1 для SG1



Данная политика безопасности требует (level — require), чтобы весь трафик (upper-layer — any), идущий от узлов сети 192.168.4.0/24 (т.е. от PC2) к узлам в сети 192.168.5.0/24 (к PC1) обслуживался контекстом безопасности, созданном для направления 192.168.3.101-192.168.3.100 (source-destination). Т.к. мы используем authenticated ESP, то не активируем использование контекста безопасности для протокола AH.

Рисунок 8.31. Создание политики безопасности №2 для SG1



Данная политика безопасности аналогична предыдущей, за исключением адресов назначения пакетов и направления трафика.

Рисунок 8.32. Создание политики безопасности №1 для SG2

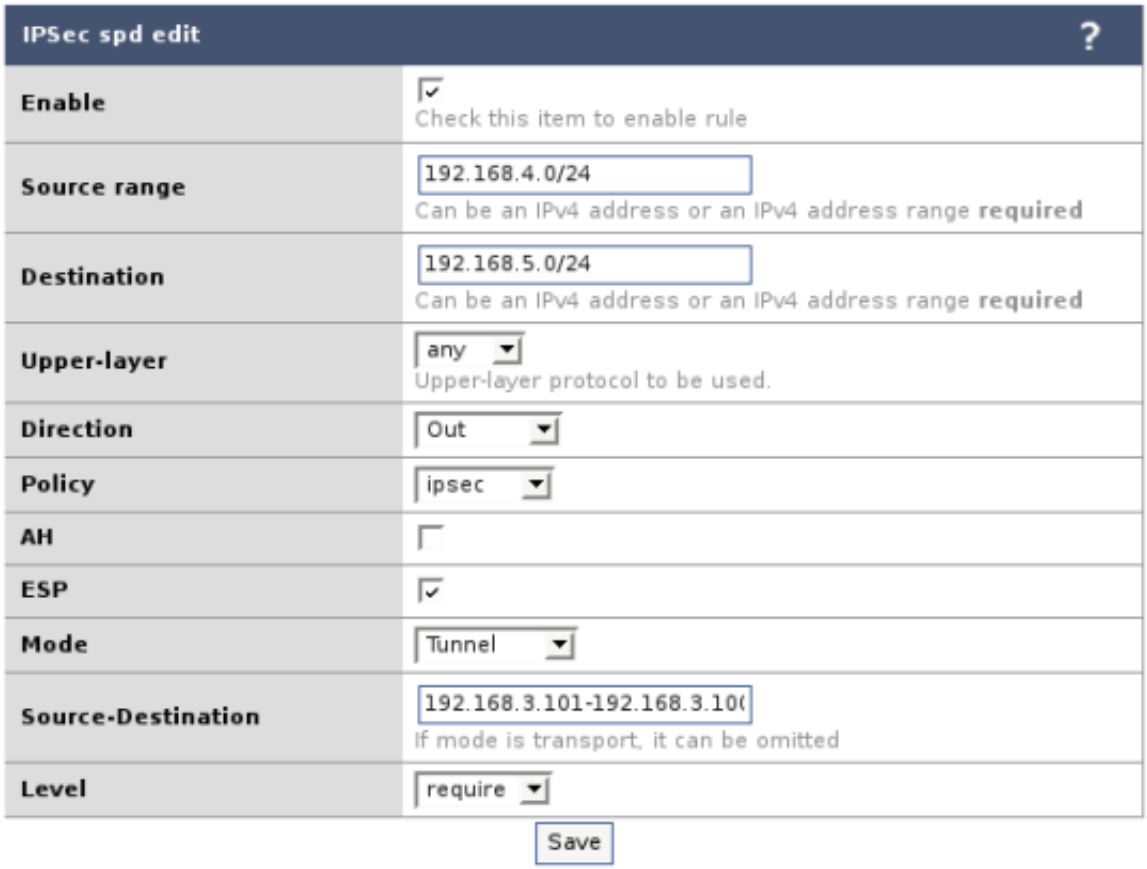
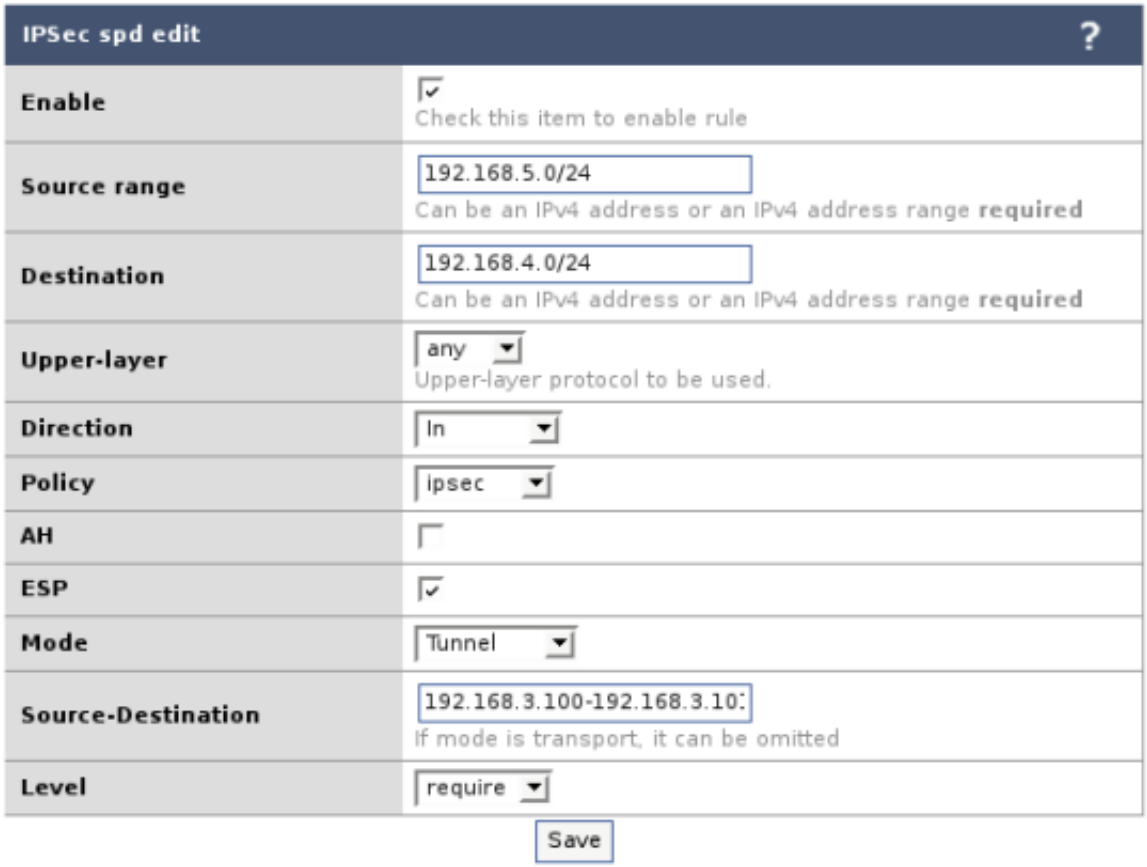


Рисунок 8.33. Создание политики безопасности №2 для SG2



Эти политики безопасности отличаются от аналогичных для маршрутизатора SG1 только направлением трафика.

После настройки IPSec трафик на интерфейсе eth1 (192.168.2.100) маршрутизатора SG1 следующий:

```
1. 09:36:23.736136 IP 192.168.3.101 > 192.168.3.100:
 ESP(spi=0x00002774,seq=0x10), length 116
2. 09:36:23.736136 IP 192.168.4.1 > 192.168.5.1:
 ICMP echo request, id 29460, seq 1, length 64
3. 09:36:23.738225 IP 192.168.3.100 > 192.168.3.101:
 ESP(spi=0x00002775,seq=0x16f), length 116
4. 09:36:24.732904 IP 192.168.3.101 > 192.168.3.100:
 ESP(spi=0x00002774,seq=0x11), length 116
5. 09:36:24.732904 IP 192.168.4.1 > 192.168.5.1:
 ICMP echo request, id 29460, seq 2, length 64
6. 09:36:24.734876 IP 192.168.3.100 > 192.168.3.101:
 ESP(spi=0x00002775,seq=0x170), length 116
```

Проведём небольшой анализ трафика. На интерфейс от маршрутизатора SG2 (192.168.3.101) приходит ESP пакет (строка 1), который после обработки IPSec выглядит, как ICMP запрос от PC2 к PC1 (строка 2). Следует заметить, что по ESP пакету нельзя сказать, между какими узлами идёт обмен информацией. ICMP запрос отправляется узлу PC1 через интерфейс eth0 (192.168.5.100), поэтому в данном листинге его не видно. На тот же интерфейс приходит ответ, который отправляется маршрутизатору SG2 после обработки IPSec в виде ESP пакета (строка 3).

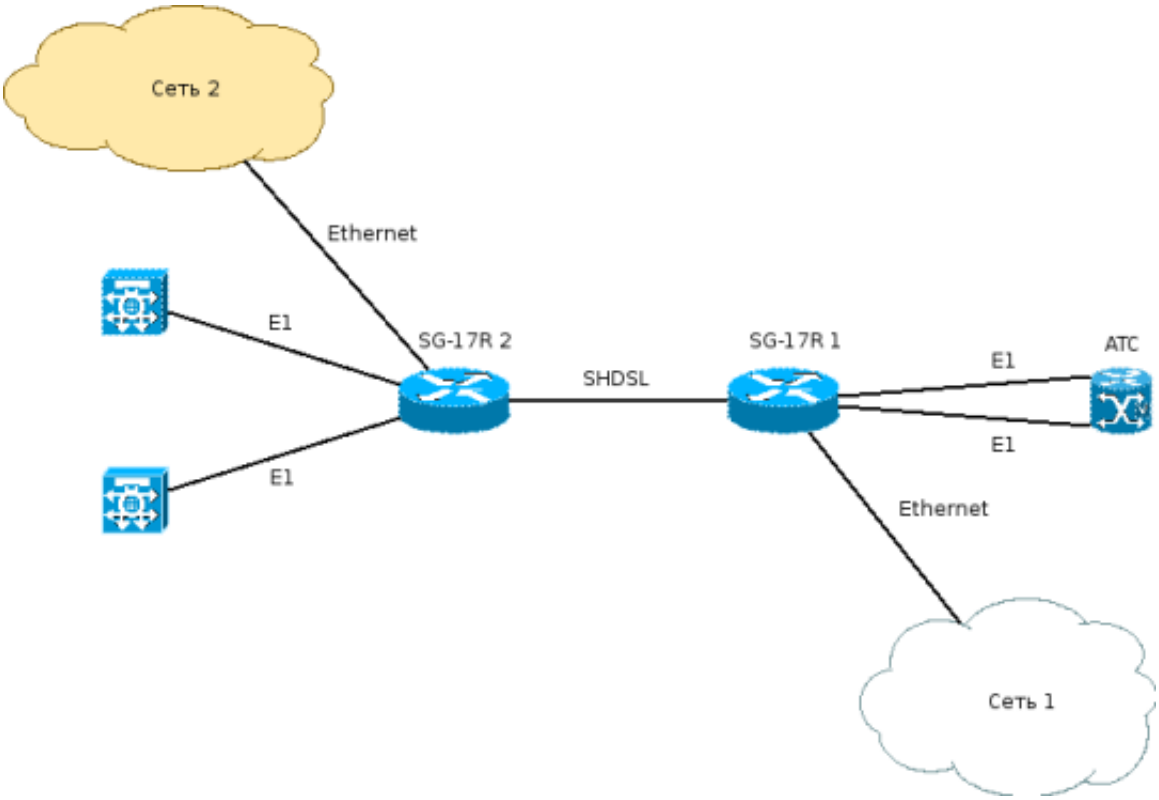
Глава 9. Мультиплексирование

Конфигурирование

Мультиплексирование используется для передачи трафика с одного интерфейса на другой, минуя центральный процессор. *SG-17R* позволяет одновременно мультиплексировать и маршрутизировать сетевой трафик.

В общем виде это можно представить так:

Рисунок 9.1. Схема сети

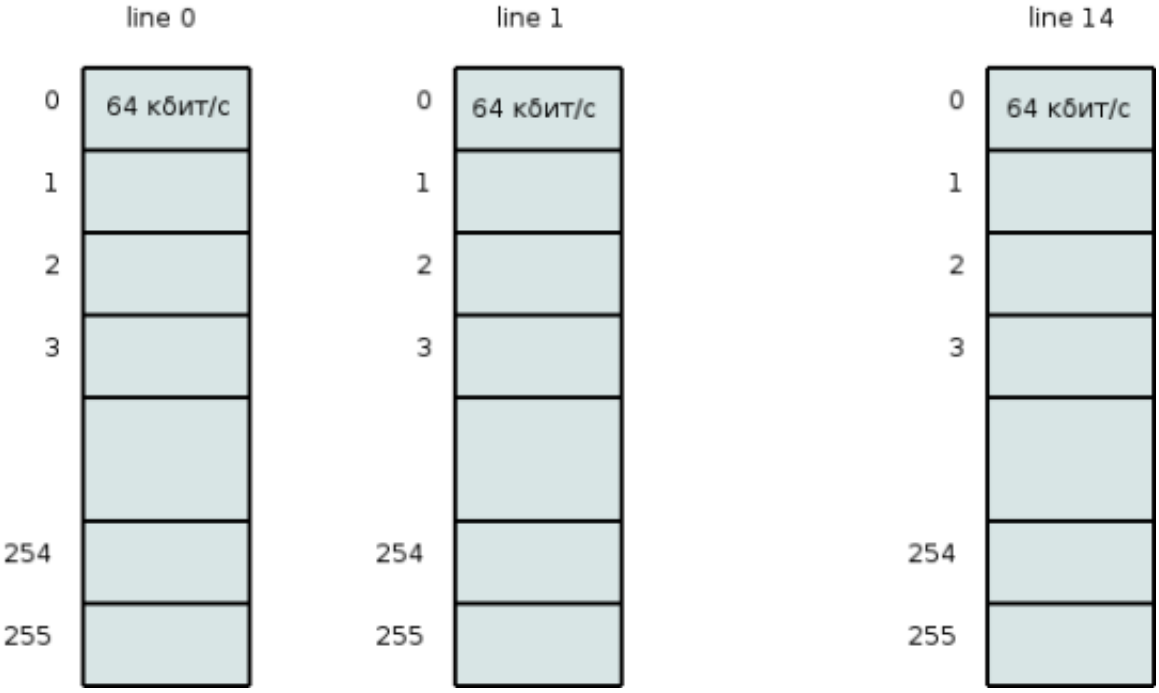


В приведенном примере к маршрутизаторам SG-17R подключено два канала E1, а так же сеть TCP/IP по Ethernet. Два маршрутизатора соединены между собой через SHDSL. Максимальная скорость SHDSL составляет 5696 кбит/с, т.е. по одному каналу SHDSL можно передать два канала E1 (2048 кбит/с каждый), и останется неиспользованными 1600 кбит/с.

Для передачи потоков E1 используется мультиплексирование: оба входных потока E1 мультиплексируются в канал SHDSL, по которому они передаются на второй маршрутизатор, где происходит демультиплексирование, и потоки расходятся к клиентам. Оставшаяся полоса SHDSL используется для передачи TCP/IP трафика между двумя Ethernet сетями.

