

СОДЕРЖАНИЕ

1. Знакомство с ROSA Enterprise Linux Server	2
1.1. Базовые службы ROSA Enterprise Linux Server	2
1.2. Системные требования	2
2. Установка ROSA Enterprise Linux Server	3
3. Просмотр и изменение структуры разделов для установки Rosa Enterprise Linux Server	11
3.1. Конфигурирование устройств хранения, используемых системой	11
3.2. Добавление стандартного устройства	12
3.3. Добавление аппаратного RAID	12
3.4. Многопутевая настройка	13
3.5. Добавление других устройств SAN	15
3.6. Поиск устройств хранения данных	16
3.7. Сведения об устройствах хранения, имеющихся в системе	17
3.8. Настройка параметров добавляемого устройства	17
4. Настройка сетевых подключений	21
4.1. Проводные соединения	22
4.2. Беспроводные соединения	35
4.3. Мобильные соединения	37
4.4. DSL-соединения	43
5. Выбор устанавливаемых элементов ROSA Enterprise Linux Server	47
5.1. Настройка ROSA Directory Server	48
5.2. Базовая конфигурация MMC	49
6. Настройка служб и инструментов сервера ROSA	55
7. Основные компоненты RDS	57
7.1. Настройки Samba PDC и файлового сервера	57
7.2. Поддержка квот пользователей	58
7.3. Настройки модуля аудита для RDS	58

1 Знакомство с ROSA Enterprise Linux Server

Современные средства развертывания и поддержки серверных решений масштаба предприятия предъявляют новые требования к автоматизации задач поддержки и администрирования приложений, а также управления доступом пользователей к ресурсам предприятия. ROSA Enterprise Linux Server обладает всем необходимым набором возможностей для поддержки работы многих пользователей в распределенной среде. Созданный на базе серверных разработок Red Hat и Mandriva, дополненных инструментами для развёртывания частных облаков, а также для централизованного управления сетевыми ресурсами, ROSA Enterprise Linux Server легко интегрируется в любую среду предприятия.

ROSA Enterprise Linux Server является полностью открытым программным обеспечением, включает поддержку серверных аппаратных платформ и систем хранения, защищен от внешних угроз.

1.1 Базовые службы ROSA Enterprise Linux Server

- Групповая работа (электронная почта, календарь, задачи, мгновенные сообщения, аудио- и видеоконференции, совместная работа над документами).
- Размещение веб-сайта организации и других веб-приложений (веб-службы).
- Контроль и статистика доступа в интернет (проxy-сервер).
- Управление учетными записями пользователей и компьютеров (службы каталога, инвентаризации, политики управления).
- Создание и размещение виртуальных серверов и рабочих мест и доступ к ним (службы виртуализации, терминальные службы).
- Безопасный доступ пользователей "извне"к внутренним ресурсам (VPN-сервер).
- Хранилище данных и документов (службы доступа к файлам).
- Защита и резервное копирование данных (антивирусные службы и службы резервного копирования).
- Набор сервисов и служб для построения частных и публичных облачных инфраструктур (IaaS). В состав также входит сервис для организации распределенного хранения данных и удобный веб-интерфейс.

1.2 Системные требования

Минимальная рекомендуемая конфигурация для ROSA Enterprise Linux Server:

- Процессор типа Intel Xeon E5-2600 или аналог
- Оперативная память: 4 Гб

– Дисковое пространство: 12 Гб

ROSA Enterprise Linux Server поддерживает как 32-битную, так и 64-битную аппаратную платформу ОС. Соответствующую версию ROSA Enterprise Linux Server можно загрузить с [официального сайта компании «РОСА»](#).

2 Установка ROSA Enterprise Linux Server

Процесс установки ROSA Enterprise Linux Server аналогичен установке других программ, работающих в среде Linux. Для установки этого программного обеспечения можно использовать графическую утилиту.

Чтобы начать установку ROSA Enterprise Linux Server, выполните следующие действия:

1) Запустите мастер установки ROSA Enterprise Linux Server. Для этого скопируйте дистрибутив соответствующей версии ROSA Enterprise Linux Server, загруженный с сайта (см. ссылку выше), на флеш-носитель или запишите его на CD/DVD. Для установке с флеш-носителя воспользуйтесь утилитой [ROSA Image Writer](#).

Начальное окно работы с мастером установки выглядит так:

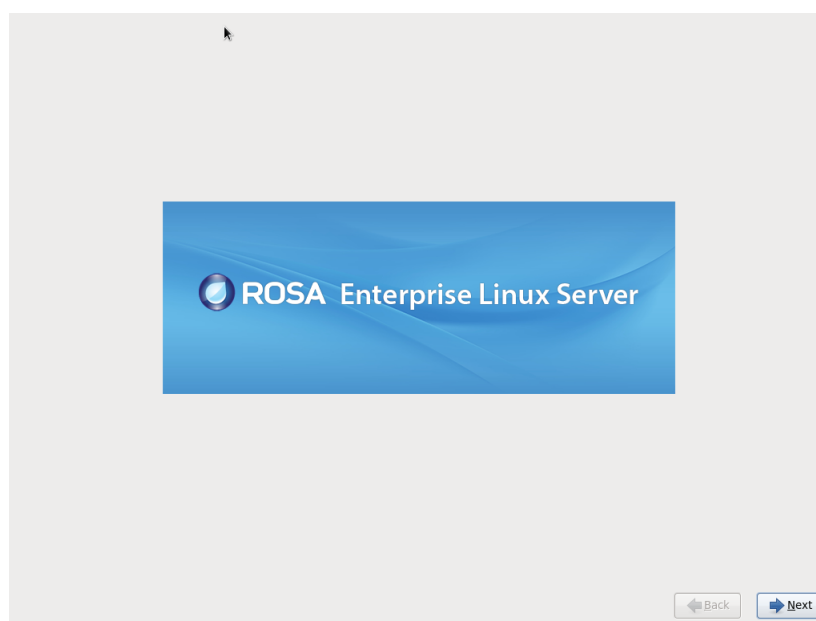


Рисунок 1

2) Продолжайте работу с мастером, выбирая язык установки. Выберите «Russian (Русский)» для русскоязычного интерфейса ROSA Enterprise Linux Server.

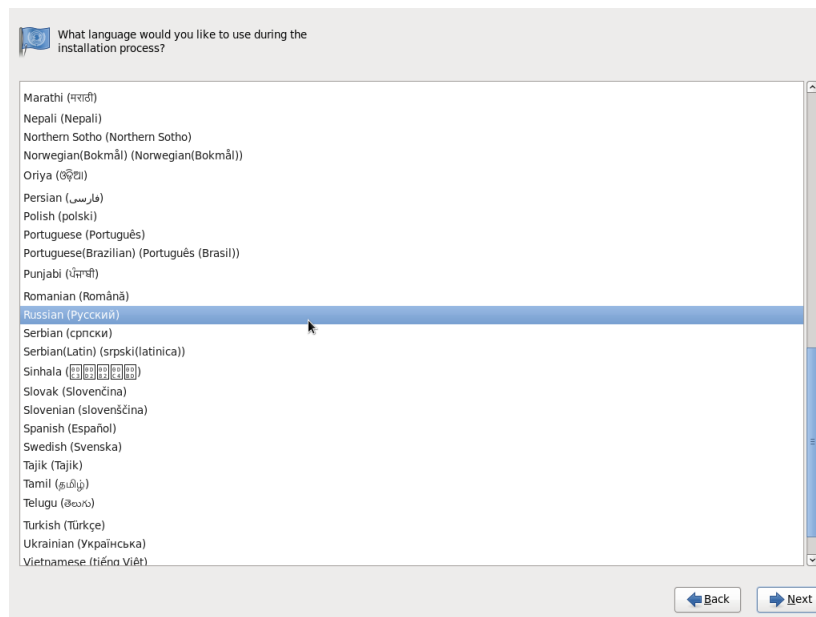


Рисунок 2

Затем на следующем экране выберите раскладку клавиатуры «Русская».

3) Выберите тип устройства, используемого при установке. Можно выбрать один из вариантов:

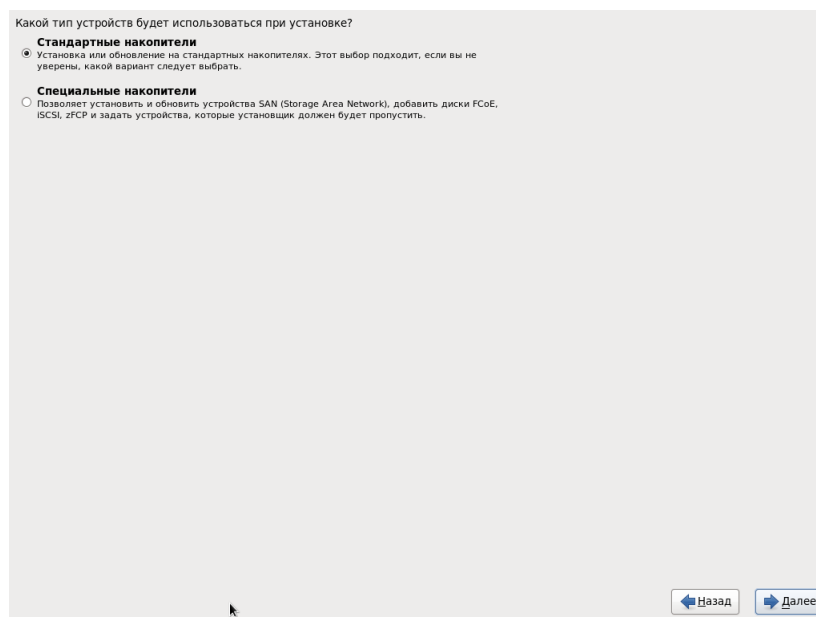


Рисунок 3

– **Стандартные накопители** — при выборе данного типа устройства мастер установки выполнит проверку имеющихся устройств хранения данных и выполнит установку на одно из этих устройств, выбранных вами.

При наличии данных на имеющихся устройствах мастер установки выдаст предупреждение, при ошибке чтения/записи для имеющихся устройств хранения данных мастер установки выдаст сообщение об ошибке.

– **Специальные накопители** — при выборе данного типа устройств вы можете самостоятельно сконфигурировать устройства для установки ROSA Enterprise Linux Server.

Параметры конфигурации специальных накопителей будут различаться для разных видов устройств. Ниже мы рассмотрим их все, см. «Просмотр и изменение структуры разделов для установки Rosa Enterprise Linux Server».

4) Далее необходимо присвоить создаваемому экземпляру сервера сетевое имя (имя узла). Введите имя сервера в поле **Имя узла**, изменив значение *localhost.localdomain* в соответствии с необходимыми настройками.

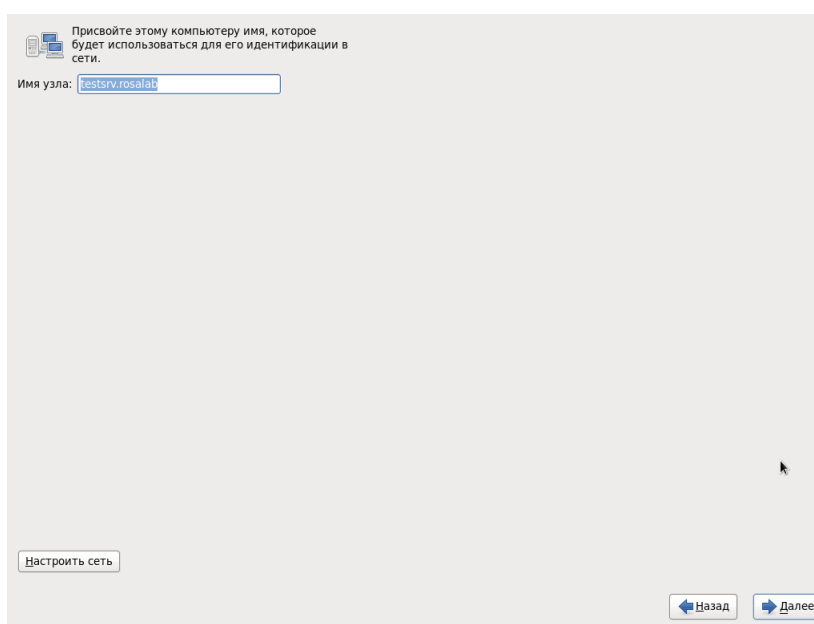


Рисунок 4

Создаваемому экземпляру сервера можно присвоить любое уникальное имя узла. Имя может содержать буквы, цифры и дефис.

5) Также можно настроить сетевые соединения. Нажмите **Настроить сеть**, и в окне **Сетевые соединения** просмотрите список доступных сетевых соединений. Можно добавить новое соединение, изменить параметры уже имеющегося соединения или удалить имеющееся соединение.

При добавлении нового соединения в окне выбора типа соединения выберите один из возможных типов:

Аппаратные типы соединений

- DSL
- InfinitiBand
- Беспроводные

- Мобильные
- Проводные

Виртуальные типы соединений

- Bond
- VLAN

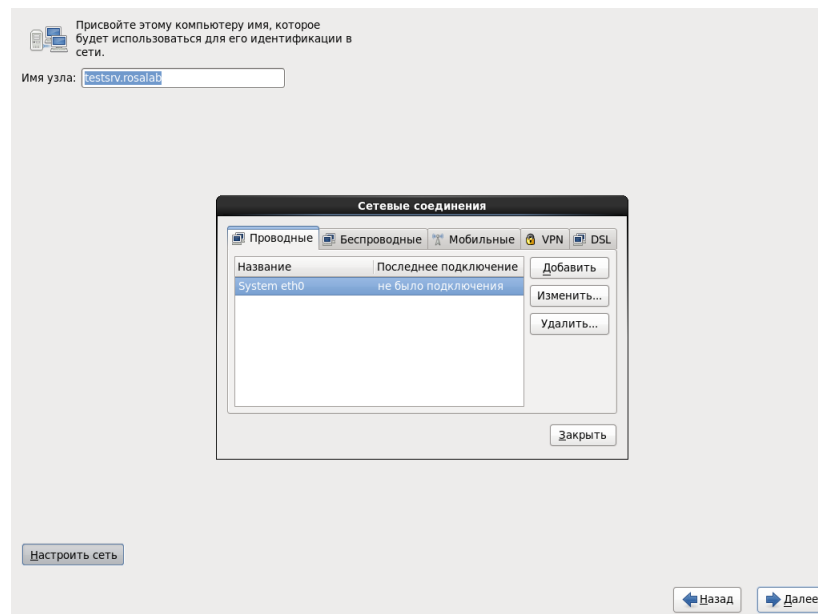


Рисунок 5

Параметры настройки соединения будут отличаться для каждого из выбранных типов соединений. Ниже мы рассмотрим их все.

6) Далее мастер установки предлагает выбрать страну и указать ближайший город в вашем часовом поясе, а также выбрать формат системного времени.

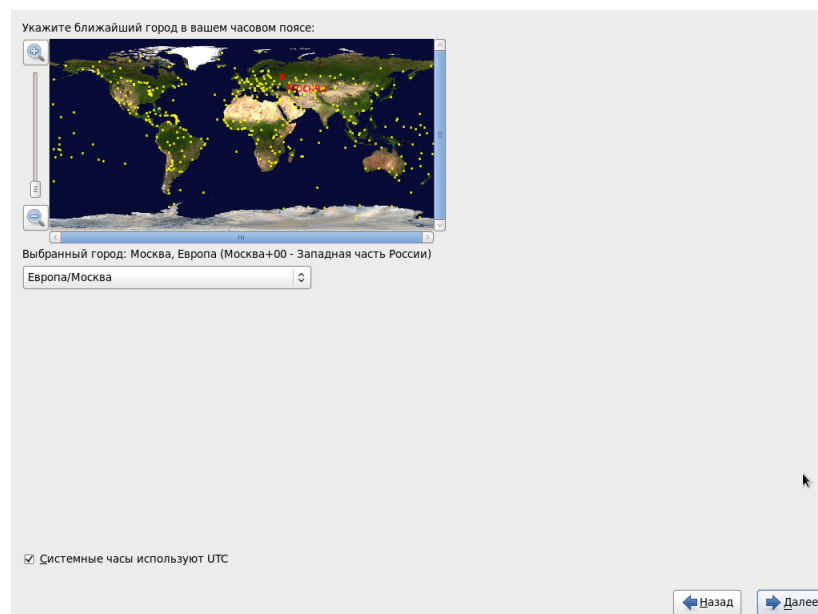


Рисунок 6

Выберите ближайший город из списка и продолжите установку.

Чтобы системное время использовало формат мирового времени UTC, установите флажок «**Системные часы используют UTC**».

7) Введите пароль учетной записи пользователя `root`.

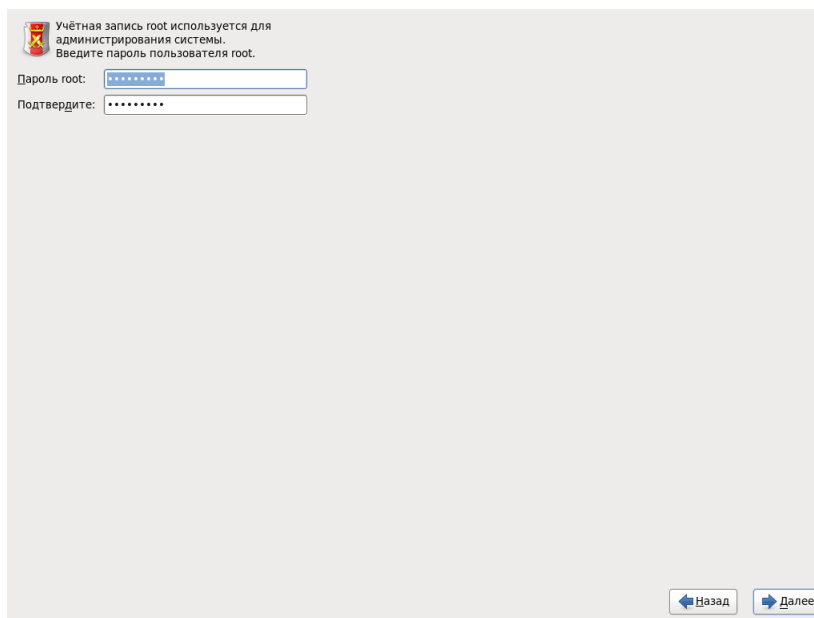
The screenshot shows a window titled "Учётная запись root используется для администрирования системы. Введите пароль пользователя root." (The root account is used for system administration. Enter the root user password). It contains two input fields: "Пароль root:" (Root password) and "Подтвердите:" (Confirm). Both fields are currently empty and have a password icon (a circle with a dot) on the right. At the bottom right, there are two buttons: "Назад" (Back) and "Далее" (Next).

Рисунок 7

8) Выберите тип установки. ROSA Enterprise Linux Server можно установить поверх существующей системы либо выбрать один из вариантов ее замещения или модификации. Также укажите параметры шифрования и при необходимости просмотрите и измените структуру раздела:

- Тип установки **Все пространство** удалит все разделы на выбранном для установки устройстве. Выбирайте этот тип установки только в том случае, если были созданы резервные копии данных, хранящихся на данном устройстве.
- Тип установки **Заменить существующую систему Linux** удаляет только разделы Linux, созданные в процессе предыдущей установки.
- Тип установки **Уменьшить существующую систему** позволяет сократить существующие разделы для освобождения места для стандартного разбиения.
- Тип установки **Использовать свободное пространство** сохранит все текущие данные и разделы неизмененными, используя только нераспределенное пространство на выбранных устройствах.
- Тип установки **Создать собственное разбиение** позволяет создать собственное разбиение на выбранных устройствах с помощью специальной утилиты создания разделов.

