D-Link®

DSA-3110

Концентратор доступ
Руководство пользователя

Rev. 2.0.7 (Sep 2008)

RECYCLABLE

Оглавление:

Описание устройства

DSA-3110 представляет собой концентратор доступа, работающий по протоколам PPTP и PPPoE . Устройство обеспечивает подключение и авторизацию пользователей, а также выдачу статистики по подключениям на внешний сервер с использованием технологии NetFlow. DSA-3110 предоставляет законченное решение, обеспечивающее подключение клиентов к Интернет внутри сетей провайдеров с выдачей статистики по израсходованному трафику на сервер хранения или биллинга, а также подключение мобильных сотрудников к внутренней сети организации по безопасному VPN-соединению с возможностью учета производимых подключившимися пользователями действий.

DSA-3110 совместим с большинством популярных операционных систем, включая Macintosh, *BSD, UNIX, Linux и Windows, и может быть интегрирован в крупную сеть.

Типовые схемы подключения

На рисунках представлены типовые схемы применения DSA-3110.

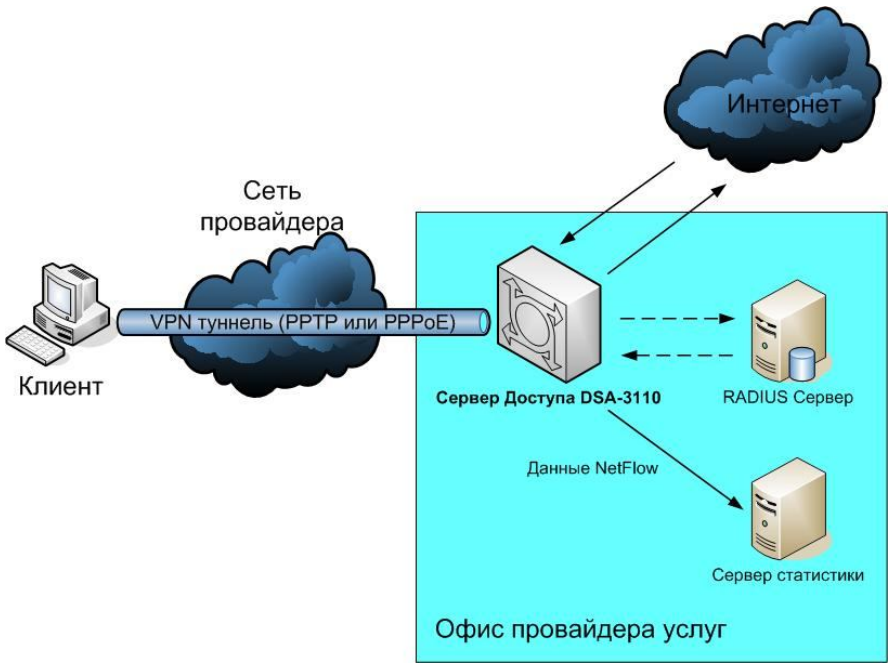

Рисунок 1. Пример использования DSA-3110 в сетях провайдеров услуг

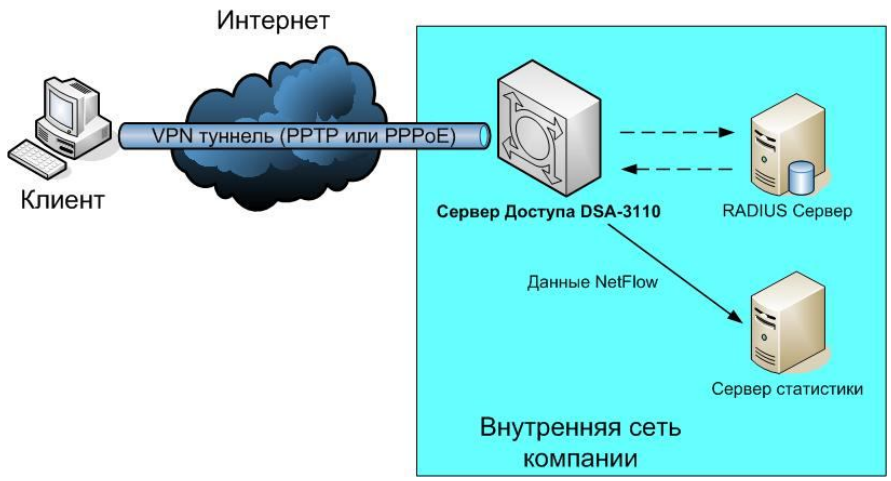

Рисунок 2. Пример использования DSA-3110 во внутренней сети компании

Описание технологий и протоколов, используемых в устройстве

Протокол PPTP

Протокол PPTP (Point to Point Tunneling Protocol) – сетевой протокол, который обеспечивает безопасную передачу пакетов PPP от удаленного клиента серверу доступа к сети через VPN туннель, созданный на основе сетей TCP/IP.

Как работает PPTP

PPTP инкапсулирует пакеты для их передачи по IP-сети через туннель, созданный между удаленным клиентом и сервером.

Инкапсуляция данных перед отправкой в туннель включает два этапа. Сначала создается информационная часть PPP. Данные проходят сверху вниз, от прикладного уровня OSI до канального. Затем полученные данные отправляются вверх по модели OSI и инкапсулируются протоколами верхних уровней.

Таким образом, во время второго прохода данные достигают транспортного уровня. Однако информация не может быть отправлена по назначению, так как за это отвечает канальный уровень OSI. Поэтому PPTP берет на себя функции второго уровня, т. е. добавляет к полученному пакету PPP-заголовок (header) и окончание (trailer). На этом создание кадра канального уровня заканчивается. Далее, PPTP инкапсулирует PPP-кадр в пакет Generic Routing Encapsulation (GRE), который принадлежит сетевому уровню. GRE инкапсулирует протоколы сетевого уровня, например IP, чтобы обеспечить возможность их передачи по IP-сетям.

После того как кадр PPP был инкапсулирован в кадр с заголовком GRE, выполняется инкапсуляция в кадр с IP-заголовком. IP-заголовок содержит адреса отправителя и получателя пакета. На рисунке 3 показана структура данных для пересылки по туннелю PPTP.

Рисунок 3. Структура данных для пересылки по туннелю PPTP.

Туннелирование позволяет повышать степень защиты данных при их передаче от удаленного клиента серверу доступа. Для этого применяются различные методы аутентификации и шифрования.

Для аутентификации пользователей PPTP может задействовать любой из протоколов, применяемых для PPP, включая *Microsoft Challenge Handshake Authentication Protocol (MSCHAP)* версии 1 и 2, *Challenge Handshake Authentication Protocol (CHAP)* и *Password Authentication Protocol (PAP)*.

Для шифрования трафика PPTP использует *протокол MPPE (Microsoft Point-to-Point Encryption)*.

MPPE – это протокол, разработанный специально для передачи зашифрованных дейтаграмм по соединению точка-точка (point-to-point). Он совместим только с протоколом аутентификации MSCHAP (версии 1 и 2) и умеет автоматически выбирать длину ключа шифрования при согласовании параметров между клиентом и сервером.

MPPE поддерживает работу с ключами длиной 40, 56 или 128 бит. PPTP изменяет значение ключа шифрации после каждого принятого пакета, используя порядковые номера пакетов.

Протокол PPP

Протокол PPP (Point-to-Point Protocol) используется для получения доступа к удаленным узлам и для связи между ними и удаленной локальной сетью. PPP представляет собой стандартный протокол инкапсуляции для переноса данных различных протоколов сетевого уровня (включая протокол IP) по последовательным каналам точка-точка.

Протокол также включает в себя механизмы для выполнения следующих действий:

- Мультиплексирование сетевых протоколов
- Проверку качества канала
- Аутентификацию
- Сжатие заголовков
- Обнаружение ошибок
- Согласование параметров канала

Протокол PPP имеет три основных функциональных компонента:

- Метод инкапсуляции дейтаграмм для последовательных каналов, основанный на протоколе HDLC.
- Протокол управления каналом LCP (Link Control Protocol), который устанавливает, конфигурирует и проверяет соединение канального уровня, а также выполняет аутентификацию.
- Протокол управления сетью NCP (Network control Protocol) устанавливает и конфигурирует различные протоколы сетевого уровня.

Протокол аутентификации PAP
При использовании протокола PPP проверка прав доступа вызывающей стороны может быть выполнена с помощью механизмов аутентификации PAP, CHAP, MS-CHAP или MS-CHAPv2 .

Протокол PAP. После успешного согласования входящего вызова сторона, запрашивающая аутентификацию, продолжает посылать свое имя и пароль до тех пор, пока подтверждающая сторона не ответит подтверждением или пока соединение не будет прекращено. Если подтверждающая сторона определит, что комбинация имени пользователя и пароля неверна, она может разорвать соединение.

Для проверки того, что пара имя пользователя/пароль верна, подтверждающая сторона просматривает локальную базу данных пользователей PAP (созданную командами указания имени пользователя и пароля) или посылает запрос на проверку аутентификации на сервер безопасности RADIUS.

Внимание: пароли протокола PAP передаются по сети открытым текстом.

Если требуется использовать более надежный метод контроля доступа, то в качестве метода аутентификации следует использовать протокол CHAP.

Протокол аутентификации CHAP
При использовании проверки прав доступа *протокола CHAP* сервер доступа после установления канала PPP посылает сообщение-запрос, содержащее случайную строку на удаленный узел. Удаленный узел отвечает значением, вычисленным на основе пароля и значения запроса с использованием односторонней хеш-функции (обычно с помощью алгоритма MD5). Результат отправляется серверу доступа в виде ответного сообщения вместе с CHAP-именем удаленного узла. Сервер доступа считывает из ответного сообщение имя узла, находит пароль для этого имени в локальной базе данных или на сервере RADIUS и подает пароль и первоначальное случайное значение запроса на хеш-генератор MD5. Вычисленное значение сравнивается с полученным значением и если величины совпадают, то аутентификация считается успешно завершенной. В противном случае соединение немедленно прерывается.
Метод CHAP обеспечивает защиту от попытки несанкционированного доступа посредством использования переменного значения запроса (challenge), который является уникальным и трудно предсказуемым. Использование повторных запросов каждые две минуты в сеансе CHAP предназначено для того, чтобы ограничить время возможности организации вторжений при любой попытке несанкционированного доступа. Сервер доступа управляет частотой и синхронизацией запросов.

Внимание: пароли CHAP на обеих сторонах линии связи должны быть идентичными.

Протокол аутентификации MS-CHAPv1
Протокол MS-CHAP v1 является механизмом аутентификации с использованием шифрования, подобным протоколу CHAP. Как и в протоколе CHAP, сервер доступа посылает удаленному клиенту случайное значение (challenge). Удаленный клиент должен отправить ответ, содержащий имя пользователя и хеш, вычисленный на основе значения запроса, идентификатора сессии и хешированного с помощью хеш-генератора MD4 пароля.
При использовании MS-CHAP v1 совместно с MPPE, общие ключи шифрования (secret) будут генерироваться каждым узлом PPP. Также протокол MS-CHAP v1 обеспечивает набор сообщений, которые позволяют пользователю изменять пароль во время процесса аутентификации.

Протокол аутентификации MS-CHAPv2
Протокол MS-CHAP v2 обеспечивает повышенный уровень безопасности для удаленных клиентов. По сравнению с MS-CHAP v1 протокол MS-CHAP v2 предоставляет следующие дополнительные функции безопасности:
Взаимная аутентификация между удаленным клиентом и сервером доступа
Отдельные ключи шифрования, генерируемые для передаваемых и принимаемых данных
Различные ключи шифрования, основанные на пароле пользователя и случайном значении (challenge).

Протокол PPPoE

Технология использования стека PPP в сети Ethernet является относительно новой, но уже получила достаточное распространение. На данный момент она определяется документом RFC 2516, который был разработан и выпущен в феврале 1999 года.

Технология PPPoE на данный момент является одной из самых дешевых и распространенных при предоставлении пользователям доступа к услугам Интернет в жилых комплексах на базе Ethernet и при использовании технологии DSL.

При этом будет поддерживаться аутентификация пользователей по протоколам PAP и CHAP, динамическое выделение IP - адресов пользователям, назначение адреса шлюза, DNS-сервера и т.д.

Так как принципом работы PPPoE является установление соединения "точка-точка" поверх общей среды Ethernet, то процесс функционирования PPPoE должен быть разделен на две стадии. В первой стадии два устройства должны сообщить друг другу свои адреса и установить начальное соединение, а во второй стадии запустить сессию PPP.

Стадия установления соединения

Стадия установления соединения между клиентом (компьютером пользователя) и сервером (концентратором доступа провайдера) делится на несколько этапов.

На первом этапе клиент посылает широковещательный запрос (адрес назначения - broadcast address) (PADI PPPoE Active Discovery Initiation) на поиск сервера со службой PPPoE. Этот запрос получают все пользователи сети, но ответит на него только тот, у кого есть поддержка службы PPPoE. Ответный пакет от концентратора доступа (PADO PPPoE Active Discovery Offer) посылается в ответ клиенту, но если в сети есть много устройств со службой PPPoE, то клиент получит много пакетов PADO. В этом случае, программное обеспечение клиента выбирает необходимый ему концентратор доступа и посылает ему пакет (PADR PPPoE Active Discovery Request) с информацией о требуемой службе (требуемый класс обслуживания зависит от услуг провайдера), имя провайдера и т.д. После получения запроса, концентратор доступа подготавливается к началу PPP сессии и посылает клиенту пакет PADS (PPPoE Active Discovery Session-confirmation). Если все запрашиваемые клиентом службы доступны (в состав этого пакета входит уникальный номер сессии, присвоенный концентратором), то начинается второй этап - стадия установленной сессии. Если требуемые клиентом услуги не могут быть предоставлены, клиент получает пакет PADS с указанием ошибки в запросе услуги.

Стадия установленной сессии

Сессия начинается с использованием пакетов PPP. Принцип работы протокола PPP был рассмотрен выше. При установлении PPP-сессии пользователь может быть аутентифицирован при помощи RADIUS, и его трафик будет учитываться как при обычном модемном доступе. Ему можно назначить динамический IP- адрес из пула адресов концентратора, установить настройки шлюза и DNS-сервера. Желательно, чтобы концентратор доступа посылал периодические запросы клиенту для определения его состояния. Эта операция необходима для того, чтобы клиент, который по какой-либо причине не оборвал сессию корректным образом, не считался существующим, и для него не резервировались ресурсы концентратора доступа.

Завершение соединения PPPoE происходит по инициативе клиента или концентратора доступа при помощи посылки пакета PADT (PPPoE Active Discovery Terminate).

В протоколе PPPoE предусмотрены некоторые дополнительные функции, например, такие как защита от DoS атак (Denial of Service). Защита от некоторых типов DoS атака

реализована путем добавления в пакеты PADI специального поля AC-Cookie, которое позволяют концентратору доступа ограничивать количество одновременных сессий PPPoE на одного клиента.

Сервер RADIUS

Протокол RADIUS (Remote Authentication Dial-In User Services) был разработан компанией Livingston Enterprises, Inc как протокол аутентификации (authentication) и учета (accounting) удаленных клиентов. RADIUS работает на основе модели клиент/сервер, в которой пользовательская информация передается между сервером и клиентом RADIUS.