Для мультиплексирования в маршрутизаторе выделена шина, состоящая из 16 линий, каждая из которых содержит 256 тайм-слотов. Каждый тайм-слот на линии соответствует тайм-слоту в E1 или SHDSL, т.е. имеет скорость 64 кбит/с. E1 содержит 32 тайм-слота, SHDSL — 89 тайм-слотов. Интерфейсы E1 (E1) и SHDSL (dsl) могут выставлять на нее данные, полученные из физической линии, и принимать данные, выставленные другим интерфейсом.

Рисунок 9.2. Физическая организация мультиплексирования



Все устройства, участвующие в мультиплексировании трафика, должны тактироваться одним сигналом. Для этого при настройке мультиплексирования необходимо указать, какой интерфейс будет задавать тактовый сигнал.

Маршрутизатор может иметь два задающих источника синхросигнала для мультиплексирования, каждый из которых определяет *домен*. Каждая линия относится либо к домену A, либо к домену B, соответственно, все интерфейсы, относящиеся к этой линии, так же относятся либо к домену A, либо к B. Задающий синхросигнал можно использовать либо локальный, либо удаленный.

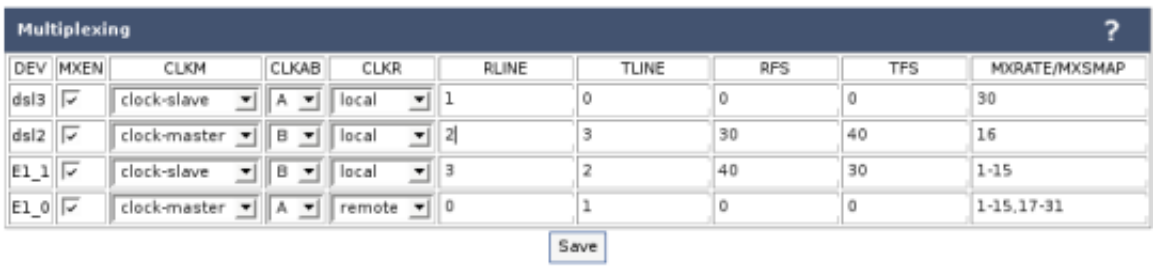
Важно

В одном домене должно быть одно и только одно устройство (интерфейс), задающее тактовый сигнал! Все остальные устройства домена должны быть установлены в режим *clock slave*. Таким образом, от одного устройства тактируются все устройства, находящиеся в данном домене.

Для работы мультиплексирования необходимо активировать сетевые интерфейсы (поставить флажки Enabled и Auto), которые участвуют в передаче трафика. Сделать это можно на странице настройки сетевого интерфейса (Network/имя_сетевого_интерфейса).

Ниже представлена страница конфигурации мультиплексирования, которая находится по адресу System/Multiplexing.

Рисунок 9.3. Настройка мультиплексирования



- *mxen* — интерфейс принимает участие в мультиплексировании.
- *clkm* — синхронизация интерфейса:
  - *clock-master* — интерфейс является источником синхронизации для данного домена.
  - *clock-slave* — интерфейс является приёмником синхронизации.
- *clkab* — определяет, к какому домену синхронизации относится интерфейс.
- *clkr* — источник синхронизации:
  - *local* — использовать для тактирования локальный клок.
  - *remote* — использовать для тактирования внешний клок.
- *rline* — номер линии, на которую интерфейс будет выставлять данные, полученные из физической линии.
- *tline* — номер линии, с которой данный интерфейс забирает данные (выставленные другим интерфейсом, участвующим в мультиплексировании) для передачи в физическую линию.
- *rfs* — номер тайм-слота линии, начиная с которого на неё выставляются данные этим интерфейсом.
- *tfs* — номер тайм-слота линии, начиная с которого с неё забираются данные.
- *mxrate* — число тайм-слотов, отводимых для мультиплексирования (для интерфейсов SHDSL).
- *mxsmap* — карта тайм-слотов, используемых для мультиплексирования (для интерфейсов E1). Эта карта не должна пересекаться с картой, которая задаётся при настройки интерфейса E1 для передачи IP трафика. Карта задаётся в виде "1-16", "16-31", ...

Важно

Тайм-слот в E1 может использоваться *только* либо для мультиплексирования, либо для маршрутизации, поэтому карта тайм-слотов, задаваемых для мультиплексирования параметром `mxsmap` не должна пересекаться с картой тайм-слотов, указанных при настройке E1 для использования в передаче IP-трафика.

Если при настройке были допущены ошибки, будет показана диагностическая информация:

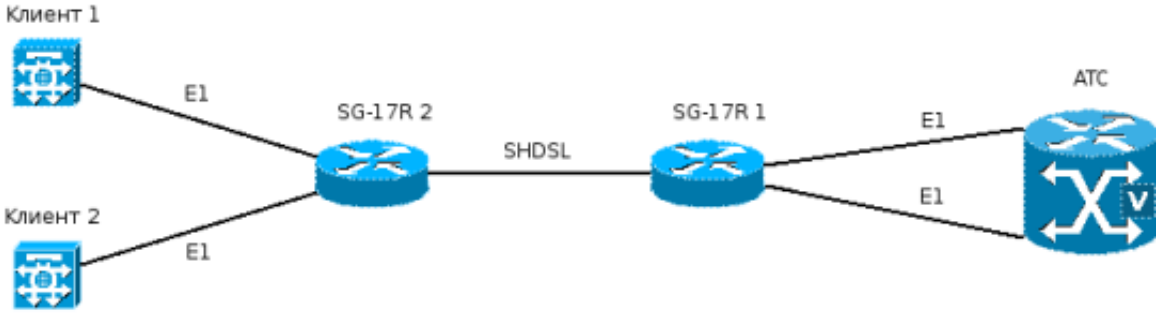
```
Checking status:
Errors detected:

WARNING: Line2: timeslots 45 written but not read
WARNING: Line3: timeslots 55 read but not written
```

Примеры конфигурации

Рассмотрим работу мультиплексирования на примере следующей сети:

Рисунок 9.4. Пример сети



Требуется передать два канала E1 (unframed mode) от АТС к Клиенту 1 и Клиенту 2 по каналу SHDSL.

Т.к. источник сигнала для обоих каналов E1 один — АТС, то не имеет значения, какой из интерфейсов E1 будет тактировать линии мультиплексирования. В нашем распоряжении имеется 16 линий, имеющих по 256 тайм-слотов. Для удобства, мы задействуем две из них — одну для приема трафика, вторую — для передачи.

Схема мультиплексирования будет выглядеть следующим образом:

- Интерфейс E1 `E1_0` получает из физической линии данные и выставляет их на линию 0 (с нулевого тайм-слота). Для передачи в физическую линию данные берутся с линии 1, с нулевого тайм-слота. Так же этот интерфейс является источником синхронизации для данного домена.
- Интерфейс E1 `E1_1` работает так же, как `E1_0`, только выставляет и забирает данные начиная с 32 тайм-слота (и не подает синхросигнал, т.е. работает в режиме *clock slave*).
- Интерфейс SHDSL `dsl0` выставляет данные, полученные из физической линии, на линию 1 (откуда их заберут интерфейсы E1), а данные для передачи в физическую линию берет с линии 0 (куда их выставляют интерфейсы E1). Число тайм-слотов, которые использует интерфейс для мультиплексирования, равно 64 (по 32 с каждого интерфейса E1).

Описанная схема проиллюстрирована ниже:

Рисунок 9.5. Взаимодействие интерфейсов на линии 0

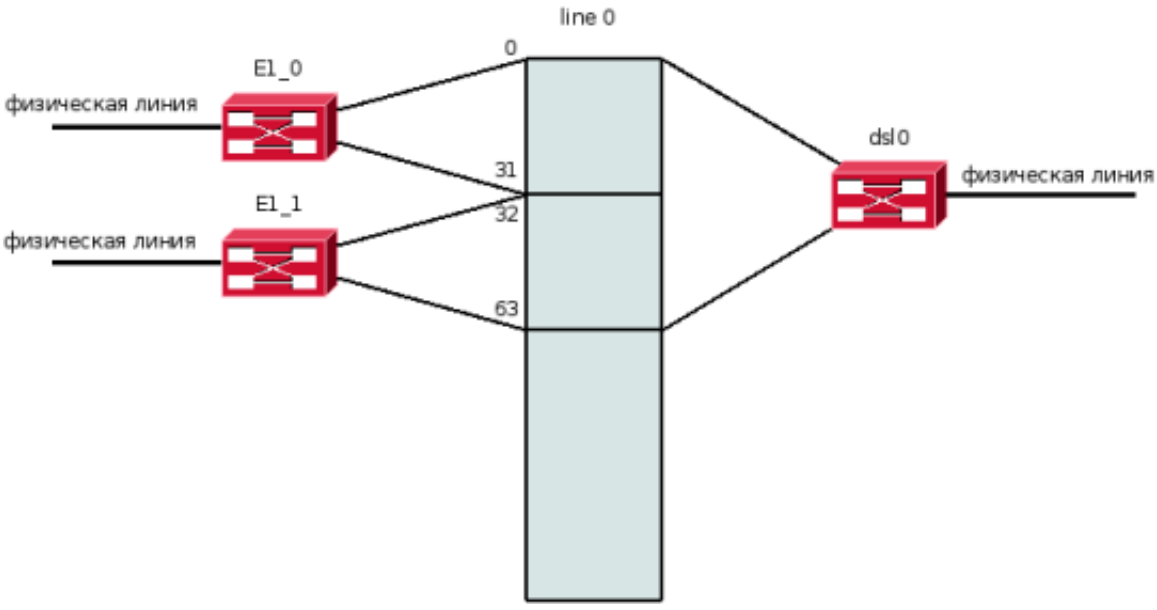
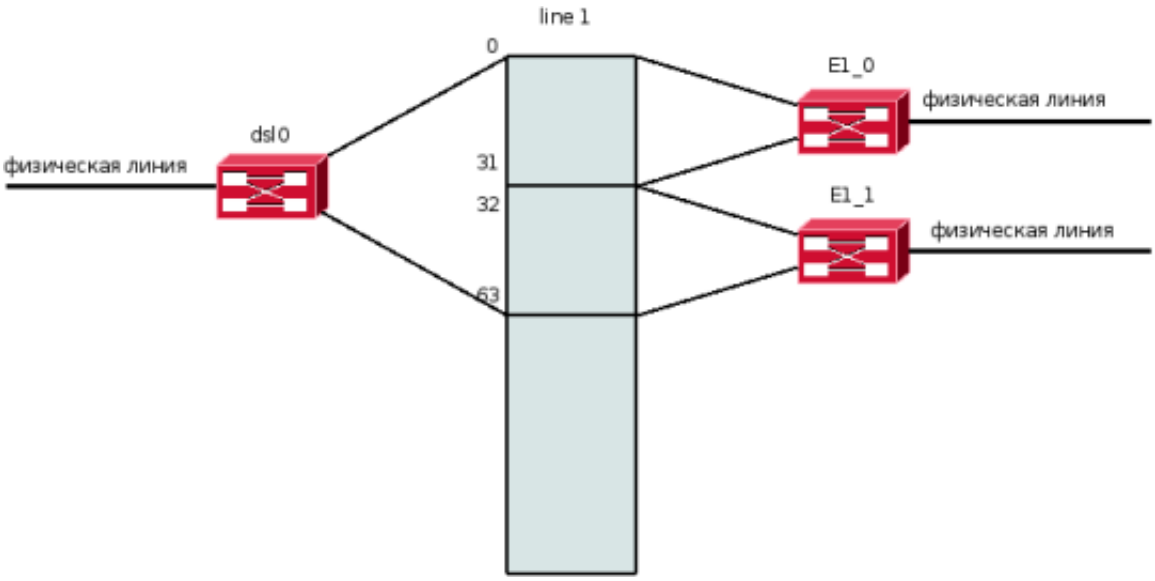


Рисунок 9.6. Взаимодействие интерфейсов на линии 1



Для реализации этой схемы необходимо установить следующие параметры:

- Интерфейс E1 *E1_0*
  - `rline = 0`
  - `rfs = 0`
  - `tline = 1`
  - `tfs = 0`
  - `mxsmap = "0-31"`
  - `clkm = 1`
  - `clkr = 1`
  - `clkab = 0`
- Интерфейс E1 *E1_1*
  - `rline = 0`
  - `rfs = 32`
  - `tline = 1`
  - `tfs = 32`
  - `mxsmap = "0-31"`
  - `clkm = 0`
  - `clkr = 0`
  - `clkab = 0`
- Интерфейс SHDSL *dsl0*
  - `rline = 1`

- *rfs = 0*
- *tline = 0*
- *tfs = 0*
- *mxrate = 64*
- *clkm = 0*
- *clkr = 0*
- *clkab = 0*

Замечание

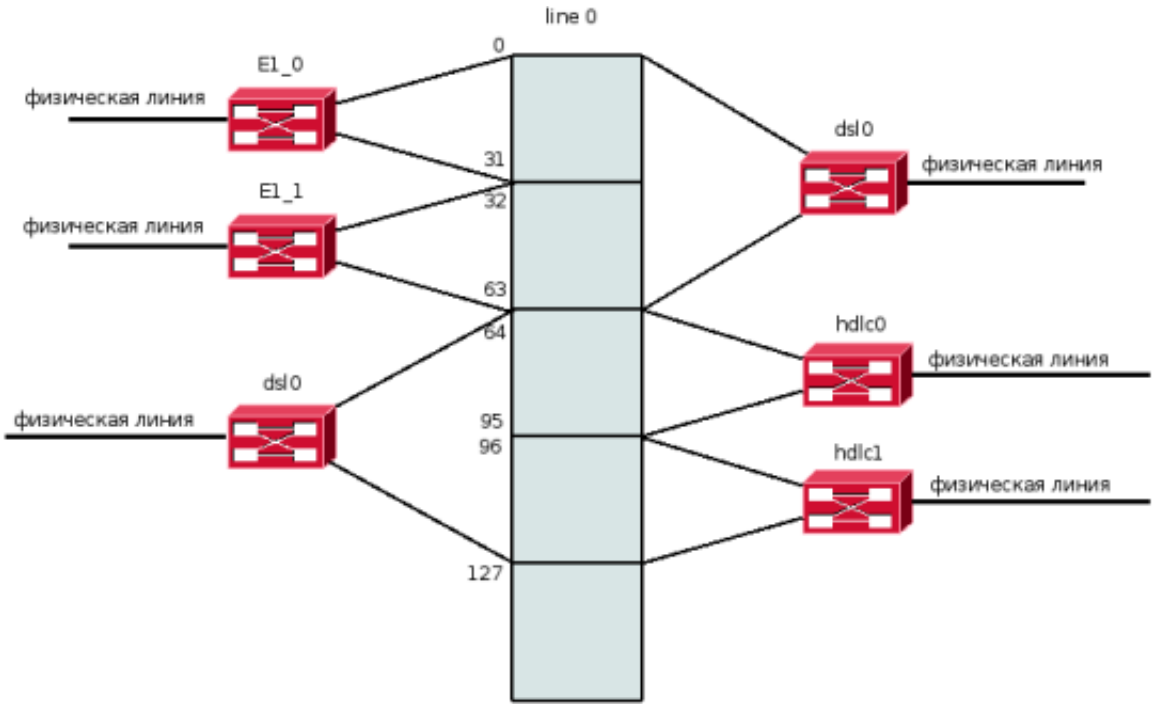
Так же для этих интерфейсов необходимо активировать мультиплексирование — установить параметр *mxen*.