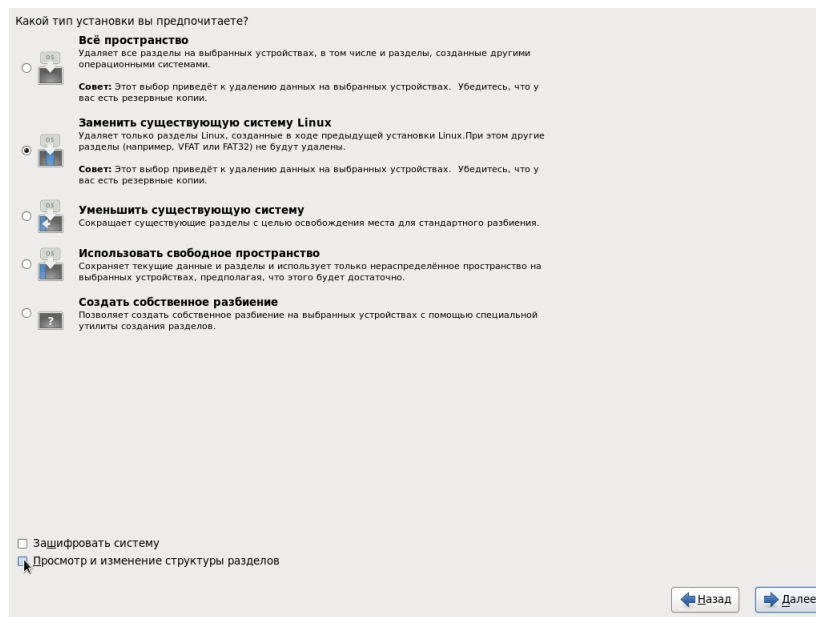


Рисунок 8

Для каждой из перечисленных конфигураций возможно создать и сконфигурировать собственный набор устройств, установив флажок **Просмотр и изменение структуры разделов**. Ниже мы рассмотрим, какие параметры доступны для настройки.

9) Утилита установки выводит список операционных систем загрузчика. По умолчанию, список содержит пункт *Rosa Linux Enterprise Server*, который выбран как образ загрузки по умолчанию. По желанию можно удалить или добавить операционные системы в меню загрузчика, выбрав по умолчанию другой образ загрузки и/или изменив устройство для установки операционной системы.

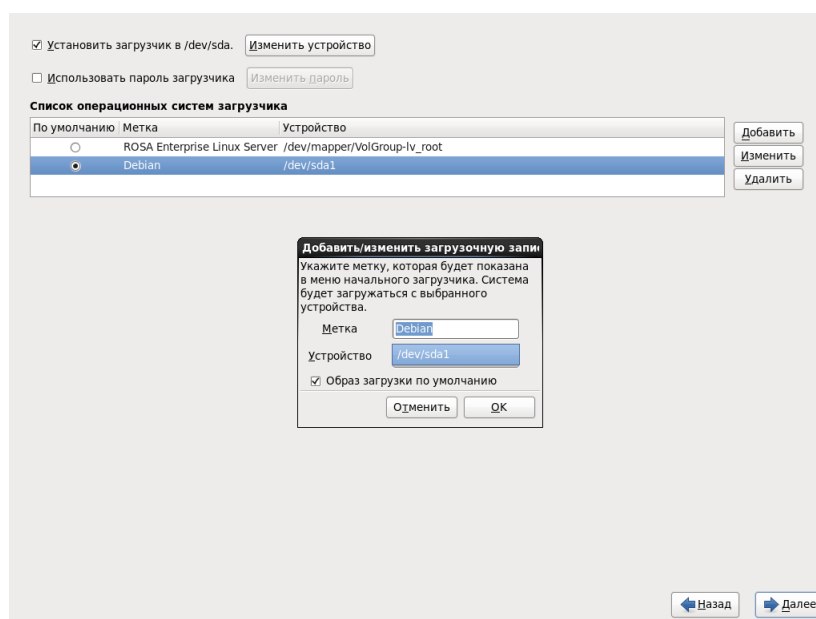


Рисунок 9

10) Мастер установки выводит список вариантов установки, которые представляют со-

бой рабочие конфигурации Rosa Linux Enterprise Server, предназначенные для различных целей. По умолчанию выбирается стандартная конфигурация Rosa Linux Enterprise Server.

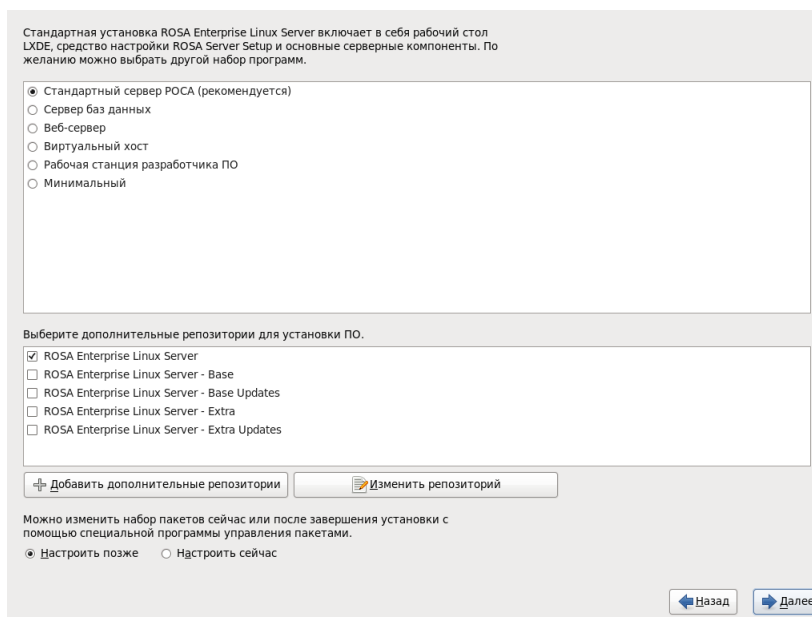


Рисунок 10

Кроме выбора рабочей конфигурации, можно выбрать дополнительные репозитории для установки ПО, добавить дополнительные репозитории и задать их основные параметры или изменить уже имеющиеся (настроенные репозитории). Можно выбрать один из следующих типов репозитория:

– **FTP/HTTP** — такой тип репозитория используется, когда установка выполняется с удаленного хоста (на удаленном хосте размещен дистрибутив). Для такой установки вам необходимо указать имя репозитория и web-адрес сервера.

Если для доступа к репозиторию используется прокси-сервер, необходимо установить флажок **Настройка прокси** и указать имя узла и порт прокси-сервера, а также имя пользователя прокси-сервера и пароль прокси-сервера.

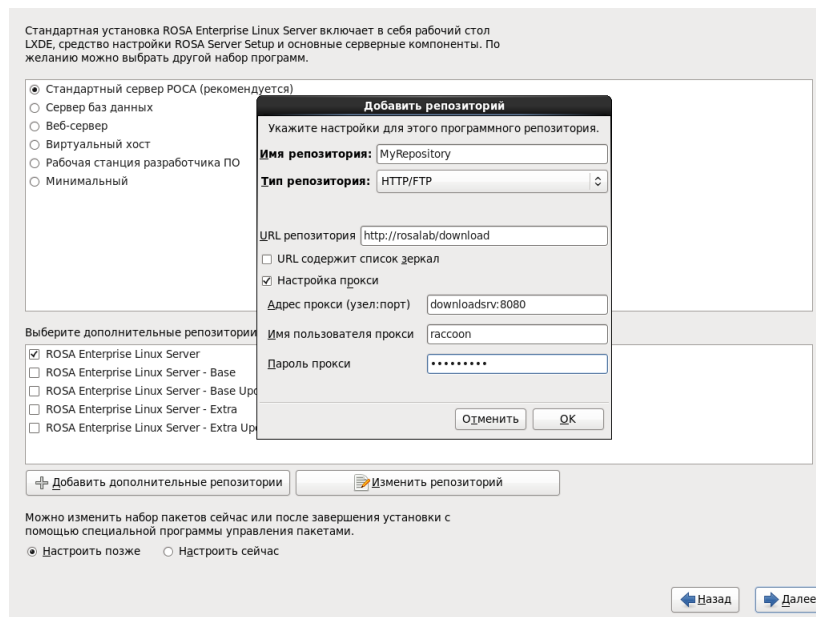


Рисунок 11

– **CD/DVD** — такой тип репозитория используется, когда установка выполняется с CD- или DVD-носителя. Для такой установки потребуется указать имя репозитория. Система самостоятельно определит наличие соответствующих устройств на компьютере, где выполняется установка.

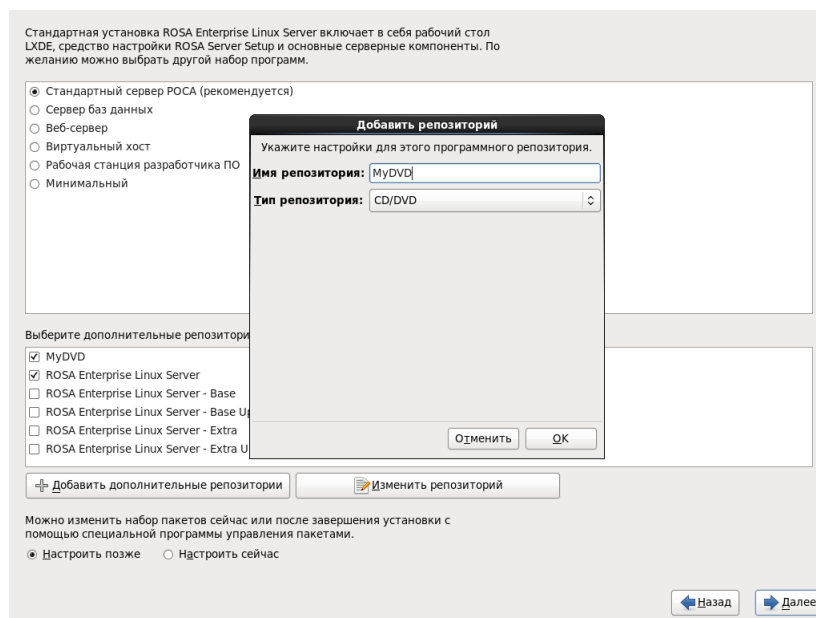


Рисунок 12

– **NFS** — такой тип репозитория используется при установке с локального сетевого ресурса. Потребуется указать имя сервера, на котором размещен репозиторий, и путь к дистрибутиву системы. Также может потребоваться указать параметры.

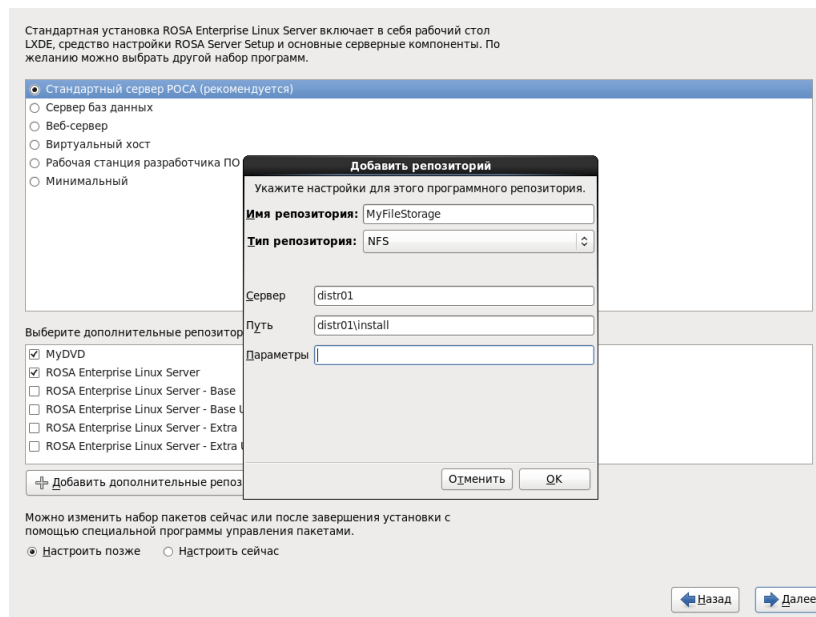


Рисунок 13

11) Далее завершите установку и первоначальное конфигурирование ROSA Enterprise Linux Server. После завершения процесса автоматической установки перезагрузите систему.

3 Просмотр и изменение структуры разделов для установки Rosa Enterprise Linux Server

3.1 Конфигурирование устройств хранения, используемых системой

При выборе параметра **Специальные накопители** можно использовать один из определенных мастером установки видов накопителей или добавить собственное устройство, которое будет использоваться для устанавливаемой системы, а затем сконфигурировать его.

При конфигурировании устройств можно использовать более понятные имена. Для этого нажмите кнопку *Параметры устройства* и установите флажок **Использовать понятные имена** для многопутевых устройств. В файле конфигурации этот флажок устанавливает для параметра `user_friendly_names` значение `true`.

В списке устройств, определяемых системой при установке, перечислены следующие виды устройств:

- Стандартные устройства — все напрямую подключенные устройства, такие, как жесткие диски. Можно добавить устройство в список и сконфигурировать его, задав дополнительные параметры.

– Аппаратный RAID — накопители, подключенные к аппаратному RAID-контроллеру. Можно добавить устройство в список и сконфигурировать его, задав дополнительные параметры.

– Многопутевые устройства — накопители, для доступа к которым в одной и той же системе можно использовать несколько путей.

– Другие устройства SAN — любые другие устройства в сети хранения данных. В частности, к ним относятся LUN FCP, доступные по единственному пути.

3.2 Добавление стандартного устройства

Вкладка **Добавление стандартного устройства** позволяет добавить стандартное устройство в список поддерживаемых устройств Rosa Linux Enterprise Server.

На данной вкладке отображается список стандартных устройств, обнаруженных программой установки. В таблице свойств стандартных устройств можно вывести дополнительные сведения об устройствах, нажав небольшое раскрывающееся меню в правом верхнем углу таблицы.

Чтобы выбрать стандартные устройства из числа перечисленных в таблице устройств, установите флажки в первом поле таблицы рядом с именами выбираемых устройств.

Для добавления нового стандартного устройства нажмите кнопку *Добавить*.

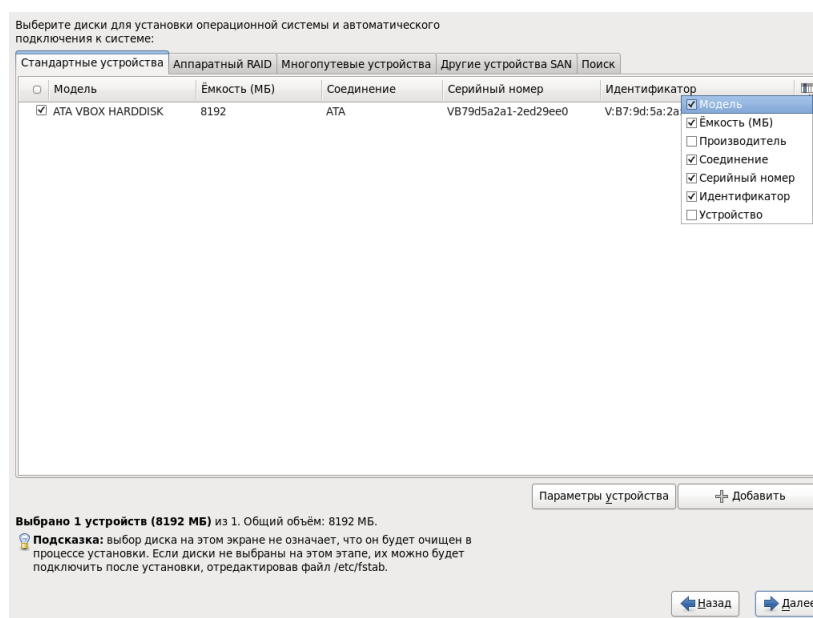


Рисунок 14

3.3 Добавление аппаратного RAID

Вкладка **Аппаратный RAID** позволяет добавить аппаратный RAID в список поддерживаемых устройств Rosa Linux Enterprise Server.

На данной вкладке отображается список аппаратных RAID, обнаруженных программой установки. В таблице свойств аппаратных RAID можно вывести дополнительные сведения об этих устройствах, нажав небольшое раскрывающееся меню в правом верхнем углу таблицы.

Чтобы выбрать аппаратные RAID из числа перечисленных в таблице устройств, установите флажки в первом поле таблицы рядом с именами выбираемых устройств.

Для добавления нового аппаратного RAID нажмите кнопку *Добавить*.

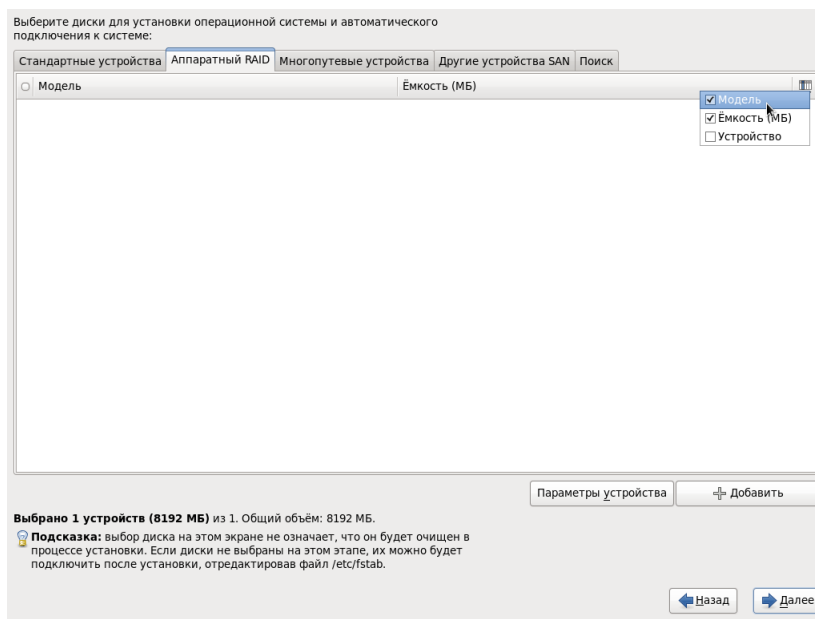


Рисунок 15

3.4 Многопутевая настройка

В системах с несколькими физическими путями к устройствам хранения используется пакет **multipath**.

Чтобы обеспечить сохранение постоянства LUN (адреса дискового устройства в сетях хранения) в среде multipath, необходимо присвоить псевдонимы многопутевым устройствам. Каждому устройству хранения соответствует UUID, который выполняет функции ключа для создаваемых имен. Определить UUID устройства можно с помощью команды `scsi_id`:

```
# scsi_id -g -s /block/sdc
```

Многопутевые устройства создаются в каталоге `/dev/mpath`.

Настройки многопутевых устройств хранятся в файле `/etc/multipath.conf`. Они содержат уникальные идентификаторы целевых устройств и пользовательские имена (alias), под которыми целевые устройства будут отображаться в системе.

В приведенном ниже примере будет определено 2 устройства в файле

/etc/multipath.conf:

```
multipaths {  
    multipath {  
        wwid          3600805f300159870000000000768a0019  
        alias         dvmp1  
    }  
    multipath {  
        wwid          3600805f300159870000000000d643001a  
        alias         dvmp2  
    }  
}
```

В результате будет создано два LUN с именами /dev/mpath/dvmp1, /dev/mpath/dvmp2. Теперь сопоставление идентификаторов именам будет сохраняться между перезагрузками.

При добавлении многопутевого устройства в список устройств, доступных для ROSA Enterprise Linux Server, система автоматически добавит выбранный тип устройства (iSCSI или FCoE) в список многопутевых устройств.

Для добавления многопутевого устройства откройте вкладку **Многопутевые устройства**.

