iRZ automation

GSM роутер iRZ RUH 3G HSDPA/UMTS/ EDGE/GPRS

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Оглавление

1. Требования техники безопасности

Ограничения на использование устройства вблизи других электронных устройств:

- выключайте роутер в больницах или вблизи от медицинского оборудования (например: кардиостимуляторов, слуховых аппаратов). Могут создаваться помехи для медицинского оборудования;
- выключайте роутер в самолетах. Примите меры против случайного включения;
- выключайте роутер вблизи автозаправочных станций, химических предприятий, мест проведения взрывных работ. Могут создаваться помехи техническим устройствам;
- на близком расстоянии роутер может создавать помехи для телевизоров, радиоприемников.

Предохраняйте роутер от воздействия пыли и влаги.

Ненадлежащее использование лишает вас права на гарантию.

2. Общая информация

2.1.Назначение устройства

GSM роутер iRZ RUH 3G, используя технологию 3G, обеспечивает надёжный высокоскоростной доступ в Интернет отдельного устройства или целой сети. Он может быть использован для любого распределенного бизнеса, требующего передачи большого объема информации - подключения к сети Интернет компьютеров и сетей, торговых автоматов и банкоматов, промышленного оборудования, систем охраны и наблюдения, а так же для удалённого мониторинга и управления.

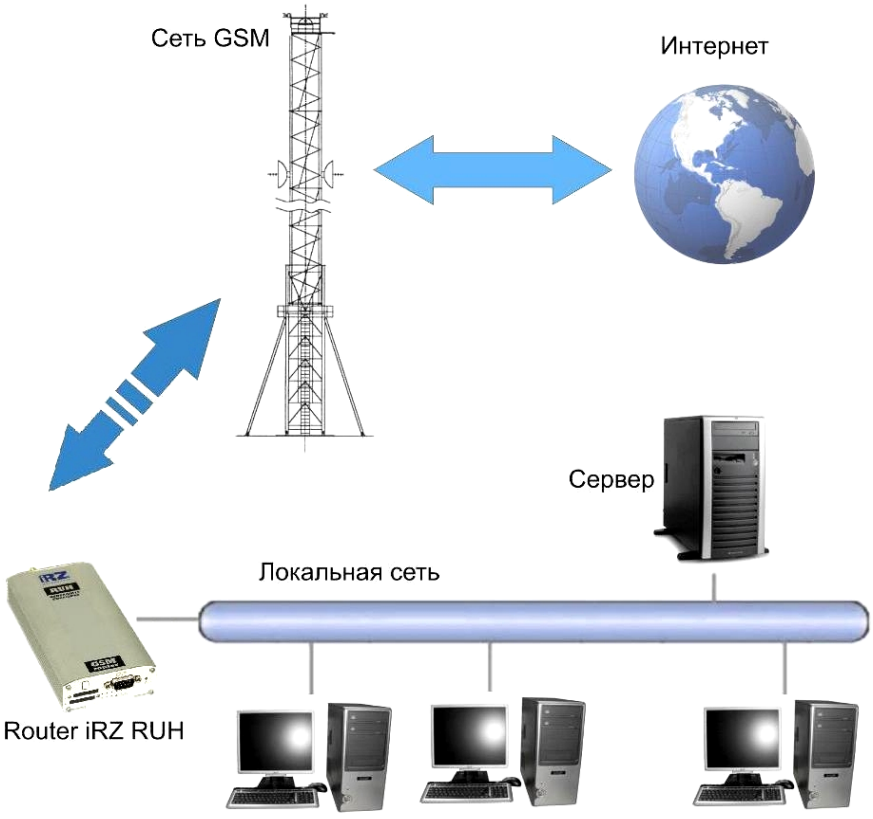
Высокая производительность данной платформы и наличие двух разъёмов для сим-карт позволяет устройству решать дополнительные задачи, не ухудшая качества выполнения основных функций.