Концентратор доступа выступает в роли клиента RADIUS и отвечает за взаимодействие с выделенным сервером RADIUS. Он осуществляет пересылку пользовательской информации серверу RADIUS и ответов сервера удаленным клиентам. Сервер RADIUS хранит базу данных пользователей, на основании которой клиентам разрешается или запрещается доступ в сеть, а также ведет учет израсходованных пользователями ресурсов.

Служба преобразования сетевых адресов NAT

Служба NAT (Network Address Translation) представляет механизм использования одних и тех же приватных IP-адресов в нескольких внутренних подсетях, уменьшая тем самым потребность в зарегистрированных IP-адресах.

Устройство, поддерживающее функцию NAT, располагается на границе внутренней и внешней сети и преобразует внутренние локальные адреса в уникальные глобальные IP-адреса перед отправкой пакетов во внешнюю сеть. Преобразование, осуществляемое NAT, может быть *статическим* или *динамическим*. *Статическое преобразование* происходит в том случае, если пользователь самостоятельно конфигурирует адреса в таблице соответствий. При этом конкретные внутренние адреса отображаются в заранее указанные внешние адреса. При *динамическом преобразовании* пограничное устройство с функцией NAT настраивается таким образом, чтобы внутренние адреса преобразовывались во внешние из заранее определенного пула адресов. Также несколько внутренних узлов сети могут использовать один внешний IP-адрес, позволяя экономить адресное пространство.

NetFlow

NetFlow – это технология сбора статистики о пакетах, проходящих через маршрутизирующее устройство сети и выдачи ее на внешний коллектор.

NetFlow формирует таблицу потоков для входящих и исходящих IP-пакетов. Поток NetFlow определяется как ненаправленный поток пакетов между данным источником и приемником. Источник и приемник определяются с помощью IP-адресов и номеров портов транспортного уровня.

В частности, поток определяется комбинацией следующих ключевых полей пакета:

- IP-адресом источника
- IP-адресом назначения
- Номером порта TCP/UDP источника
- Номером порта TCP/UDP назначение
- Типом протокола 3 уровня
- Типом сервиса (ToS)
- Входным логическим интерфейсом

Эти семь полей уникально определяют поток. Если пакет отличается от другого значением хотя бы одного ключевого поля, считается, что этот пакет принадлежит другому потоку. В потоке также могут присутствовать и другие поля (например, номер автономной системы) в зависимости от версии экспортной записи (export record), которую вы конфигурируете. Все потоки хранятся в кэше NetFlow.

Основными компонентами NetFlow являются кэш NetFlow, в котором хранится информация о потоке IP и NetFlow экспорт (export) или транспортный механизм, который отсылает данные NetFlow сетевому коллектору.

Для каждого активного потока NetFlow создает запись в кэше (запись о потоке). Каждая такая запись содержит поля, которые позднее будут экспортированы коллектору. Для экспорта данных NetFlow использует дейтаграммы UDP.

Характеристики DSA-3110

Аппаратные характеристики:
- Процессор: Intel Xscale 533MHz
- 64MB RAM
- 16 MB Flash ROM
- 7 портов 10/100Base-TX Fast Ethernet
- 4 независимо конфигурируемых интерфейса 10/100Base-TX
- Внешний блок питания 5В 3А
- Светодиодные индикаторы питания и состояния подключений к интерфейсам
- Консольный порт RS-232

Программное обеспечение:
- Базовая операционная система: Linux
- Сервер PPTP
- Сервер PPPoE
- Экспорт статистики (аккаунтинг) по протоколу NetFlow v.5
- NAT
- Статическая маршрутизация
- Внешний syslog-сервер
- Авторизация VPN-подключений: локально или RADIUS
- Поддержка до 250 пользователей в локальной базе
- Поддержка до 50 одновременных подключений
- Внутренний DHCP сервер
- WEB-интерфейс управления
- SSH-сервер
- Интерфейс командной строки CLI
- Telnet сервис (по умолчанию отключен)
- Конфигурация интерфейсов со статическим адресом ,DHCP, PPTP, PPPoE
- Многочисленные возможности iptables, ip и других утилит, доступные для настройки через стандартную командную строку встроенного Linux.

Установка

DSA-3110 обеспечивает возможность конфигурирования на основе Web- интерфейса, что позволяет использовать в качестве станции управления любой компьютер, оснащенный Web-браузером, независимо от операционной системы, и через консольное подключения (читайте об этом подробнее в документе DSA-3110 CLI Guide).

Включение DSA-3110. Начало работы с устройством.

Перед тем, как начать настройку концентратора доступа, необходимо установить с ним физическое соединение. Для этого потребуется:

1. Компьютер с ОС Linux, *BSD, UNIX, Windows или MacOS
2. Web-браузер с поддержкой JavaScript (Mozilla, Netscape Navigator, Microsoft IE, Opera...)
3. Кабели Ethernet для подключения к сети (RJ-45)
4. Консольный Кабель RS-232, входящий в комплект к устройству (в случае консольного подключения)

Далее:

1. Подключите один конец кабеля RJ-45 к любому из портов встроенного коммутатора (порты 4-7), а другой конец к доступному порту Ethernet компьютера или коммутатора существующей локальной сети.
2. Подключите адаптер питания, включенный в комплект поставки к устройству и к сети питания 220В.

Подключение к DSA-3110 через порт RS-232

Для того чтобы подключиться порту RS-232 управления устройства, на рабочей станции необходимо:

- Подключить консольный кабель, входящий в комплект устройства, к свободному COM-порту рабочей станции одним концом (например, к порту COM1) и к порту RS-232 устройства DSA-3110 другим концом.

- Запустить программу HyperTerminal (в Windows XP программа HyperTerminal находится в Меню «Пуск»- Программы –Стандартные- Связь- HyperTerminal) или иную терминальную программу, со следующими параметрами соединения

- Создайте соединение с указанными ниже параметрами и подключитесь к консольному режиму устройства (как создать соединение в программе Hyperterminal смотрите на рисунках 4-6).

Параметры консольного соединения:
Скорость порта (Bit per second) –115200
Количество бит данных (Data Bits)-8
Контроль четности (Parity) – None
Количество стоп-бит (Stop Bits) - 1
Контроль потока (Flow Control) - None

По умолчанию для авторизации в консольном режиме установлены следующие имя пользователя и пароль: имя пользователя (**User name) - root**, пароль (**Password) - admin**.

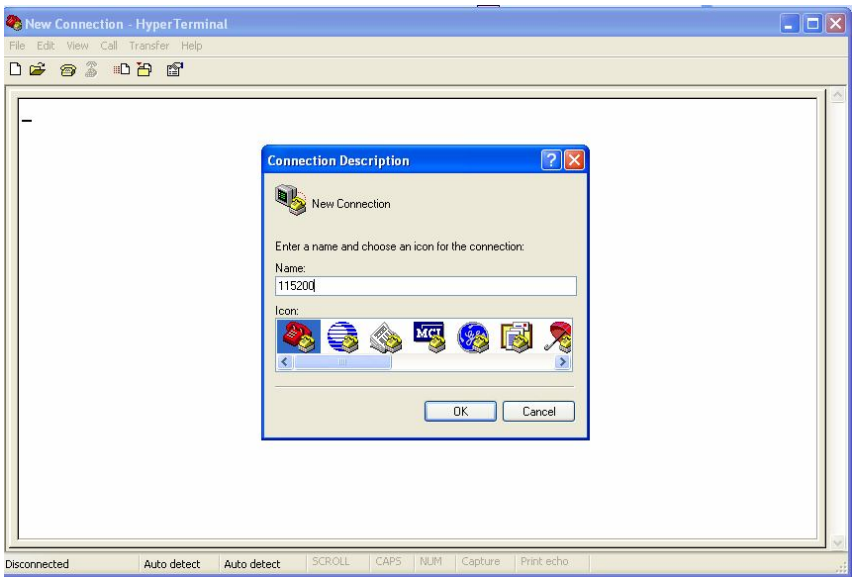

Рисунок 4

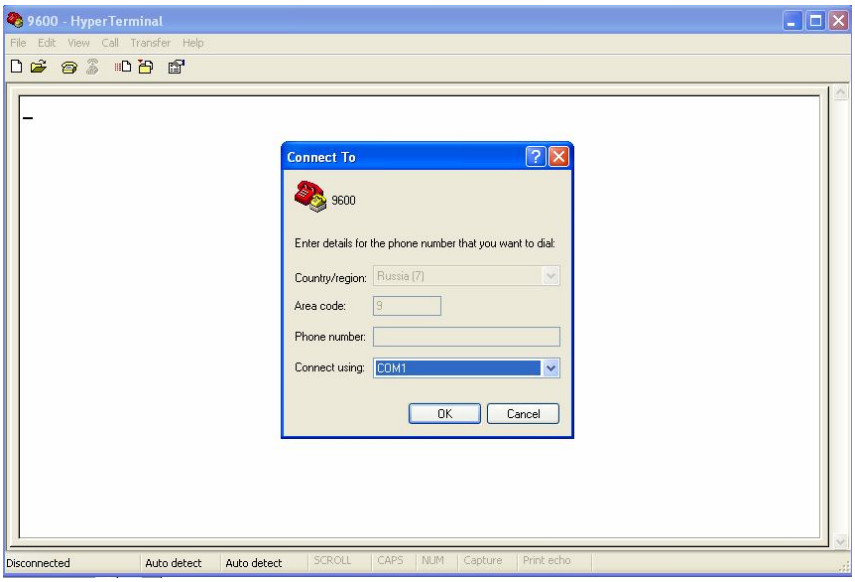

Рисунок 5

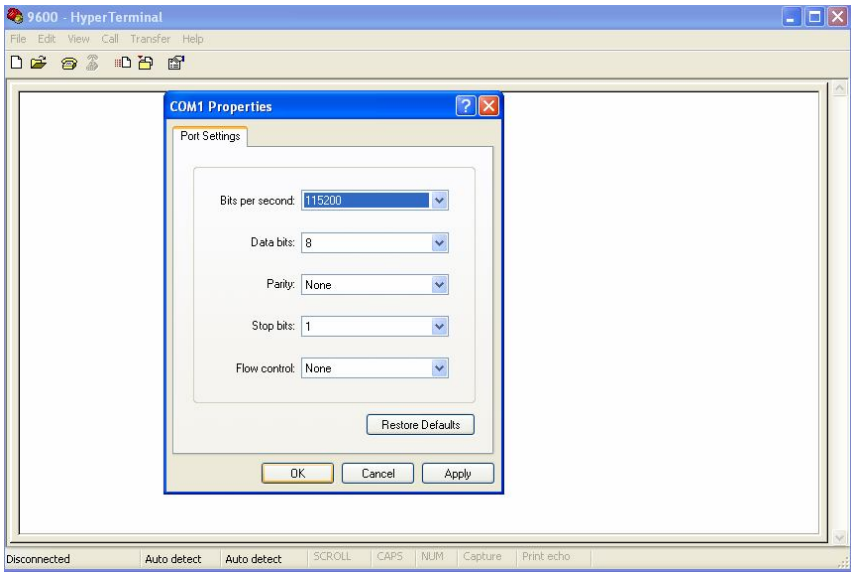

Рисунок 6

Подключение к Web-интерфейсу

Web-интерфейс управления состоит из дружественного пользовательского графического интерфейса (GUI), запускающегося на клиенте и HTTP-сервера, запускающегося на DSA-3110. Связь между клиентом и сервером обычно осуществляется через TCP/IP соединение с номером порта HTTP равным 80.

Для того чтобы подключиться к Web-интерфейсу управления устройства, на рабочей станции необходимо запустить Web-браузер, в адресной строке которого ввести IP-адрес DSA-3110. IP-адрес DSA-3110 установленный по умолчанию 192.168.1.254:

1.Откройте Web-браузер
2.Введите **IP-адрес** DSA-3110 (http://192.168.1.254)

Примечание: Если вы изменили IP-адрес, назначенный DSA-3110 по умолчанию, убедитесь, что был введен правильный IP-адрес.

По умолчанию установлены следующие имя пользователя и пароль:
имя пользователя (**User name) - admin**, пароль (**Password) - admin**.
В целях повышения безопасности сети рекомендуется изменить пароль администратора. Пожалуйста, перейдите на вкладку **Система -> Пароль администратора** для смены пароля. После успешной регистрации появится окно статуса системы:

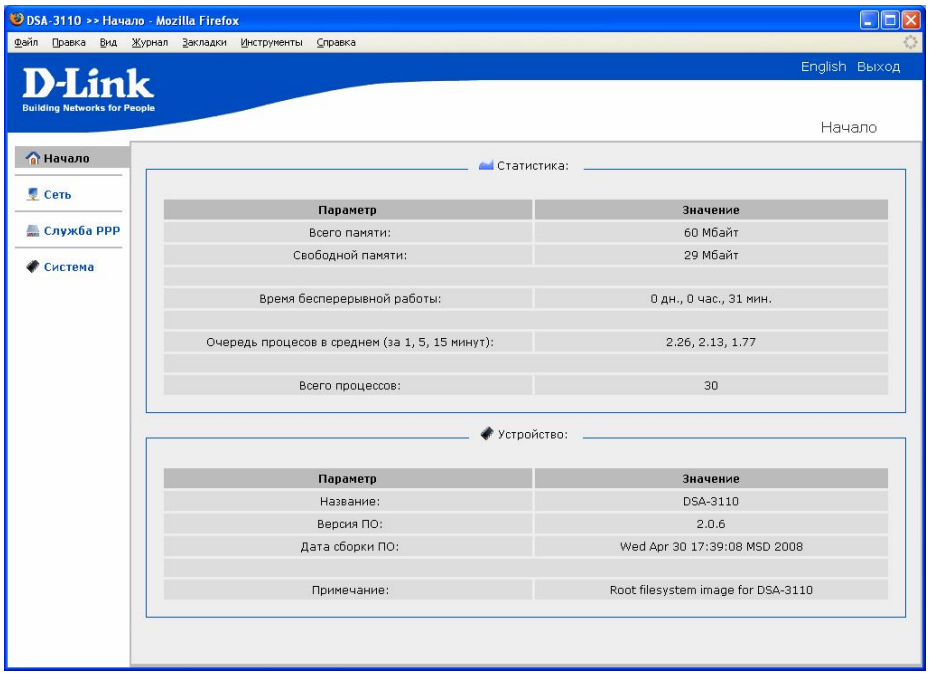

Рисунок 7. Окно статуса системы.

В устройстве имеется встроенная возможность переключения языка Web-интерфейса с помощью одного клика. Для этого нажмите на надпись **English** или **Russian** в правом верхнем углу экрана. Переключение языка доступно из любого меню и подменю.

Внимание: Для применения настроек, измененных в меню Web-интерфейса устройства требуется сохранить произведенные изменения в меню **Система->Конфигурация->Сохранить** и перезагрузить устройство.

Внимание: Изменение настроек DSA-3110 через Web-интерфейс происходит не мгновенно. Для применения некоторых изменений может потребоваться некоторое время, поэтому подождите, пока устройство произведет все необходимые внутренние операции.