Следуя этой логике, конфигурацию на втором маршрутизаторе можно выполнить аналогичным образом. Единственное отличие, в нашем случае, будет заключаться в изменении интерфейса, являющегося источником синхронизации. Эту функцию будет выполнять интерфейс SHDSL *dsl0*, т.к. именно он получает мультиплексированный поток от первого маршрутизатора, подключенного к АТС.

Подсказка

Вообще, не обязательно для приема и отправки информации использовать разные линии. Для этих целей можно задействовать одну линию, правильно указав тайм-слоты, начиная с которых каждый интерфейс выставляет или забирает данные с линии. Пример такой конфигурации приведен ниже:

Рисунок 9.7. Использование одной линии для выставления и получения данных



Глава 10. VoIP

Основные сведения

Маршрутизатор позволяет организовывать IP-телефонию с помощью модулей MR-17V, которые могут быть укомплектованы портами FXO или FXS. Порты FXO используются для подключения к телефонной сети общего пользования (ТфОП, или PSTN), либо к офисным АТС (PBX). Порты FXS используются для подключения к маршрутизатору телефонных аппаратов.

При работе с VoIP каждый маршрутизатор имеет свой уникальный трёхзначный номер, который используется для обращения к нему со стороны других маршрутизаторов. Так же, каждый канал модуля VoIP (FXO/FXS) имеет двухзначный номер, уникальный для конкретного маршрутизатора, для приёма или совершения звонков.

Таким образом, формат номера, используемый для звонков через маршрутизатор, выглядит следующим образом:

xxx yy [zzz...], где:

- *xxx* — номер маршрутизатора.
- *yy* — номер канала.
- *[zzz...]* — дополнительный номер, например, при звонке через АТС.

Например, если номер маршрутизатора 100, и мы хотим позвонить на его второй порт, то набор номера с телефона, подключённого к этому маршрутизатору либо другому, выглядит следующим образом: 100 02.

Так же, при наборе номера с телефона, подключённого к маршрутизатору, доступны следующие коды:

- Вместо набора номера маршрутизатора можно набрать:
  - * — звоним на собственный маршрутизатор;
  - # — звоним по номеру из адресной книги.
- Вместо набора номера канала можно набрать:
  - * — звоним на первый свободный FXO порт;
  - # — звоним через SIP-сервер (только абонентам, зарегистрированным на SIP-сервере, указанном в настройке. Для звонков абонентам других SIP-серверов — их необходимо добавить в адресную книгу и звонить через неё).

Для звонков на другие маршрутизаторы необходимо получить IP-адрес маршрутизатора по его номеру. Для этих целей используется таблица маршрутизации, которая хранит соответствие между номером маршрутизатора и его IP-адресом. Как правило, содержимое этой таблицы одинаково на всех маршрутизаторах сети.

Чтобы ускорить набор часто набираемых или длинных номеров, используется адресная книга. В неё заносится короткий номер, используемый для быстрого набора (с предварительным набором «#»), и соответствующий ему полный номер.

В демоне IP-телефонии svd реализована поддержка режима Hotline. Смысл его заключается в следующем: при поднятии трубки телефона, подключённого к FXS порту,

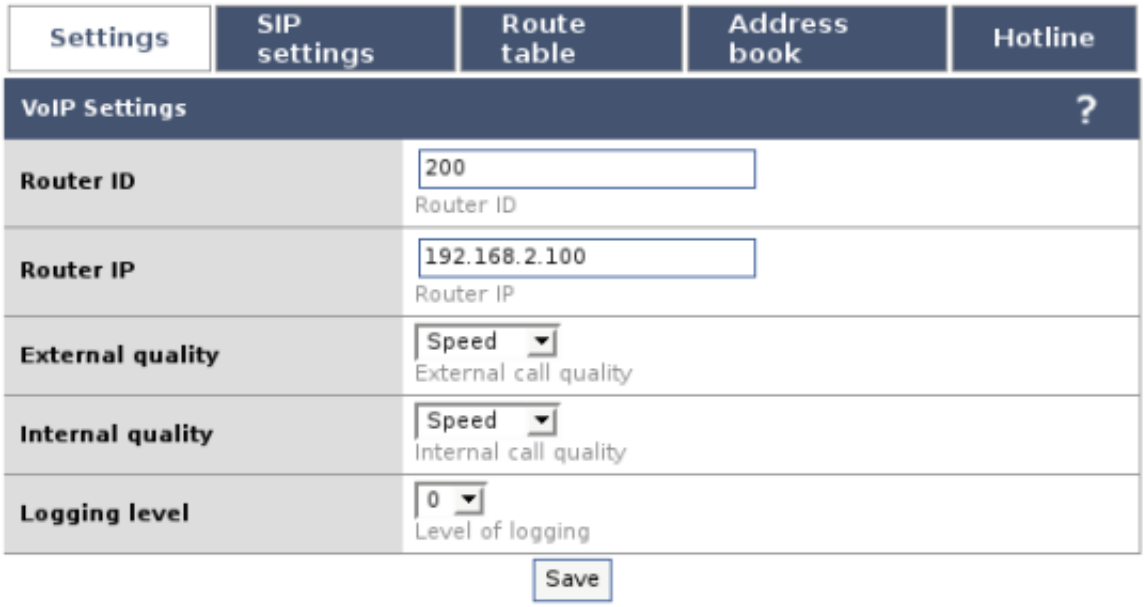
демон может начать автоматический набор записанного номера. При поступлении звонка на порт FXO (подключенный к PSTN или PBX) либо при входящем SIP-звонке, демон может сделать переадресацию вызова на другой порт (отличный от набранного пользователем, совершающего вызов), либо перенаправить звонок на другой маршрутизатор.

При записи полных номеров в таблицы телефонной книги и Hotline допускается использовать специальный символ — «,», означающий секундную задержку при наборе номера.

Настройка основных параметров

Настройка VoIP выполняется на странице System/VoIP, которая состоит из нескольких вкладок, отвечающих за разные аспекты настройки. На вкладке Settings настраиваются основные параметры, её содержимое приведено ниже.

Рисунок 10.1. Основные настройки VoIP



- *Router ID* — уникальный трёхзначный номер маршрутизатора.
- *Router IP* — IP-адрес маршрутизатора, который будет использоваться при звонках.
- *External quality* — качество звонков, совершаемых через SIP-сервер.
- *Internal quality* — качество звонков, совершаемых на другие порты или маршрутизаторы.
- *Logging level* — уровень детализации диагностических сообщений.

Качество звонков имеет три уровня:

- *Speed* — минимальное использование полосы пропускания, низкое качество звонка.
- *Medium* — среднее использование полосы пропускания, среднее качество звонка.
- *Quality* — максимальное использование полосы пропускания, лучшее качество звонка.

Настройки взаимодействия с SIP-сервер

Вкладка SIP settings предназначена для настройки звонков через SIP-прокси, т.е. когда маршрутизатор направляет телефонные звонки через сервер IP-телефонии. Содержимое страницы этой вкладки показано ниже.

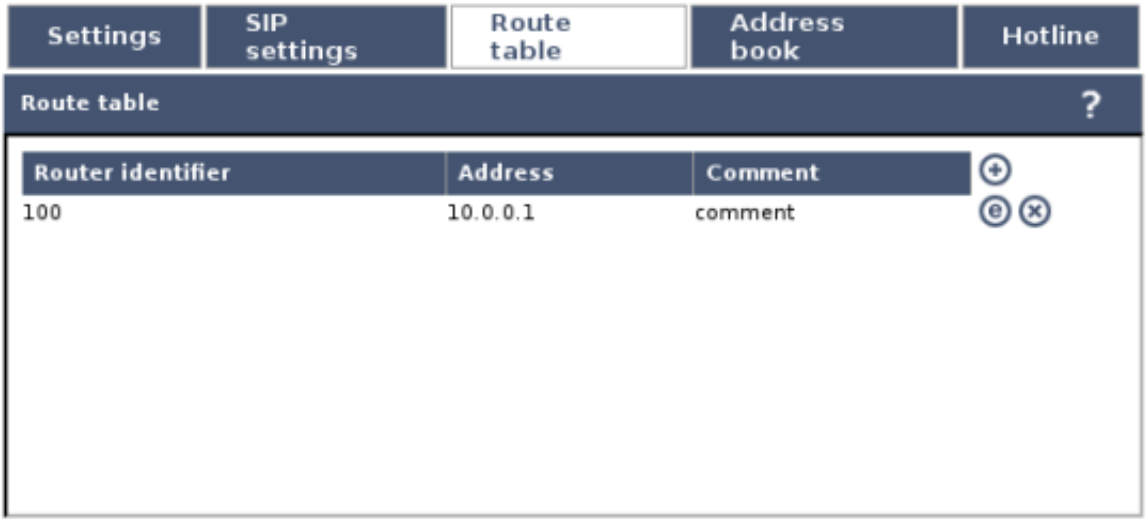
Рисунок 10.2. Настройки взаимодействия с SIP-серверами

- *SIP server* — адрес SIP-прокси, через который будут совершаться вызовы.
- *Username* — имя пользователя на SIP-прокси, которое будет использоваться маршрутизатором.
- *Password* — пароль пользователя на SIP-прокси, который будет использоваться маршрутизатором.

Маршрутизация звонков

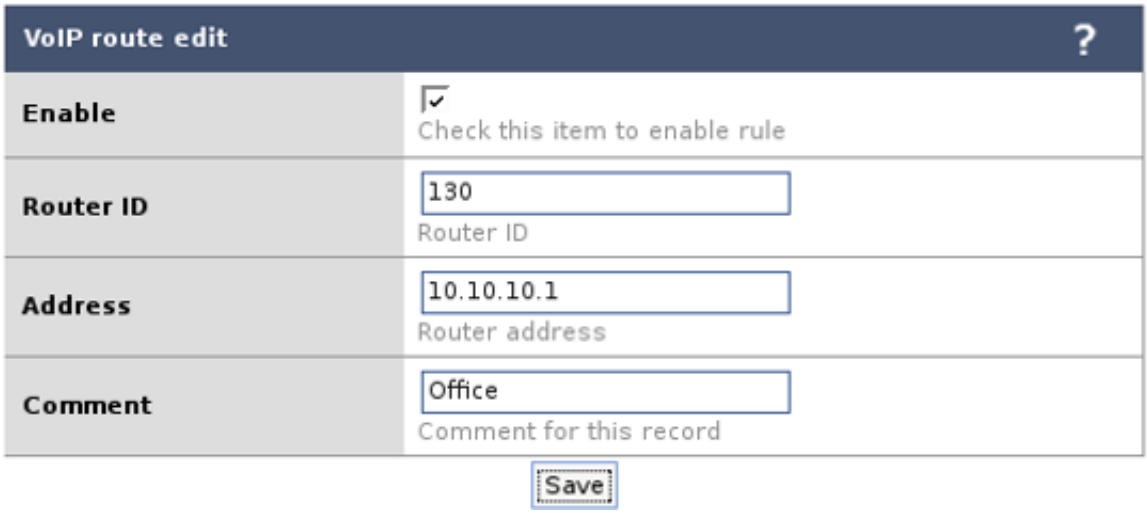
Вкладка Route table используется для управления таблицей маршрутизации VoIP. Она содержит таблицу, отображающую соответствие номеров маршрутизаторов их IP-адресам. Содержимое вкладки представлено ниже.

Рисунок 10.3. Маршрутизация звонков



Добавление новой записи в таблицу показано на рисунке ниже.

Рисунок 10.4. Маршрутизация звонков: добавление новой записи

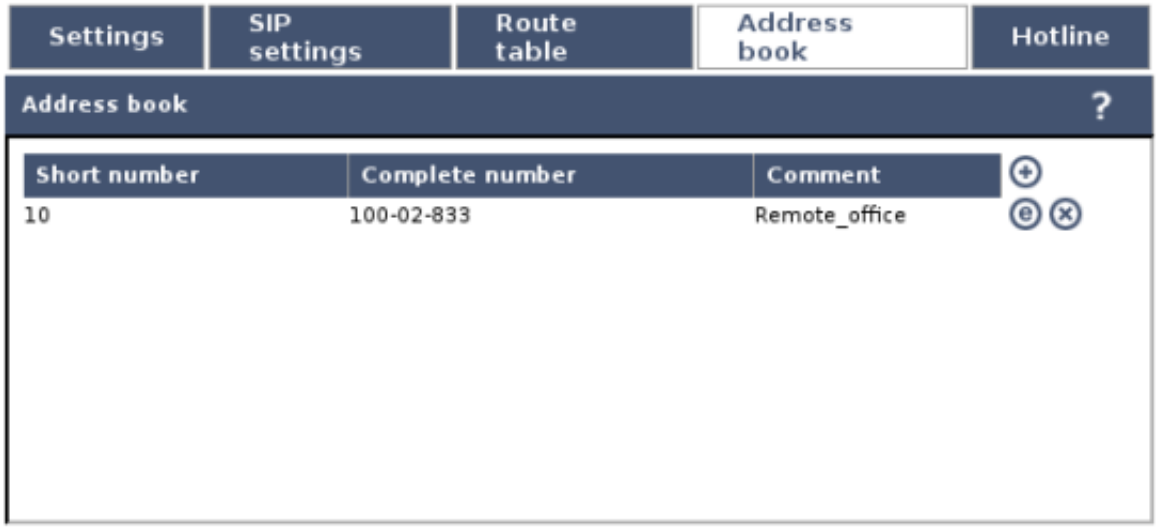


- *Enable* — активна ли запись. Если запись не активна, то она не будет добавлена в конфигурационный файл.
- *Router ID* — номер маршрутизатора, для которого добавляется соответствие.
- *Address* — адрес маршрутизатора.
- *Comment* — комментарий для записи.

Адресная книга

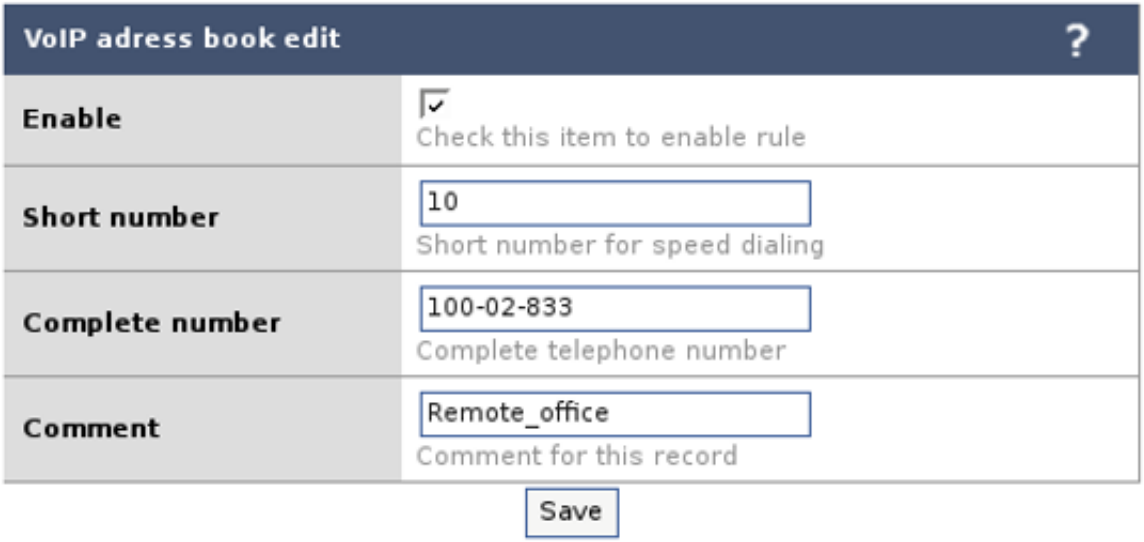
Вкладка Address book содержит адресную книгу, которая используется для быстрого набора телефонных номеров. К примеру, для номера 100 02 833 можно задать короткий номер 10, и для набора использовать номер #10. Содержимое вкладки показано ниже.