Устройство работает под управлением операционной системы Linux. Для отображения работы роутера используются светодиодные индикаторы.

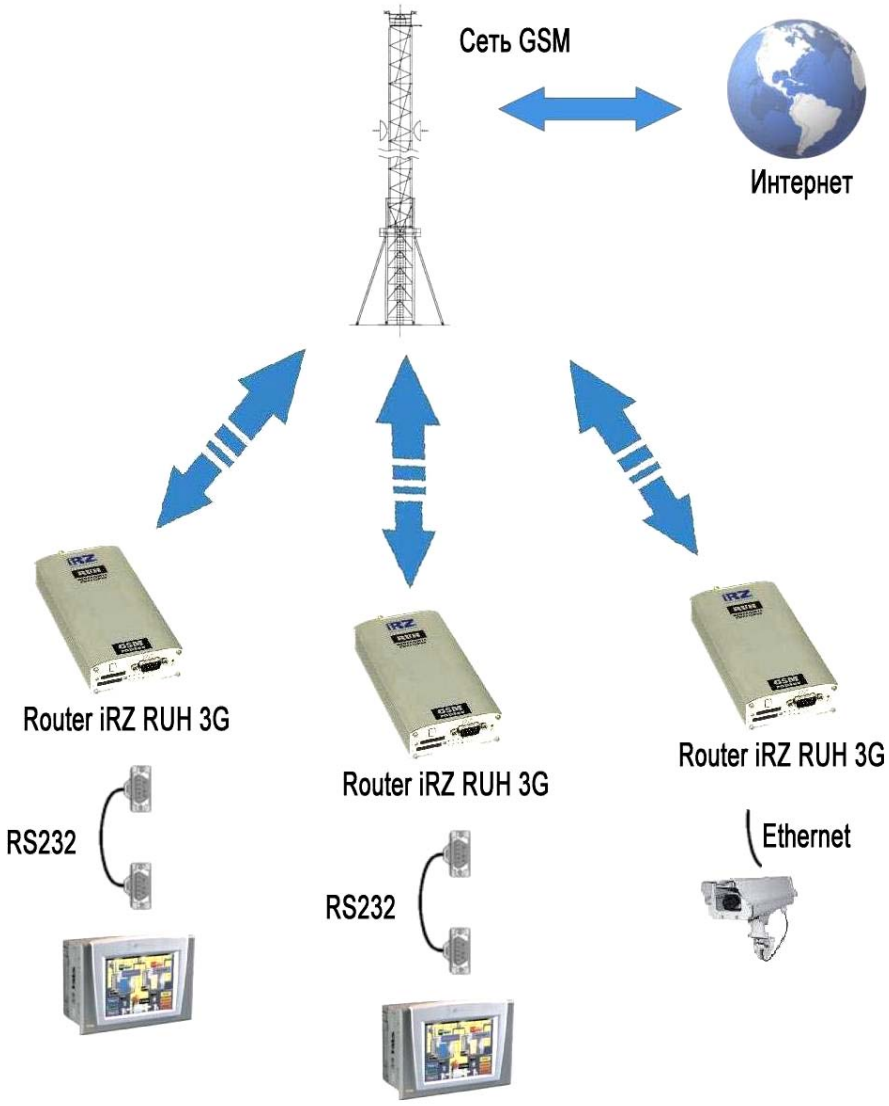
Выполнен в прочном алюминиевом корпусе.

2.2. Типовое применение

- доступ в интернет компьютера или целой сети;



- подключение к сети интернет торговых автоматов и банкоматов, промышленного оборудования и систем охраны и наблюдения, а также для удаленного мониторинга и управления;



2.3. Комплектация

Комплект GSM роутера iRZ RUH 3G:

- роутер iRZ RUH;
- блок питания 12В/1000мА;
- GSM антенна;
- 2 сетевых кабеля;
- заводская упаковка.