Настройка устройства с помощью WEB-интерфейса

Меню-Сеть

Данный пункт меню используется для трех целей:

- Настройки сетевых параметров физических интерфейсов устройства;
- Настройки трансляции адресов (NAT).
- Настройки серверов имен (DNS) и доменов поиска

Порты eth-0 –eth-3 имеют следующую привязку к цифровым обозначениям портов, нанесенных на корпус устройства:
Eth-0 – порты 4 -7
Eth-1 – порт 3
Eth-2 - порт 1
Eht-3 - порт 2

Порты 4-7 - представляют собой коммутатор с изолированными портами (т.е. передача пакетов между портами коммутатора запрещена, только на другие интерфейсы).

По умолчанию на устройстве создан 1 интерфейс Ethernet со статическим IP адресом: Eth-0 - 192.168.1.254

Настройка сетевых интерфейсов

- Откройте меню **Сеть**

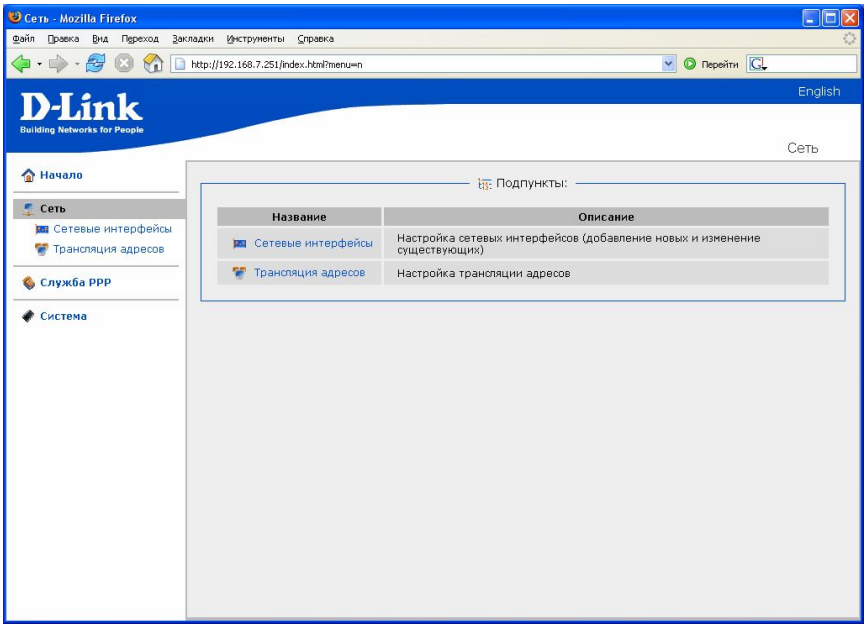

Рисунок 8. Меню Сеть.

- Выберите **Сетевые интерфейсы**

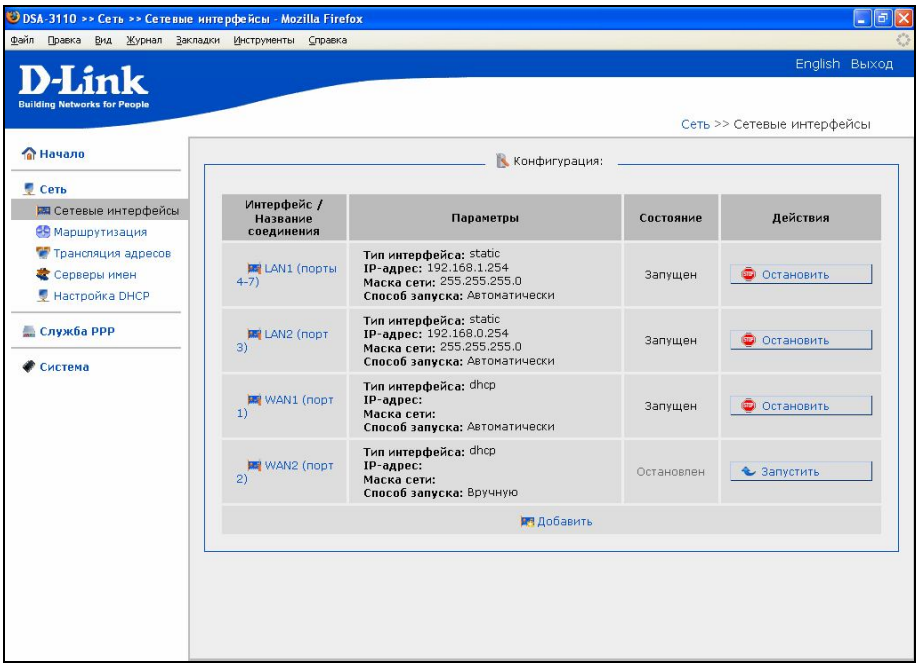

Рисунок 9. Меню Сеть -> Сетевые интерфейсы

- Выберите из списка необходимый физический интерфейс для конфигурирования и нажмите на «**Изменить**» для изменения настроек выбранного интерфейса.
- В появившейся форме выберите тип интерфейса: **Статический**, **DHCP**.

Либо

- Нажмите кнопку **Добавить** для конфигурирования виртуальных интерфейсов (тип интерфейса PPTP или PPPoE)

Настройка статического интерфейса

Данный тип интерфейса является единственным возможным для интерфейсов eth0(LAN1) и eth1 (LAN2) и одним из вариантов для интерфейсов eth2(WAN1) и eth3(WAN2).

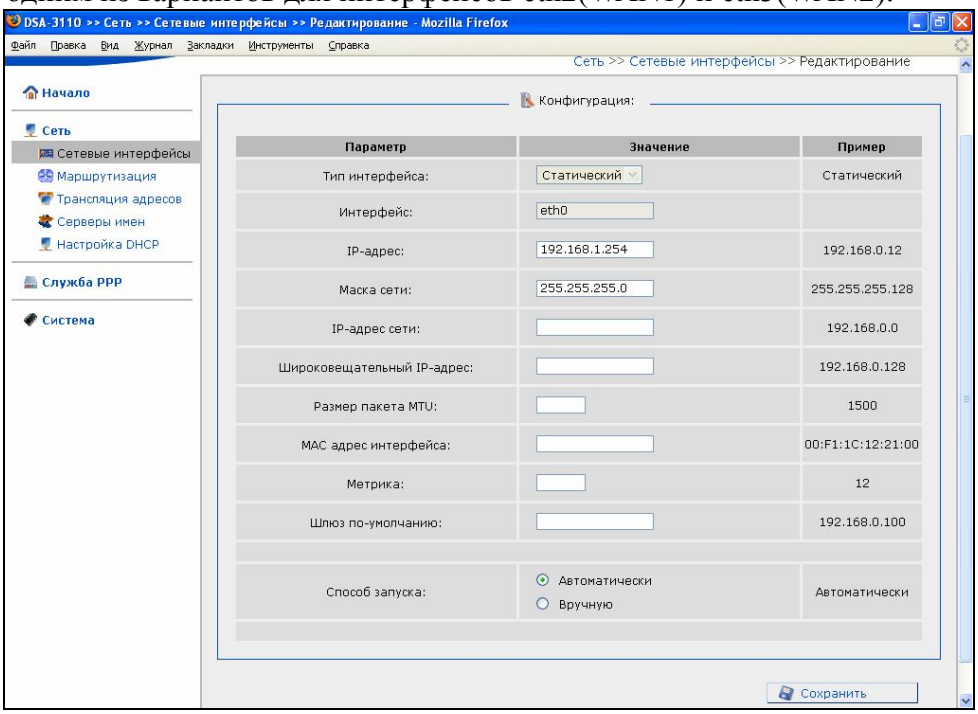

Рисунок 10. Настройка статического IP адреса на интерфейсе

- **IP-адрес**: присваиваемый интерфейсу IP-адрес
- **Маска сети**: маска подсети
- **IP-адрес сети**: адрес IP-сети конфигурируемого интерфейса, *необязательный параметр*, определяется автоматически по маске подсети.
- **Широковещательный IP-адрес**: адрес сети для рассылки широковещательных пакетов. *Необязательный параметр*, определяется автоматически по маске подсети.
- **MAC-адрес интерфейса**: аппаратный адрес для установки на интерфейс. *Необязательный параметр*.
- **Размер пакета MTU**: позволяет вручную сконфигурировать максимальный размер передаваемого интерфейсом пакета. *Необязательный параметр.*
- **Метрика**: метрика интерфейса. Позволяет назначить приоритет интерфейса. *Необязательный параметр*.
- **Шлюз по умолчанию**: IP-адрес шлюза по умолчанию. Задает адрес для маршрутизации пакетов во внешние сети (применим только для WAN интерфейсов). *Необязательный параметр.*

Нажать кнопку **Сохранить**

Настройка интерфейса DHCP

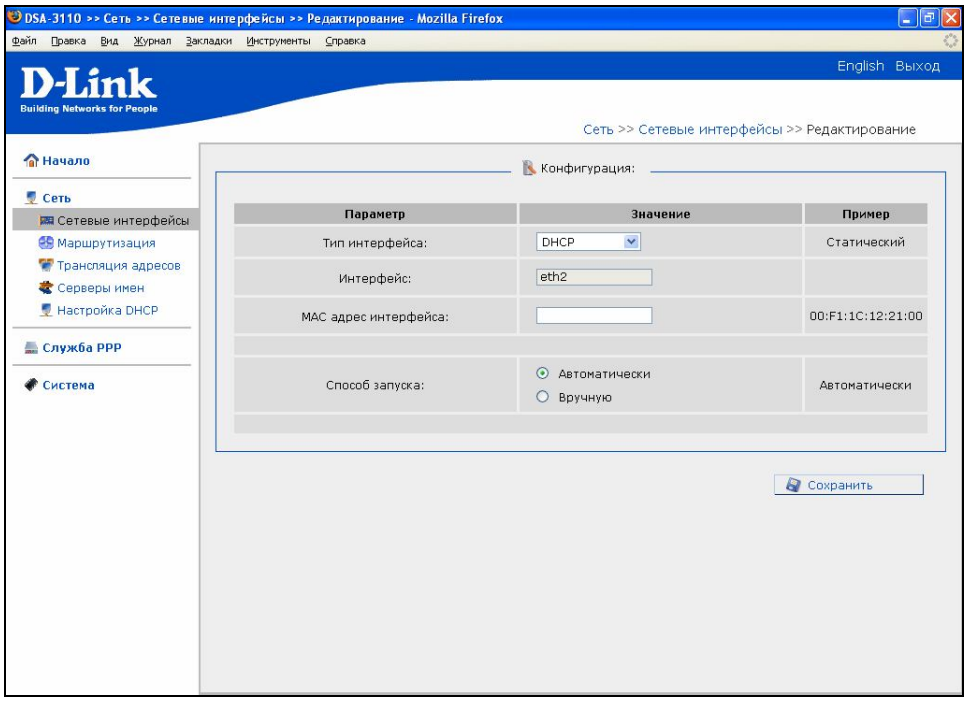

Рисунок 11. Настройка DHCP клиента на интерфейсе.

- **Имя**: название конфигурируемого интерфейса
-
- **Тип интерфейса**: способ конфигурации данного интерфейса (DHCP)
- **Имя хоста**: имя для идентификации при получении адреса от сервера DHCP. *Необязательный параметр*.
- **MAC-адрес интерфейса**: аппаратный адрес для установки на интерфейс. *Необязательный параметр*.
- **Способ запуска**: позволяет включить или выключить автоматический запуск данного интерфейса при загрузке устройства.

Нажать кнопку **Сохранить**

Добавление или изменение настроек интерфейса PPTP

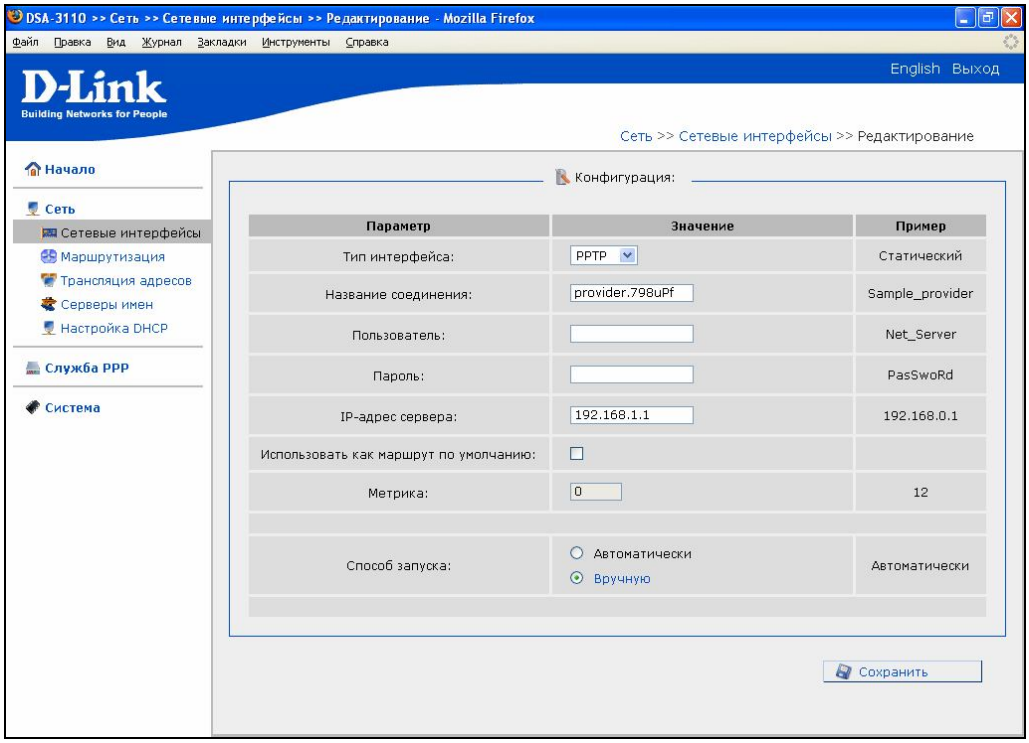

Рисунок 12. Настройка PPTP клиента на интерфейсе

- **Тип интерфейса**: способ конфигурации данного интерфейса (PPTP)
- **Название соединения**: имя соединения для идентификации. *Необязательный параметр*.
- **Пользователь**: Имя пользователя для регистрации на PPTP сервере.
- **Пароль**: Пароль пользователя для регистрации на PPTP сервере.
- **IP –адрес сервера:** IP адрес PPTP сервера.
- **Использовать как маршрут по умолчанию:** Использовать IP адрес сервера как маршрут по умолчанию (адрес назначения всех пакетов, для которых не был найден маршрут)
- **Метрика:** Параметра служащий для определения приоритетности данного соединения перед другими
- **Способ запуска**: позволяет включить или выключить автоматический запуск данного интерфейса при загрузке устройства.