На данной вкладке отображается список многопутевых устройств, которые имеются в системе. В таблице свойств многопутевых устройств можно вывести дополнительные сведения об этих устройствах, нажав небольшое раскрывающееся меню в правом верхнем углу таблицы.

Для поиска устройств вы можете воспользоваться фильтром по следующим параметрам устройства:

- Соединения
- Производитель
- Идентификатор

Чтобы выбрать многопутевые устройства из числа перечисленных в таблице устройств, установите флажки в первом поле таблицы рядом с именами выбираемых устройств.

Для добавления нового многопутевого устройства нажмите кнопку *Добавить*.

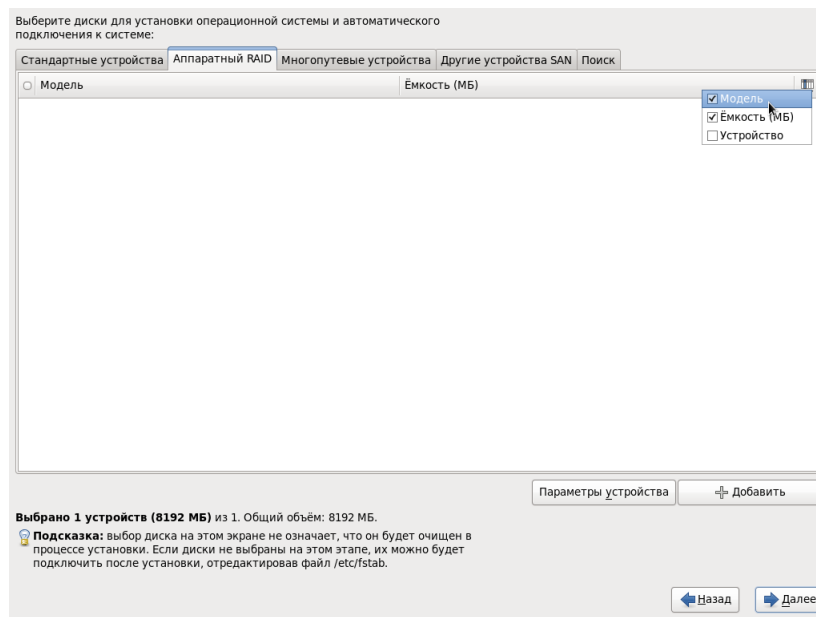


Рисунок 16

3.5 Добавление других устройств SAN

Вкладка **Другие устройства SAN** позволяет добавить устройства SAN (Storage Area Network) в список поддерживаемых устройств Rosa Linux Enterprise Server.

На данной вкладке отображается список устройств SAN, обнаруженных программой установки. В таблице свойств устройств SAN можно вывести дополнительные сведения об этих устройствах, нажав небольшое раскрывающееся меню в правом верхнем углу таблицы.

Для поиска устройств можно воспользоваться фильтром по следующим параметрам устройства:

- Соединения
- Производитель
- Идентификатор

Чтобы выбрать устройства SAN из числа перечисленных в таблице устройств, установите флажки в первом поле таблицы рядом с именами выбираемых устройств. Для добавления нового устройства SAN нажмите кнопку *Добавить*.

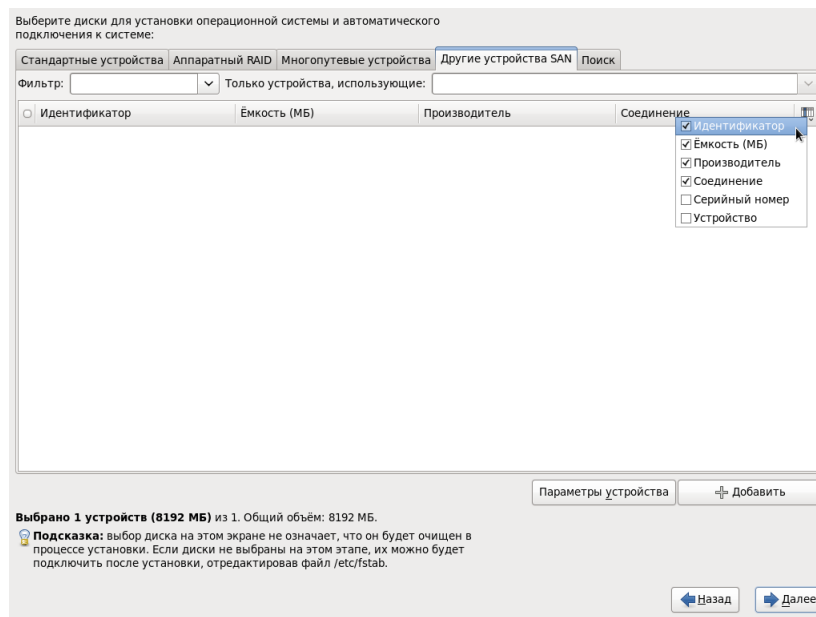


Рисунок 17

3.6 Поиск устройств хранения данных

Вкладка **Поиск** позволяет выполнить поиск доступных устройств хранения данных. Устройство можно искать по набору параметров: порт, целевой диск, LUN или по идентификатору целевого устройства. Чтобы выбрать набор параметров, используемых для поиска устройства, в поле со списком **Искать по** выберите значение **Порт / Целевое устройство / LUN** или **Идентификатор целевого устройства**.

Чтобы выбрать найденные устройства из числа перечисленных в таблице устройств, установите флажки в первом поле таблицы рядом с именами выбираемых устройств.

Для добавления нового устройства нажмите кнопку *Добавить*.

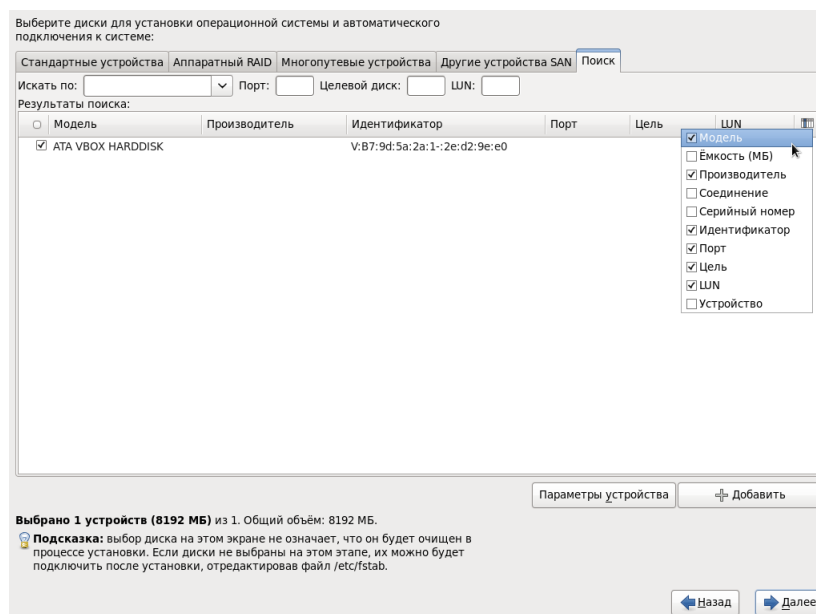


Рисунок 18

3.7 Сведения об устройствах хранения, имеющихся в системе

После добавления устройств хранения, данные об устройствах записываются в конфигурационный файл `fstab` (полный путь к нему: `/etc/fstab`). Этот файл содержит информацию обо всех разделах жесткого диска и других носителях информации в установленной системе. Для добавления устройств можно отредактировать этот файл, зарегистрировавшись в системе с правами пользователя `root`.

Файл `fstab` имеет следующую структуру: каждая строка файла содержит запись об устройстве, имеющемся в системе. Каждая запись включает в себя следующие поля, которые разделяются пробелом или табуляцией:

```
<file system> <dir> <type> <options> <dump> <pass>
```

- поле `<file system>` (файловая система) содержит имя монтируемого устройства;
- поле `<dir>` (каталог) определяет путь, по которому смонтирована файловая система;
- поле `<type>` (тип) содержит тип файловой системы монтируемого устройства;
- поле `<options>` содержит варианты монтирования файловой системы (значения в этом поле ограничиваются набором вариантов монтирования устройства: например, `auto`, `noauto`, `defaults`, `nodev` и др.);
- поле `<dump>` используется утилитой `dump` для того чтобы решить, когда делать резервную копию. Возможные значения поля — 0 и 1. Если 0, то `dump` игнорирует файловую систему, если 1, то `dump` сделает резервную копию. Для большинства разделов в данном поле записывается 0.
- поле `<pass>` (пропуск) используется утилитой `fsck`. Утилита `fsck` проверяет значение, записанное в поле `<pass>`, и решает, в каком порядке проверять файловую систему. Возможные значения 0, 1 и 2. Файловые системы со значением `<pass>`, равным 0, не будут проверены утилитой `fsck`. У корневой системы должен быть наибольший приоритет, 1, остальные файловые системы должны иметь приоритет 2.

3.8 Настройка параметров добавляемого устройства

При добавлении устройств возможно выбрать различные виды накопителей: накопители iSCSI или накопители FCoE SAN.

Чтобы добавить новое устройство, в окне выбора диска для установки операционной системы нажмите кнопку *Добавить*. При этом открывается окно **Доп. параметры накопителей**, которое позволяет задать параметры устройства для установки операционной системы.

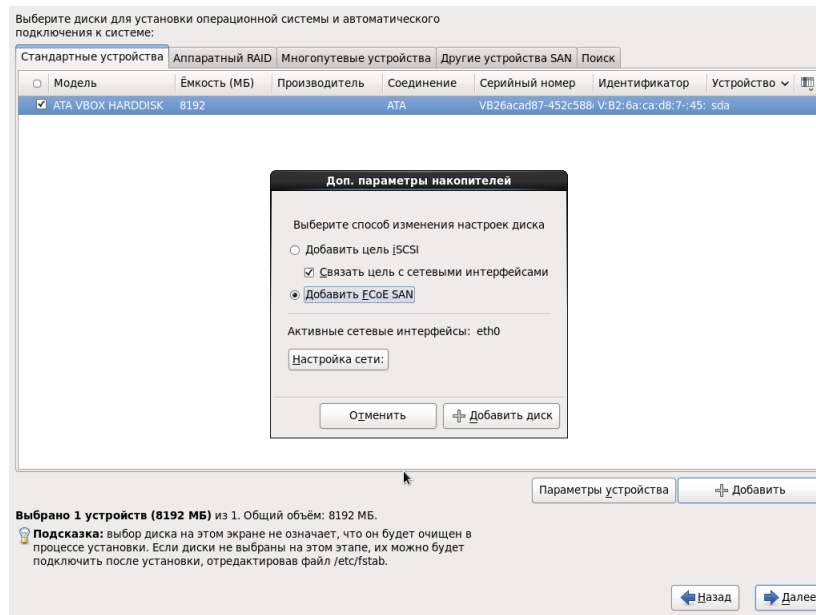


Рисунок 19

Настройка параметров iSCSI

Для настройки устройства iSCSI откройте окно параметров, выбрав в окне **Доп. Параметры накопителей** опцию **Добавить цель iSCSI**, затем нажмите **Добавить диск**.

Для того чтобы связать подключаемое устройство с сетевыми интерфейсами, установите флажок **Связать цель с сетевыми интерфейсами**.

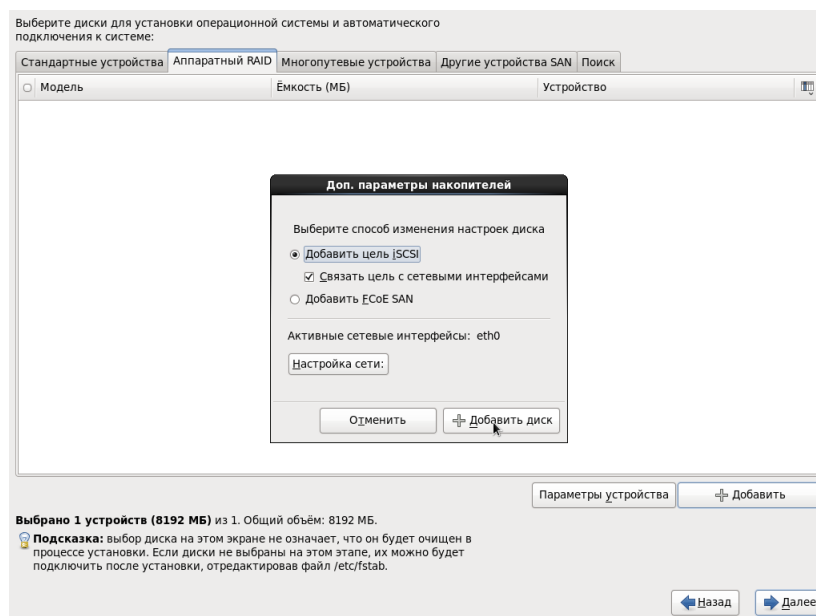


Рисунок 20

Введите адрес IP цели iSCSI и уникальное имя инициатора для идентификации системы и выберите режим аутентификации при подключении к этому устройству.

Можно выбрать один из следующих режимов аутентификации:

- **Без аутентификации** — в этом случае проверка подлинности инициатора iSCSI и

цели iSCSI выполняться не будет.

– **Пара CHAP** — в этом случае для обеспечения односторонней проверки подлинности будет использоваться протокол CHAP. С помощью этого метода цель iSCSI проверяет подлинность каждого инициатора iSCSI, но инициатор iSCSI не проверяет подлинность цели iSCSI.

– **Прямая и обратная пара CHAP** — в этом случае CHAP можно использовать для проверки подлинности цели iSCSI, которую выполняет инициатор iSCSI.

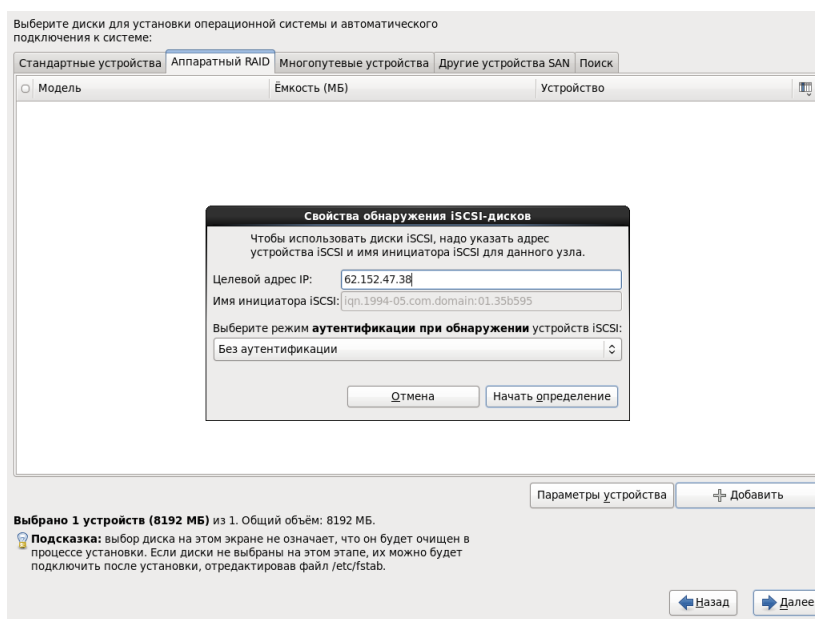


Рисунок 21

Если цель iSCSI для аутентификации использует протокол CHAP (Challenge Handshake Authentication Protocol), укажите имя пользователя и пароль CHAP.

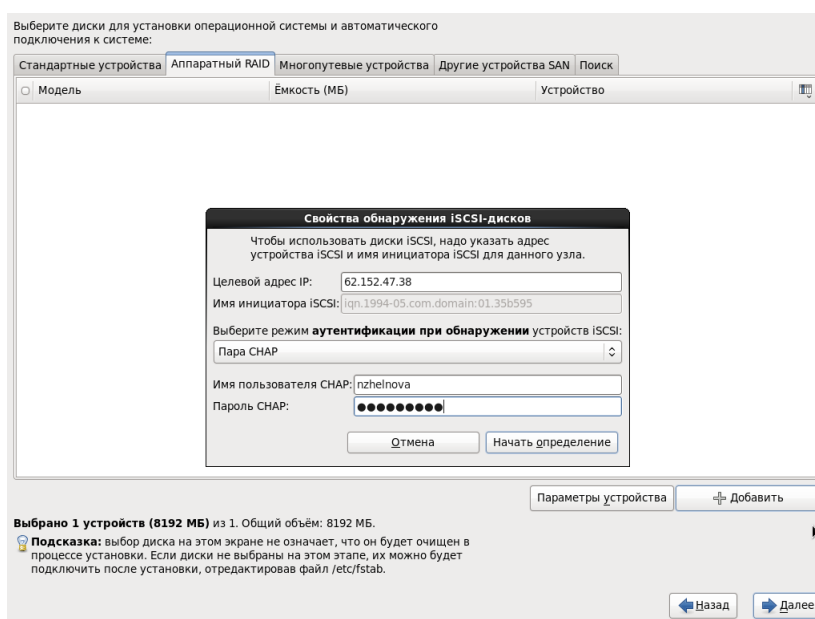


Рисунок 22

При использовании двухсторонней (иногда называется взаимной) аутентификации, CHAP введите имя пользователя и пароль CHAP, а также обратное имя пользователя и пароль.

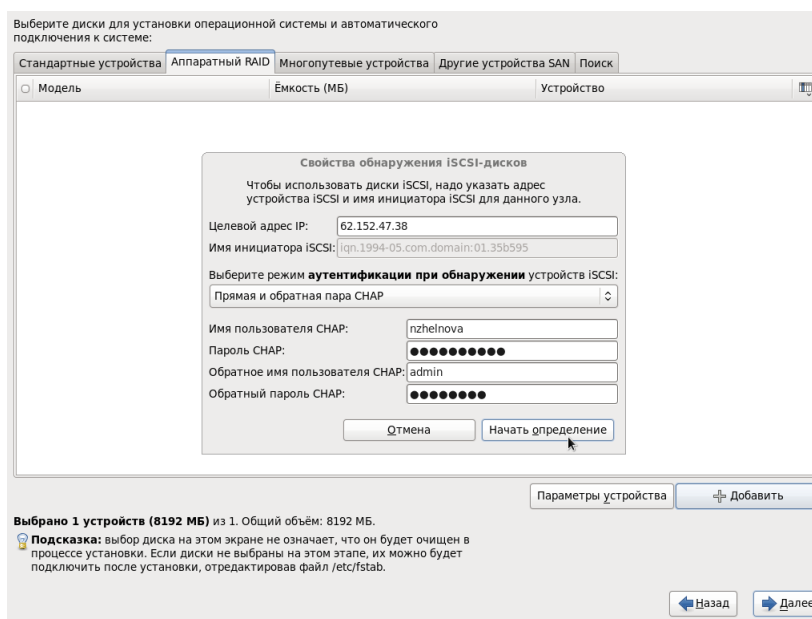


Рисунок 23

После этого нажмите кнопку *Начать определение* для поиска устройства выбранного типа на хосте с указанным IP-адресом. Если указанные устройства будут найдены, их можно будет выбрать и добавить их в список устройств, которые будут поддерживаться системой. Если система не обнаружит устройств указанного типа с заданным набором параметров, она выведет на экран соответствующее сообщение. В этом случае повторите процесс добавления устройства, указав корректные значения параметров.

Настройка параметров FCoE

Для настройки FCoE SAN выберите **Добавить FCoE SAN** и нажмите кнопку *Добавить диск*.