2.4. Характеристики

Основные характеристики:

- настройка NAT для доступа к внутренним ресурсам сети извне;
- клиент DynDNS для обновления информации о доменном имени при использовании динамического IP-адреса;
- GRE, IPsec и OpenVPN туннели;
- синхронизация внутренних часов с внешними источниками;
- два разъёма для SIM-карт, автоматическое переключение между ними или по команде через веб-интерфейс. Автоматическое переключение происходит либо при потере связи с оператором, либо по расписанию. В случае переключения при потере связи возможен возврат к приоритетной SIM-карте.

Стандарты связи:

- HSDPA (скорость обмена данными: передачи - до 0.38 Мбит/с, приема - до 3.6 Мбит/с);
- EDGE;
- GPRS;
- USSD;
- SMS;

Характеристики аппаратной части:

- процессор ARM920T;
- динамическое ОЗУ 64 MB;
- Flash-память 8 MB;
- Ethernet 10/100Mbit.

Электропитание:

- напряжение питания от 8 до 30 В;
- ток потребления не более:
  - при напряжении питания +12 В - 800мА;
  - при напряжении питания +24 В - 400мА.

Физические характеристики:

- габариты не более 170x78x32 мм,
- вес не более 190 гр.,
- диапазон рабочих температур от -30°C до +70°C,
- диапазон температуры хранения от -50°C до +85°C.

Интерфейсы:

- разъём DB9 для подключения коммуникационного кабеля, интерфейс RS-232:
  - сбор данных или управление оборудованием средствами дополнительного программного обеспечения,
  - соединение двух удалённых устройств с COM-интерфейсами через сеть Internet,
- разъём Ethernet 10/100 Mbit,
- разъём USB A - USB Host. Для подключения внешнего устройства (flash-диски, переходники USB-COM) - централизованное хранение файлов,
- разъём питания,
- разъём SMA для подключения GSM антенны.

2.5. Внешний вид

Роутер iRZ RUH 3G исполнен в промышленном варианте - в прочном и лёгком алюминиевом корпусе. Внешний вид представлен на рис.2.5.1 и рис.2.5.2.

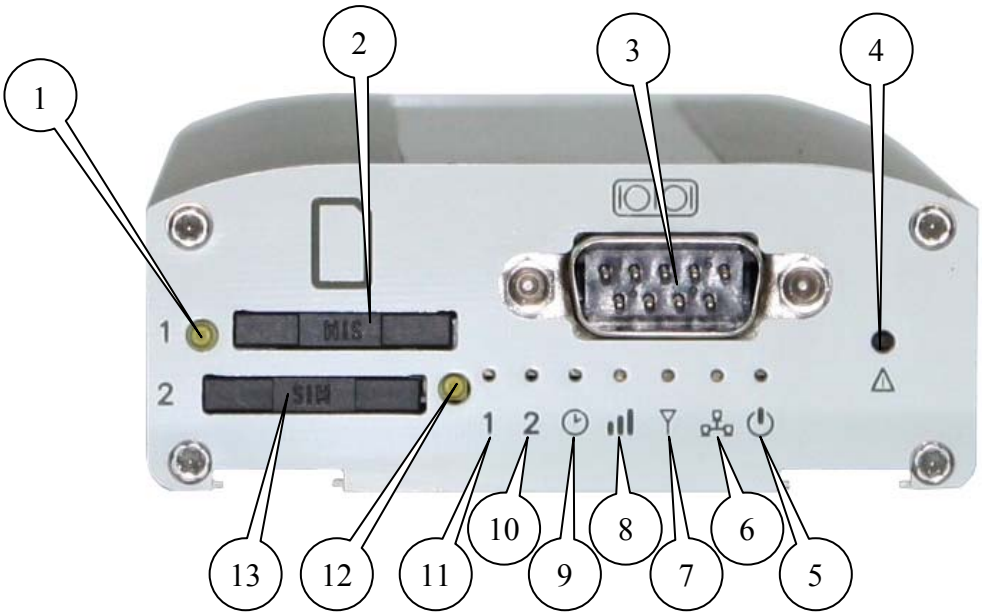


Рис.2.5.1 Вид спереди.