Нажать кнопку **Сохранить**

Добавление или изменение настроек интерфейса PPPoE

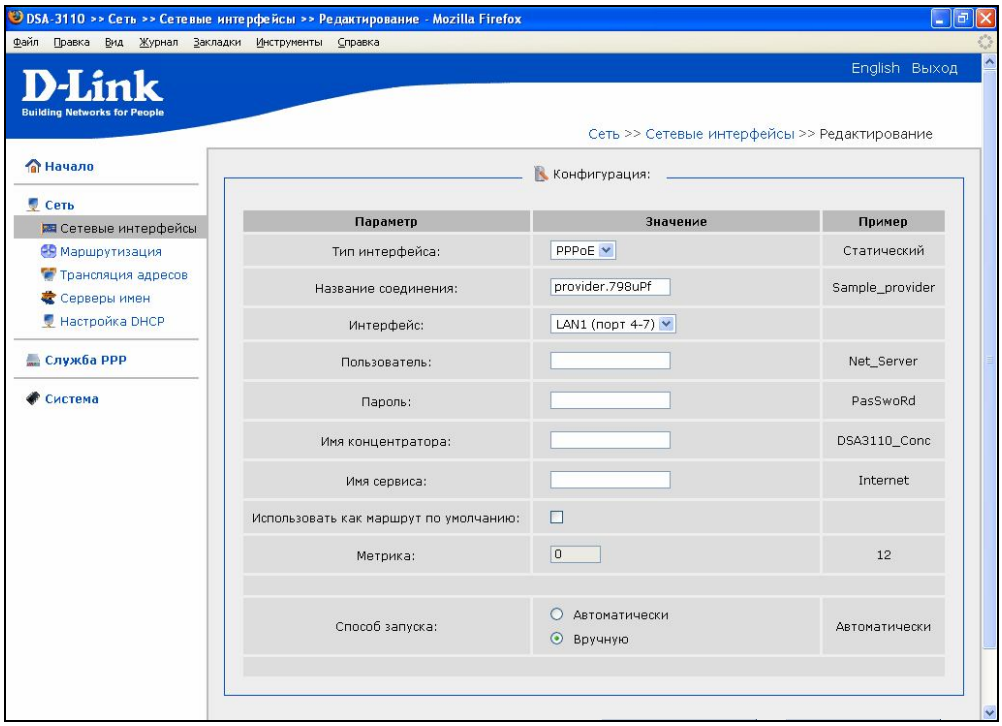

Рисунок 13. Настройка PPPoE клиента на интерфейсе

- **Тип интерфейса**: способ конфигурации данного интерфейса (PPPoE)
- **Название соединения**: имя соединения для идентификации. *Необязательный параметр*.
- **Интерфейс**: наименование интерфейса, к которому будет «привязан» конфигурируемый PPPoE интерфейс.
- **Пользователь**: Имя пользователя для регистрации на PPPoE сервере.
- **Пароль**: Пароль пользователя для регистрации на PPPoE сервере.
- **Имя концентратора:** Имя PPPoE сервера провайдера
- **Имя сервиса:**
- **Использовать как маршрут по умолчанию:** Использовать IP адрес сервера как маршрут по умолчанию (адрес назначение всех IP пакетов, для которых не был найден маршрут)
- **Метрика:** Параметра служащий для определения приоритетности данного соединения перед другими
- **Способ запуска**: позволяет включить или выключить автоматический запуск данного интерфейса при загрузке устройства.

Нажать кнопку **Сохранить**

После изменения настроек физических интерфейсов или добавления/изменения настроек виртуальных интерфейсов вы получите **Новую** конфигурацию интерфейсов (см. рис.14). В данной закладке меню вы можете сохранить новую конфигурацию с помощью кнопки **Применить,** либо отказаться от ее сохранении с помощью кнопки **Удалить.**

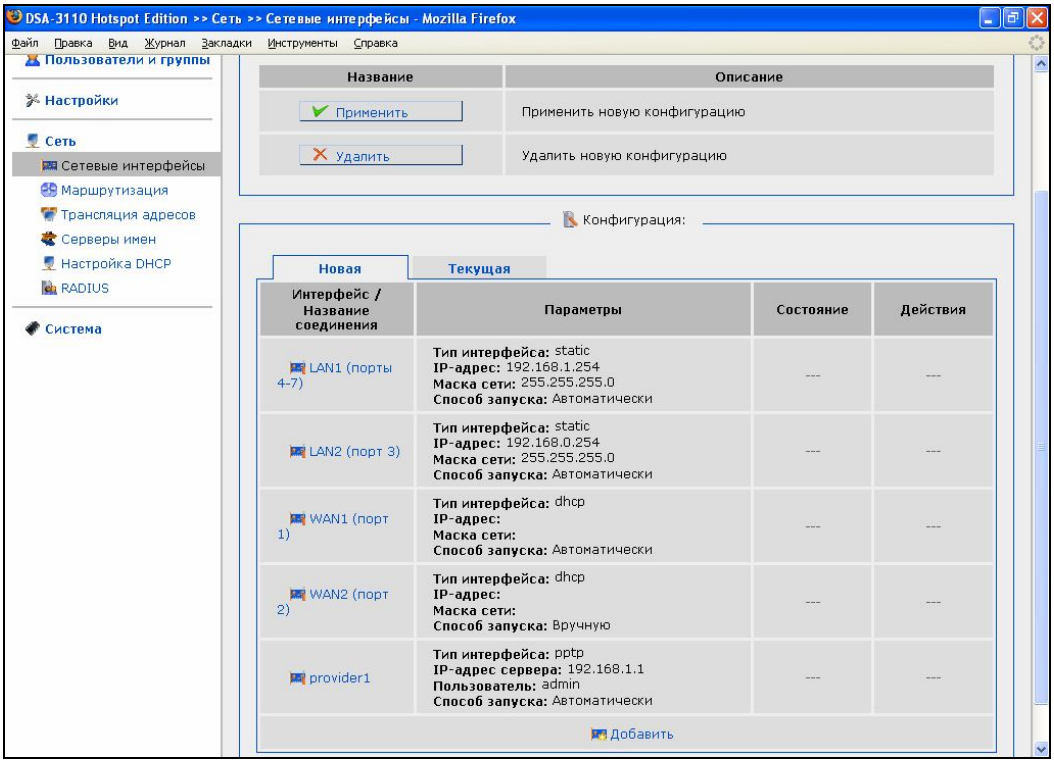

Рисунок 14. Сохранение изменений конфигурации интерфейсов

Маршрутизация

Это пункт предназначен для добавления в систему статических маршрутов (маршрутов к сетям, непосредственно не присоединенным к устройству, но доступным через интерфейсы устройства).

Изменение настроек статической маршрутизации:

- Откройте меню **Сеть- Маршрутизация**
- Нажмите кнопку **Добавить маршрут**
- Введите настройки маршрута:
  Сеть направления - сеть назначения, к которой прописывается данный маршрут
  Маска сети направления - маска сети назначения
  Шлюз – IP адрес, через который доступна сеть назначения
  Метрика- метрика маршрута
  Через интерфейс - укажите интерфейс, через который доступна сеть назначения. В случае указания значения данного параметра **Автоматически**, интерфейс будет вычислен устройством на основе данных об присоединенных сетях.
- Нажмите кнопку **Сохранить**

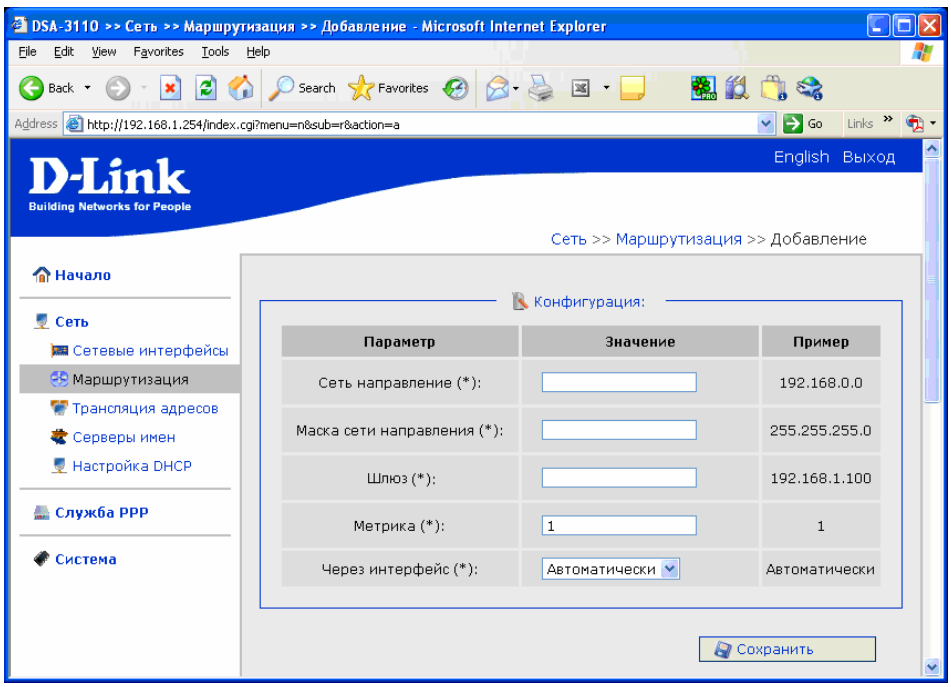

Рисунок 15. Добавление статического маршрута

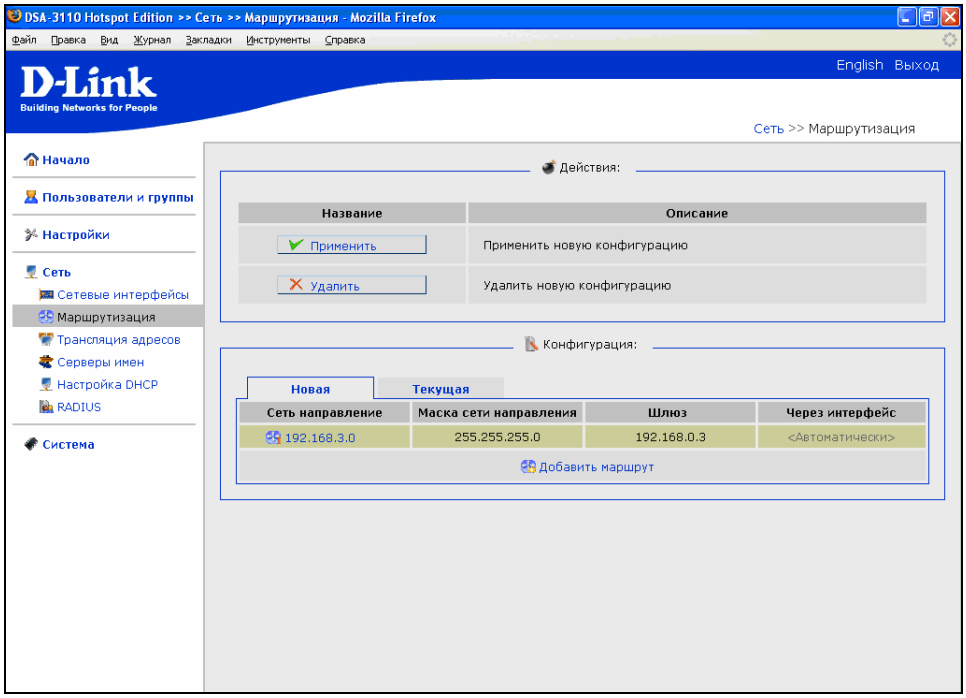

Рисунок 16. Применение статического маршрута

Нажмите кнопку **Применить**, для применения новой конфигурации маршрутов.

Трансляция сетевых адресов

Выберите этот пункт меню для настройки NAT (Network address translation).
Данный пункт меню используется, чтобы объявить подсети, которым требуется трансляция адресов. Физический интерфейс, используемый для трансляции той или иной сети, выбирается автоматически на основании сетевых настроек, сделанных в пункте Сеть - Сетевые интерфейсы.

По умолчанию NAT осуществляется для сетей 192.168.1.0/24 и 172.22.0.0/24

- Откройте меню **Сеть- Трансляция адресов**
- Нажмите **Редактировать**

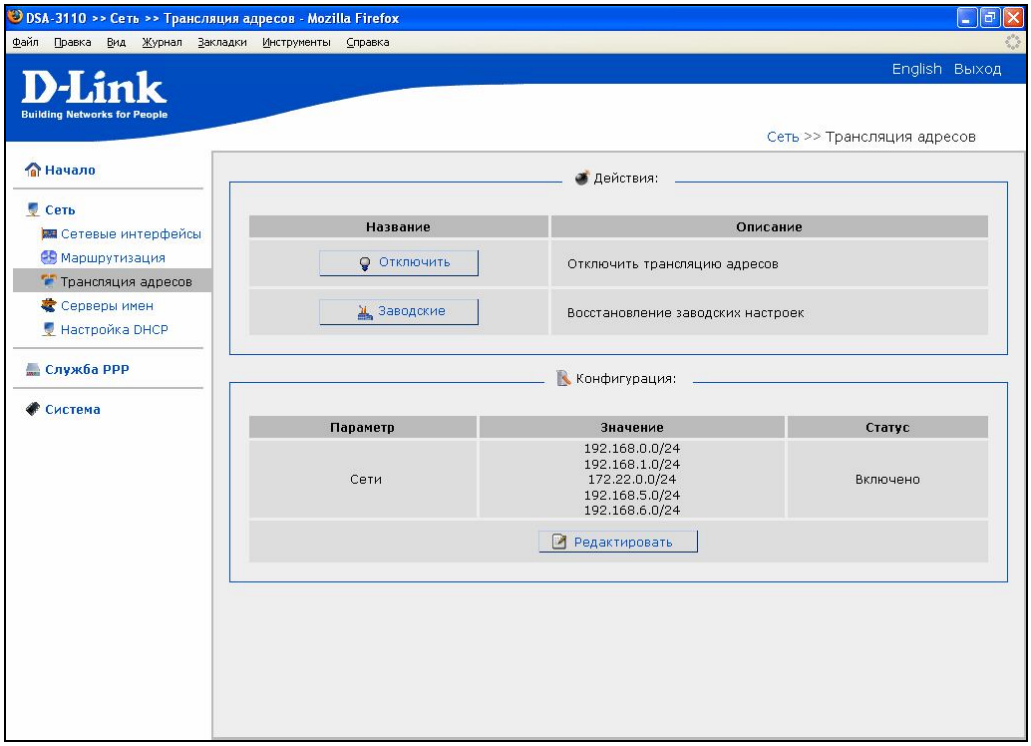

Рисунок 17. Меню Сеть – Трансляция адресов

- Введите подсеть и через слеш количество двоичных разрядов сетевой маски, которые равны 1 (например, /16 соответствует 255.255.0.0, /24 255.255.255.0 , /30 – 255.255.255.252 и т. д.).
- Нажмите кнопку **Сохранить**.