Рисунок 10.5. Адресная книга



Добавление новой записи в таблицу показано ниже.

Рисунок 10.6. Адресная книга: добавление новой записи

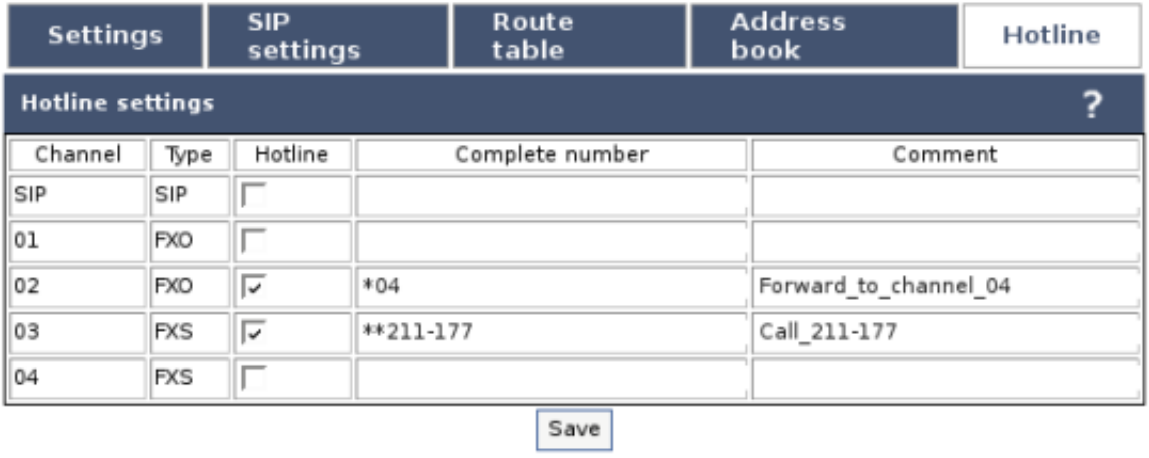


- *Enable* — активна ли запись. Если запись не активна, то она не будет добавлена в конфигурационный файл.
- *Short number* — короткий номер.
- *Complete number* — полный номер, вызываемый при наборе «#короткий_номер». Здесь так же может быть указан SIP-номер в виде user@sipserver.domen, с указанием префикса, что это SIP-номер.
- *Comment* — комментарий для записи.

Режим Hotline

Вкладка Hotline отвечает за настройку соответствующего режима работы VoIP. Т.к. настройки Hotline привязываются к конкретным каналам модуля и особенности работы зависят от типа канала (FXO/FXS), то в таблице выводятся доступные каналы и их типы. Содержимое вкладки показано ниже.

Рисунок 10.7. Таблица настройки Hotline



На маршрутизаторе имеется 3 типа канала для режима Hotline, и, соответственно, 3 способа реагирования:

- *SIP* — переадресация вызова на другой канал или маршрутизатор при входящем SIP-звонке.
- *FXO* — переадресация вызова на другой канал или маршрутизатор при входящем звонке на канал FXO (подключаемый к PSTN или PBX).
- *FXS* — набор номера маршрутизатором при поднятии трубки на телефоне, подключённом к каналу FXS.

Рассмотрим параметры, отвечающие за настройку режима Hotline:

- *Channel* — номер канала.
- *Type* — тип канала.
- *Hotline* — при установленном флажке переводит канал в режим Hotline.
- *Complete number* — полный номер, набираемый маршрутизатором при обнаружении отслеживаемого события (поднятия трубки или входящем вызове).
- *Comment* — комментарий.

Глава 11. SNMP

Введение в SNMP

SNMP — Simple Network Management Protocol — простой протокол управления сетями. Протокол позволяет производить мониторинг сетевых устройств (маршрутизаторов, мультиплексоров, мостов и др.) и сервисов (веб-серверов, почтовых серверов, серверов DNS) и управлять их конфигурацией.

Управление и мониторинг осуществляется по схеме агент-менеджер. Агент — ПО, работающее на сетевом устройстве, которое подлежит мониторингу или управлению, менеджер — ПО, собирающее информацию с агентов для мониторинга либо управления. Взаимодействие, как правило, осуществляется с помощью транспортного протокола UDP, порт 161. Так же возможно использование протокола TCP.

Объекты, над которыми можно выполнять операции (чтения или записи) адресуются по уникальным номерам. Например, 1.3.6.1.2.1.1.1 соответствует объекту SysDescr — описанию системы, который может иметь следующее значение: *STRING Linux sigrand 2.6.16 #1 Tue Nov 7 21:37:48 NOVT 2007 mips*.

MIB — Management Information Base — база данных информации управления. MIB описывает объекты и какие операции над ними можно выполнять. Если объект входит в состав MIB, то к нему можно обращаться по имени, а не по числовому индексу.

Аутентификация производится на основе "сообщества" — каждый агент относится к тому или иному сообществу. При получении команды производится проверка, принадлежит ли он к сообществу, указанному в команде. Если да — команда будет принята и обработана, иначе — проигнорирована. Сообщество представляет из себя простую строку, по-умолчанию используется два сообщества — public для просмотра объектов, private — для их изменения.

Уровень поддержки SNMP маршрутизатором

Для поддержки протокола SNMP на маршрутизаторе используется свободный программный пакет *net-snmp*, поддерживающий все актуальные версии протокола SNMP, в состав которого входит демон *snmpd*, выполняющий функции агента.

Маршрутизатором поддерживается *MIB-2*, предоставляющий общую информацию о системе (информацию о сетевых интерфейсах, таблицы маршрутизации, системную информацию), а так же *HDSL2-SHDSL-LINE-MIB*, содержащий объекты, используемые для мониторинга и управления каналами SHDSL.

MIB-2 является стандартной MIB и входит в состав большинства менеджеров, в то время как HDSL2-SHDSL-LINE-MIB является специфичным для определённого типа устройств. Загрузить этот файл можно либо из источников в Интернете, либо по ссылке [http://sigrand.ru/temp/HDSL2-SHDSL-LINE-MIB-rfc4319.txt].

На данный момент по SNMP доступен только мониторинг маршрутизатора и SHDSL каналов и регенераторов, возможность управления будет добавлена в ближайшее время.

Настройка SNMPD

Настройка демона *snmpd* хранится в файле */etc/snmp/snmpd.conf* и заключается в установлении прав доступа на получение и изменение объектов.

Содержимое конфигурационного файла имеет следующий вид:

```
com2sec  ro  default    public
com2sec  rw  localhost  private

group  public   v1   ro
group  public   v2c  ro
group  public   usm  ro
group  private  v1   rw
group  private  v2c  rw
group  private  usm  rw

view  all  included  .1

access  public   ""  any  noauth  exact  all  none  none
access  private  ""  any  noauth  exact  all  all   all
```

Директива *com2sec* устанавливает соответствие между сообществом и именем безопасности, а так же устаналивает адреса, которые могут относится к этим сообществам. В приведенном выше конфигурационном файле первая директива определяет, что сообщество public соответствует безопасности ro, и ему соответствуют любые IP-адреса. Вторая директива определяет соответствие сообществу private безопасности rw, и ограничивают доступ только самим маршрутизатором.

Директива *group* определяет, к какой группе какая безопасность относится. В нашем примере, к группе public относится безопасность ro, а к группе private — безопасность rw. v1, v2c, usm определяют модель безопасности. v1 относится к протоколу SNMP первой версии, v2c — ко второй, usm — SNMPv3.

Директива *view* определяет имя области видимости, и что в неё входит. В нашем случае имя области видимости — all, и в неё входит всё дерево MIB.

Последняя директива *access* определяет права доступа различных групп. В нашем примере обеим группам разрешён доступ без аутентификации, но группе public — только для чтения, а группе private — для чтения и записи.

Более подробную информацию вы можете найти на сайте проекта net-snmp, в частности по ссылке [http://net-snmp.sourceforge.net/wiki/index.php/Vacm].

Взаимодействие SNMPD с EOCD

SNMPD получает информацию о состоянии SHDSL-канала от демона *EOCD*. Таким образом, чтобы иметь возможность получать информацию о состоянии SHDSL-канала через SNMP, необходимо сконфигурировать демон EOCD. После того, как информация будет доступна через утилиту **eoc-info** — информацию можно будет получить через SNMP. Подробнее о назначении и настройки демона EOCD можно прочитать в разделе Мониторинг SHDSL каналов.

Пример использования

В качестве примера рассмотрим мониторинг SHDSL-канала маршрутизатора. Для этого получим информацию о числе регенераторов, затухании сигнала и соотношении сигнал/шум.

Числовое имя объекта, соответствующего числу регенераторов, обнаруженных на линии (Hdsl2ShdslStatusNumAvailRepeaters) равно 1.1.3.6.1.2.1.10.48.1.2.1.1.

Для затухания сигнала (Hdsl2ShdslEndpointCurrAtn) это имя равно 1.1.3.6.1.2.1.10.48.1.5.1.1.11.1.2.1 для клиентской стороны (слейва) и 1.3.6.1.2.1.10.48.1.5.1.1.11.2.1.1 для мастера, а для соотношения сигнал/шум (Hdsl2ShdslEndpointCurrSnrMgn) — 1.3.6.1.2.1.10.48.1.5.1.2.11.1.2.1 и 1.3.6.1.2.1.10.48.1.5.1.2.11.2.1.1 соответственно. Значения этих параметров приведены ниже:

```
1.3.6.1.2.1.10.48.1.2.1.1.11 = Gauge32 0
1.3.6.1.2.1.10.48.1.5.1.1.11.1.2.1 = INTEGER 0
1.3.6.1.2.1.10.48.1.5.1.1.11.2.1.1 = INTEGER 0
1.3.6.1.2.1.10.48.1.5.1.2.11.1.2.1 = INTEGER 19
1.3.6.1.2.1.10.48.1.5.1.2.11.2.1.1 = INTEGER 17
```

Т.е. число регенераторов равно 0, затухание сигнала на обоих сторонах соединения — 0 dB, соотношение сигнал/шум на клиентской стороне 19 dB, на стороне мастера — 17 dB.

При использовании специализированного ПО, поддерживающего загрузку MIB-ов, возможно получение информации в более удобной форме.

Поддерживаемое ПО для управления по SNMP

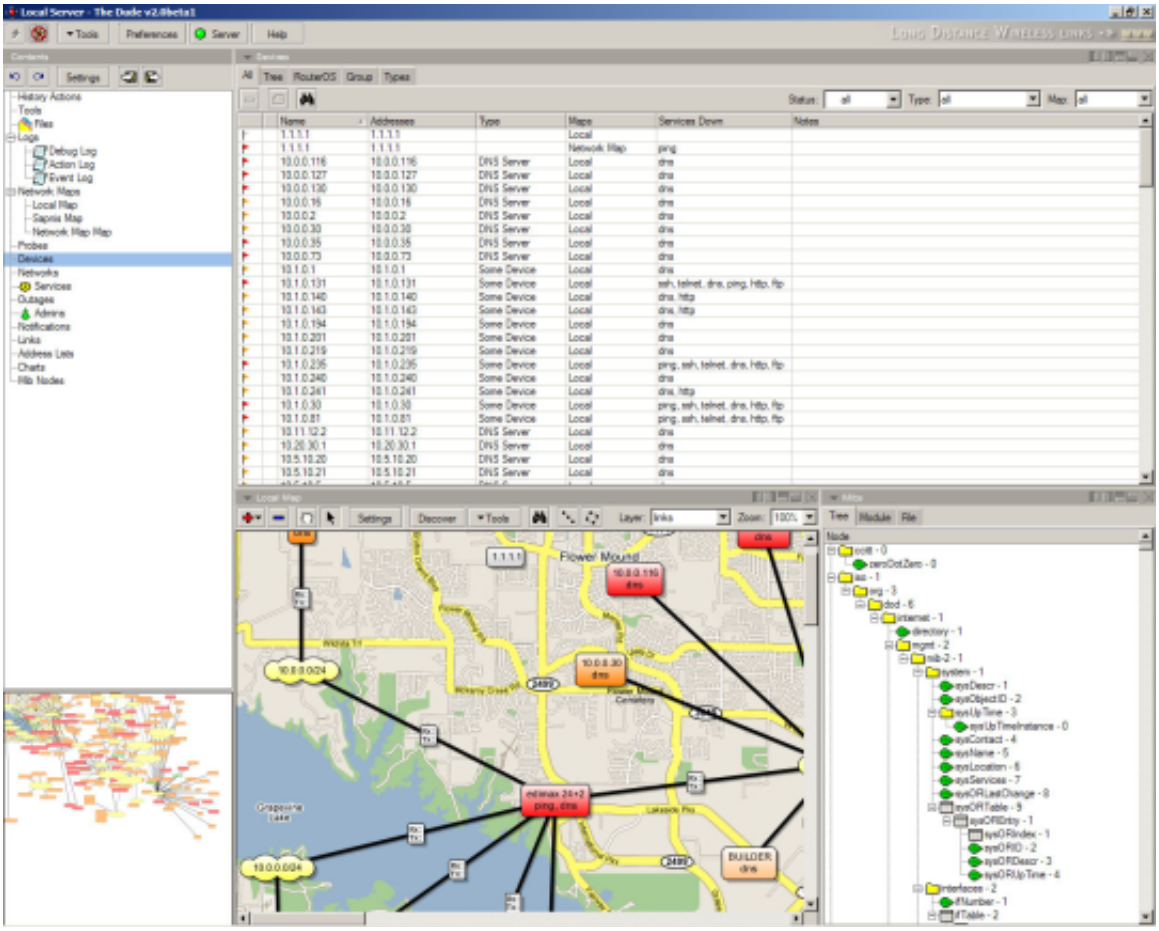
Для реализации поддержки протокола SNMP используется свободный программный пакет *net-snmp*, что позволяет работать со всеми программными продуктами, совместимыми с net-snmp.

Дополнительно был проведён краткий обзор доступного программного обеспечения, результаты которого представлены ниже.

The Dude

The Dude — бесплатный программный продукт для работы по протоколу SNMP, работает под ОС MS Windows.