На рисунке 2.5.1 цифрами обозначено:

1. кнопка извлечения лотка SIM-карты №1,
2. лоток SIM-карты №1,
3. разъём DB9 для подключения коммуникационного кабеля, интерфейс RS232,
4. кнопка сброса настроек,
5. индикатор питания,
6. индикатор локальной сети,
7. индикатор типа соединения,
8. индикатор уровня GSM сигнала,
9. индикатор загрузки роутера или обновления ПО,
10. индикатор активности SIM-карты №2,
11. индикатор активности SIM-карты №1,
12. кнопка извлечения лотка SIM-карты №2,
13. лоток SIM-карты №2.

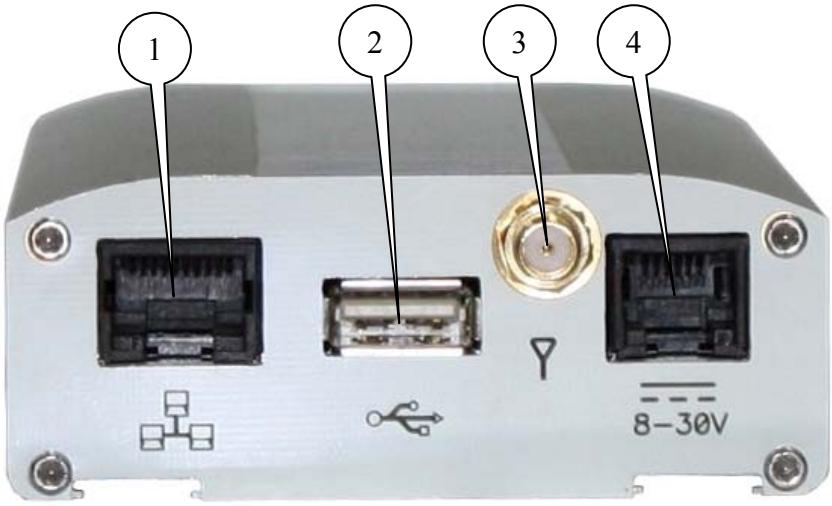


Рис.2.5.2 Вид сзади.

На рисунке 2.5.2 цифрами обозначено:

1. разъём сети Ethernet,
2. разъём USB Host,
3. разъём SMA для подключения GSM антенны,
4. разъём питания.

2.6. Интерфейсы

2.6.1. Разъём DB9 (RS232)

Разъём DB9 для подключения коммуникационного кабеля, интерфейс RS-232.

- сбор данных или управление оборудованием средствами дополнительного программного обеспечения,
- соединение двух удалённых устройств с COM-интерфейсами через сеть Internet.