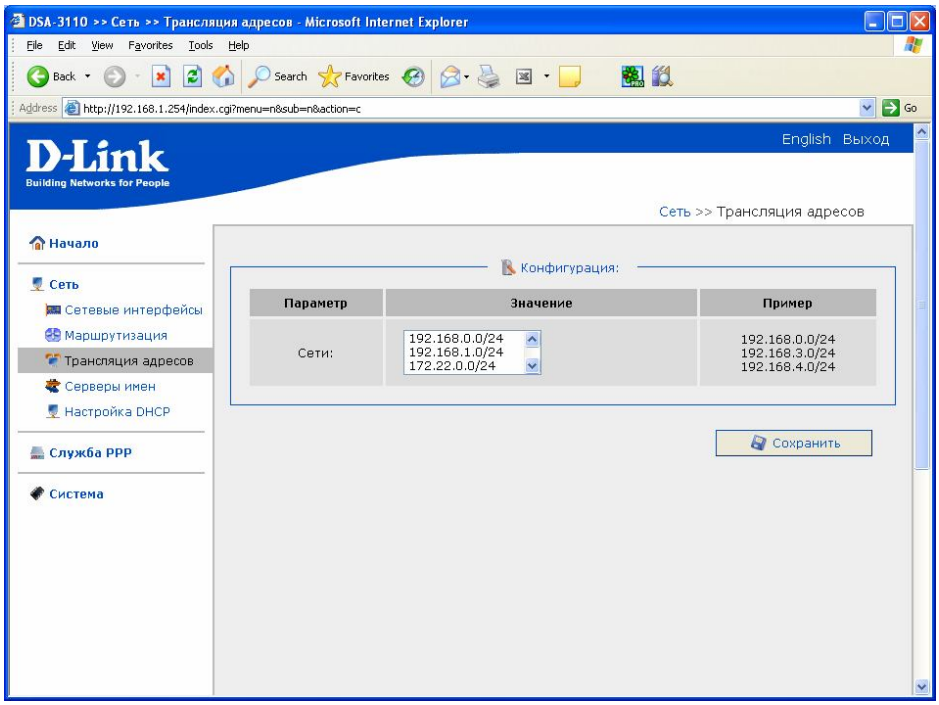

Рисунок 18. Настройка Трансляции адресов.

Сервера имен

Это пункт предназначен для добавления в систему серверов имен (DNS серверов) и доменов поиска.

Первые используются для сопоставления IP и имени сервера в Интрасетях или Интернете (обычно указываются провайдером или назначаются администратором сети), вторые нужны для автоподстановки домена первого или второго уровня при указании неполного имени (например, указываете yandex - подставляется yandex.ru) .

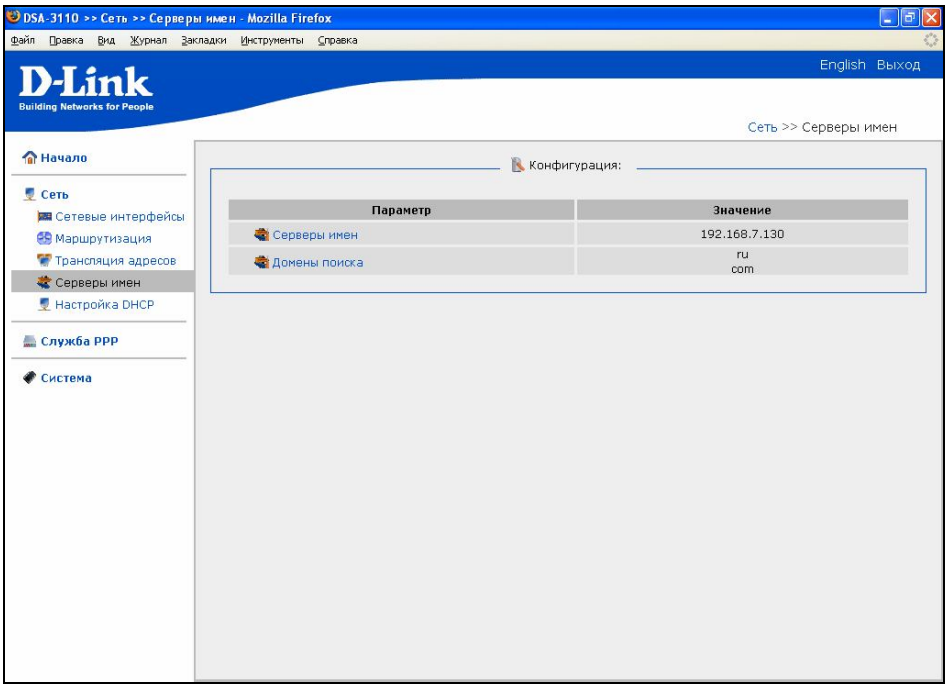

Рисунок 19. Серверы имен

Добавление DNS сервера

- Откройте меню **Сеть -> Серверы имен**
- Выберите **Серверы имен**
- Введите в поле **значение** IP адреса DNS серверов (разрешается один IP адрес в каждой строчке, но не более 3 IP адресов)
- Нажмите кнопку **Сохранить**

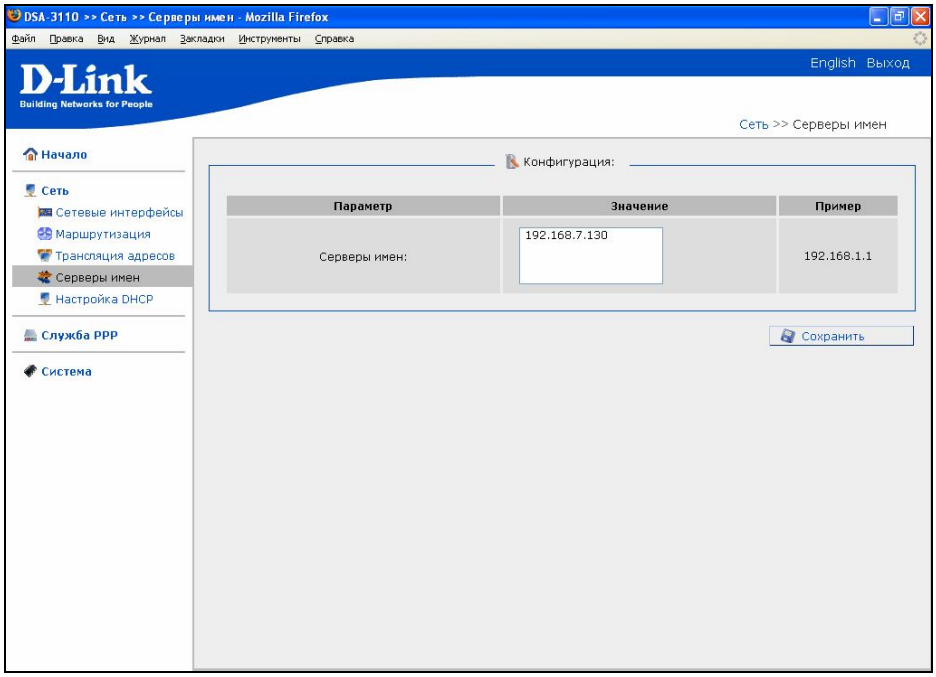

Рисунок 20. Добавление Сервера имен

Добавление Домена поиска

- Откройте меню **Сеть -> Серверы имен**
- Выберите **Домены поиска**
- Введите в поле **значение** имена доменов первого или второго уровня (разрешается одно имя в каждой строчке, но не более 3 IP адресов)
- Нажмите кнопку **Сохранить**

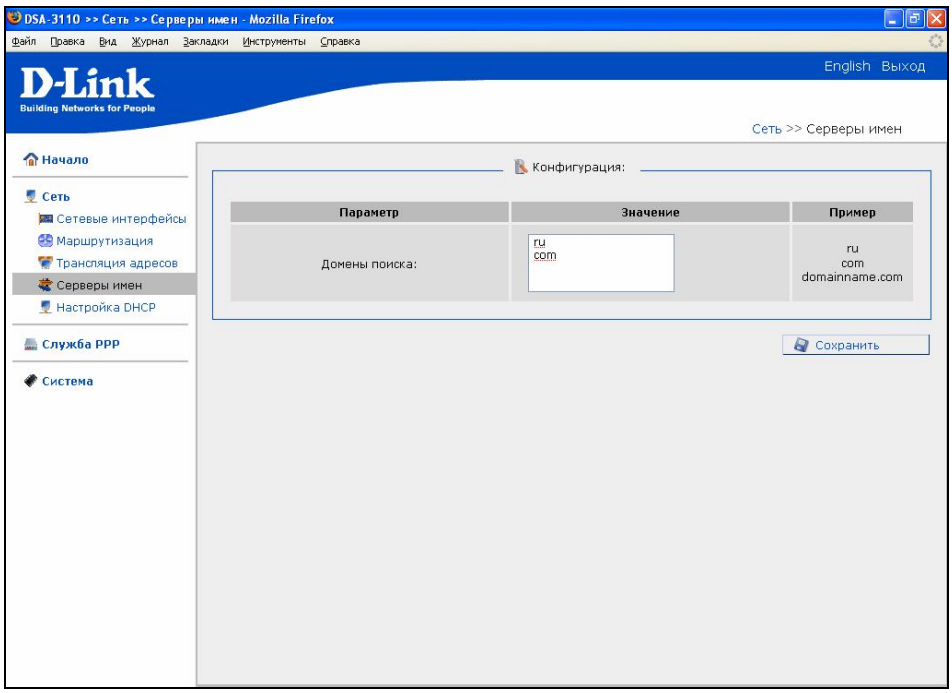

Рисунок 21. Добавление домена поиска

DHCP Сервер

Это пункт предназначен для настройки внутреннего DHCP сервера устройства.
Данный сервер используется для автоматической выдачи IP адресов пользователям, подключенным к интерфейсу LAN1.
В настройках данного пункта меню можно

- Непосредственно включить или выключить внутренний DHCP сервер (отметить поле **DHCP включен**);
- Установить начальный и конечный IP-адрес пула IP адресов, используемых для выдачи DHCP сервером IP адресов клиентам. Для этого в полях **Начало диапазона** и **Конец диапазона,** устанавливается соответственно четвертый октет начального и конечного IP адреса (первые три октета IP адреса принимаются равными октетам интерфейса LAN1 и отображаются на WEB-интерфейсе (они равны умолчанию 192.168.1.).
- Время жизни выделенного IP адреса для DHCP в минутах (время выделения IP адреса, через которое в отсутствие от устройства подтверждения о необходимости сохранения это IP адрес отзывается и может быть отдан другому устройству).

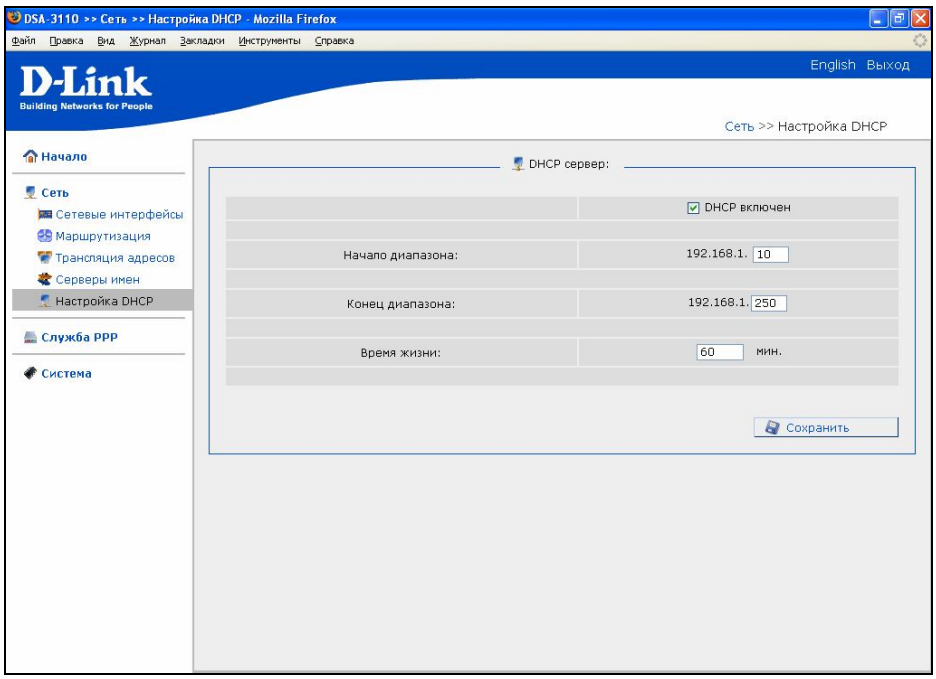

Рисунок 22. Настройка внутреннего DHCP сервера

Меню-Служба PPP

Раздел описывает настройку сервера доступа (внутреннего сервера PPTP или PPPoE). **Внимание:** Одновременно может использоваться **как один** из протоколов доступа, **так и оба** вместе, однако база данных пользователей является общей для обоих протоколов.

Настройка параметров сервера доступа осуществляется через Web-интерфейс: Откройте меню **Служба PPP**

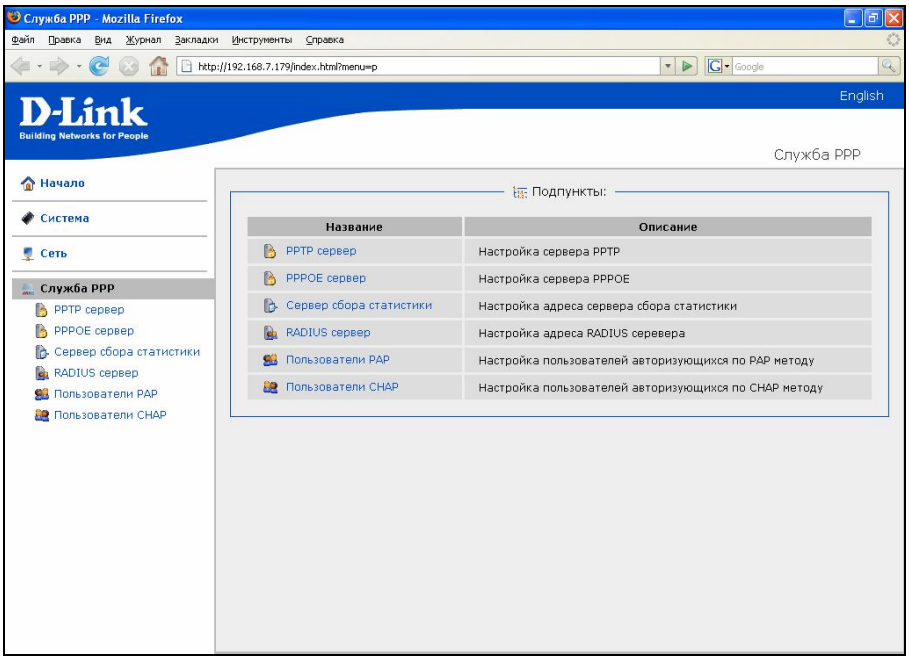

Рисунок 23. Меню Служба PPP.

PPTP Сервер

Этот пункт меню предназначен для определения настроек внутреннего PPTP сервера.