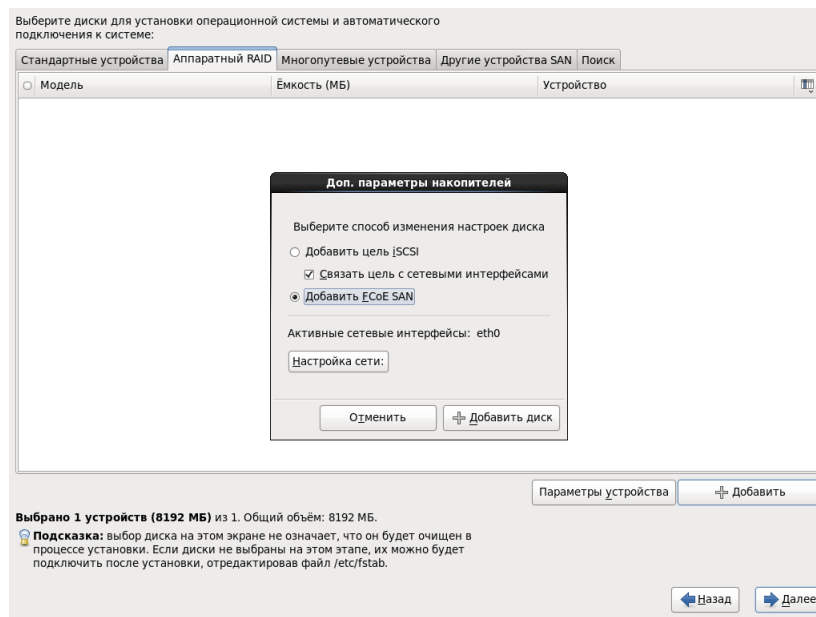


Рисунок 24

В следующем окне выберите интерфейс, подключенный к переключателю FCoE, и нажмите кнопку добавления дисков.

4 Настройка сетевых подключений

Рассматриваемые здесь параметры относятся к параметрам, общим для всех устанавливаемых системах на базе Linux. Они могут применяться для предварительной настройки сети, и их можно определить как в основном файле параметров, так и в файле конфигурации CMS. Другие параметры должны быть заданы в основном файле параметров.

Чтобы изменить настройки сетевых подключений, нажмите кнопку *Настройка сети*. При этом откроется окно сетевых соединений.

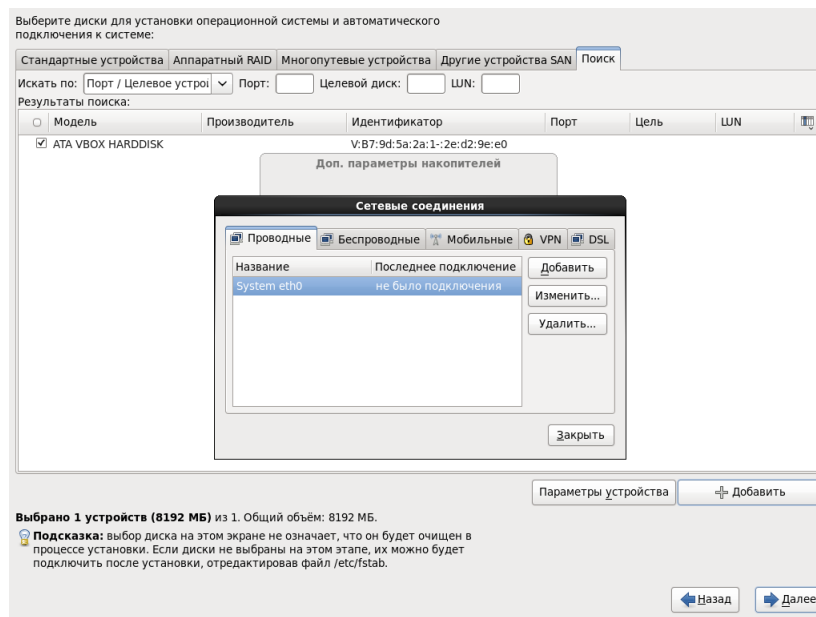


Рисунок 25

Возможно сконфигурировать сетевые соединения следующих типов:

- **Проводные** — обычные соединения по сети Ethernet;
- **Беспроводные** — соединения, использующие беспроводные точки доступа;
- **Мобильные** — соединения, использующие мобильные протоколы для доступа к сети;
- **VPN** — соединения, использующие виртуальные частные сети;
- **DSL** — соединения, использующие цифровые абонентские линии

4.1 Проводные соединения

В окне **Сетевые соединения** на вкладке **Проводные** перечислены уже имеющиеся проводные соединения. По умолчанию список содержит соединение, настроенное на первой стадии установки, а также соединение eth0 (OSA, LCS).

Чтобы добавить новое соединение, нажмите кнопку *Добавить*. Чтобы изменить существующее соединение, выберите его и нажмите кнопку *Изменить*. Появится окно с набором вкладок, о которых будет рассказано далее.

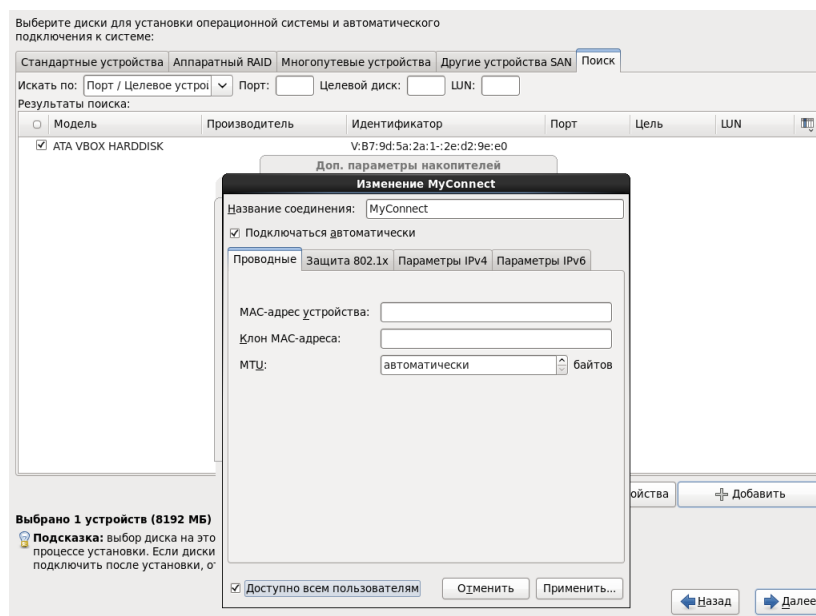


Рисунок 26

Общие параметры настройки проводных соединений

Вкладка **Проводные** окна настроек проводного соединения позволяет задать следующие параметры проводного соединения: MAC-адрес устройства, клон MAC-адреса (физический адрес оборудования, который используется при привязке провайдера к MAC-адресу устройства) и максимальный размер блока (в байтах) при передаче через интерфейс.

Защита 802.1x

Вкладка **Защита 802.1x** позволяет настроить контроль сетевого доступа в зависимости от порта. Для этого установите флажок **Использовать защиту 802.1X для этого соединения** и введите необходимые данные. Параметры настройки содержат следующие пункты:

Аутентификация — выбор метода аутентификации. Возможно выбрать один из следующих методов:

- **TLS** (Transport Layer Security);
- **FAST** — метод, использующий туннелирование для защиты сетевого трафика;
- **Туннельный TLS** – (TTLS или EAP-TTLS);
- **Защищенный EAP (PEAP)** (Protected Extensible Authentication Protocol).

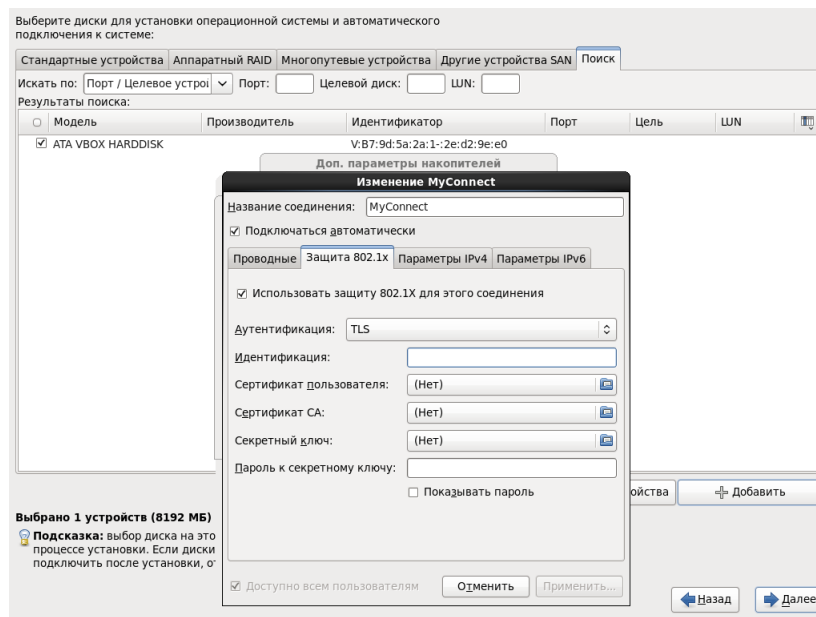


Рисунок 27

Для метода аутентификации TLS укажите значения следующих параметров:

- **Идентификация** — введите данные сервера;
- **Сертификат пользователя** — укажите путь к файлу сертификата X.509, закодированному с помощью правил DER (Distinguished Encoding Rules) или PEM (Privacy Enhanced Mail)
- **Сертификат CA** — укажите путь к файлу сертификата CA, закодированному с помощью правил DER (Distinguished Encoding Rules) или PEM (Privacy Enhanced Mail)
- **Секретный ключ** — укажите путь к файлу секретного ключа, закодированному с помощью правил DER (Distinguished Encoding Rules), PEM (Privacy Enhanced Mail) или PKCS#12 (Personal Information Exchange Syntax Standard).
- **Пароль к секретному ключу** — укажите пароль для ключа, указанного в поле **Секретный ключ**. Установите флажок **Показывать пароль**, чтобы видеть вводимый пароль.

Для метода аутентификации FAST укажите значения следующих параметров:

- **Анонимная идентификация** — введите имя компьютера для гостевой учетной записи;
- **Allow Automatic PAC Provisioning** — установите этот флажок, если необходимо выполнять автоматическое предоставление данных о пользователях при первоначальной ошибке аутентификации EAP-FAST и выберите, какие пользователи смогут проходить такую процедуру (**Anonymous / Authenticated / Both**);
- **PAC file** — укажите путь к PAC-файлу;

- **Внутренняя аутентификация** — укажите способ внутренней аутентификации пользователей (GTC / MSCHAPv2)
- **Имя пользователя** — укажите имя пользователя, используемое для аутентификации. Данное имя позволяет не вводить имя пользователя и пароль повторно: при аутентификации будут использоваться сохраненное имя пользователя и пароль;
- **Пароль** — введите пароль этого пользователя.

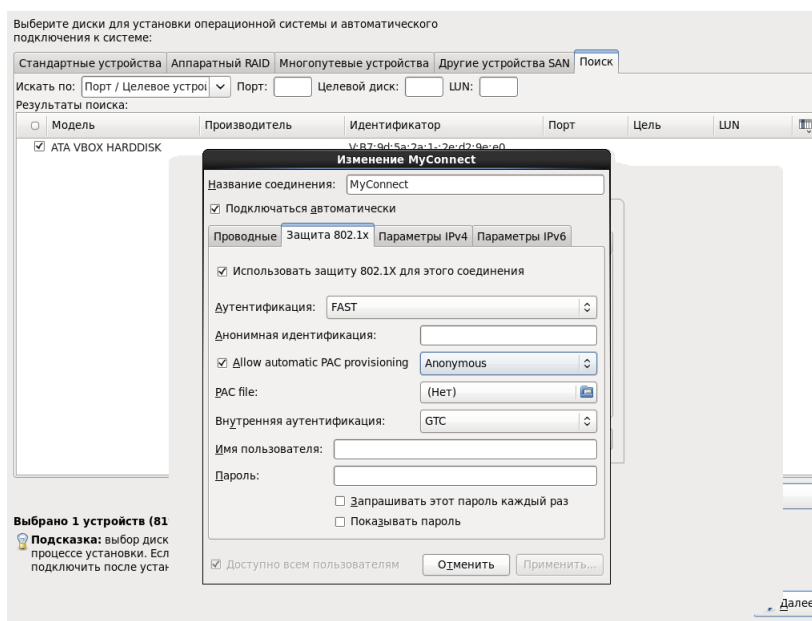


Рисунок 28

Для метода аутентификации **Туннельный TLS** укажите значения следующих параметров:

- **Анонимная идентификация** — введите имя компьютера для гостевой учетной записи;
- **Сертификат СА** — укажите путь к файлу сертификата СА, закодированному с помощью правил DER (Distinguished Encoding Rules) или PEM (Privacy Enhanced Mail)
- **Внутренняя аутентификация** — укажите способ внутренней аутентификации пользователей (GTC / MSCHAPv2)
- **Имя пользователя** — укажите имя пользователя, используемое для аутентификации. Данное имя позволяет вам не вводить имя пользователя и пароль повторно: при аутентификации будут использоваться сохраненное имя пользователя и пароль;
- **Пароль** — введите пароль этого пользователя.

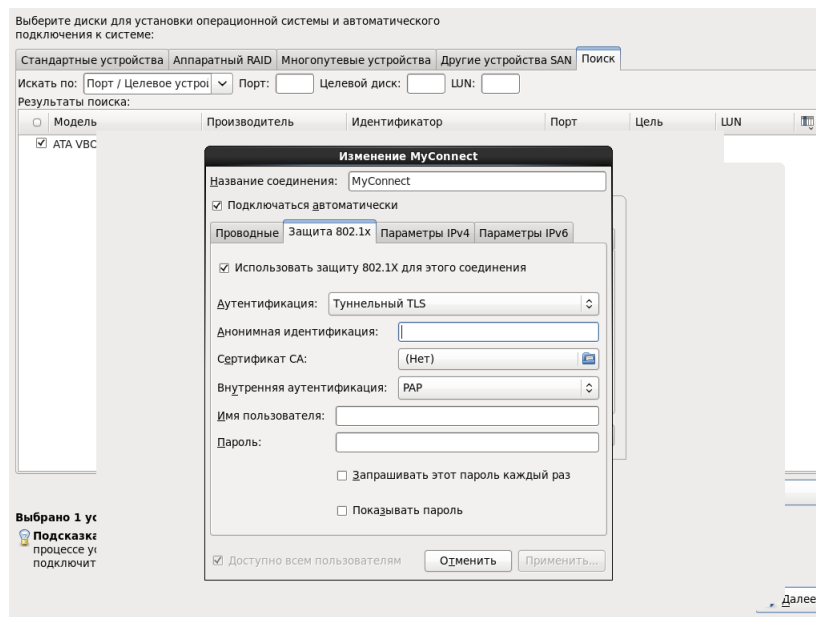


Рисунок 29

Для метода аутентификации **Защищенный EAP (PEAP)** укажите значения следующих параметров:

- **Анонимная идентификация** — введите имя компьютера для гостевой учетной записи;
- **Сертификат CA** — укажите путь к файлу сертификата CA, закодированному с помощью правил DER (Distinguished Encoding Rules) или PEM (Privacy Enhanced Mail);
- **Версия PEAP** — укажите, какая версия будет использоваться для аутентификации (по умолчанию выбрано значение, позволяющее определять версию автоматически);
- **Внутренняя аутентификация** — выберите способ внутренней аутентификации (MSCHAPv2 / MD5 / GTC);
- **Имя пользователя** — укажите имя пользователя, используемое для аутентификации. Данное имя позволяет вам не вводить имя пользователя и пароль повторно: при аутентификации будут использоваться сохраненное имя пользователя и пароль;
- **Пароль** — введите пароль этого пользователя.

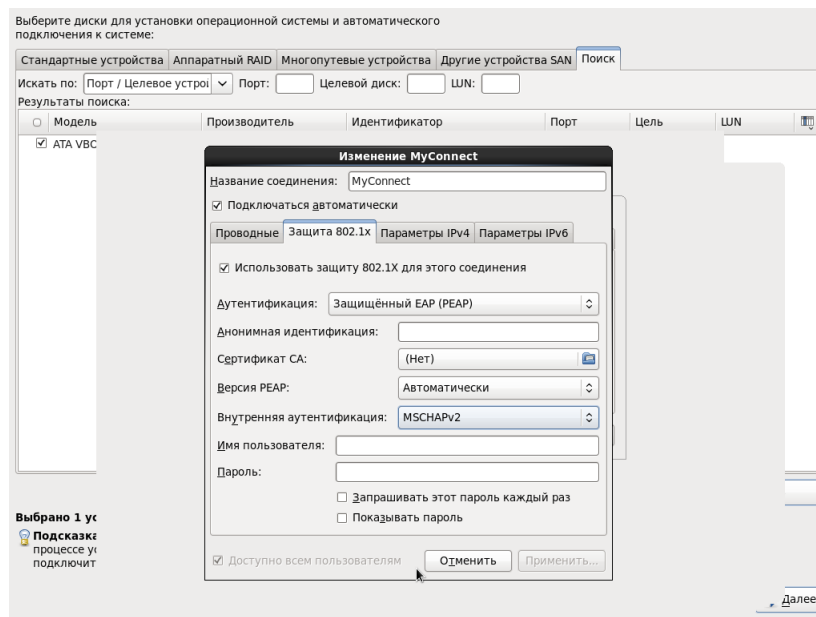


Рисунок 30

Параметры IPv4 Вкладка **Параметры IPv4** позволяет определить настройки соединения, использующего протокол IPv4: адрес, маска сети, шлюз, серверы DNS и суффикс поиска DNS.

В таблице **Адреса** данной вкладки указываются существующие адреса, маска сети и шлюзы, настроенные для данного соединения. Можно изменить эти данные, выбрав один из профилей настройки параметров IPv4.

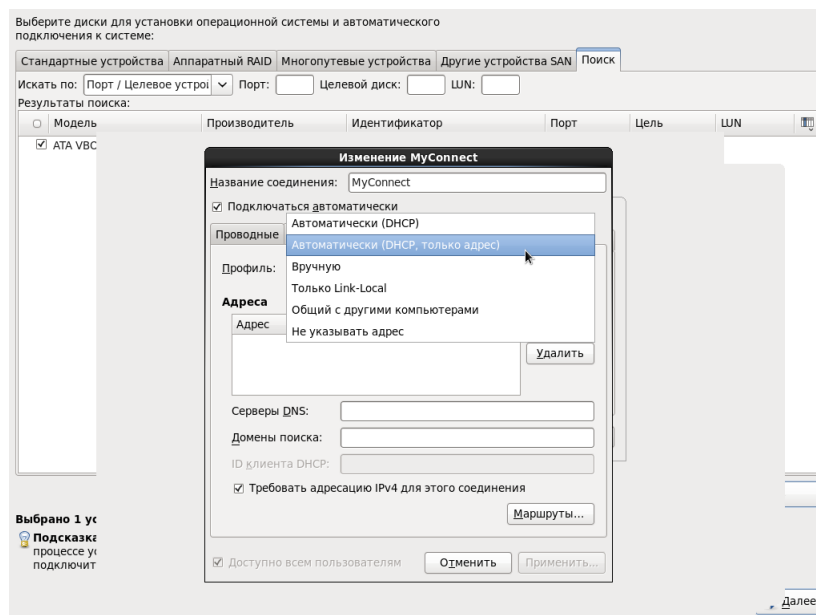


Рисунок 31

В поле со списком **Профиль** выберите настройки, которые определяются службой DHCP. Можно выбрать один из следующих вариантов:

- **Автоматически (DHCP)** — параметры IPv4 определяются службой DHCP;

– **Автоматически (DHCP, только адрес)** — адрес IPv4, маска сети и адрес шлюза настраиваются службой DHCP, но серверы имен и домены поиска должны быть настроены вручную;

– **Вручную** — параметры IPv4 для статической конфигурации определяются вручную;

– **Только Link-Local** — интерфейсу будет назначен локальный адрес в диапазоне 169.254/16.