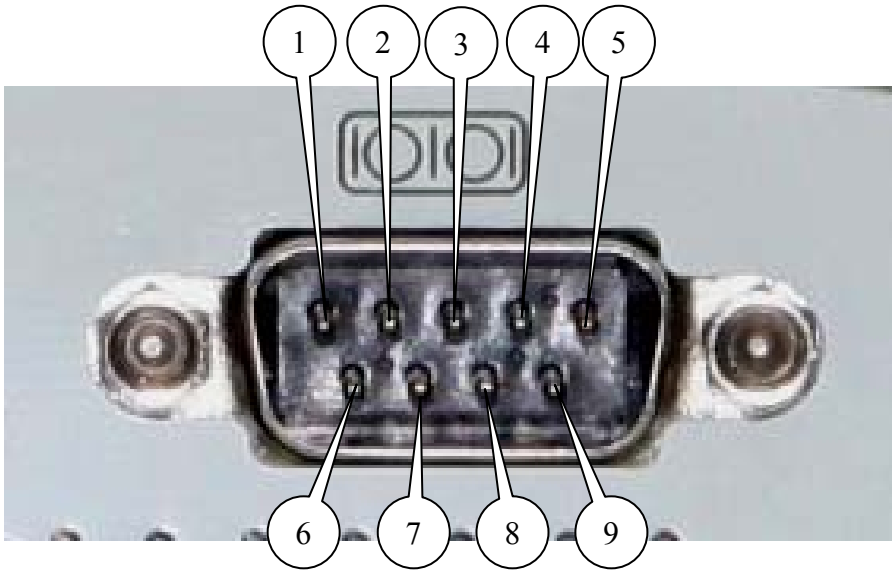


Рис.2.6.1 Разъём DB9

Таблица 2.6.1 Назначение выводов разъёма DB9

Вывод	Сигнал	Направление	Назначение
1	не используется	-	-
2	RXD	Device - Router	Прием данных
3	TXD	Router - Device	Передача данных
4	не используется	-	-
5	GND	общий	Корпус системы
6	не используется	-	-
7	не используется	-	-
8	не используется	-	-
9	не используется	-	-

2.6.2. Разъём питания RJ11

Разъём используется для подключения питания.

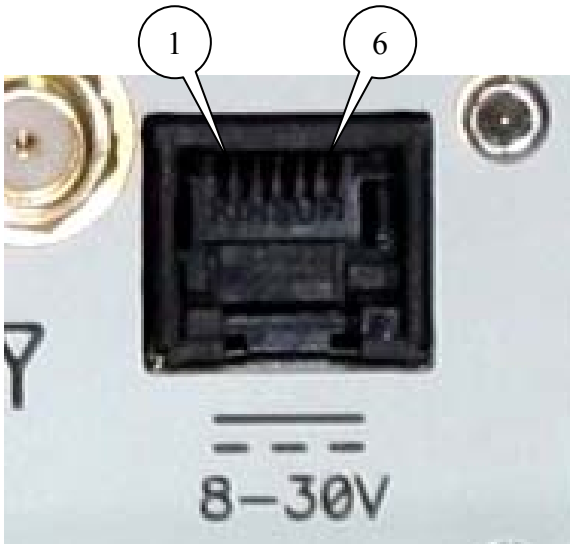


Рис.2.6.2 Разъём RJ11

Таблица 2.6.2 Назначение выводов разъёма питания

Контакт	Сигнал	Назначение
1	+ U пит	Положительный полюс постоянного напряжение питания. Защищен предохранителем и схемой защиты от перенапряжений (при подаче на вход напряжения более 30В) и неправильной полярности
2	не используется	
3	не используется	
4	не используется	
5	не используется	
6	GND	Корпус системы

2.6.3. Разъём USB A

USB Host, позволяющий подключать внешние устройства, такие как flash-диски. Это позволяет пользователю организовывать централизованное хранение файлов.

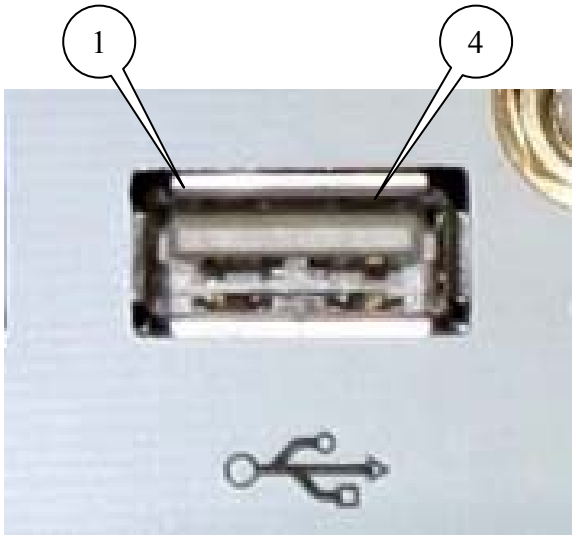


Рис.2.6.3 Разъём RJ11

Таблица 2.6.3 Назначение выводов USB разъёма

Контакт	Сигнал	Назначение
1	VBUS	Цепь питания периферийных устройств, +5В, 500мА
2	D-	Прием/передача данных
3	D+	Прием/передача данных
4	GND	Корпус системы