Рисунок 11.1. The Dude



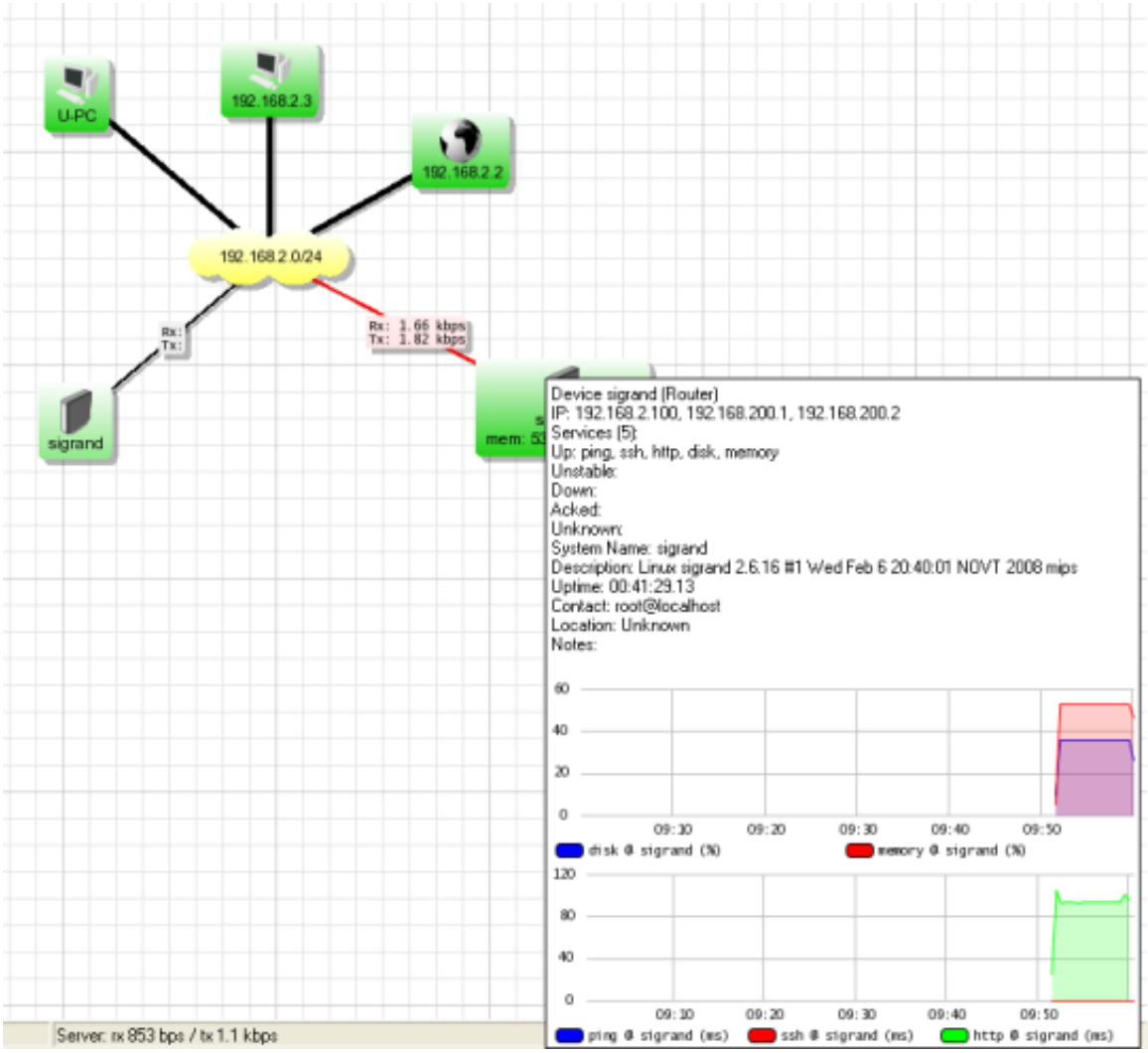
Достоинства:

- Автоматически определяет устройства сети.
- Рисует карту сети, позволяет добавлять на карту новые устройства, выводить на карту значения SNMP-переменных.
- Выполняет мониторинг устройств, построение графиков в режиме реального времени.
- Имеет несколько удобных встроенных утилит для сетевого администрирования и мониторинга (терминалы, snmpwalk).
- Удобные режимы просмотра SNMP информации (список, дерево, таблица).

Недостатки:

- Неправильно отображаются индексы интерфейсов в табличном представлении.
- Возможно некорректное отображение SnmpAdminString для имён SHDSL профилей.

Рисунок 11.2. The Dude: маршрутизаторы Sigrand

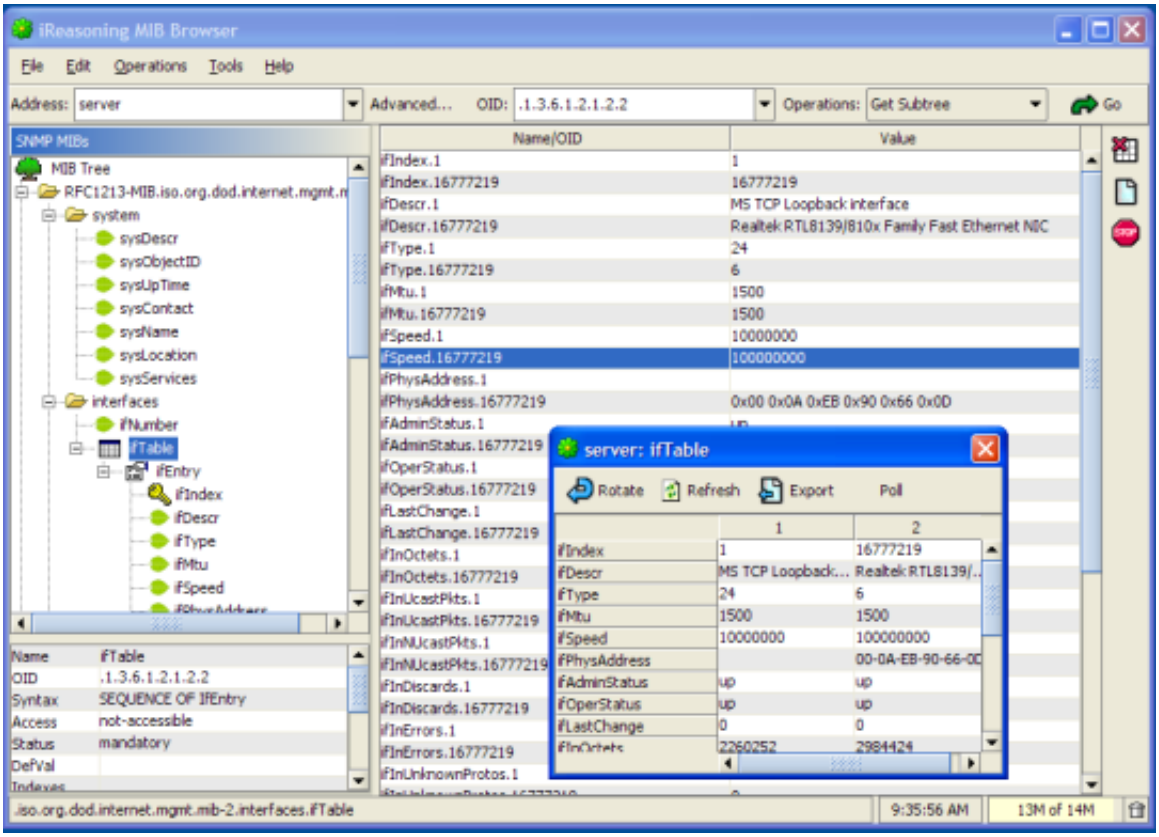


Домашняя страница проекта: The Dude [http://www.mikrotik.com/thedude.php].

MIB Browser

MIB Browser, разработка компании iReasoning, доступна в платной и бесплатной версии, различающихся лицензиями и функциональностью. Заявлена поддержка платформ Windows, Mac OS X и Linux.

Рисунок 11.3. MIB Browser



Достоинства:

- Удобный интерфейс.
- Табличный просмотр SNMP таблиц.

Недостатки:

- Бесплатная версия не поддерживает SNMPv3, позволяет загружать дополнительно к имеющимся не более 5 MIB.
- Возможно некорректное отображение SnmpAdminString для имён SHDSL профилей.

Домашняя страница проекта: MIB Browser [http://www.ireasoning.com/mibbrowser.shtml].

OpenNMS

OpenNMS — веб-приложение, написано на языке Java, использует для работы СУБД PostreSQL и Apache Tomcat, позволяет вести мониторинг промышленных сетей. Является свободным программным обеспечением (бесплатным), доступно для платформ, на которых работает Apache Tomcat (как правило, это Linux сервера).

Рисунок 11.4. OpenNMS

Достоинства:

- Судя по всему, OpenNMS использует *net-snmp* для работы по протоколу SNMP, что даёт полную совместимость с оборудованием *Sigrand*.

Домашняя страница проекта: OpenNMS [http://www.opennms.org/index.php/Main_Page].

Глава 12. Примеры конфигурации

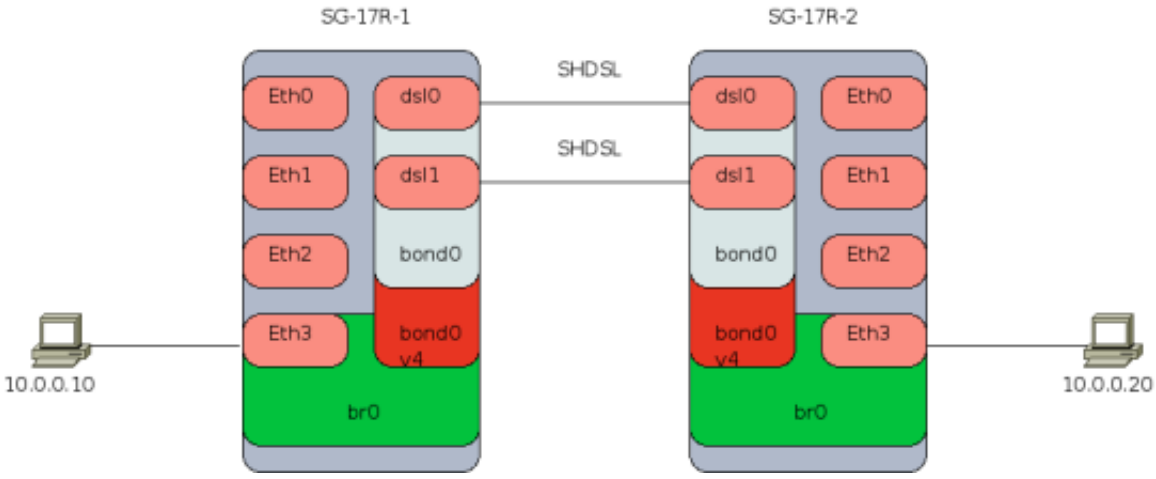
VLAN

Организация независимых каналов между Ethernet-интерфейсами

Данный пример рассматривает организацию независимых каналов между Ethernet-портами устройств, соединённых через SHDSL (функциональность 1 и 2).

Рассмотрим организацию передачи данных с порта eth3 одного устройства на порт eth3 другого устройства через соединения SHDSL. При необходимости, можно задействовать все порты устройств (eth0, eth1, eth2). Схему взаимодействия между устройствами можно изобразить следующим образом:

Рисунок 12.1. Схема взаимодействия устройств



Устройства соединены двумя каналами SHDSL, которые объединены в бондинг. Поверх этого бондинга создан VLAN с VLAN ID равным 4. Бридж реализует передачу пакетов между интерфейсами bond0v4 (интерфейс VLAN) и eth3.

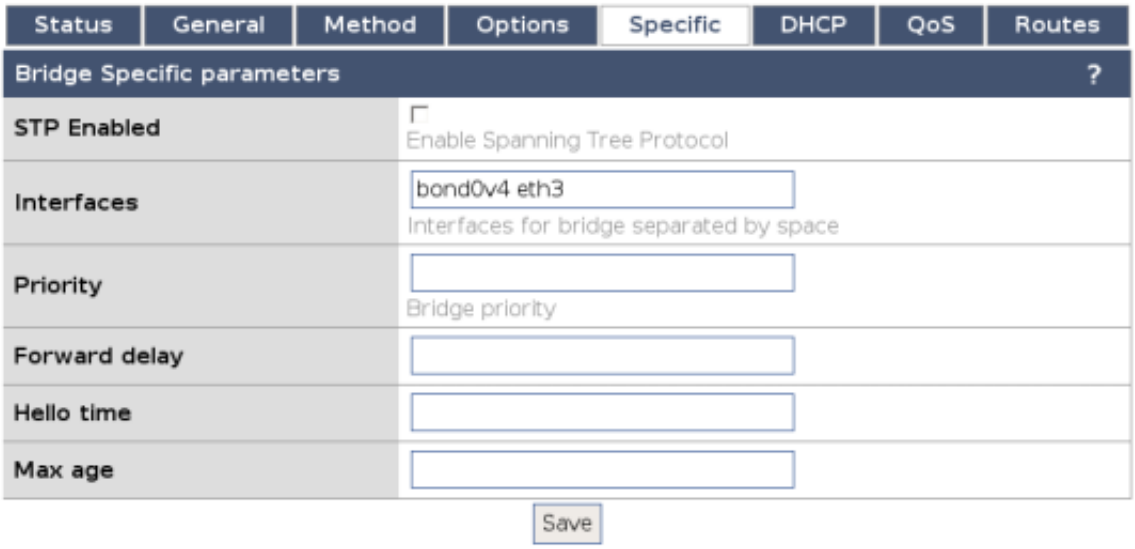
Настройка начинается с настройки физического соединения между маршрутизаторами (см. настройку SHDSL).

Затем создадим бондинг из интерфейсов dsl0 и dsl1 (см. настройку Bonding). В результате у нас будет интерфейс *bond0*.

Далее, нам необходимо создать VLAN поверх бондинга. Число интерфейсов VLAN зависит от того, между сколькими портами ethernet мы будем организовывать независимую передачу данных — по одному VLAN на каждый порт. Детально процедура настройки интерфейса VLAN рассмотрена в соответствующем разделе. Т.е. нам надо создать VLAN интерфейс поверх интерфейса bond0 с номером VLAN ID равным 4. В итоге мы получим интерфейс *bond0v4*.

Заключительным этапом является создание моста (см. настройка моста). Мост состоит из интерфейсов *bond0v4* и *eth3*, между которыми осуществляется передача трафика. Число интерфейсов моста так же зависит от числа портов, между которыми организуется обмен трафиком — на каждый порт один мост. Ниже приведена вкладка Specific страницы настройки интерфейса моста.

Рисунок 12.2. Вкладка Specific интерфейса моста (br*)



Таким образом, если мы хотим организовать передачу между портами eth2, мы должны создать ещё один VLAN поверх интерфейса *bond0*, к примеру с VLAN ID 3, создать ещё один интерфейс моста, и добавить в него интерфейсы *bond0v3* и *eth2*.