Выберите **Сервер PPTP**

На появившейся странице будет отображена текущая конфигурация сервера PPTP

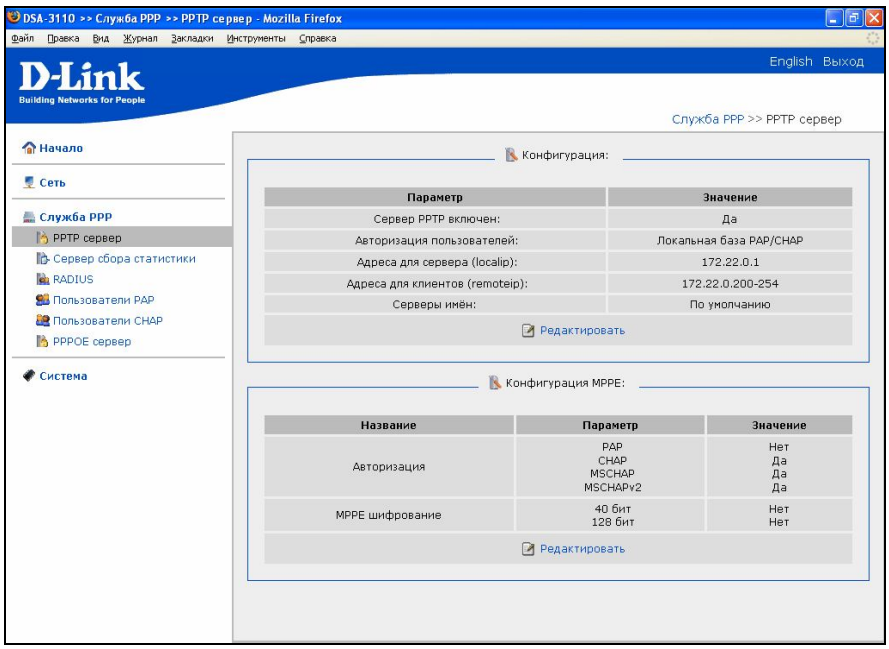

Рисунок 24. Меню Служба PPP- PPTP сервер.

Нажмите Конфигурация **-Редактировать**

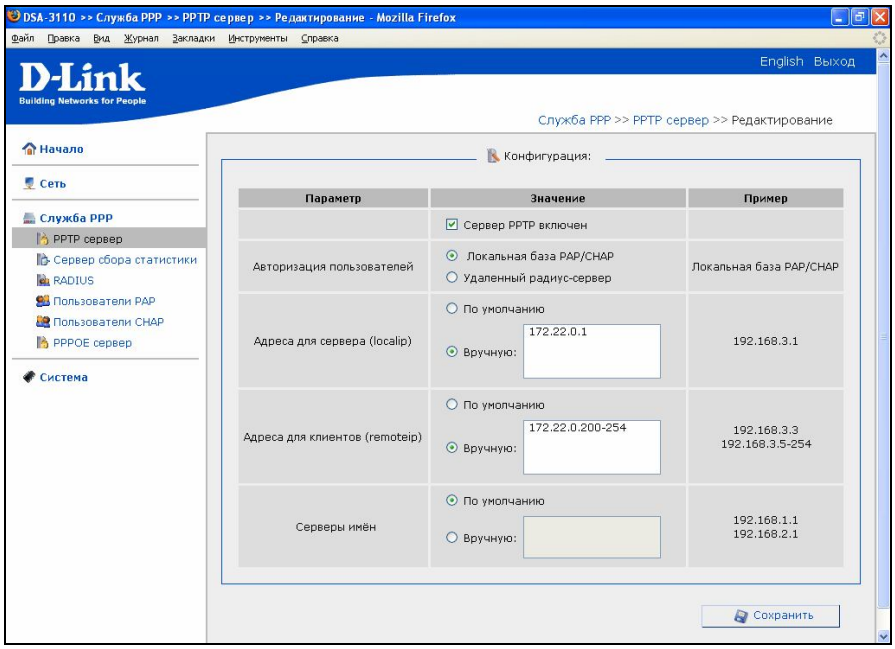

Рисунок 25. Настройка PPTP сервера.

Сервер PPTP включен: флаг, включающий или выключающий внутренний PPTP сервер на устройстве
Авторизация пользователей: выбор базы данных пользователей – локально или удаленная на внешнем сервере RADUIS

Внимание: при использовании базы данных внешнего сервера RADIUS пользователи в локальной базе авторизоваться не будут!

Адреса для сервера (localip): список адресов, используемых сервером PPP со своей стороны. Допускается перечисление сетей через запятую, указание диапазонов через дефис.
Адреса для клиентов (remoteip): список адресов, выделяемых сервером подключающимся клиентам. Допускается перечисление сетей через запятую, указание диапазонов через дефис.
Серверы имен: список IP адресов, назначаемых в качестве серверов имен (DNS) при PPP соединениях.

По окончанию изменения настроек нажмите кнопку. С**охранить**

Нажмите **Конфигурация MPPE- Редактировать**

PAP, CHAP, MSCHAP, MSCHAPv2: флаги, включающий соответствующие протоколы авторизации на PPTP сервере устройства
40бит, 128бит : флаги, включающие шифрование PPTP соединений (MPPE) с выбранной длиной ключа

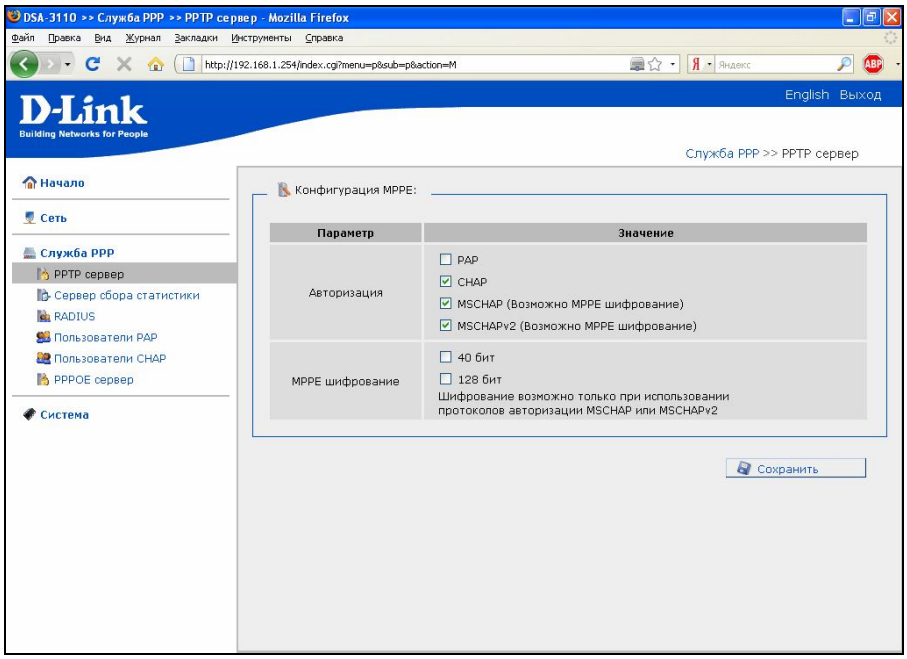

Рисунок 26. Настройка PPTP сервера.

По окончанию изменения настроек нажмите кнопку. С**охранить**

PPPoE Сервер

Этот пункт меню предназначен для определения настроек внутреннего PPPoE сервера

Выберите пункт меню **PPPoE сервер**

На появившейся странице будет отображена текущая конфигурация сервера PPPoE

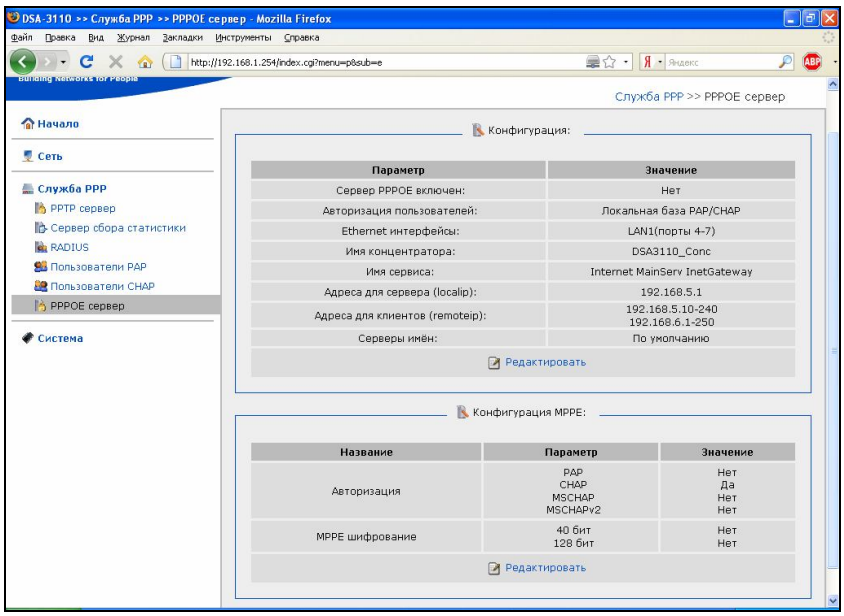

Рисунок 27. Меню Служба PPP- PPPoE сервер.

Нажмите **Конфигурация- Редактировать**

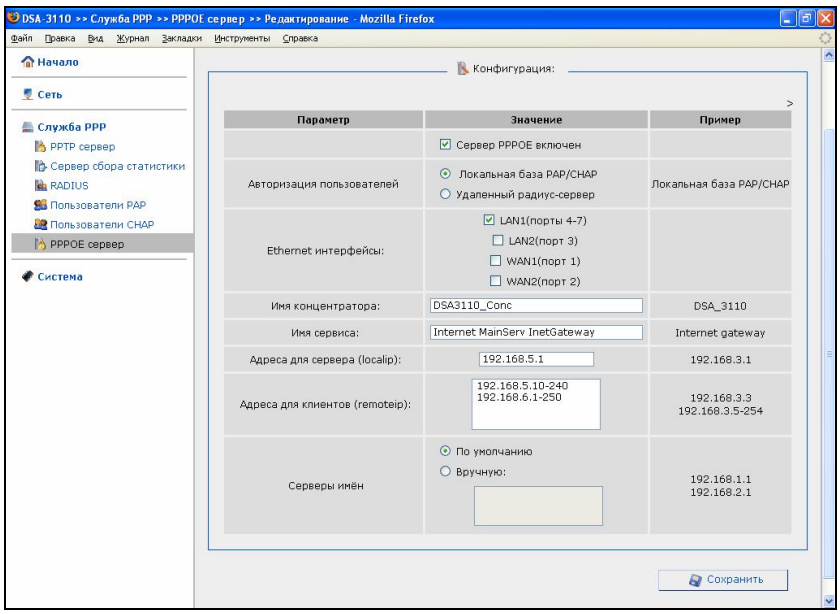

Рисунок 28. Настройка PPPoE сервера

Сервер PPPoE включен: флаг, включающий или выключающий внутренний PPPoE сервер на устройстве
Авторизация пользователей: выбор базы данных пользователей – локально или удаленная на внешнем сервере RADUIS
Внимание: при использовании базы данных внешнего сервера RADIUS пользователи в

локальной базе авторизоваться не будут!

Ethernet интерфейсы: флаг, определяющий на каких из физических интерфейсов устройства (eth0-eth4) производится авторизация клиентов по протоколу PPPoE внутренним сервером устройства
Имя концентратора: имя (Access Concentrator name), назначаемое PPPoE серверу в сети Ethernet. Применяется при наличии в сети нескольких PPPoE серверов для разделения сервисов, предоставляемых этими серверами доступа (AC name может пересылаться в пакетах PADR и служить для выбора клиентом нужного PPPoE сервера).
Имя сервиса: имя (Service name), назначаемое PPPoE серверу в зависимости от типа услуги, предоставляемой сетью, в которую производится доступ. На практике, при наличии нескольких PPPoE серверов в сети, используется для выбора клиентом нужного PPPoE сервера (Service name пересылается в пакетах PADO и сравнивается с запрошенным клиентом именем).
Адреса для сервера (localip): список адресов, используемых сервером PPPoE со своей стороны. Допускается перечисление сетей через запятую, указание диапазонов через дефис.
Адреса для клиентов (remoteip): список адресов, выделяемых сервером подключающимся клиентам. Допускается перечисление сетей через запятую, указание диапазонов через дефис.
Серверы имен: список IP адресов, назначаемых в качестве серверов имен (DNS) при PPP соединениях.

По окончанию изменения настроек нажмите кнопку **Сохранить.**

Нажмите **Конфигурация MPPE- Редактировать**

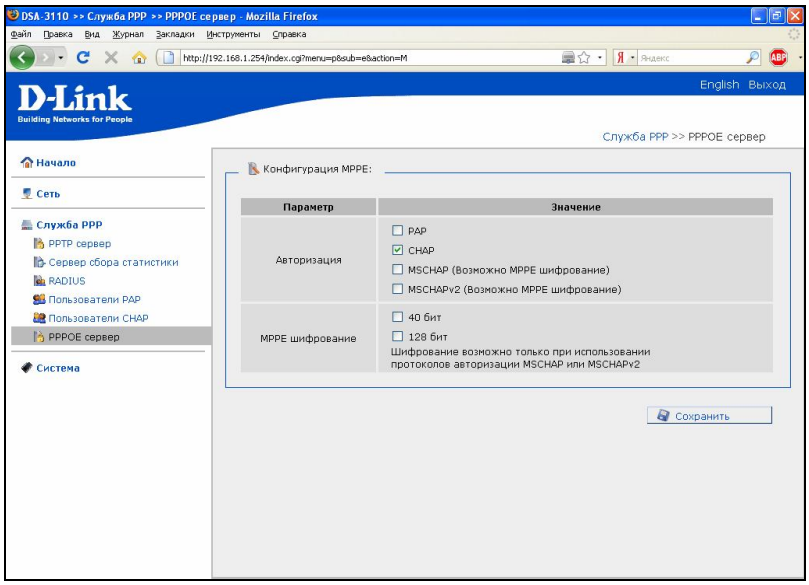

Рисунок 29. Настройка PPPoE сервера

PAP, CHAP, MSCHAP, MSCHAPv2: флаги, включающий соответствующие протоколы авторизации на PPPoE сервере устройства
40бит, 128бит : флаги, включающие шифрование PPPoE соединений (MPPE) с выбранной длиной ключа

По окончанию изменения настроек нажмите кнопку **Сохранить.**

Конфигурация сервера сбора статистики

Этот пункт меню предназначен для определения настроек внешнего сервера сбора статистики (NetFlow коллектора).