2.6.4. Разъём сети Ethernet

Ethernet 10/100 Мбит/с. Подключение отдельного компьютера или целой сети, устройств для сбора данных и управления.

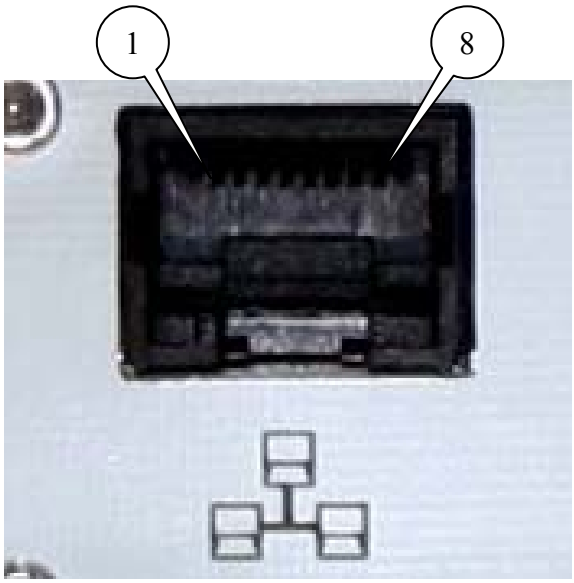


Рис.2.6.4 Разъём RJ11

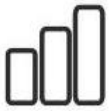
Таблица 2.6.4 Назначение выводов USB разъёма

Контакт	Сигнал	Направление	Назначение
1	ETX P	Router - PC	Передача, положительный полюс
2	ETX N	Router - PC	Передача, отрицательный полюс
3	ERX P	PC - Router	Прием, положительный полюс
4	не используется	-	
5	не используется	-	
6	ERX N	PC - Router	Прием, отрицательный полюс
7	не используется	-	
8	не используется	-	

2.7. Индикация состояния

На переднюю панель выведено 7 светодиодов, которые информируют о режиме работы.

Таблица 2.7.1 Назначение светодиодных индикаторов

Обозначение	Назначение, режим работы
1	Выбрана SIM-карта №1
2	Выбрана SIM-карта №2
	Роутер занят – происходит загрузка роутера, сохранение настроек или обновление внутренней программы. Дождитесь погасания индикатора перед началом работы. Не отключайте питание при включённом индикаторе!
	Уровень GSM сигнала: • красный цвет - слабый уровень сигнала, • желтый цвет - средний уровень сигнала, • зеленый цвет - хороший уровень сигнала.
	Тип GSM соединения: • зеленый цвет – 3G, • желтый цвет – EDGE/GPRS, • выключен – соединение не установлено.
	Локальная сеть: • горит в случае подключения сетевого кабеля, • мигает при передаче данных по локальной сети.
	Наличие питания – горит при подаче питания.

3. Подключение и настройка

3.1. Подключение роутера к компьютеру для настройки

Перед подачей питания необходимо установить SIM-карту в роутер. Для чего необходимо:

- достать SIM-лоток, нажав на кнопку извлечения SIM-лотка (рис.2.5.1) длинным тонким предметом (разогнутая скрепка, зубочистка и т. п.);
- установить SIM-карту в SIM-лоток;
- вставить SIM-лоток с SIM-картой в роутер так, чтобы края SIM-лотка попали в пазы держателя.