– **Общий с другими компьютерами** — в этом случае система будет предоставлять доступ к сети для других компьютеров. Интерфейсу будет назначен адрес в диапазоне 10.42.x.1/24. Серверы DHCP и DNS будут запущены, а при подключении интерфейса к системе с NAT (Network Address Translation) будут использоваться настройки по умолчанию;

– **Игнорировать (Не указывать адрес)** — IPv4 отключен.

Для профиля **Автоматически (DHCP)** возможно только указать ID клиента DHCP и настроить маршруты IPv4 для данного проводного соединения.

В качестве параметра ID клиента DHCP укажите имя сетевого соединения (в качестве данного значения можно использовать MAC-адрес клиентского хоста). Значение должно быть уникально в пределах подсети.

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*.

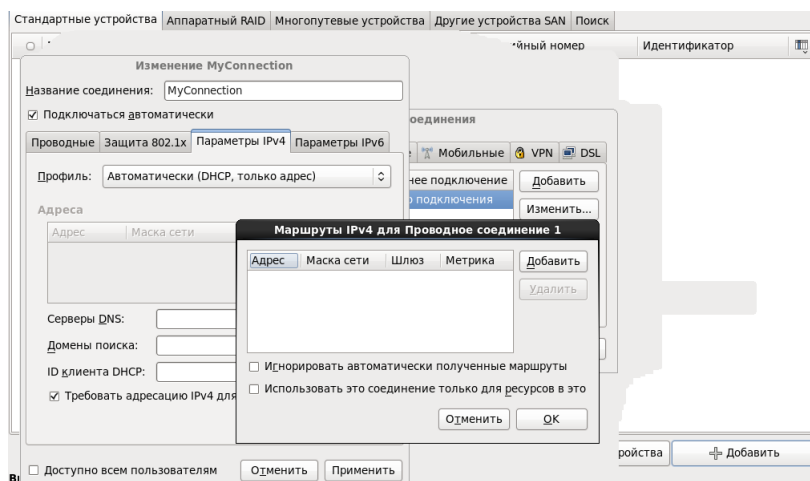


Рисунок 32

Далее в окне настройки маршрутов IPv4 выполните следующие действия:

– Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.

– Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.

– Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv4 для этого соединения**, чтобы разрешить это соединение в сети IPv6. Этот вариант используется в случаях, если настройка IPv4 завершилась неудачей, а настройка IPv6 удалась.

Для профиля **Автоматически (DHCP, только адрес)** можно указать следующие параметры:

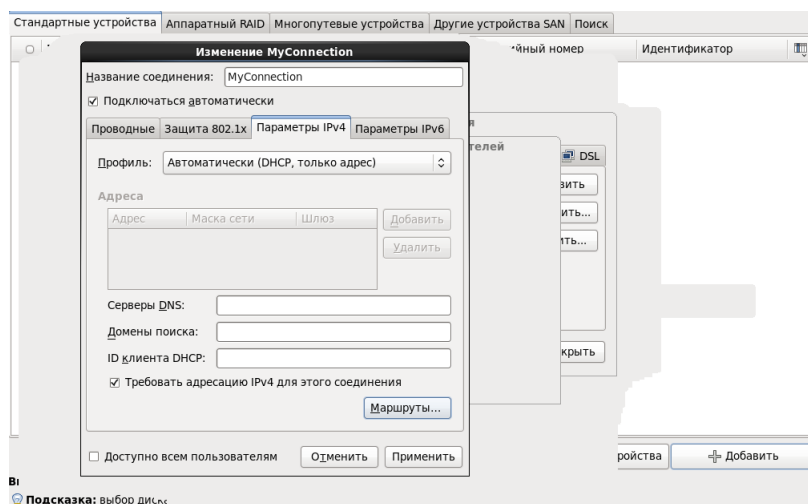


Рисунок 33

- **Серверы DNS** — введите список серверов DNS, разделив их запятой;
- **Домены поиска** — перечислите домены, которые будут участвовать в поиске сервера имен;
- **ID клиента DHCP** — укажите имя сетевого соединения (в качестве данного значения можно использовать MAC-адрес клиентского хоста). Значение должно быть уникально в пределах подсети.

Настройка маршрутов IPv4 для этого профиля выполняется аналогично настройке маршрутов IPv4 для профиля Автоматически (DHCP):

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*. Затем в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, что-

бы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv4 для этого соединения**, чтобы разрешить это соединение в сети IPv6. Этот вариант используется в случаях, если настройка IPv4 завершилась неудачей, а настройка IPv6 удалась.

Для профиля **Вручную** можно указать следующие параметры:

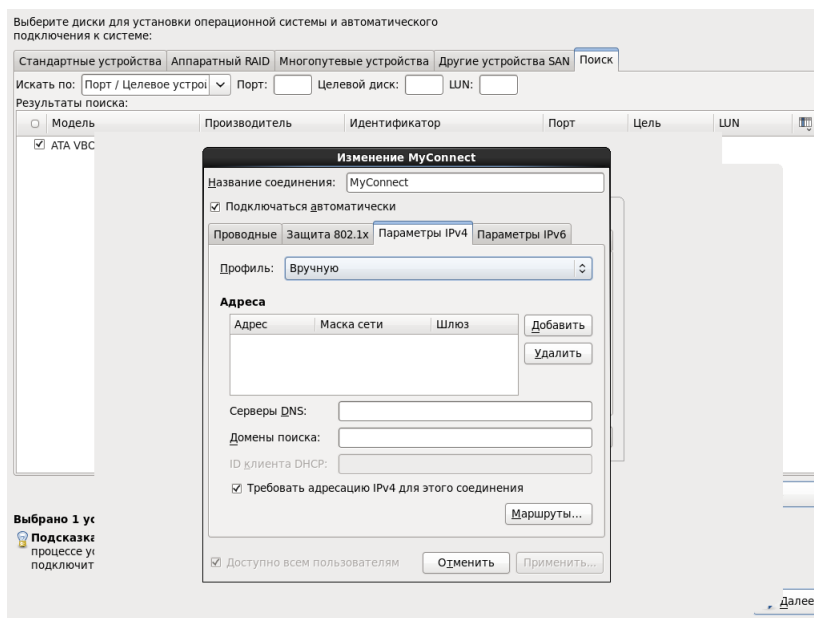


Рисунок 34

- IP-адрес интерфейса;
- Маску сети;
- Шлюз сети;
- Серверы DNS — введите список серверов, разделив их запятой;
- Домены поиска — перечислите домены, которые будут участвовать в поиске сервера имен.

Настройка маршрутов IPv4 для этого профиля выполняется аналогично настройке маршрутов IPv4 для профиля Автоматически (DHCP).

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*. Затем в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.

– Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv4 для этого соединения**, чтобы разрешить это соединение в сети IPv6. Этот вариант используется в случаях, если настройка IPv4 завершилась неудачей, а настройка IPv6 удалась.

Для профилей **Только Link-Local** и **Общий с другими компьютерами** возможно только настроить маршруты IPv4 для данного проводного соединения. Настройки маршрутов IPv4 для этих профилей выполняются аналогично настройке маршрутов IPv4 для профиля Автоматически (DHCP).

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*. Затем в окне настройки маршрутов IPv4 выполните следующие действия:

– Нажмите *Добавить*, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.

– Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.

– Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv4 для этого соединения**, чтобы разрешить это соединение в сети IPv6. Этот вариант используется в случаях, если настройка IPv4 завершилась неудачей, а настройка IPv6 удалась.

Параметры IPv6

На вкладке **Параметры IPv6** можно изменить настройки IPv6 для выбранного соединения.

Вкладка **Параметры IPv6** позволяет определить настройки соединения, использующего протокол IPv6: адрес, префикс сети, шлюз, серверы DNS и суффикс поиска DNS.

В таблице **Адреса** данной вкладки указываются существующие адреса, префиксы сети и шлюзы, настроенные для данного соединения. Вы можете изменить эти данные, выбрав один из профилей настройки параметров IPv6.

В поле со списком **Профиль** выберите настройки, которые будут определяться службой DHCP.

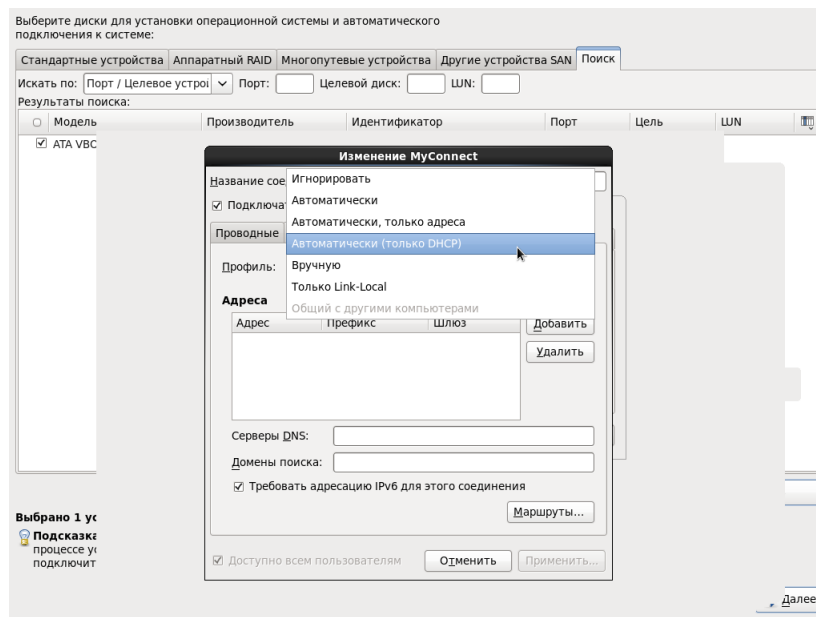


Рисунок 35

- **Игнорировать** — игнорировать IPv6 для заданного соединения
- **Автоматически** — параметры IPv6 определяются службой DHCP.
- **Автоматически, только адреса** — адрес IPv6, префикс и адрес шлюза настраиваются службой DHCP, но серверы DNS и домены поиска должны быть настроены вручную.
- **Вручную** — параметры IPv6 для статической конфигурации определяются вручную.
- **Только Link-Local** — интерфейсу будет назначен локальный адрес с префиксом `fe80::/10`.

Для профиля **Автоматически** или **Автоматически (только DHCP)** возможно только настроить маршруты IPv6 для данного проводного соединения.

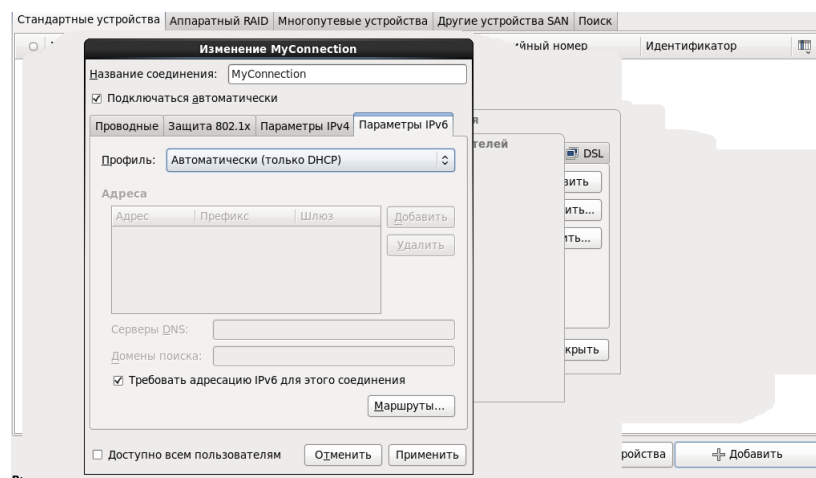


Рисунок 36

Для того чтобы настроить маршруты IPv6 для данного проводного соединения, нажмите кнопку *Маршруты*.

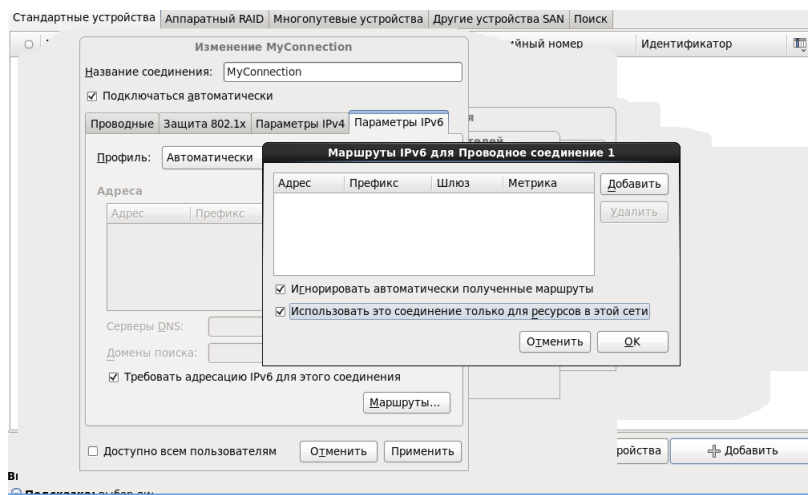


Рисунок 37

Далее в окне настройки маршрутов IPv6 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, префикс, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv6 для этого соединения**, чтобы разрешить это соединение в сети IPv4. Этот вариант используется в случаях, если настройка IPv6 завершилась неудачей, а настройка IPv4 удалась.

Для профиля **Автоматически**, только адреса возможно указать следующие параметры:

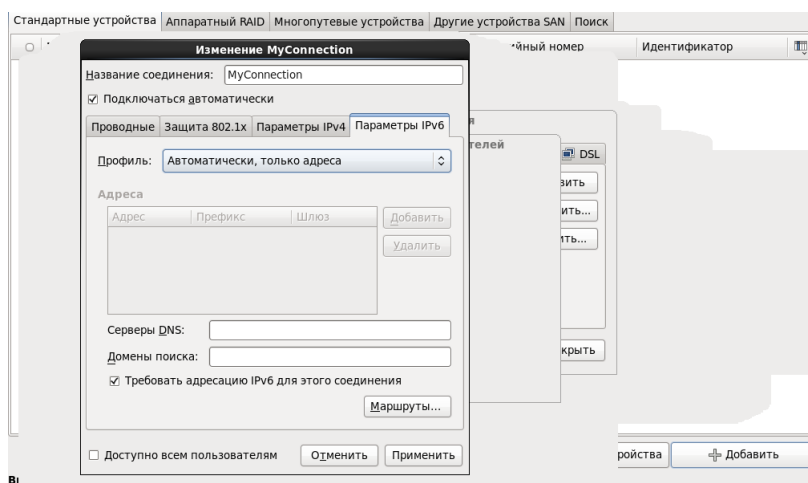


Рисунок 38

- **Серверы DNS** — введите список серверов DNS, разделив их запятой;

– **Домены поиска** – перечислите домены, которые будут участвовать в поиске сервера имен.

Настройка маршрутов IPv6 для этого профиля выполняется аналогично настройке маршрутов IPv6 для профиля **Автоматически (DHCP)**.

Для того чтобы настроить маршруты IPv6 для данного проводного соединения, нажмите кнопку *Маршруты*. Затем в окне настройки маршрутов IPv6 выполните следующие действия:

– Нажмите **Добавить**, чтобы добавить IP-адрес, префикс, адрес шлюза и метрику для нового статического маршрута.

– Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.

– Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv6 для этого соединения**, чтобы разрешить это соединение в сети IPv4. Этот вариант используется в случаях, если настройка IPv6 завершилась неудачей, а настройка IPv4 удалась.

Для профиля **Вручную** можно задать значение следующих параметров соединения:

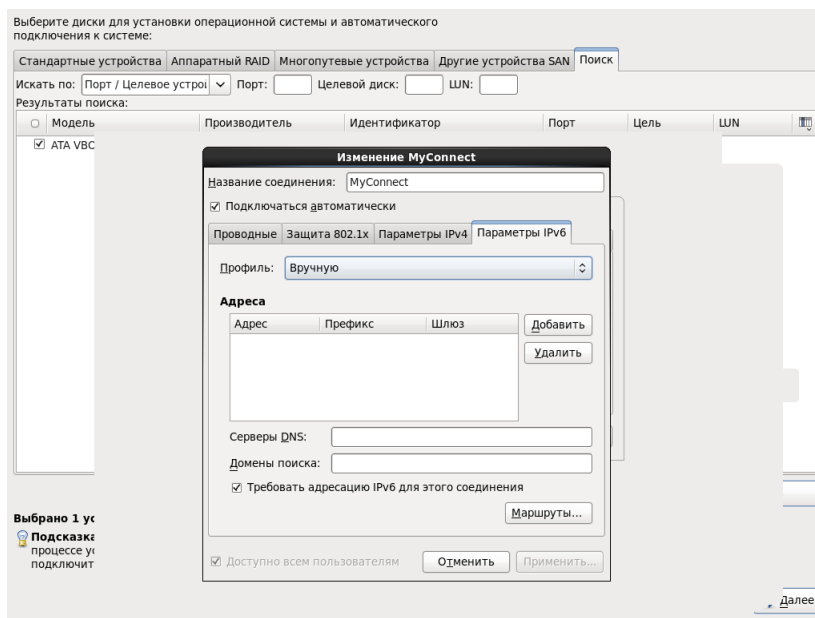


Рисунок 39

– **Серверы DNS** — введите список серверов DNS, разделив их запятой;

– **Домены поиска** — перечислите домены, которые будут участвовать в поиске сервера имен.

Настройка маршрутов IPv6 для этого профиля выполняется аналогично настройке

маршрутов IPv6 для профиля **Автоматически (DHCP)**.

Для того чтобы настроить маршруты IPv6 для данного проводного соединения, нажмите кнопку *Маршруты*. Затем в окне настройки маршрутов IPv6 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, префикс, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Отмените выбор **Требовать адресацию IPv6 для этого соединения**, чтобы разрешить это соединение в сети IPv4. Этот вариант используется в случаях, если настройка IPv6 завершилась неудачей, а настройка IPv4 удалась.

Для профиля **Только Link-Local** можно выполнить только настройку маршрутов для данного проводного соединения.

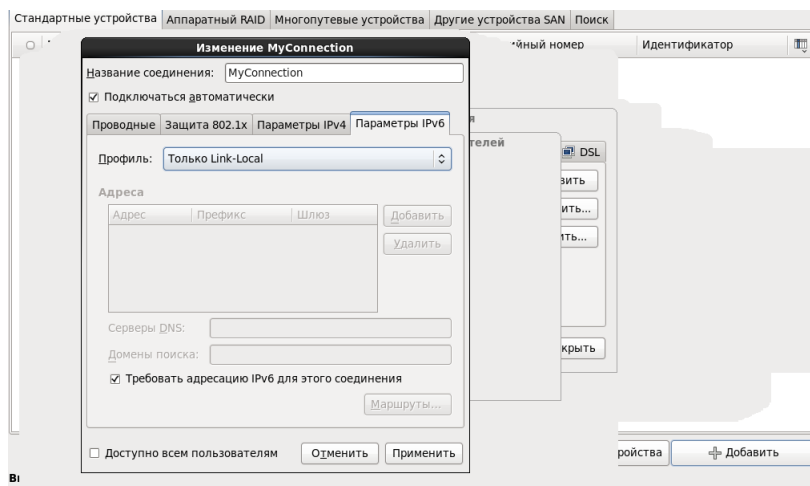


Рисунок 40

Отмените выбор **Требовать адресацию IPv6 для этого соединения**, чтобы разрешить это соединение в сети IPv4. Этот вариант используется в случаях, если настройка IPv6 завершилась неудачей, а настройка IPv4 удалась.