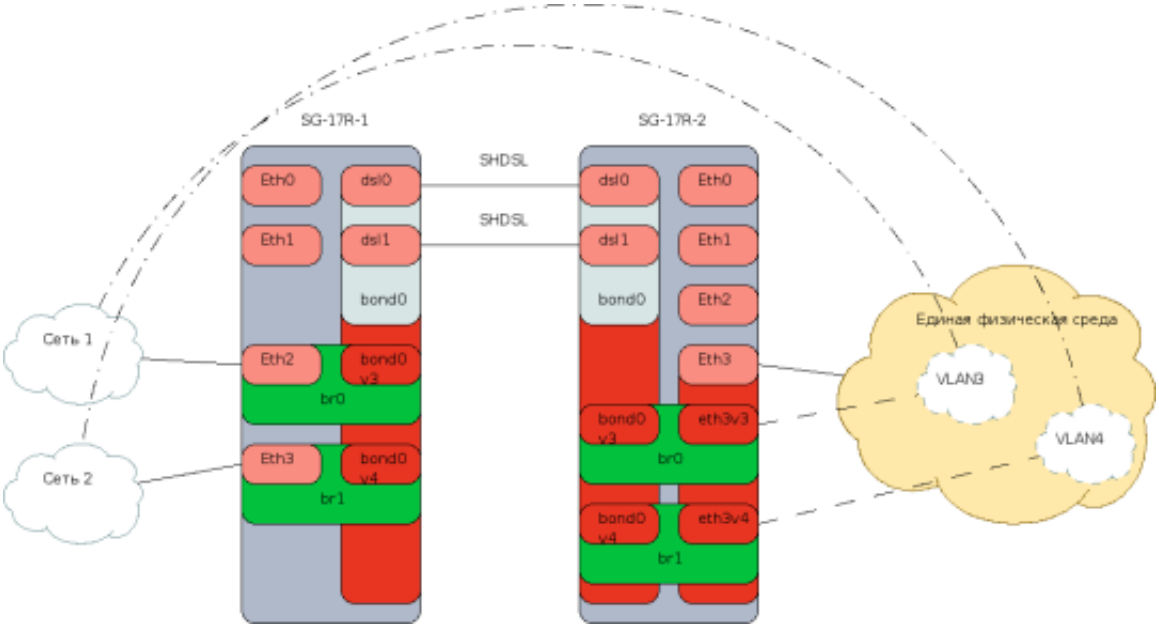
Замечание

Если необходимо организовать управление устройством по порту, который участвует в передачи данных (добавлен в мост), то его IP-адрес (по которому производится настройка) необходимо назначить интерфейсу моста, в который входит данный порт. Более подробно это описывается в соответствующей главе.

Распределение трафика по Ethernet-портам в зависимости от VLAN ID

Допустим, мы хотим организовать передачу VLAN-трафика, поступающего на trunk-порт одного устройства через SHDSL-канал, а на втором устройстве, в зависимости от номера VLAN ID, передавать трафик (со снятым тегом VLAN) на соответствующий ethernet-порт. Это т.н. "функциональность 3".

Рисунок 12.3. Структурная схема



Идея построения схемы заключается в том, что на устройстве SG2, один из ethernet-портов которого выступает в роли trunk-порта, создаются интерфейсы VLAN, трафик которых надо передать на соответствующие порты другого устройства.

К примеру, к устройству SG2 (например, к четвёртому ethernet-порту) подключена сеть, в которой работает несколько сетей VLAN с номерами 3 и 4. Нам необходимо соединить сеть с VLAN ID 3 с сетью, подключённой к третьему ethernet-порту устройства SG1. Так же необходимо соединить сеть с VLAN ID 4 с сетью, подключённой к четвёртому ethernet-порту устройства SG1. Следует заметить, что сети, подключённые к SG2 являются обычными LAN сетями, поэтому передаваемый туда трафик должен идти без заголовков VLAN.

Настройка данной схемы разбивается на два этапа: настройка SG1 и настройка SG2. Подразумевается, что физическое соединение между устройствами (например, по SHDSL) уже настроено. В нашем примере мы используем бондинг поверх каналов SHDSL.

Настройка SG1

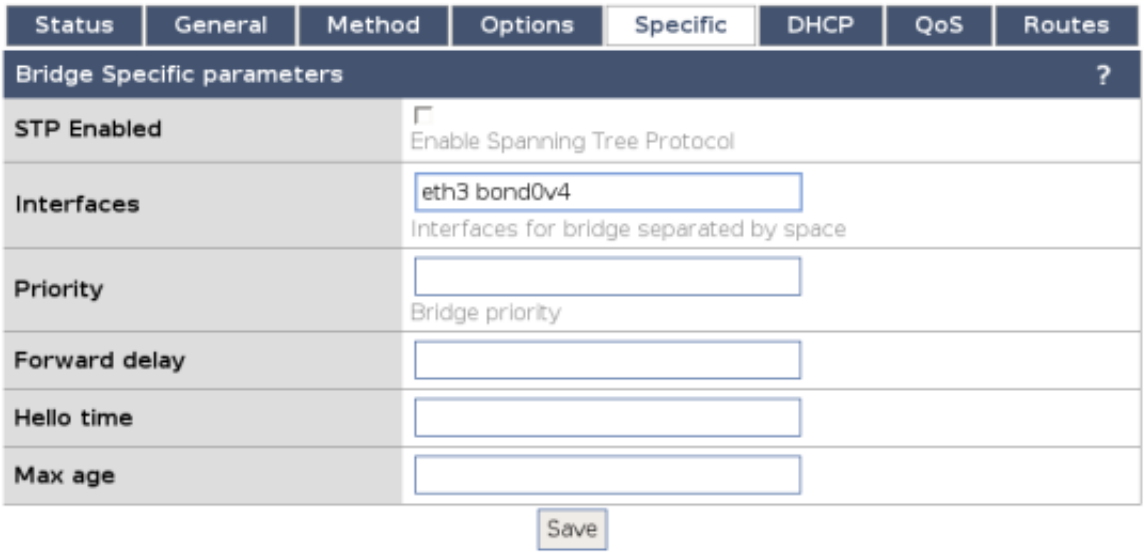
В общем, настройка заключается в создании интерфейсов VLAN поверх интерфейса бондинга и создании моста между соответствующим интерфейсом ethernet и интерфейсом VLAN. Рассмотрим это более детально.

Создадим на основе интерфейса *bond0* интерфейс VLAN с VLAN ID *4* (см. настройка VLAN). Созданный интерфейс имеет имя *bond0v4*. Здесь же создадим интерфейс моста, к примеру, его имя будет *br0*.

Настроим интерфейсы, которые войдут в состав моста: *bond0v4* и *eth3*. Настройка заключается в активации флажка Enabled на вкладке General страницы настройки интерфейса.

Перейдём на страницу настройки моста, вкладку Specific. Укажем интерфейсы, между которыми будет передаваться трафик: *bond0v4* и *eth3*.

Рисунок 12.4. Привязка к физическим интерфейсам



На вкладке General активируем флажки Enabled и Auto.

Если необходимо организовать передачу нескольких VLAN на порты SG1, то приведённая последовательность действий повторяется для каждой VLAN. В данной конфигурации максимальное число VLAN равно 4, оно ограничено числом ethernet-портов устройства.

Настройка SG2

Перед настройкой нам необходимо решить, какой из ethernet-портов устройства будет выполнять функции trunk-порта, т.е. к которому будут подключены сети VLAN.

Для выбранного trunk-порта создаются интерфейс VLAN, и соответствующий ему интерфейс VLAN на основе интерфейса бондинга. Затем создаётся мост между соответствующим интерфейсом VLAN trunk-порта и интерфейсом VLAN бондинга. Идея заключается в том, что каждый интерфейс VLAN, созданный поверх trunk-порта, получает свой трафик и передаёт его "своему" интерфейсу бондинга. На втором устройстве (SG1) бондинг передаёт его соответствующему ethernet-порту. Рассмотрим эти действия подробнее.

Настройка начинается с создания интерфейсов VLAN с одинаковыми VLAN ID на интерфейсах бондинга (к примеру, *bond0*) и ethernet-порта, выбранного в роли trunk-порта (*eth3*). Пусть созданные интерфейсы имеют имена *bond0v4* и *eth3v4*. Здесь же создадим интерфейсы моста, по одному на каждую пару интерфейсов VLAN.

Настроим интерфейсы, входящие в состав моста. Для этого выставим флажки Enabled на вкладке General для интерфейсов *eth3* (т.к. это trunk-порт), *bond0v4* и *eth3v4*.

Перейдём к настройке интерфейса моста: откроем вкладку Specific и укажем, из каких интерфейсов будет состоять мост, в нашем примере это интерфейсы *bond0v4* и *eth3v4*.

На вкладке General активируем флажки Enabled и Auto. Таким образом, мы получаем один или несколько интерфейсов моста, передающих трафик между интерфейсами VLAN, созданными поверх trunk-порта и поверх бондинга.

Ограничение доступа к управлению устройством с помощью VLAN

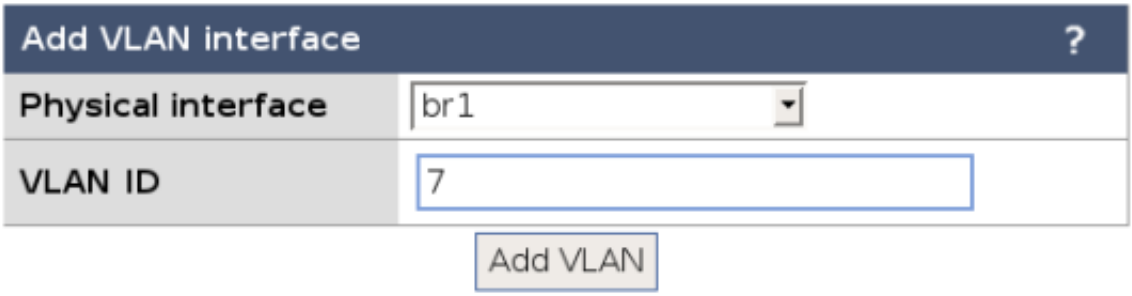
Для ограничения доступа к управлению устройством можно использовать технологию VLAN. Для этого на основе интерфейса, через который осуществляется управление, создаётся интерфейс VLAN, которому назначается IP-адрес, а адрес с нижележащего интерфейса снимается.

Рассмотрим ограничение доступа по VLAN на том же примере организации независимых каналов между Ethernet-интерфейсами.

Предположим, что мы управляем устройством через порт eth0 используя IP-адрес 192.168.2.100. Нам требуется использовать порт eth0 для передачи данных, как было рассмотрено в приведённом выше примере, и организовать управление устройством с компьютера, относящемуся к определённой сети VLAN.

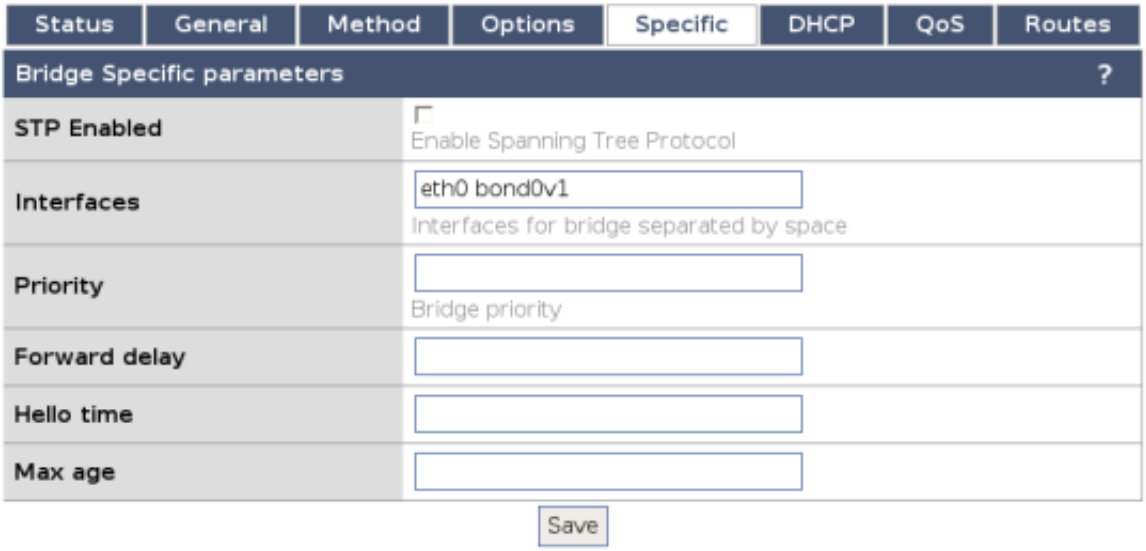
Выполним часть последовательности действий, описанных в приведённом выше разделе, а именно: настроим физическое соединение, создадим бондинг и необходимый VLAN поверх него (*bond0v1*). Теперь нам необходимо создать мост. Перейдём на страницу управления динамическими интерфейсами (Network/Interfaces) и создадим интерфейс моста, пусть у него будет имя *br1*. Тут же создадим на основе нового интерфейса моста *br1* VLAN с нужным нам VLAN ID, пусть имя нового интерфейса будет *br1v7*.

Рисунок 12.5. Создание интерфейса VLAN на основе моста



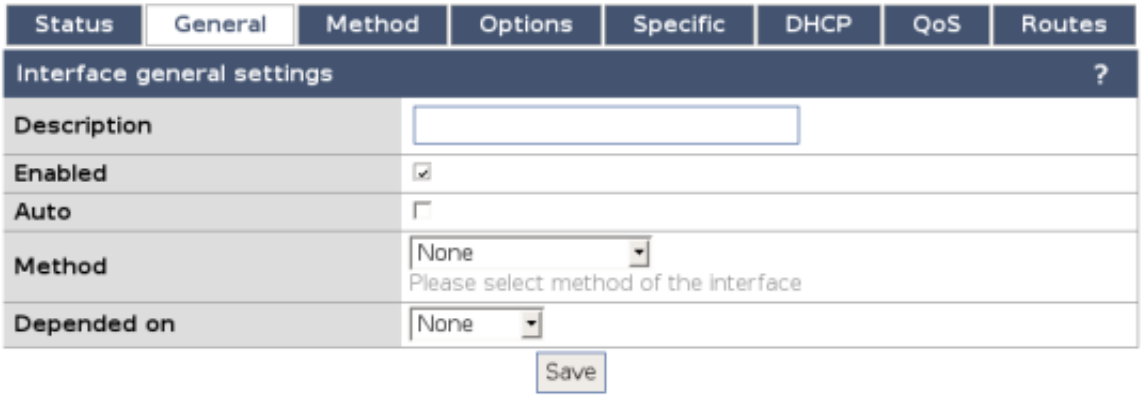
Перейдём на страницу настройки интерфейса моста *br1*, выберем вкладку Specific и пропишем нужные нам интерфейсы: eth0 и bond0v1.