Выберите **Сервер сбора статистики**

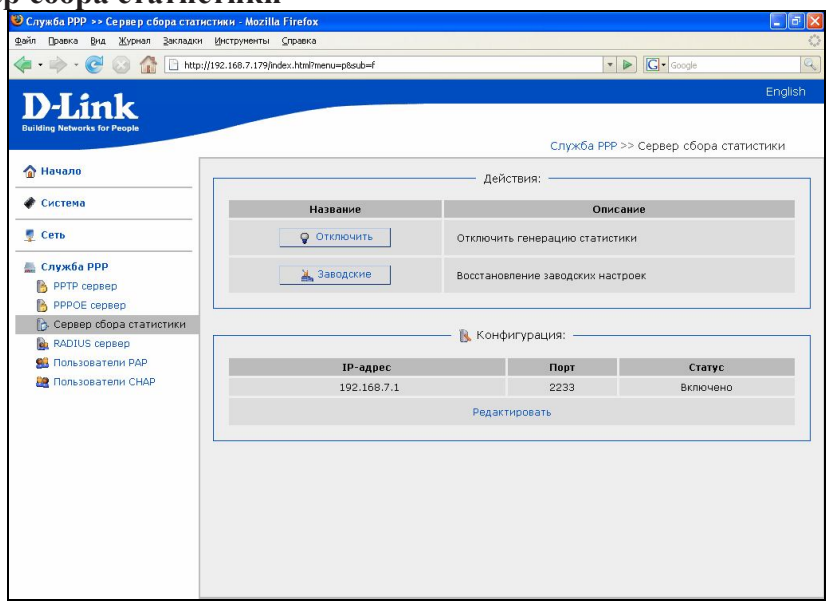

Рисунок 30. Меню Служба PPP- Сервер сбора статистики.

Отключить: нажатие этой кнопки приведет к отключению сбора и выдачи статистики. Используйте эту опцию, если вам не требуется сбор статистики о подключающихся пользователях или у вас нет сервера сбора статистики.
Заводские: нажатие этой кнопки приведет к сбросу настроек сервера к заводским установкам. Используйте эту опцию в случае необходимости возврата настроек к заводским, например в случае повреждения файла настройки в интерфейсе командной строки CLI.

Для редактирования настроек нажмите на адрес сервера в таблице **Параметры**:

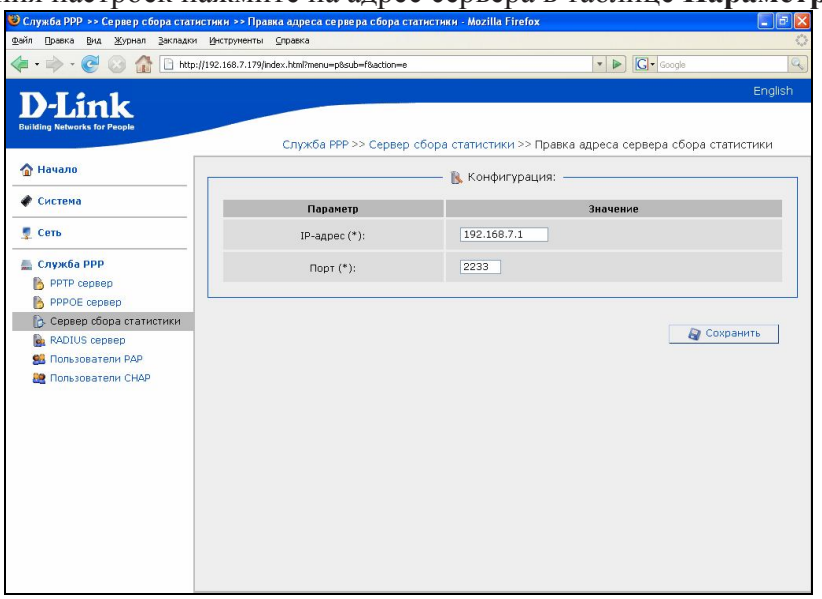

Рисунок 31. Настройка сервера сбора статистики.

IP- адрес: введите IP-адрес сервера сбора статистики
Порт: введите номер порта, через который ПО сбора статистики принимает данные.
По окончанию изменения настроек нажмите кнопку **Сохранить**

Настройка сервера RADIUS

Выберите этот пункт меню для определения настроек внешнего RADIUS сервера.
Выберите **Сервер RADIUS**
На появившейся странице будет отображена текущая конфигурация сервера RADIUS.

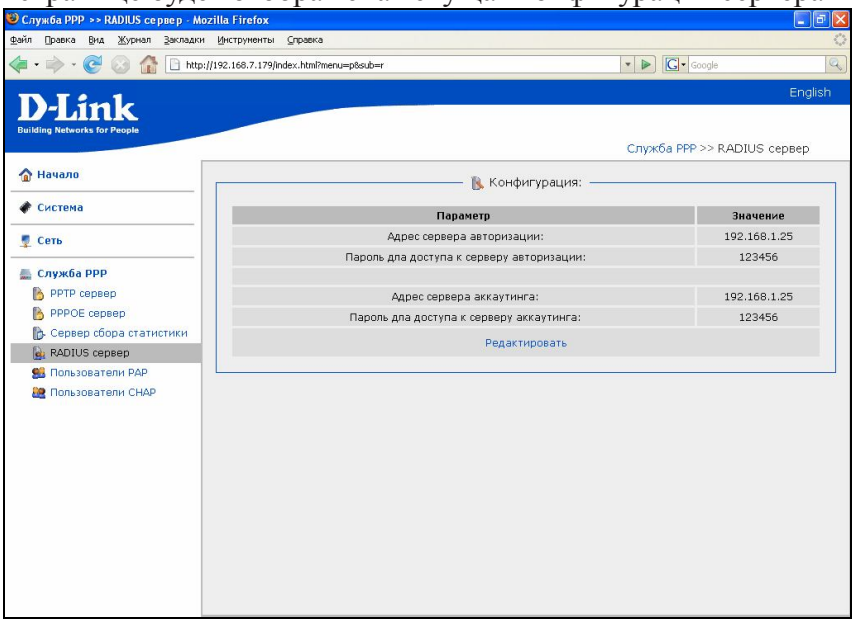

Рисунок 32. Меню Служба PPP – RADIUS сервер.

Нажмите **Редактировать**

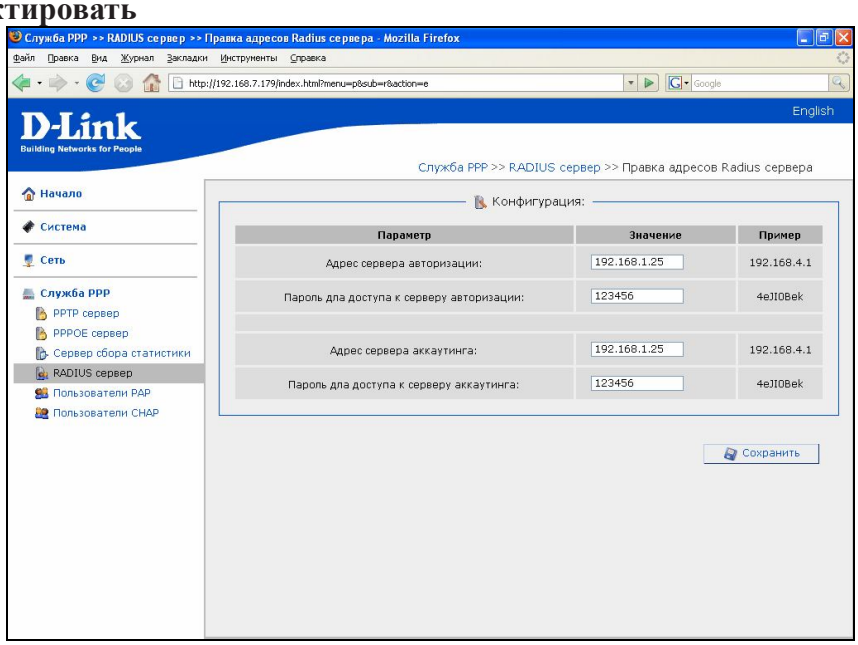

Рисунок 33. Настройка сервера RADIUS.

Адрес сервера авторизации: введите IP-адрес RADIUS-сервера, осуществляющего авторизацию клиентов
Пароль для доступа к серверу авторизации: введите пароль (secret), используемый для обмена с данным сервером
Адрес сервера аккаунтинга: введите IP-адрес RADIUS-сервера, осуществляющего аккаунтинг подключений
Пароль для доступа к серверу аккаунтинга: введите пароль (secret), используемый для обмена с данным сервером
По окончанию изменения настроек нажмите кнопку **Сохранить**

Работа с локальной базой пользователей

Локальная база пользователей состоит из двух независимых баз, содержащих учетные записи пользователей, авторизующихся по протоколу PAP и CHAP соотвественно. Вы можете добавлять, изменять и удалять учетные записи в каждой из баз.
Примечание: пользователи, автризующиеся по протоколам MS-CHAP и MS-CHAPv2 должны заносится в базу данных CHAP.

Для работы с базой пользователей, авторизующихся по протоколу PAP, нажмите **Пользователи PAP**. Для работы с базой авторизующихся по CHAP нажмите **Пользователи CHAP**. Работа с обеими базами идентична.

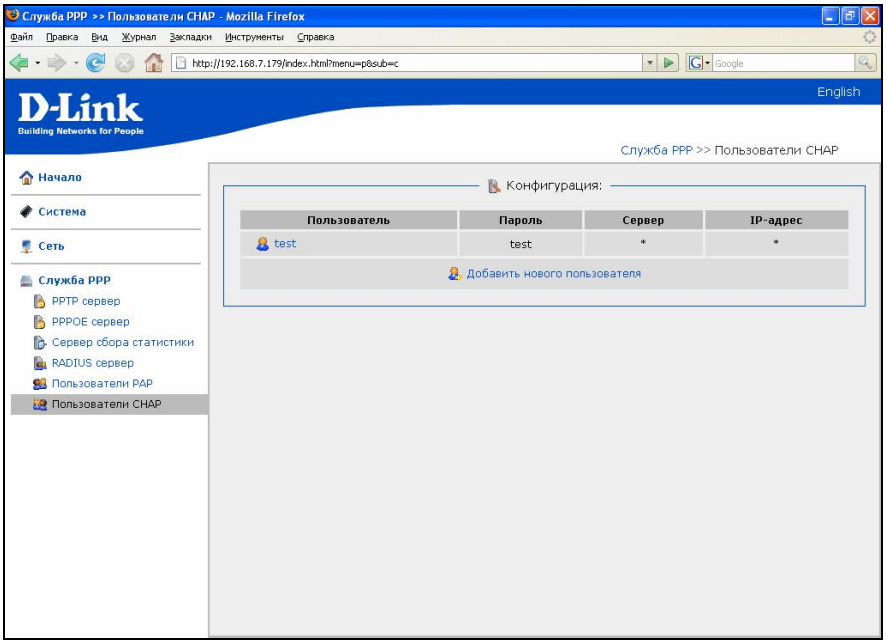

Рисунок 34. Меню Служба PPP- Пользователи CHAP

После выбора базы появится список существующих учетных записей. Для редактирования нажмите на нужной записи, для добавления новой записи нажмите **Добавить нового пользователя:**

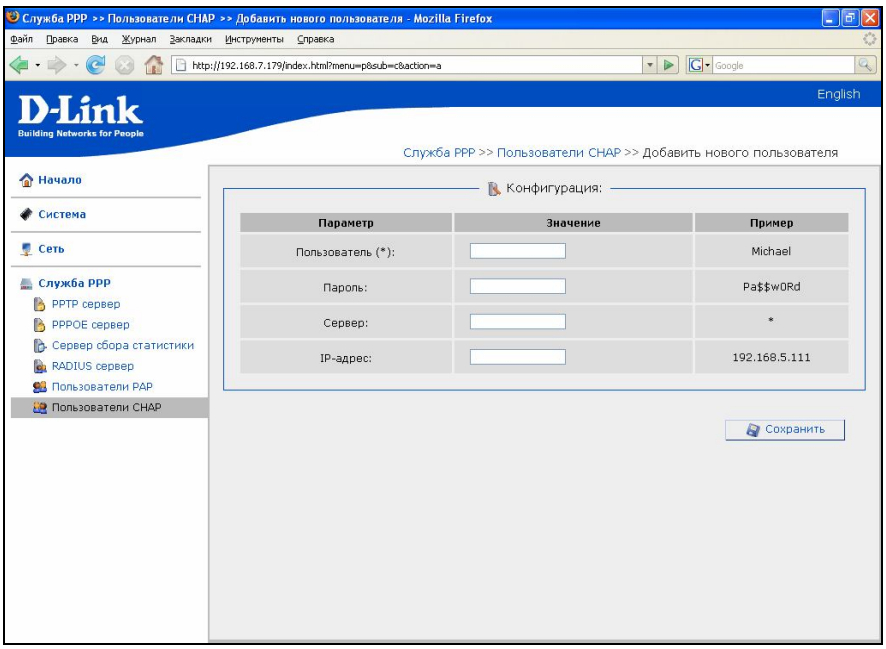

Рисунок 35. Настройка локальной базы пользователей

- **Логин**: имя учетной записи, используется как имя пользователя при подключении
- **Пароль**: пароль учетной записи
- **Сервер**: имя сервера для подключения, *необязательный параметр*
- **IP -адрес**: позволяет задать данной учетной записи постоянный IP- адрес

- По окончанию изменения настроек нажмите кнопку **Сохранить**

Меню-Система

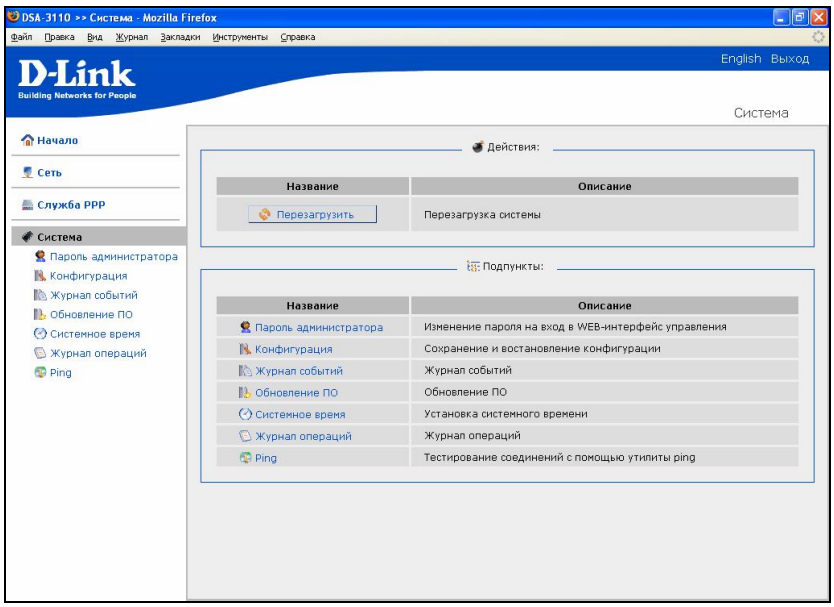

Рисунок 36. Меню Система.