4.2 Беспроводные соединения

В окне **Сетевые соединения** на вкладке **Беспроводные** перечислены уже имеющиеся беспроводные соединения. Если ни одно беспроводное соединение не было настроено, данный список будет пуст.

Чтобы добавить новое соединение, нажмите кнопку *Добавить*. Чтобы изменить существующее соединение, выберите его и нажмите кнопку *Изменить*. Появится окно с набором вкладок, о которых будет рассказано далее.

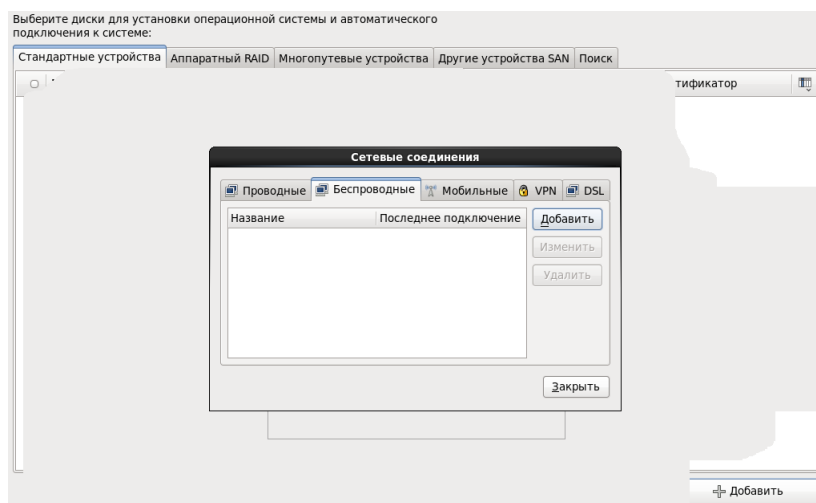


Рисунок 41

Общие параметры настройки беспроводного соединения

Вкладка **Беспроводные** окна настроек проводного соединения позволяет задать следующие параметры проводного соединения: сеть (идентификатор SSID, или имя сети), режим точки доступа, BSSID (MAC-адрес точки доступа, к которой вы подключаетесь), MAC-адрес устройства, клон MAC-адреса (физический адрес оборудования, который используется при привязке провайдера к MAC-адресу устройства) и максимальный размер блока (в байтах) при передаче через интерфейс.

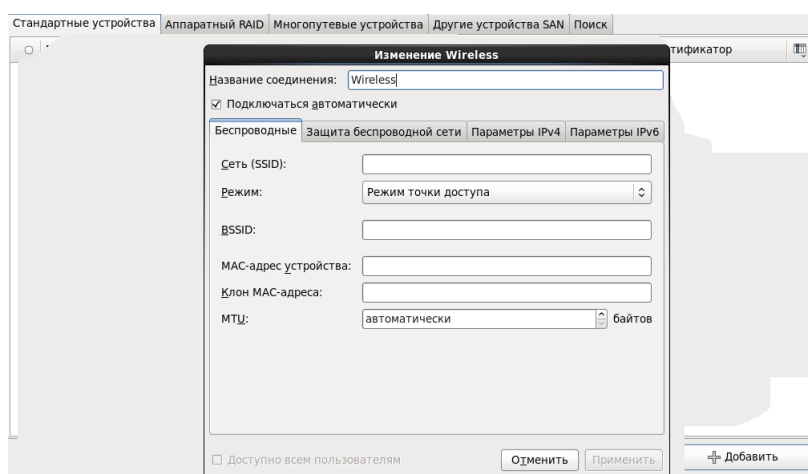


Рисунок 42

Защита беспроводной сети

Вкладка **Защита беспроводной сети** позволяет указать метод защиты беспроводной сети, к которой вы подключаетесь.

В поле со списком **Защита** выберите метод защиты, используемый вашей беспроводной сетью.

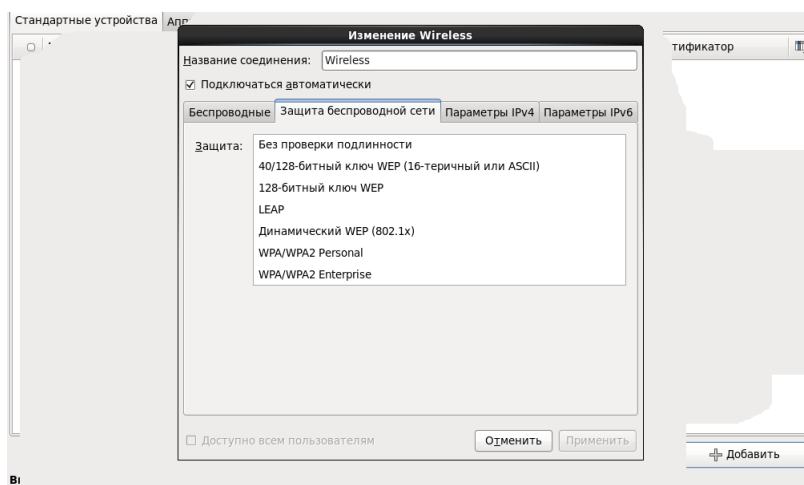


Рисунок 43

Параметры IPv4

Вкладка **Параметры IPv4** позволяет определить настройки соединения, использующего протокол IPv4: адрес, маска сети, шлюз, серверы DNS и суффикс поиска DNS.

Настройка параметров IPv4 для беспроводных соединений полностью аналогична настройке параметров IPv4 для проводных соединений (см. раздел «Проводные соединения - Параметры IPv4»).

Параметры IPv6

На вкладке **Параметры IPv6** можно изменить настройки IPv6 для выбранного соединения.

Вкладка **Параметры IPv6** позволяет определить настройки соединения, использующего протокол IPv6: адрес, префикс сети, шлюз, серверы DNS и суффикс поиска DNS.

Настройка параметров IPv6 для беспроводных соединений полностью аналогична настройке параметров IPv6 для проводных соединений (см. раздел «Проводные соединения - Параметры IPv6»).

4.3 Мобильные соединения

В окне **Сетевые соединения** на вкладке **Мобильные** перечислены уже имеющиеся мобильные соединения. Если ни одно мобильное соединение не было настроено, данный список будет пуст.

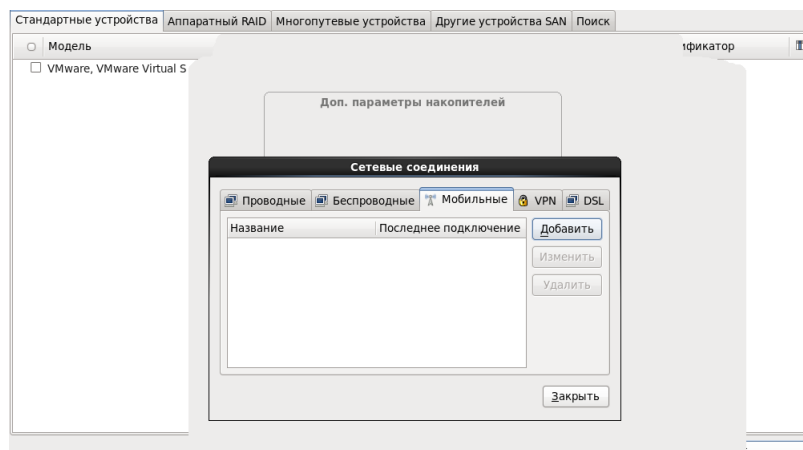


Рисунок 44

Чтобы добавить новое соединение, нажмите кнопку *Добавить*. Чтобы изменить существующее соединение, выберите его и нажмите кнопку *Изменить*. Появится окно выбора типа сотовой связи для данного соединения.

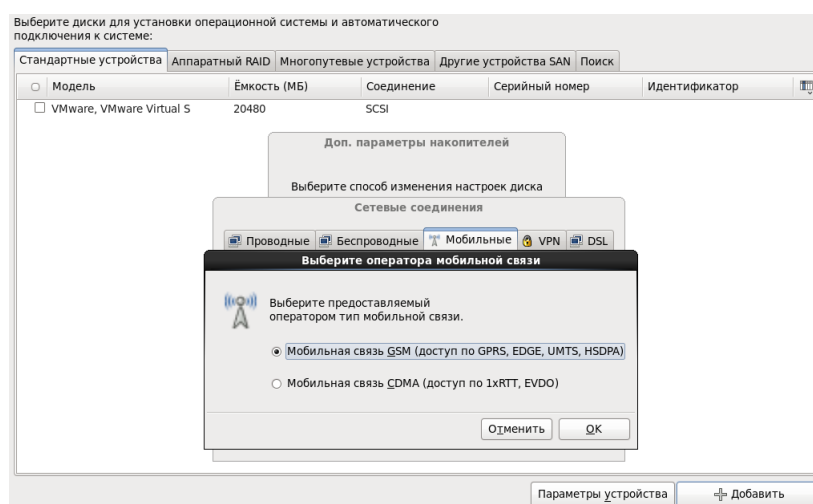


Рисунок 45

Можно выбрать используемый для данного соединения тип мобильной связи: GSM или CDMA. Параметры настройки мобильного соединения зависят от типа выбранной связи.

Настройки мобильной связи GSM

Вкладка **Мобильные** настроек мобильной связи GSM позволяет задать основные и дополнительные параметры связи.

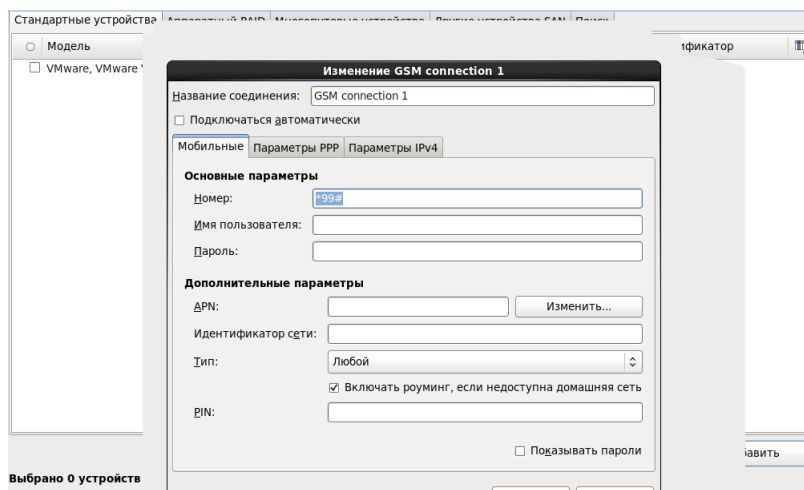


Рисунок 46

В группе **Основные параметры** укажите следующие данные о GSM-связи, используемой для данного соединения:

- **Номер** — номер, используемый для соединения, вместе с кодом выхода на линию;
- **Имя пользователя** — имя пользователя для GSM-канала мобильной сети передачи данных;
- **Пароль** — пароль пользователя мобильной сети передачи данных

В группе **Дополнительные** укажите следующие данные о GSM-связи, используемой для данного соединения:

- **APN (Access Point Name)** — имя точки доступа, шлюз из мобильной сети передачи данных, через который осуществляется доступ к услугам передачи данных
- **Идентификатор сети** — идентификатор (имя) сети передачи данных;
- **Тип** — тип сети (выберите один из вариантов: любой, 3G, 2G, предпочитать 3G, предпочитать 2G)
- **PIN** (Personal Identification Number, личный опознавательный номер) — PIN-код для доступа к мобильной сети передачи данных

Установите флажок **Включать роуминг**, если недоступна домашняя сеть, если вы хотите использовать услуги роуминга для данного соединения.

Параметры PPP

Вкладка **Параметры PPP** позволяет выбрать параметры подключений по протоколу PPP: выбрать методы аутентификации, выбрать параметры шифрования MMPE, определить, будет ли использоваться сжатие данных, а также разрешить или запретить посылать эхо-пакеты PPP.

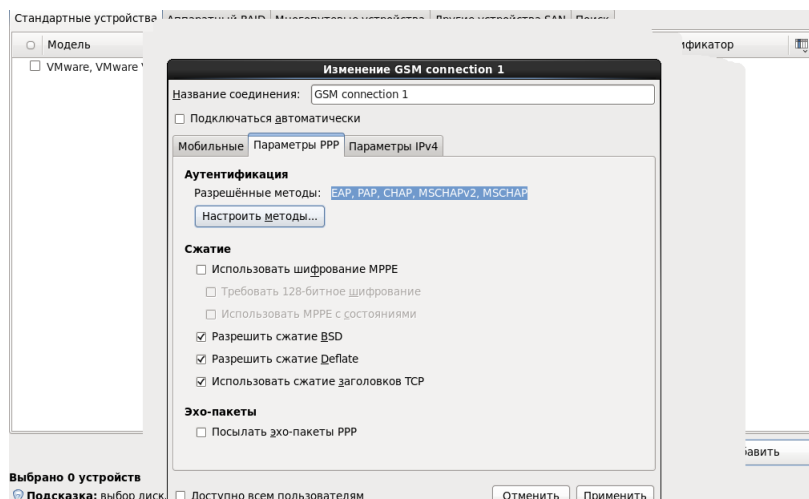


Рисунок 47

Параметры IPv4

Вкладка **Параметры IPv4** позволяет определить настройки соединения, использующего протокол IPv4: серверы DNS и домены поиска DNS.

В таблице **Адреса** данной вкладки указываются существующие адреса, маска сети и шлюзы, настроенные для данного соединения. Изменить эти данные можно, выбрав один из профилей настройки параметров IPv4.

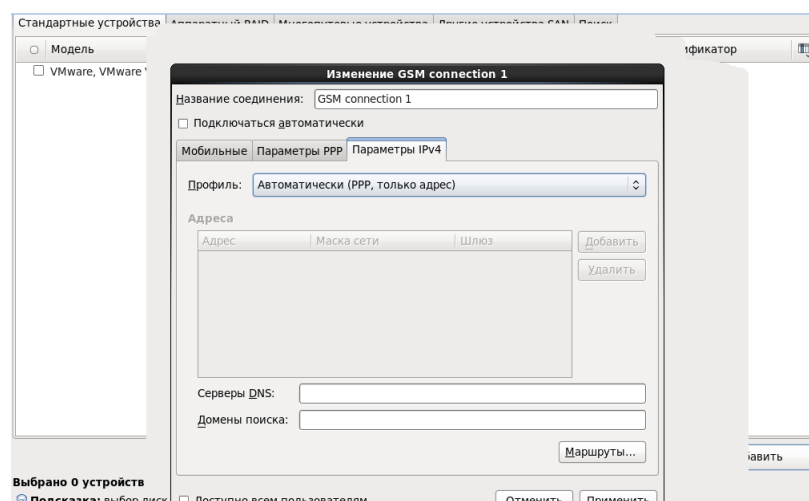


Рисунок 48

В поле со списком **Профиль** выберите настройки, которые определяются службой DHCP. Можно выбрать один из следующих вариантов:

- **Автоматически (PPP)** – параметры IPv4 задаются автоматически, для соединения используется протокол PPP (настройки протокола PPP рассматривались в разделе «Настройки мобильной связи GSM – Параметры PPP»);
- **Автоматически (PPP, только адрес)** – адрес IPv4, маска сети и адрес шлюза настраиваются автоматически, но серверы имен и домены поиска должны быть настроены вручную

Для профиля **Автоматически (PPP)** возможно только настроить маршруты IPv4 для данного проводного соединения, нажав кнопку *Маршруты*.

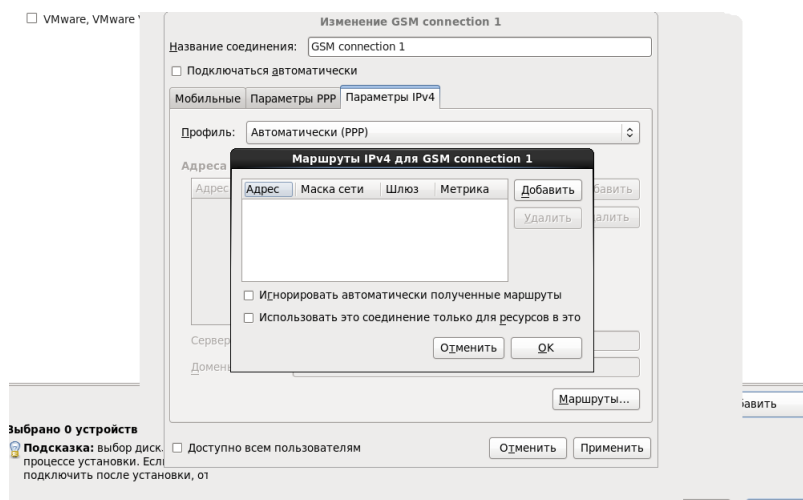


Рисунок 49

Далее в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Для профиля **Автоматически (PPP, только адрес)** укажите следующие параметры:

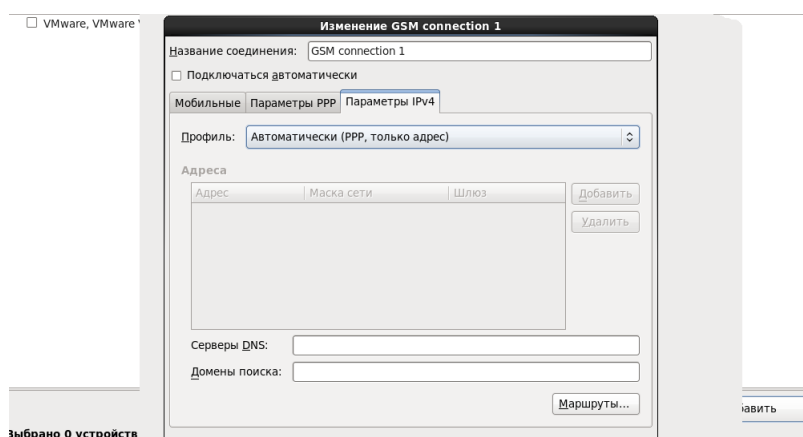


Рисунок 50

- **Серверы DNS** — введите список серверов DNS, разделив их запятой;
- **Домены поиска** — перечислите домены, которые будут участвовать в поиске сервера имен.

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*.

Далее в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Настройки мобильной связи CDMA

Вкладка **Мобильные** настроек мобильной связи CDMA позволяет задать параметры связи этого типа:

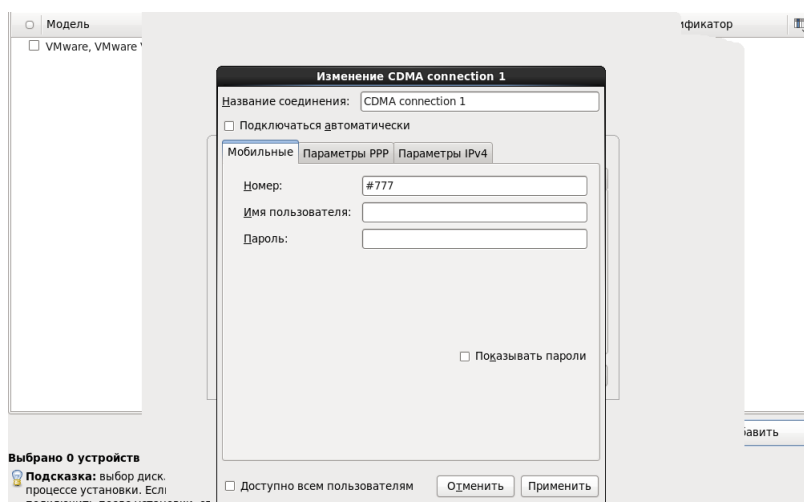


Рисунок 51

Параметры PPP

Вкладка **Параметры PPP** позволяет выбрать параметры подключений по протоколу PPP: выбрать методы аутентификации, выбрать параметры шифрования MMPE, определить, будет ли использоваться сжатие данных, а также разрешить или запретить посылать эхо-пакеты PPP.