Рисунок 12.6. Добавление интерфейсов в мост



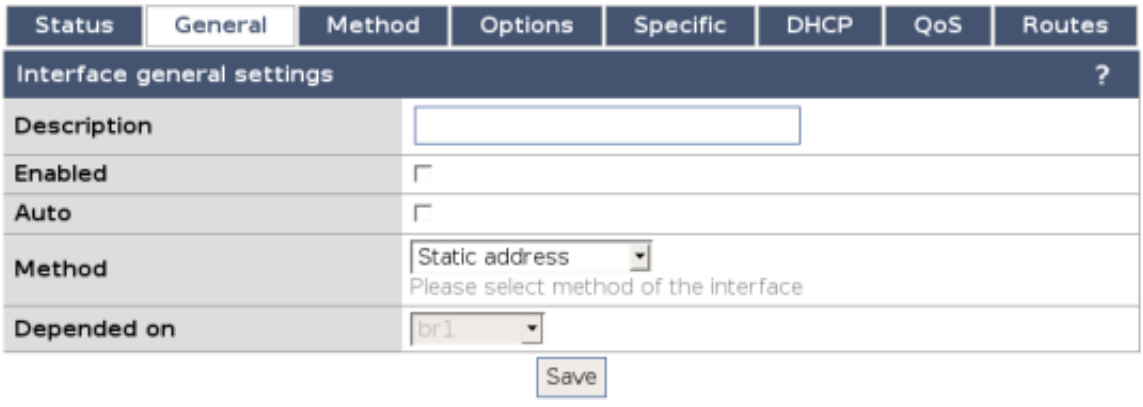
Затем перейдём на вкладку General и активируем интерфейс — поставим флажок Enabled (Auto выставлять не надо — это заблокирует доступ к устройству).

Рисунок 12.7. Активация интерфейса моста



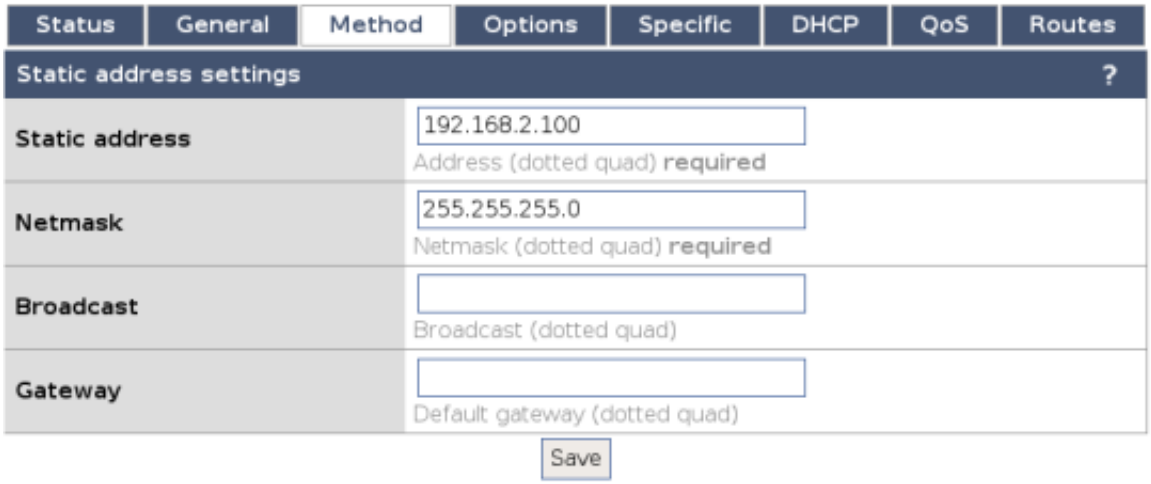
Теперь перейдём к настройке интерфейса VLAN, созданного на основе сконфигурированного интерфейса моста. Для этого перейдём на его страницу настройки и выберем вкладку General, на которой выберем статический (Static) способ установки IP-адреса.

Рисунок 12.8. Установка метода назначения IP-адреса



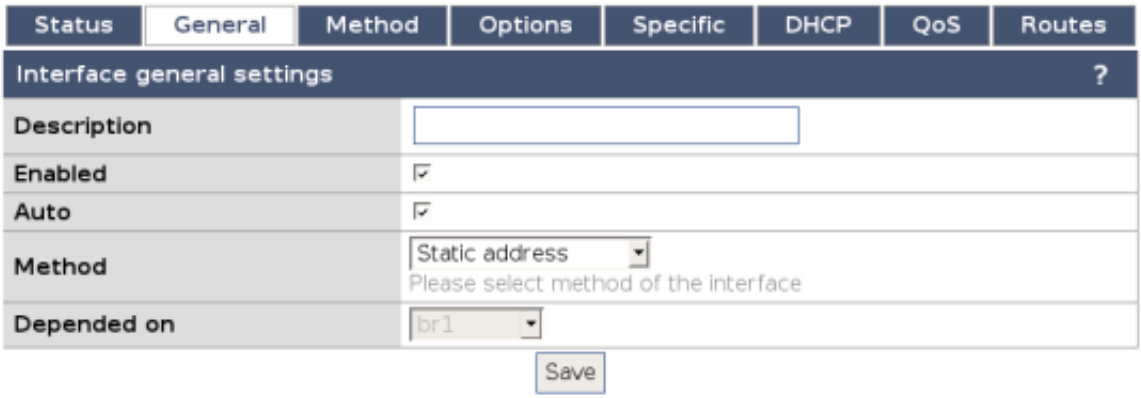
Перейдём на вкладку Method, где пропишем нужный IP-адрес и маску сети.

Рисунок 12.9. Назначение IP-адреса



И в завершении вернёмся на вкладку General и активируем флажки Enabled и Auto.

Рисунок 12.10. Запуск интерфейса VLAN



Запуск интерфейса VLAN приведёт к запуску интерфейса моста, в итоге с интерфейса *eth0* будет снят IP-адрес, а на интерфейс VLAN, созданного на основе моста, будет назначен указанный нами IP-адрес.

Важно

После запуска интерфейса VLAN страница не будет загружена до конца, т.к. доступ к устройству без тега VLAN будет закрыт. С этого момента управлять устройством можно только с VLAN, номер которой совпадает с указанным при создании интерфейса VLAN *VLAN ID*.

Организация управления устройством через интерфейс, входящий в состав моста или бондинга

В случае, если порт, через который осуществляется управление устройством, необходимо добавить в состав моста или бондинга, IP-адрес, используемый для управления, следует назначить интерфейсу, в состав которого включается порт. Например, порт eth0 используется для управления и ему назначен IP-адрес

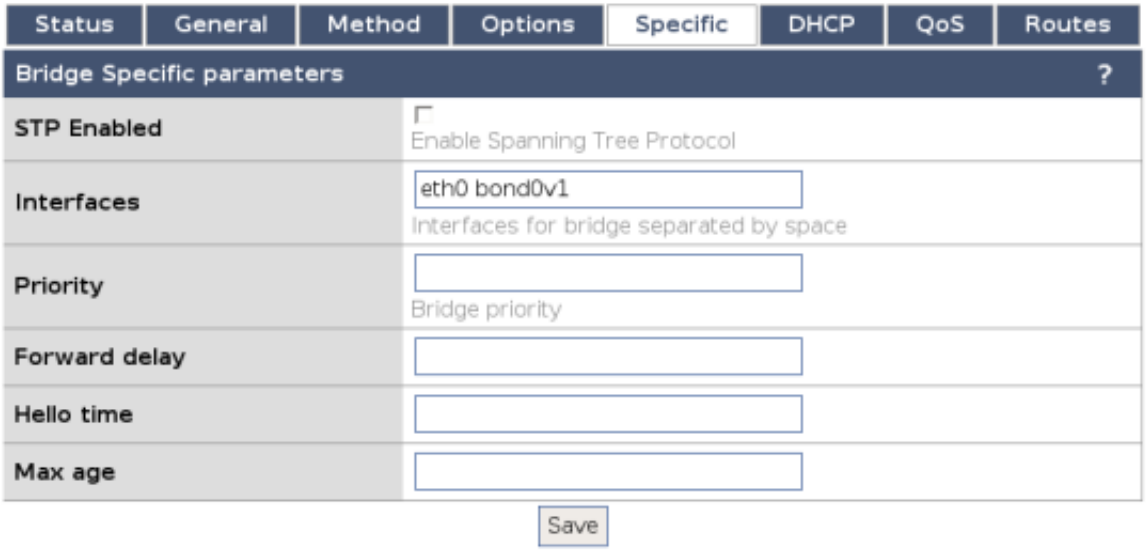
192.168.2.100. Тогда, при включении этого порта в состав моста (интерфейса br0), то интерфейсу br0 назначается IP-адрес 192.168.2.100.

Т.к. в случае непоследовательных действий есть вероятность потери управления над устройством, рассмотрим эту конфигурацию более подробно на примере организации независимых каналов между Ethernet-интерфейсами.

Допустим, мы управляем устройством через порт *eth0* по IP-адресу 192.168.2.100, и хотим включить этот порт в мост для организации передачи данных, т.е. реализовать т.н. "функциональность 1". Но т.к. этот порт используется для управления, необходима другая последовательность действий по организации моста.

Допустим, мы выполнили последовательность действий, описанных в приведённом выше разделе, а именно: настроили физическое соединение, создали бондинг и необходимый VLAN поверх него (*bond0v1*). Теперь нам необходимо создать мост. Здесь последовательность действий немного меняется. Создадим интерфейс моста, пусть у него будет имя *br1*. Перейдём на его страницу настройки, выберем вкладку Specific и пропишем нужные нам интерфейсы: eth0 и bond0v1.

Рисунок 12.11. Добавление интерфейсов в мост

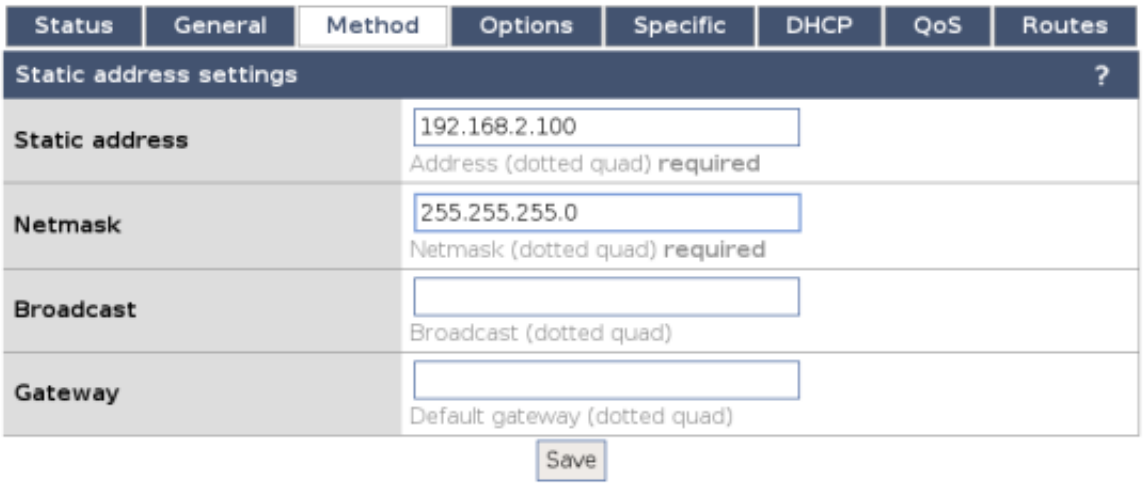


Затем перейдём на вкладку General и выберем статический (Static) метод назначения адреса. На данном этапе нельзя активировать интерфейс (выставлять флажки Enabled и Auto)!

Рисунок 12.12. Установка метода назначения IP-адреса

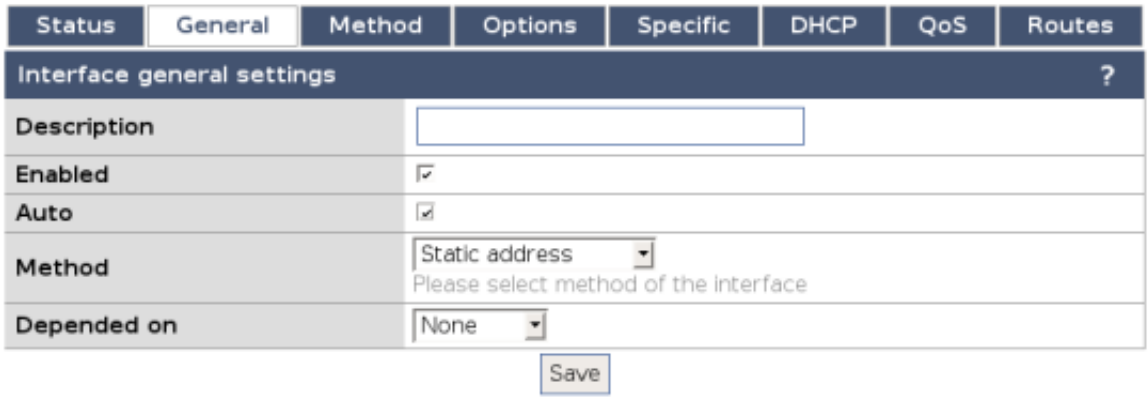
Перейдём на вкладку Method, где пропишем нужный IP-адрес и маску сети.

Рисунок 12.13. Назначение IP-адреса



И в завершении вернёмся на вкладку General и активируем флажки Enabled и Auto.

Рисунок 12.14. Запуск моста



После сохранения настроек с интерфейса eth0 будет снят IP-адрес, а на интерфейс моста будет назначен введённый нами IP-адрес, через который возможно дальнейшее управление устройством.

Подсказка

В случае, если на интерфейс моста назначается тот же IP-адрес, что был на интерфейсе порта, возможно пропадание на некоторое время связи с устройством. Связано это с тем, что MAC-адрес моста соответствует одному из интерфейсов, которые в него входят, и если будет выбран MAC-адрес не интерфейса порта, которому принадлежал IP-адрес, то надо будет заместить в локальном ARP-кэше компьютера старое соответствие MAC-адреса IP-адресу. Сделать это можно либо вручную, удалив соответствующую запись из ARP-кэша, либо подождав некоторое время.

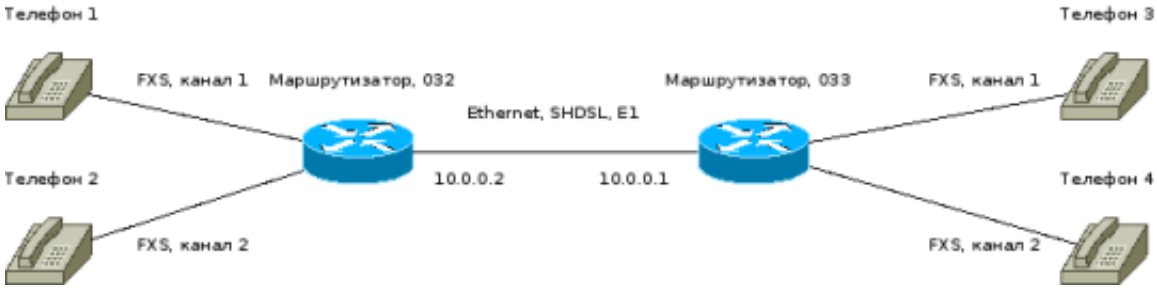
VoIP

Обычные телефоны работают как два IP-телефона

В маршрутизатор устанавливаются модули VoIP с каналами FXS, к которым подключаются обычные аналоговые телефоны. Используя эти телефоны, можно

совершать звонки на телефоны, подключенные к тому же маршрутизатору, либо на другие маршрутизаторы фирмы Сигранд. Пример схемы подключения показан ниже.

Рисунок 12.15. Обычные телефоны работают как два IP-телефона



В данном примере в сети работает два маршрутизатора, с номерами 032 и 033 и адресами 10.0.0.2 и 10.0.0.1 соответственно. К каждому маршрутизатору подключён аналоговый телефон, маршрутизаторы между собой соединены по любой технологии — Ethernet, SHDSL или E1.