Перезагрузить - нажатие этой кнопки приводит к перезагрузке устройства

Пароль администратора

Выберите этот пункт для изменения параметров учетной записи администратора для доступа к WEB-интерфейсу настройки

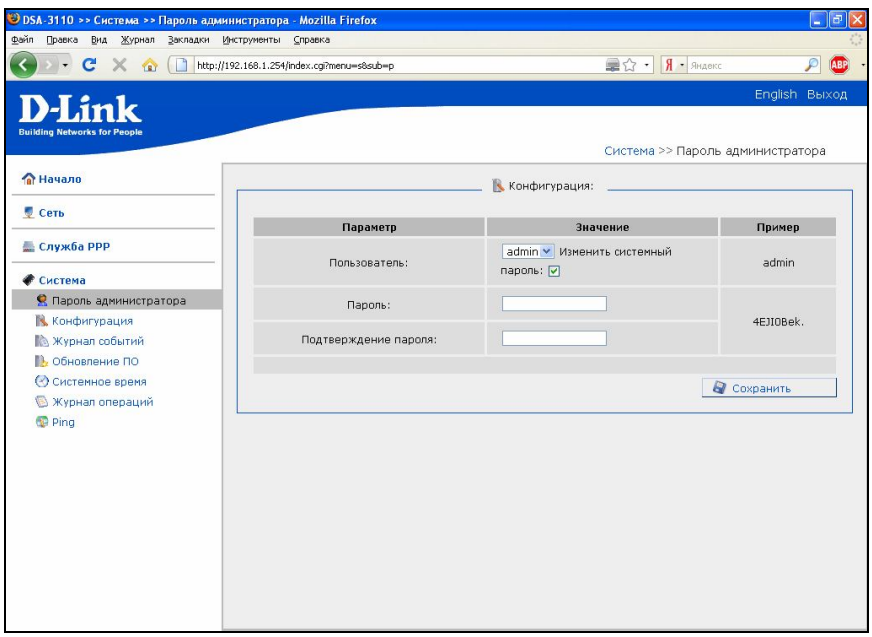

Рисунок 37. Изменение пароля администратора

Логин: имя пользователя с правами администратора. Введите новое имя пользователя или оставьте поле без изменений для сохранения старого значения.
Пароль: введите новый пароль WEB-администратора
Подтверждение пароля: введите новый пароль еще раз для исключения ошибок и опечаток при вводе.
Опция **Изменить системный пароль** позволяет менять пароль на введенный не только для доступа к WEB- интерфейсу, но и командному (CLI) режиму. Редомендуется держать эту опцию включенной.
По окончанию изменения настроек нажмите кнопку **Сохранить**

Конфигурация

Выберите этот пункт для сохранения изменений или сброса параметров устройства к заводским установкам.

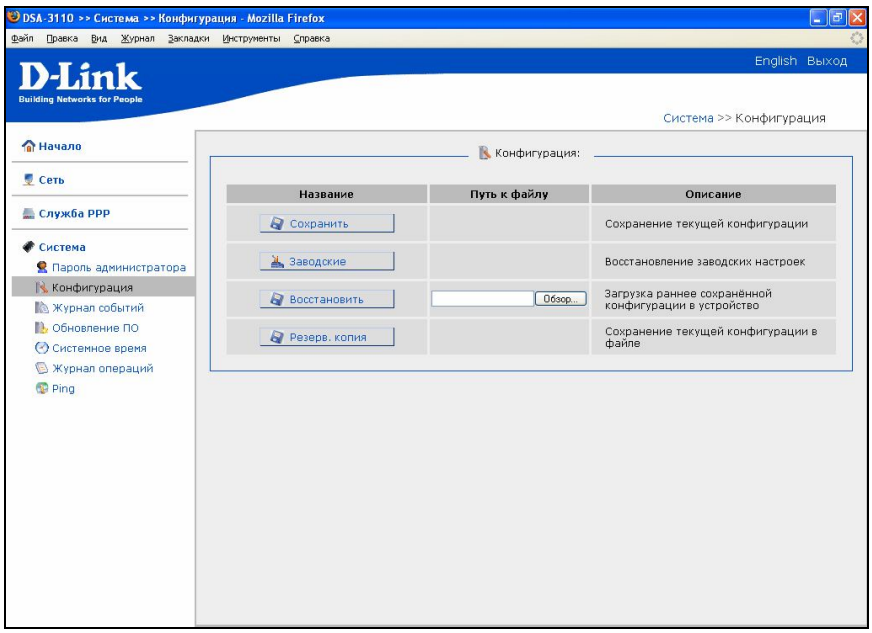

Рисунок 38. Меню работы с конфигурацией системы

Кнопка **Сохранить**: нажмите для сохранения изменений конфигурации устройства в энергонезависимой памяти.

Внимание: Этот пункт меню сохраняет изменение настроек, сделанных во всех разделах меню в энергонезависимой памяти.

Кнопка **Заводские**: нажмите для сброса всех параметров устройства к заводским установкам.
Кнопка **Восстановить**: нажмите на эту кнопку для загрузки сохраненной конфигурации устройства с персонального компьютера
Кнопка **Резерв.копия**: нажмите на эту кнопку для сохранения конфигурации устройства на персональный компьютер.

Журнал событий

Выберите этот пункт для просмотра внутреннего лог файла системы.
В данном логе кроме результатов загрузки устройства и работы внутренней операционной системы устройства будут отмечаться также события входа и выхода пользователей с указанием времени.
При указании отметки **Удаленное журналирование** и вводе IP адреса в поле **Сервер**, будет осуществляться передача данного лога по протоколу Syslog на UDP порт 514 указанного IP адреса.

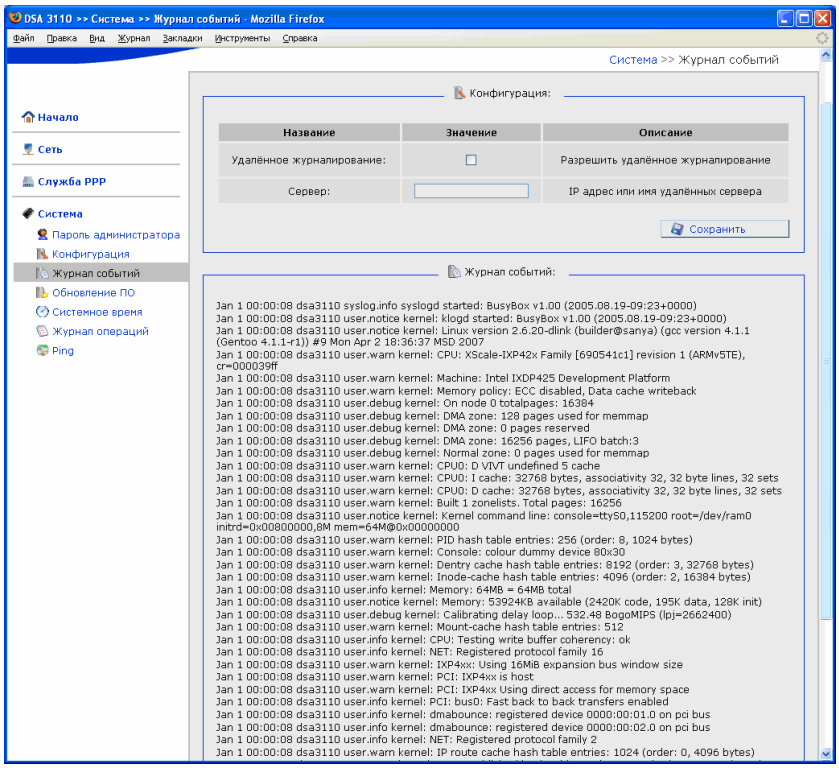

Рисунок 39. Журнал событий

Обновление ПО

Выберите этот пункт для просмотра обновления встроенного ПО устройства.

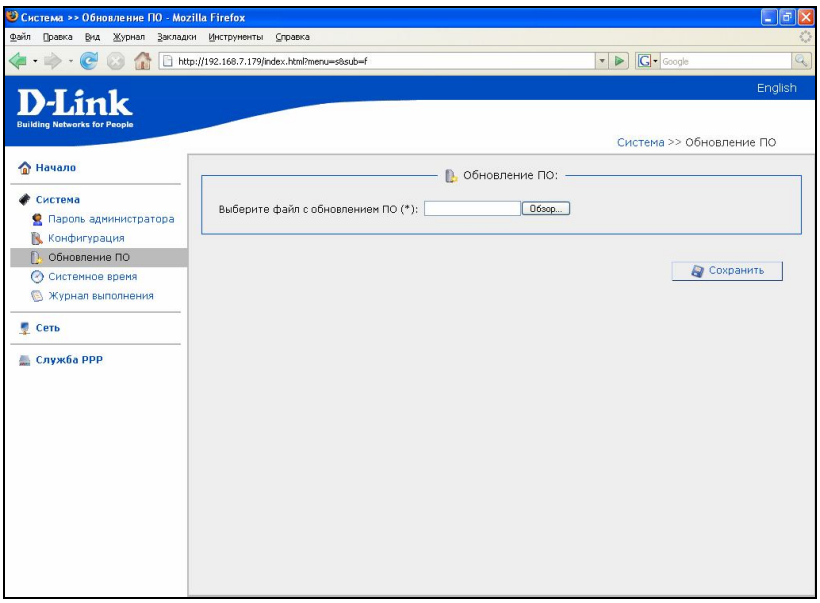

Рисунок 40. Обновление ПО через Web-интерфейс

Для обновления ПО:
Нажмите кнопку **Обзор**
Выберите файл ПО на локальном компьютере
Нажмите **Сохранить**
Подождите несколько минут. По окончанию процедуры устройство будет автоматически перезагружено.

Системное время

Выберите этот пункт для ручной синхронизации внутренних часов устройства.

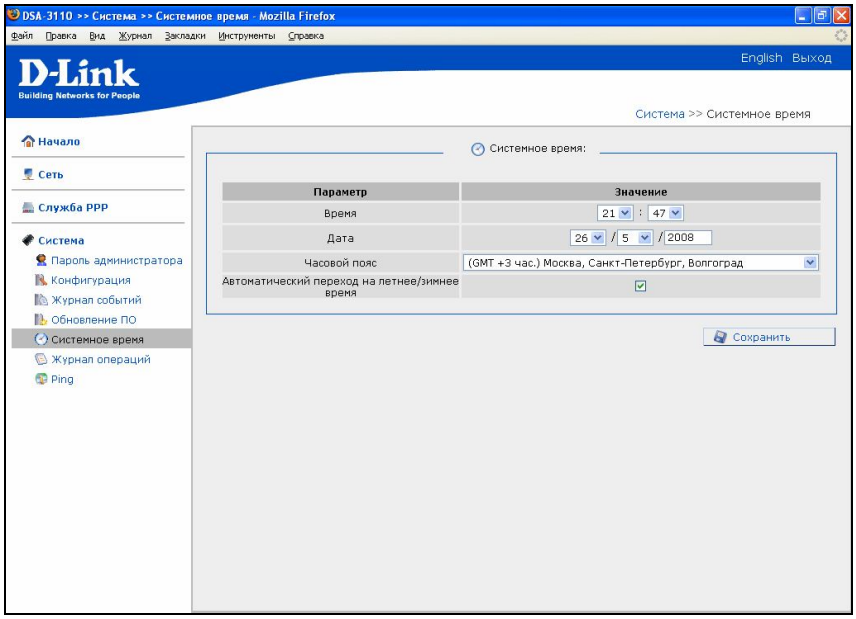

Рисунок 41. Настройка системного времени

Для установки часов:
Введите текущее время и дату в поля **Время, Дата**
Выберите Ваш временной пояс (для Москвы **GMT+3**)
Нажмите кнопку **Сохранить.**

Журнал операций

Выберите этот пункт для просмотра выполнения последних операций с устройством (Log).
На рисунке 32 в журнале выполнения операции показан лог апгрейда (обновления ПО).

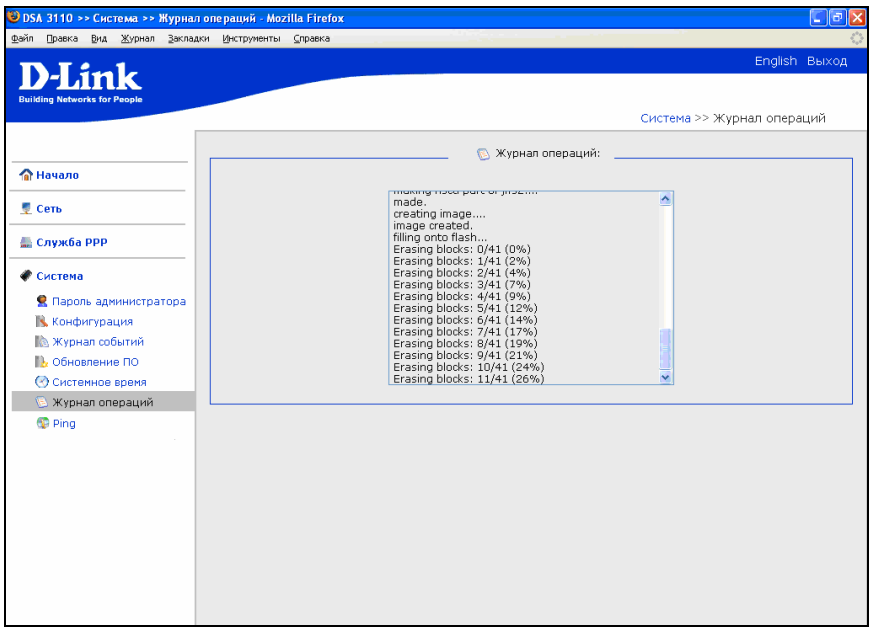

Рисунок 42. Настройка системного времени

Ping

Выберите этот пункт меню для проверки доступности того или иного IP адреса непосредственно из WEB-интерфейса устройства.
Для этого:

- Задайте **Адрес назначения**
- **Количество** эхо запросов
- Нажмите кнопку **Запустить**
- В поле **Результат** появится результат эхо запросов к заданному IP адресу.

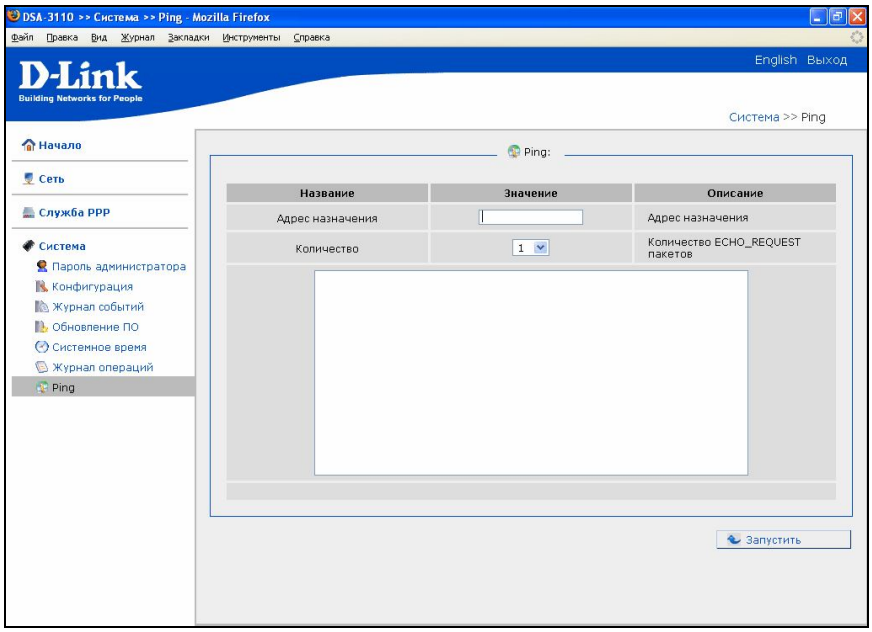

Рисунок 43. Ping (эхо-запрос)