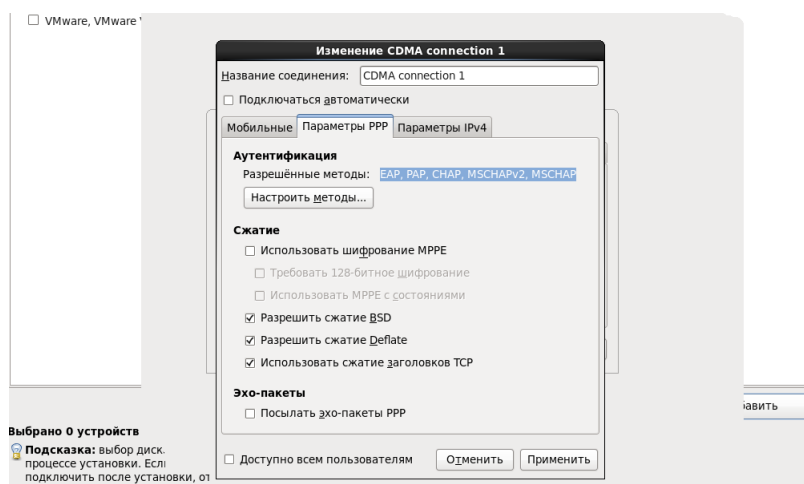


Рисунок 52

Параметры IPv4

Настройка параметров IPv4 для CDMA-соединения полностью аналогична процедуре настройки параметров IPv4 для GSM-соединения (см. раздел «Настройки мобильной связи GSM – Параметры IPv4»)

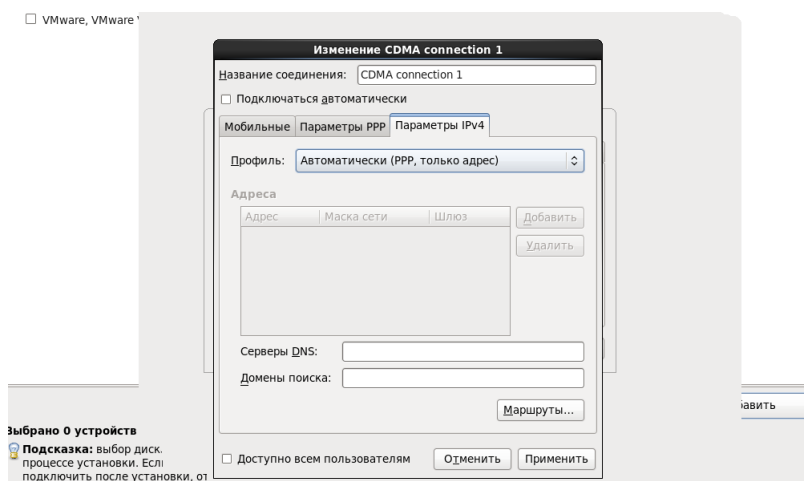


Рисунок 53

4.4 DSL-соединения

В окне **Сетевые соединения** на вкладке **DSL** перечислены уже имеющиеся DSL-соединения. Если ни одно DSL-соединение не было настроено, данный список будет пуст.

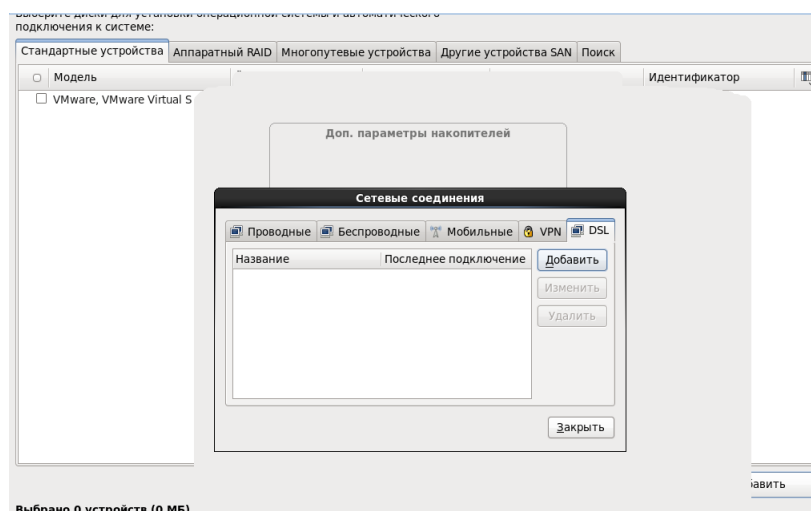


Рисунок 54

Чтобы добавить новое соединение, нажмите кнопку *Добавить*. Чтобы изменить существующее соединение, выберите его и нажмите кнопку *Изменить*. Появится окно со вкладками параметров для данного соединения.

Общие параметры настройки DSL-соединений

Вкладка **DSL** окна настроек DSL-соединения позволяет задать следующие параметры проводного соединения: имя пользователя, имя службы, пароль.

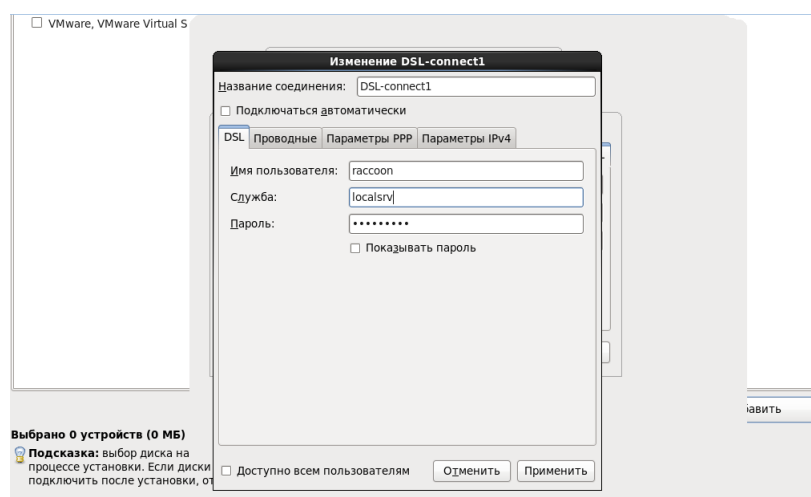


Рисунок 55

Проводные соединения

На вкладке **Проводные** можно задать параметры проводного DSL-соединения: MAC-адрес устройства, клон MAC-адреса (физический адрес оборудования, который используется при привязке провайдера к MAC-адресу устройства) и максимальный размер блока (в байтах) при передаче через интерфейс.

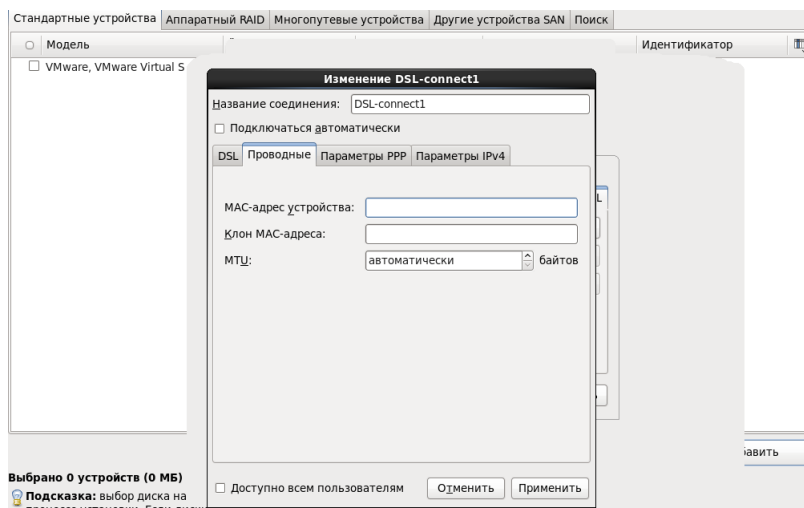


Рисунок 56

Параметры PPP

Вкладка **Параметры PPP** позволяет выбрать параметры подключений по протоколу PPP: выбрать методы аутентификации, выбрать параметры шифрования MPPE, определить, будет ли использоваться сжатие данных, а также разрешить или запретить посылать эхо-пакеты PPP.

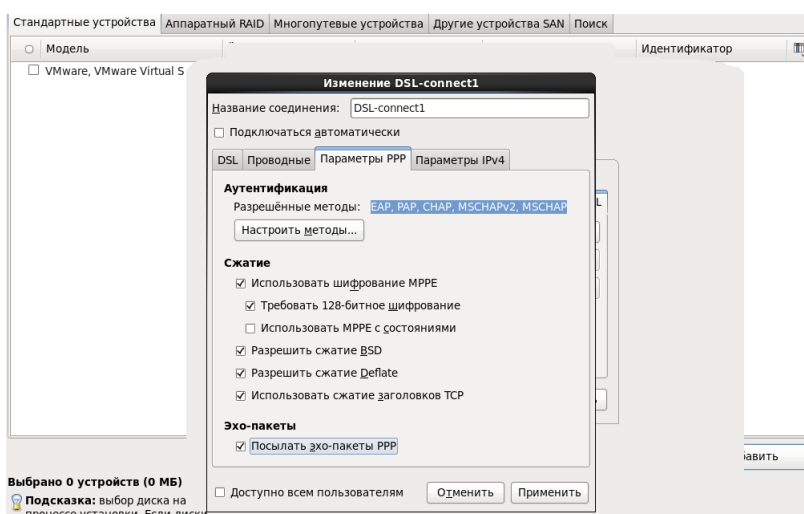


Рисунок 57

Параметры IPv4

Вкладка **Параметры IPv4** позволяет определить настройки соединения, использующего протокол IPv4: адрес, маска сети, шлюз, серверы DNS и домены поиска DNS.

В таблице **Адреса** данной вкладки указываются существующие адреса, маска сети и шлюзы, настроенные для данного соединения. Изменить эти данные можно, выбрав один из профилей настройки параметров IPv4.

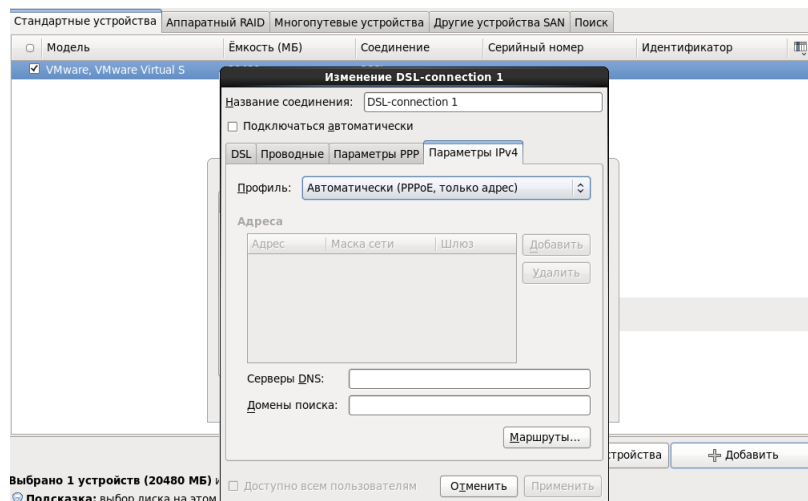


Рисунок 58

- **Серверы DNS** — введите список серверов DNS, разделив их запятой;
- **Домены поиска** — перечислите домены, которые будут участвовать в поиске сервера имен.

Для того чтобы настроить маршруты IPv4 для данного проводного соединения, нажмите кнопку *Маршруты*.

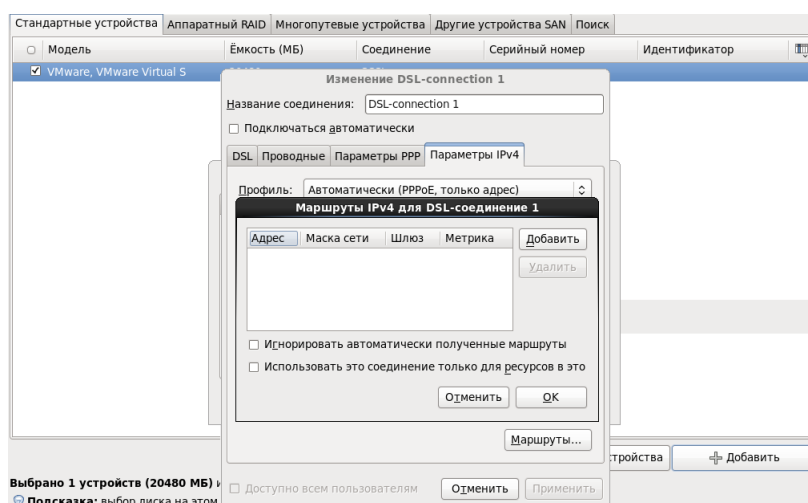


Рисунок 59

Далее в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

Для профиля **Вручную** можно определить серверы имен и домены поиска, определить используемые IP-адреса, а также настроить маршруты IPv4 для данного DSL-соединения:

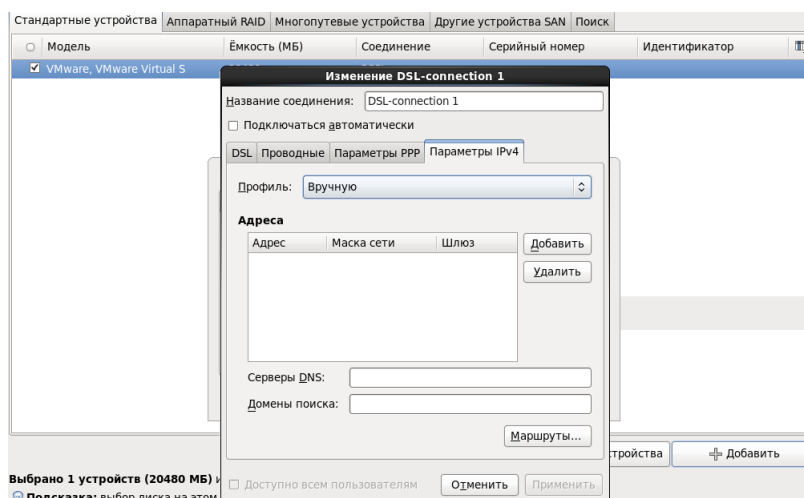


Рисунок 60

- **Серверы DNS** — введите список серверов DNS, разделив их запятой;
- **Домены поиска** — перечислите домены, которые будут участвовать в поиске сервера имен;
- **Адреса** — чтобы ввести допустимые адреса DSL-соединения, нажмите кнопку **Добавить** и укажите адрес, маску подсети и шлюз IPv4 для данного соединения.

Для того чтобы настроить маршруты IPv4 для данного соединения, нажмите кнопку *Маршруты*.

Далее в окне настройки маршрутов IPv4 выполните следующие действия:

- Нажмите **Добавить**, чтобы добавить IP-адрес, маску сети, адрес шлюза и метрику для нового статического маршрута.
- Выберите **Игнорировать автоматически полученные маршруты**, чтобы использовать только заданные здесь маршруты.
- Выберите **Использовать это соединение только для ресурсов в этой сети**, чтобы ограничить соединение пределами локальной сети.

5 Выбор устанавливаемых элементов ROSA Enterprise Linux Server

В зависимости от того, какой набор необходимых инструментов ROSA Enterprise Linux Server будет выбран при установке, могут быть доступны различные службы.

Для завершения установки сконфигурируйте ROSA Enterprise Linux Server, выбрав набор служб.

Возможно выбрать службы ROSA Directory Server и набор служб инструментов каталога.

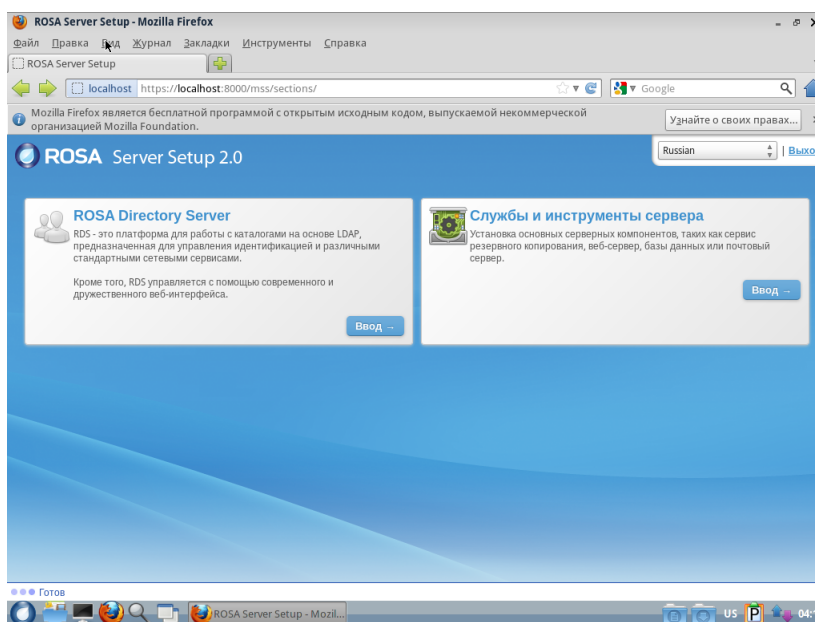


Рисунок 61

5.1 Настройка ROSA Directory Server

ROSA Directory Server — это основа для системы управления доступом, сервиса каталогов и управления сетевыми сервисами. ROSA Directory Server представляет собой службу каталогов уровня предприятия, предназначенную для централизованного управления доступом к ресурсам на множестве сетевых серверов.

ROSA Directory Server позволяет управлять идентификацией, сетевыми ресурсами, компьютерной системой и правами через веб-интерфейс.

Чтобы перейти к установке компонентов ROSA Directory Server, нажмите кнопку *Войти* на панели ROSA Directory Server. Откроется окно настроек установки ROSA Directory Server.

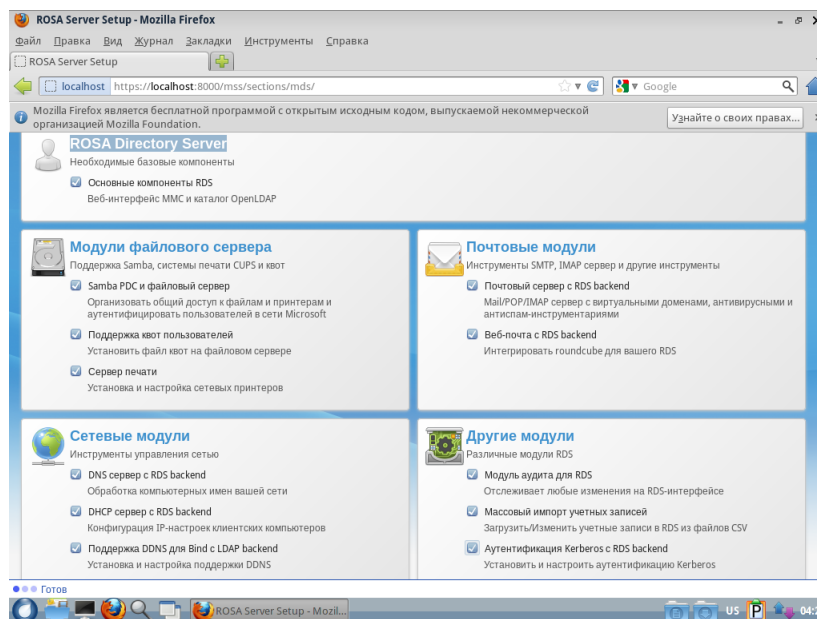


Рисунок 62

Набор возможностей ROSA Directory Server включает в себя:

- Основные компоненты RDS: web-интерфейс MMC (Mandriva ManagementConsole) и каталог OpenLDAP.
- Модули файлового сервера: Samba PDC и файловый сервер, поддержка квот пользователей и сервер печати.
- Сетевые модули: DNS сервер с серверной частью ROS backend, DHCP сервер с ROS backend, поддержка DDNS с Bind для LDAP backend.
- Почтовые модули: почтовый сервер с RDS backend, web-почта с RDS backend
- Другие модули: модуль аудита для RDS, массовый импорт учетных записей, аутентификация Kerberos с RDS backend.