Для настройки IP-телефонии необходимо внести данные в таблицы маршрутизации, адресной книги и Hotline. Для удобства, примеры настроек представлены не в виде скриншотов, а в виде текстовых таблиц, приведённых ниже.

Таблица маршрутизации имеет одинаковое содержимое на всех маршрутизаторах одной сети и приведена ниже.

Таблица 12.1. Таблица маршрутизации

№ маршрутизатора	Адрес маршрутизатора	Комментарий
032	10.0.0.2	Маршрутизатор 032
033	10.0.0.1	Маршрутизатор 033

Адресная книга заполняется для каждого маршрутизатора отдельно, так как могут использоваться различные сокращённые номера. Адресная книга для маршрутизаторов приведена в таблицах ниже.

Таблица 12.2. Адресная книга маршрутизатора 032

Короткий номер	Полный номер	Комментарий
00	* 01	Телефон 1 (первый вариант набора номера)
01	032 02	Телефон 2 (второй вариант набора номера)
02	033 01	Телефон 3
03	033 02	Телефон 4

Таблица 12.3. Адресная книга маршрутизатора 033

Короткий номер	Полный номер	Комментарий
00	032 01	Телефон 1
01	032 02	Телефон 2
02	* 01	Телефон 3
03	* 02	Телефон 4

С такой конфигурацией возможны следующие способы вызова:

- С телефона 1 на телефон 2:
  1. напрямую:
     a. * 02
     b. 032 02 (с явным указанием номера своего маршрутизатора)
  2. через адресную книгу: #01
- С телефона 1 на телефон 4:
  1. напрямую: 033 02
  2. через адресную книгу: #03

При использовании режима Hotline можно создать конфигурацию, при которой после поднятия трубки на телефоне будет автоматически происходить набор номера, заданный для канала FXS, к которому подключён телефон. Настройка Hotline для маршрутизатора 032 приведена в таблице ниже.

Таблица 12.4. Таблица Hotline для маршрутизатора 032

Номер канала	Полный номер	Комментарий
01 (FXS)	033 01	Автодозвон на телефон 3
02 (FXS)	032 01	Автодозвон на телефон 1

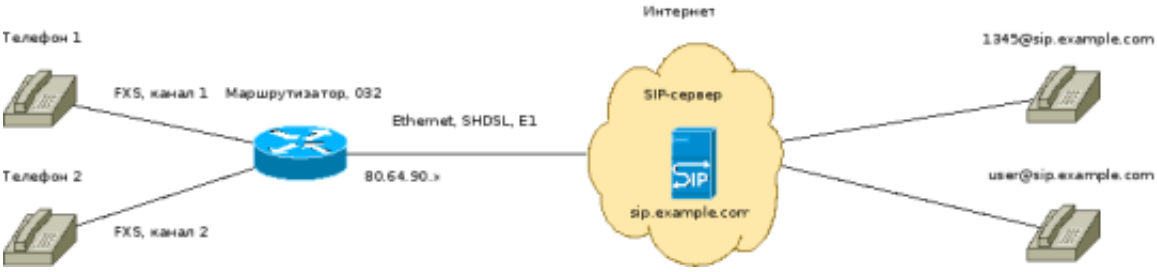
Эта конфигурация задаёт следующее поведение:

- при подъёме телефонной трубки на телефоне 1 производится автоматический дозвон на телефон 3.
- при подъёме телефонной трубки на телефоне 2 производится автоматический дозвон на телефон 1.

Организация телефонного соединения через VoIP-шлюз

В маршрутизатор установлены модули VoIP с каналами FXS для подключения аналоговых телефонов. Маршрутизатор имеет доступ к VoIP-шлюзу, который позволяет совершать вызовы на IP-телефоны, так же подключённые к этому шлюзу. Пример схемы подключения показан ниже.

Рисунок 12.16. Организация телефонного соединения через VoIP-шлюз



Для совершения вызовов на IP-телефоны, подключённые к VoIP-шлюзу, необходимо произвести соответствующую настройку маршрутизатора, как показано на рисунке ниже, а именно — указать адрес SIP-прокси и регистрационную информацию.

Рисунок 12.17. Настройки для вызовов через VoIP-шлюз

Так как маршрутизатор не совершает вызовы по VoIP на другие маршрутизаторы, то таблица маршрутизации не используется. Для упрощения набора номера и для возможности совершения звонков на IP-телефоны с нецифровыми номерами, внесём данные в адресную книгу, которая представлена ниже в таблице.

Таблица 12.5. Адресная книга

Короткий номер	Полный номер	Комментарий
00	* 01	Телефон 1
01	* 02	Телефон 02
02	* # 1345@sip.example.com #	Звонок на 1345@sip.example.com
03	032 # user@sip.example.com #	Звонок на user@sip.example.com

С такой конфигурацией возможны следующие способы вызова:

- С телефона 1 на телефон 2:
  1. напрямую: * 02
  2. через адресную книгу: #01
- С телефона 2 на user@sip.example.com:
  1. напрямую: невозможно, т.к. номер не цифровой
  2. через адресную книгу: #03
- С телефона 1 на 1345@sip.example.com:
  1. напрямую: * # 1345 #
  2. через адресную книгу: #02

Здесь мы так же можем настроить режим Hotline для автоматического набора номера при поднятии трубки на аналоговых телефонах. Так же, использование SIP-шлюза позволяет использовать Hotline для переадресации входящих SIP-вызовов на любой телефон, доступный для вызова с маршрутизатора. Настройки режима Hotline приведены ниже в таблице.

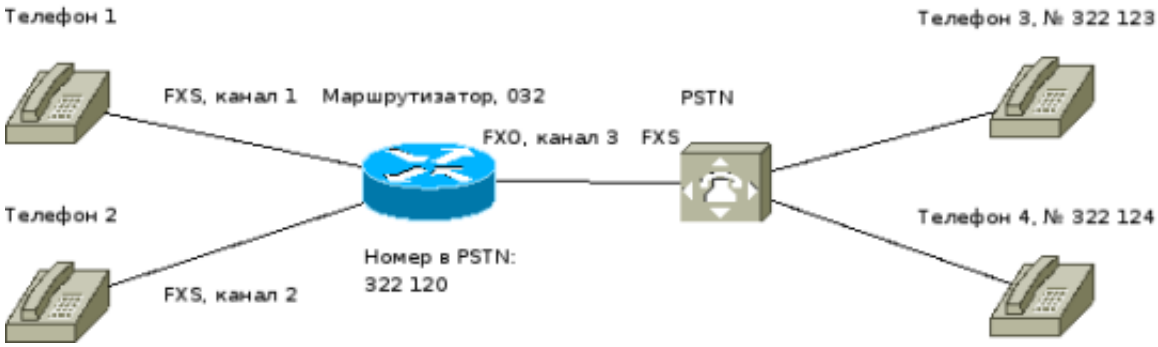
Таблица 12.6. Таблица Hotline

Номер канала	Полный номер	Комментарий
01 (FXS)	* # 1345@sip.example.com #	Автодозвон при подъёме трубки на телефоне 1 на 1345@sip.example.com
# (SIP)	* 02	Переадресация всех входящих SIP-звонков на телефон 2

Организация связи через АТС

В маршрутизатор установлены модули VoIP с каналами FXS, для подключения аналоговых телефонов, и FXO, для подключения к АТС — например, к городской сети (ТфОП, или PSTN). На АТС для маршрутизатора выделен номер 322 120. Схема, иллюстрирующая пример, показана ниже на рисунке.

Рисунок 12.18. Организация связи через АТС



В данном случае таблица маршрутизации так же не используется, по желанию можно настроить адресную книгу для быстрого набора номеров. Настройки адресной книги приведены ниже в таблице.

Таблица 12.7. Адресная книга

Короткий номер	Полный номер	Комментарий
00	* 01	Телефон 1
01	032 02	Телефон 2
02	* * , 322 123	Телефон 3
03	032 * , 322 124	Телефон 4

Замечание

Напомним, что символ «*» вместо номера канала означает звонок через первый свободный канал FXO. В нашем случае канал FXO один, поэтому можно всегда использовать этот символ для более быстрого набора номера.

С такой конфигурацией возможны следующие способы вызова:

- С телефона 1 на телефон 2:

  1. напрямую: * 02

2. через адресную книгу: #01

- С телефона 2 на телефон 4:

  1. напрямую: * *, дождаться сигнала АТС, 322 124

  2. через адресную книгу: #03

- С телефона 3 на телефон 1:

  1. напрямую:

     a. 322 120, дождаться сигнала маршрутизатора, * 01

     b. 322 120, дождаться сигнала маршрутизатора, 032 01

Режим Hotline позволяет реализовать возможности, указанные ниже в таблице.

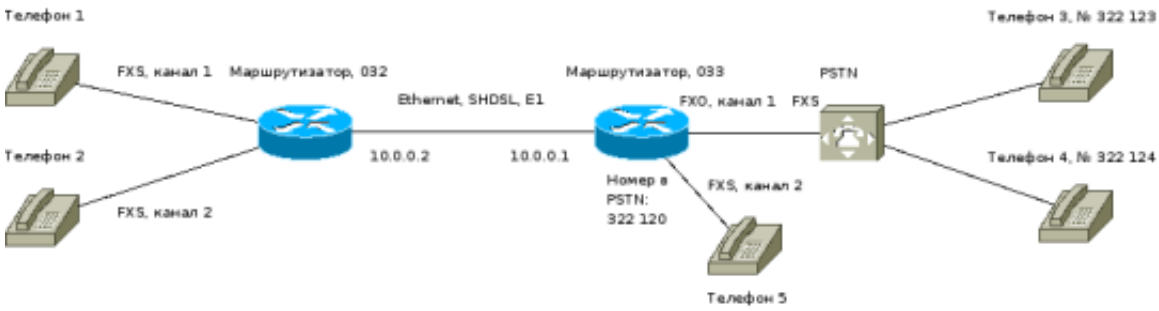
Таблица 12.8. Таблица Hotline для маршрутизатора

Номер канала	Полный номер	Комментарий
01 (FXS)	* * , 322 124	Автодозвон при подъёме трубки на телефоне 1 на телефон 4
03 (FXO)	* 01	Переадресация входящих от PSTN звонков на телефон 1

Организация связи через АТС с использованием двух маршрутизаторов

Рассмотрим более сложный вариант сети, представленной в предыдущем примере. В сети работает два маршрутизатора, к которым подключены аналоговые телефоны. Маршрутизаторы соединены между собой по технологиями Ethernet/SHDSL/E1, и к одному из маршрутизаторов подключена АТС. Необходимо реализовать возможность вызовов между телефонами, подключёнными к маршрутизаторам, и между маршрутизаторами и АТС. Схема сети представлена ниже на рисунке.

Рисунок 12.19. Организация связи через АТС с использованием двух маршрутизаторов



Так как в сети работают два маршрутизатора, необходимо настроить таблицу маршрутизации, содержимое которой представлено ниже в таблице.

Таблица 12.9. Таблица маршрутизации

№ маршрутизатора	Адрес маршрутизатора	Комментарий
032	10.0.0.2	Маршрутизатор 032
033	10.0.0.1	Маршрутизатор 033

Для быстрого набора номера настроим адресную книгу для каждого маршрутизатора, содержимое которой представлено ниже в таблицах.

Таблица 12.10. Адресная книга маршрутизатора 032

Короткий номер	Полный номер	Комментарий
00	* 01	Телефон 1
01	* 02	Телефон 2
02	033 02	Телефон 5
03	033 * , 322 123	Телефон 3
04	033 * , 322 124	Телефон 4

Таблица 12.11. Адресная книга маршрутизатора

Короткий номер	Полный номер	Комментарий
00	032 01	Телефон 1
01	032 02	Телефон 2
02	* * , 322 123	Телефон 3
03	* * , 322 124	Телефон 4

С такой конфигурацией возможны следующие способы вызова:

- С телефона 1 на телефон 2:
  1. напрямую: * 02
  2. через адресную книгу: #01
- С телефона 2 на телефон 4:
  1. напрямую: 033 *, дождаться сигнала АТС, 322 124
  2. через адресную книгу: #04
- С телефона 2 на телефон 5:
  1. напрямую: 033 02
  2. через адресную книгу: #02
- С телефона 3 на телефон 2:
  1. напрямую: 322 120, дождаться сигнала маршрутизатора, 032 02

Так же, настроим режим Hotline, как показано ниже в таблицах.

Таблица 12.12. Таблица Hotline для маршрутизатора 032

Номер канала	Полный номер	Комментарий
01 (FXS)	033 02	Автодозвон при подъёме трубки на телефоне 1 на телефон 5
02 (FXS)	033 *, 322 124	Автодозвон при подъёме трубки на телефоне 2 на телефон 4

Таблица 12.13. Таблица Hotline для маршрутизатора 033

Номер канала	Полный номер	Комментарий
01 (FX0)	032 02	Переадресация входящих от PSTN звонков на телефон 2
02 (FXO)	* * , 322 123	Автодозвон при подъёме трубки на телефоне 5 на телефон 3

Глава 13. Гарантия и обязательства

Изготовитель гарантирует работоспособность маршрутизатора при соблюдением потребителем правил эксплуатации.

Гарантийный срок устанавливается не менее 5 лет со дня продажи, отмеченного в паспорте, либо, при отсутствии отметки, с момента выпуска, указанного на маркировке.

Внимание

Гарантия на маршрутизаторы, эксплуатирующиеся на "воздушных" линиях, либо линиях с комбинированным способом прокладки, аннулируется.

Глава 14. Приложение

Особенности применения кодировок TCPAM

Кодирование TCPAM (Trellis-Coded Pulse Amplitude Modulation), используемое для передачи информации по стандарту G.SHDSL (G.991.2), имеет несколько вариантов, отличающихся степенью сложности алгоритма кодирования. Большим скоростям передачи соответствует режим с большим количеством позиций модуляции (TCPAM32), на малых скоростях используется режим с меньшим числом позиций модуляции (TCPAM16). Соответственно, с увеличением сложности алгоритма кодирования, снижается помехоустойчивость канала, и наоборот.

Поэтому, при настройке скорости линии, следует обращать особое внимание на алгоритм кодирования TCPAM и, при необходимости, изменять линейный код для достижения наилучшего результата.

Для каждой серии SHDSL соответствуют свои допустимые и рекомендуемые значения кодировок TCPAM.

SG-16

Таблица 14.1. Допустимые значения для режима CFG=LOCAL, ANNEX A

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	256..5696
TCPAM16	192..3840
TCPAM8	192..1216
TCPAM4	64..704

Таблица 14.2. Рекомендуемые значения для режима CFG=LOCAL, ANNEX A

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	2560..5696
TCPAM16	1152..2496
TCPAM8	192..1088
TCPAM4	64..128

Таблица 14.3. Допустимые значения для режима CFG=PREACT, ANNEX F

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	768..5696
TCPAM16	192..3840

Таблица 14.4. Рекомендуемые значения для режима CFG=PREACT, ANNEX F

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	2560..5696
TCPAM16	192..2496

SG-17

SG-17

Таблица 14.5. Допустимые значения

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	768..5696
TCPAM16	192..3840

Таблица 14.6. Рекомендуемые значения

Линейный код	Диапазон скоростей, кбит/с
TCPAM32	2560..5696
TCPAM16	192..2496