5.2 Базовая конфигурация MMC

Web-интерфейс MMC взаимодействует с агентами MMC, управляя директориями сервисами и ресурсами LDAP.

Стандартный путь к конфигурационному файлу web-интерфейса MMC:

`/etc/mmc/mmc.ini`

Данный каталог содержит пользовательское имя и пароль, используемые для подключения к агентам MMC. Web-сервер Apache имеет доступ на чтение к этому файлу.

В конфигурационном файле web-интерфейса MMC содержатся следующие разделы:

Таблица 1

Наименование раздела	Описание	Обязательный раздел (да/нет)
global	Глобальные параметры web-интерфейса MMC	Да
debug	Параметры отладки	Да
logintitle	Название страницы регистрации	Нет
server_x	Параметры соединения агента MMC с сервером XMLRPC	Да

Раздел **global** содержит следующие параметры:

Таблица 2

Наименование параметра	Описание	Обязательный параметр (да/нет)	Значение по умолчанию
backend	Глобальные параметры web-интерфейса MMC	Да	отсутствует
login	Пользовательское имя для аутентификации агентом MMC	Да	отсутствует
password	Пароль пользователя для аутентификации агентом MMC	Да	отсутствует
root	URL корневого каталога, где размещены web-страницы MMC	Да	отсутствует
rootfsmodules	Путь в файловой системе к папке, где размещены web-модули MMC	Да	отсутствует
maxperpage	Максимальное число элементов (пользователей, групп и т.д., отображаемых на странице web-интерфейса)	Да	отсутствует

Окончание таблицы 2

Наименование параметра	Описание	Обязательный параметр (да/нет)	Значение по умолчанию
community	Флаг, сообщающий о том, является ли установленная версия свободной или нет	Да	Да

Раздел **debug** служит для целей отладки. В отладочном режиме вызовы XML-RPC и ответы будут отображаться на web-интерфейсе MMC.

Раздел **debug** содержит следующие параметры:

Таблица 3

Наименование параметра	Описание	Обязательный параметр (да/нет)	Значение по умолчанию
level	Флаг, позволяющий включить/выключить вывод отладочной информации	Да	отсутствует

Раздел **logintitle** содержит заголовок страницы web-интерфейса MMC.

Этот раздел может использоваться для создания заголовков страниц для поддержки различных языков пользователей. Например:

```
[logintitle]
; Default page title for English and non-translated languages
C = Welcome
; French title
fr_FR = Bienvenue
; Spanish title
es_ES = Bienvenido
```

Строка заглавия должна иметь кодировку UTF-8.

Разделы **server_x** определяют множество серверов, к которым может подключаться агент MMC.

Вы можете определить насколько таких разделов: server_1, server_2, server_3 и т.д.

На странице авторизации агента MMC будут указаны все эти серверы, и существует возможность выбрать из списка тот, к которому нужно подключиться.

Параметры раздела **server_x**:

Таблица 4

Наименование параметра	Описание	Обязательный параметр (да/нет)	Значение по умолчанию (да/нет)
description	Описание, которое будет выводиться на странице авторизации агента MMC	Да	отсутствует
url	Строка подключения к серверу XMLRPC для данного агента MMC	Да	отсутствует
forgotPassword	Отображение ссылки «Забыли пароль?» на странице авторизации агента MMC	Нет	отсутствует
timeout	Значения таймаута для операций ввода-вывода для сокетов	Нет	300
verifypeer	Флаг, установка которого включает TLS-протокол; если данный флаг включен, сервер XML-RPC должен предоставить соответствующий сертификат.	Нет	0
localcert	Если флаг verifypeer включен, то параметр localcert содержит путь к файлу в формате PEM, который содержит закрытый ключ и открытый сертификат, используемый для аутентификации пользователя агентом MMC	Да, если значение verifypeer = 1	отсутствует

Окончание таблицы 4

Наименование параметра	Описание	Обязательный параметр (да/нет)	Значение по умолчанию (да/нет)
cacert	Путь к файлу в формате PEM, который содержит открытый сертификат, используемый сертификационным центром. Значение этого параметра зависит от значения параметра localcert. Сертификат, предоставляемый агентом MMC, должен быть проверен сертификационным центром.	Да, если значение <code>verifypeer = 1</code>	отсутствует

Примеры конфигурационных параметров раздела `server_x`:

```
[server_01]
description = Local MMC agent
url = http://127.0.0.1:7080
```

Для того чтобы использовать SSL при подключении к MMC агенту через web-интерфейс, задайте параметры раздела `server_x` следующим образом:

```
[server_01]
description = Local MMC agent
url = https://127.0.0.1:7080
```

Пример с использованием проверок сертификата TLS:

```
[server_01]
description = MMC agent
url = https://10.0.0.1:7080
verifypeer = 1
cacert = /etc/mmc/certs/demoCA/cacert.pem
localcert = /etc/mmc/certs/client.pem
```

Параметры, которые вы можете изменить в этом файле:

- `login` и `password`: это параметры учетной записи для подключения к агентам MMC в вашей сети (те же, что и в файле `/etc/mmc/agent/config.ini`)

- `url` — для `[server_x]`: строка URL для подключения к агенту MMC

Стандартные настройки для MMC включают в себя следующий набор параметров:

- **`ldapurl`** : URL, используемые в LDAP. Они облегчают доступ к функциям LDAP для web-сервисов, имеющих доступ к LDAP только на чтение.

LDAP URL — это ссылка URL, начинающаяся с префикса протокола `ldap://` (или `ldaps://`, если сервер поддерживает SSL-соединения). LDAP URL содержит спецификацию поискового запроса к серверу LDAP.

LDAP URL имеет следующий формат:

`ldap[s]://<hostname>:<port>/<base_dn>?<attributes>?<scope>?<filter>`

`<hostname>` — имя сервера LDAP (или его IP-адрес), например: `ldap.netscape.com` или `192.202.185.90`. По умолчанию используется имя `localhost`

`<port>` — порт сервера LDAP, по которому осуществляется подключение. По умолчанию используется значение 389.

`<base_dn>` — базовое различимое имя. Параметр DN указывает на элемент, с которого начинается поиск. Если данный параметр опущен, то поиск начинается с корневого элемента дерева службы каталогов Active Directory.

`<attributes>` — набор возвращаемых атрибутов поискового запроса. Список атрибутов перечисляют через запятую без пробелов, например: `cn,mail,telephoneNumber`. Если список атрибутов не указан, возвращается полный набор атрибутов LDAP.

`<scope>` — область поиска. Этот параметр может принимать одно из трех значений:

- `base` загружает информацию только о различимом имени (`<base_dn>`), которое содержится в URL

- `one` загружает информацию об элементах, расположенных на один уровень ниже, чем различимое имя (`<base_dn>`), указанное в URL. При этом элемент, соответствующий различимому имени, не входит в область поиска.

- `sub` загружает информацию об элементах, размещенных на всех уровнях, расположенных ниже различимого имени (`<base_dn>`), указанного в URL. При этом элемент, соответствующий различимому имени, входит в область поиска.

`<filter>` — устанавливает фильтр, используемый для поиска в указанной области. Если фильтр не задан, сервер использует фильтр (`objectClass=*`).

В данном примере для `ldapurl` устанавливается значение `ldap://127.0.0.1:389`. Это соответствует области, ограниченной локальным хостом.

- **baseDN**: базовое различимое имя вашего каталога LDAP
- **baseUsersDN**: уникальные имена структурного подразделения (`ou`), которое включает в себя пользователей LDAP (например: `ou=People, %(baseDN)`)
- **baseGroupsDN**: уникальные имена структурного подразделения (`ou`), которое включает в себя группы LDAP (например: `ou=Group, %(baseDN)`)
- **rootName**: уникальное имя администратора LDAP
- **password**: пароль администратора LDAP

6 Настройка служб и инструментов сервера ROSA

ROSA Server Setup — это инструмент для установки и настройки основных серверных компонентов через веб-интерфейс. Он позволяет быстро развернуть следующие приложения:

- сервер каталогов ROSA Directory Server;
- стек LAMP (Linux/Apache/MySQL/PHP);
- базы данных MySQL и PostgreSQL;
- файловые серверы SAMBA и NFS;
- принт-сервер CUPS;
- сетевые сервисы DHCP и DNS;
- почтовый сервер Postfix с защитой от спама и вирусов;
- сервер рассылки Mailman;
- сервис резервного копирования Bacula.

Чтобы перейти к установке компонентов ROSA Server, нажмите кнопку *Войти* на панели ROSA Server Setup. Откроется окно настроек установки ROSA Server Setup.

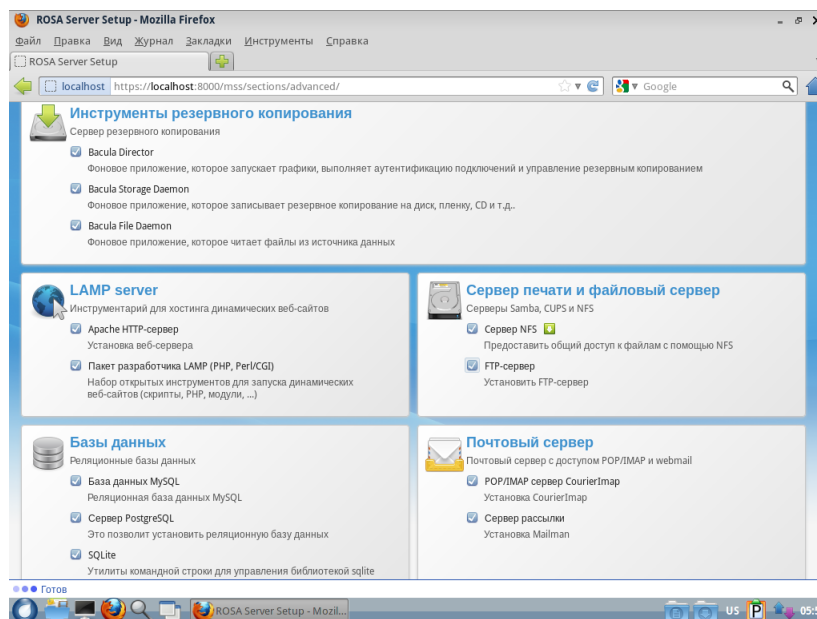


Рисунок 63

Набор возможностей ROSA Server включает в себя:

- Инструменты резервного копирования: Bacula Director, Bacula Storage Daemon, Bacula File Daemon
- LAMP server: Apache HTTP-сервер, пакет разработчика LAMP
- Базы данных: база данных MySQL, сервер PostgreSQL, SQLite
- Сервер печати и файловый сервер: сервер NFS, FTP-сервер
- Почтовый сервер: POP/IMAP сервер CourierImap, сервер рассылки

Выберите те компоненты, которые вы хотите включить в конфигурацию вашего сервера, и нажмите кнопку *Продолжить* в окне установки компонент ROSA Server.

Ниже мы подробно рассмотрим каждую из этих настроек.

После установки выбранных компонентов отображается окно настройки. Задайте пароль для тех компонентов, которые требуют установки пароля, и задайте первоначальные настройки для сервера LDAP, Samba и сервера DNS.

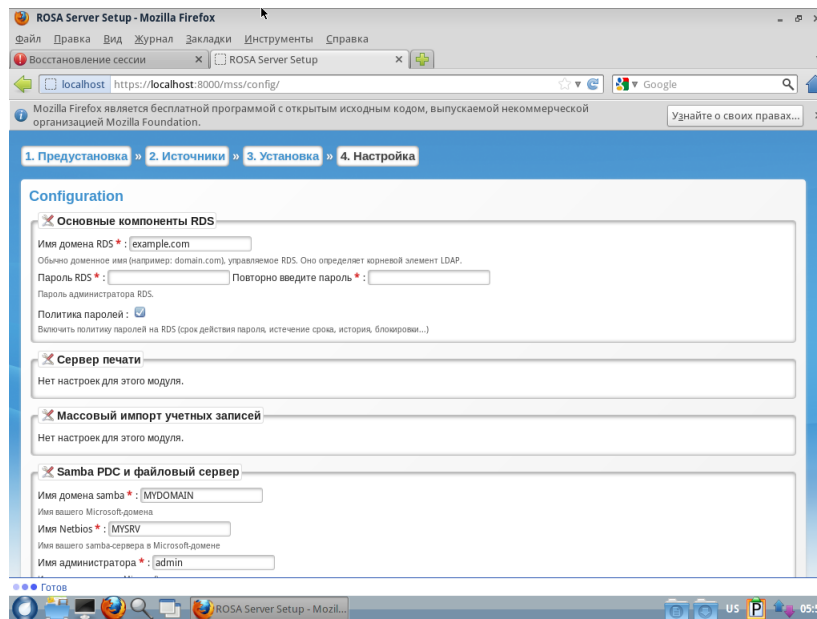


Рисунок 64

В следующем окне мастера установки нажмите кнопку *Продолжить*. Выполните конфигурацию для завершения установки и настройки выбранных компонентов.

7 Основные компоненты RDS

Назначение компонентов RDS — позволять пользователям устанавливать соединения с удаленными хостами.

Для настройки компонентов RDS задайте следующие параметры:

1) **Имя домена RDS** — имя домена, в котором будут использоваться службы RDS.

В качестве имени домена RDS следует выбрать полное доменное имя, которое будет использоваться в качестве корневого элемента LDAP.

2) **Пароль RDS** — пароль администратора RDS.

При задании пароля администратора RDS необходимо выбрать пароль, не совпадающий с паролем учетной записи `root` или с паролем, указанным при установке ROSA Directory Server.

3) Чтобы проверять задаваемые пароли RDS на сложность, включите флажок **Политика паролей**. Тогда в случае, если пользователь попытается установить недостаточно сложный пароль, система предложит ему ввести другой пароль.

7.1 Настройки Samba PDC и файлового сервера

Пакет **Samba** позволяет создавать файловые серверы и серверы печати на базе открытых систем (OpenVMS, Digital Unix, AIX, IRIX, HPUX, Solaris, FreeBSD, NetBSD, Linux,

и т.д.), а также поддерживать (с определенными ограничениями) доменную структуру Windows. Также возможно построить и сконфигурировать главный контроллер домена (Primary Domain Controller, PDC) с использованием Samba на стороне сервера.

При установке сервера печати и файлового сервера ROSA Server выполняется установка пакета Samba и указываются основные конфигурационные параметры.

Для настройки Samba PDC в мастере установки ROSA Server введите следующие данные:

- 1) **Имя домена Samba** — введите в этом поле имя домена, в котором будет установлен PDC
- 2) **Имя Netbios** — укажите имя Samba-сервера в домене
- 3) **Имя администратора** — укажите имя учетной записи администратора
- 4) **Пароль администратора** — введите пароль администратора.

7.2 Поддержка квот пользователей

ROSA Server предоставляет администратору системы возможности для мониторинга и ограничения использования дискового пространства пользователями и группами для доступных файловых систем.

Администратор ROSA Server имеет возможность определять и настраивать дисковые квоты файловой системы, устанавливать пределы квот и проверять квоты.

Для первоначальной настройки квот в поле **Файловые системы** укажите файловые системы, где будут использоваться квоты. Квоты указываются в следующем формате:

`device_path:identifier_string` (например, `/test/files:Home`).

7.3 Настройки модуля аудита для RDS

Чтобы выполнить первоначальную настройку модуля аудита для RDS, введите следующие данные:

- 1) **Пароль администратора MySQL** — введите пароль администратора MySQL в соответствующем поле и повторите ввод пароля в поле **Повторно введите пароль**.

Пароль администратора MySQL используется для создания базы данных аудита.

- 2) **Пароль MySQL Audit** — введите пароль пользователя MySQL для базы данных аудита и повторите ввод пароля в поле **Повторно введите пароль**.

Пароль MySQL Audit используется для просмотра данных аудита.

7.4 Настройки почтового сервера с RDS backend

Чтобы выполнить первоначальную настройку почтового сервера с RDS backend, введите следующие данные:

1) **Мое имя хоста** — введите полностью определённое имя домена (например: smtp.domain.com)

2) **Мои сети** — укажите, какие клиенты уполномочены отправлять почту через почтовый сервер

3) **Поддерживаемые протоколы** — выберите, какие протоколы будут поддерживаться для отправки и получения почты.

7.5 DNS-сервер с RDS backend

Для первоначальной настройки DNS-сервера с RDS backend выполните следующие настройки:

1) В полях **Мои сети** ведите параметры подсети, где располагаются ваши клиенты (например: 192.168.100.0/24).

2) В поле **Ретрансляторы запросов** укажите адреса ретрансляторов, с которых будут поступать запросы на выбранный вами DNS.

7.6 Аутентификация Kerberos с RDS backend

Для настройки параметров аутентификации Kerberos с RDS backend введите следующие данные:

1) В поле **Область** укажите область Kerberos. Как правило, значение в этом поле представляет собой имя используемого домена, набранное в верхнем регистре.

2) В поле **Имя узла KDC** укажите имя узла KDC сервера без DNS-домена. Это имя сервера KDC, на котором будет располагаться сервер дистрибуции ключей. Укажите в этом поле FQDN-имя сервера без имени домена (например, для узла kerberos.domain.ru нужно указать имя kerberos).

3) В поле **DNS домен** укажите имя DNS-домена.

4) В поле **Порт KDC** укажите порт для сервера дистрибуции ключей.

5) В поле **Порт сервера администратора** укажите порт, по которому Kerberos связывается со своей базой данных.

6) В поле **Основной ключ базы данных KDC** укажите пароль для базы данных Kerberos. Повторно введите пароль для подтверждения.

7) Установите флажок **DNS-поиск для KDC**, если необходимо проверять в SRV-записях DNS наличие информации о сервере Kerberos. Эта настройка помогает находить серверы (KDC и другие серверы) для области, если они не описаны в информации об области.

8) Установите флажок **DNS-поиск для области**, если необходимо использовать TXT-записи DNS для поиска доступных серверов (KDC и других).

9) В поле **Временной сдвиг** укажите допустимое время смещения часов относительно «эталонных». В качестве эталона у нас будет выступать сервер Kerberos, на котором работает сервис NTP. Время смещения указывается в секундах.

10) В поле **Типы шифрования TGS** укажите поддерживаемые алгоритмы шифрования допустимые на сервере выдачи билетов. Как правило, изменять значение в этом поле не требуется.

11) В поле **Разрешенные типы шифрования** через запятую перечислены все типы шифрования, которые разрешены для использования при шифровании сессионного ключа. Как правило, изменять значение в этом поле не требуется.

12) Установите флажок **Разрешить типы шифрования невысокой криптостойкости**, если вы предполагаете использовать слабозащищенные алгоритмы шифрования. Если предъявляются высокие требования к безопасности, этот флажок нужно снять.

7.7 Web-почта с RDS backend

В полях **Пароль root для MySQL** и **Поле повторного ввода пароля** задают пароль для административной записи базы данных почтового сервера.

7.8 Поддержка DDNS для Bind с LDAP backend

Установите флажок **Включить динамический DNS**, если необходимо сконфигурировать web-сервер так, чтобы DNS принимал уведомления, приходящие в реальном времени, для своей активной конфигурации (имена узлов, адреса и т.д.)

7.9 Настройки Bacula Director

Bacula Director — процесс, управляющий системой в целом (управление, планирование, восстановление из резервных копий).