При установке SIM-карты не прикладывайте сильных физических усилий. При необходимости установите вторую SIM-карту.

Подключите GSM антенну и сетевой провод. Используйте прямой кабель для подключения к коммутатору или кросс-кабель при подключении напрямую к компьютеру. С помощью блока питания подайте питание на роутер.

После подачи питания начнется загрузка роутера, горит индикатор загрузки. После того, как индикатор загрузки погаснет, роутер готов к работе.

3.2. Базовая настройка

Для настройки роутера и наблюдения за его состоянием используется web-интерфейс. Исходный IP адрес 192.168.1.1. Настройку может производить только пользователь “root” с исходным паролем “root”.

В верхней части web-интерфейса находятся закладки отслеживания состояния (Status and log), настройки (Configuration) и управления (Administration). С левой стороны расположены пункты меню для каждой закладки.

3.2.1. Параметры сетевого подключения

Если роутер iRZ RUH 3G используется для доступа в сеть Интернет только одного устройства, то необходимости перенастраивать сетевое подключение роутера нет. Нужно лишь правильно настроить устройство: указать IP-адрес из диапазона 192.168.1.2... 192.168.1.254, сетевую маску 255.255.255.0 и шлюз по умолчанию 192.168.1.1. Так же можно настроить устройство как DHCP-клиент. Тогда все эти настройки будут получены им от роутера автоматически.

В случае, если предоставляется Интернет-соединение для сети, необходимо выбрать такие настройки роутера, чтоб избежать конфликтов с уже подключёнными к сети устройствами. Обратитесь к администратору вашей сети для получения корректных настроек.

3.2.2. Доступ к web-интерфейсу

Чтобы настроить роутер, подключите его непосредственно к компьютеру с помощью перекрёстного (crossover) кабеля. Установите в свойствах сетевого соединения компьютера «Автоматически получать IP адрес». Введите в адресной строке броузера 192.168.1.1, щёлкните на ссылке «iRZ RUH 3G Router». В открывшемся окне укажите логин “root”, пароль “root”. Откроется web-интерфейс роутера. Щелкните на закладке “Configuration” и выберите пункт меню “LAN”. Вы попадёте на страницу настройки сетевого соединения роутера. Слева находится меню доступных настроек.

3.2.3. Настройка сетевого подключения

В строке IP Address укажите IP-адрес роутера. Этот адрес должен быть свободным в данной локальной сети. При необходимости измените маску подсети (поле Subnet Mask) и укажите желаемые настройки DHCP-сервера. Учтите, что для того, чтоб компьютеры в сети могли использовать интернет-соединение, установленное роутером, необходимо в настройках сетевого подключения компьютеров указать IP-адрес роутера, как шлюз по умолчанию. Также может понадобиться указать IP-адрес роутера в поле DNS-сервер.

3.2.4. Настройка GSM соединения

После того, как роутер подключен, а сетевое соединение настроено, можно настроить GSM соединение. Для чего выберете пункт меню “Internet” в закладке “Configuration” web-интерфейса.

Для установки соединения с сетью Интернет вам нужно знать имя точки доступа (APN), имя пользователя (Username) и пароль (Password). Эти данные можно получить у вашего оператора сотовой связи. Укажите номер SIM-карты. Впишите значения параметров APN, Username и Password в соответствующие поля. Для сохранения настроек и установки соединения нажмите кнопку Apply. Через некоторое время соединение будет установлено. Его состояние можно проверить на закладке “Status and log”, в пункте меню “Internet”.

3.2.5. Сброс настроек

В случае, если из-за неверных настроек не удаётся получить доступ к интерфейсу роутера или забыли пароль, можно вернуться к заводским настройкам следующим способом:

- нажмите и удерживайте кнопку сброса настроек (рис. 2.5.1),
- включите питание роутера,
- сброс настроек подтверждается трёхкратным миганием индикатора загрузки,
- отпустите кнопку сброса настроек.

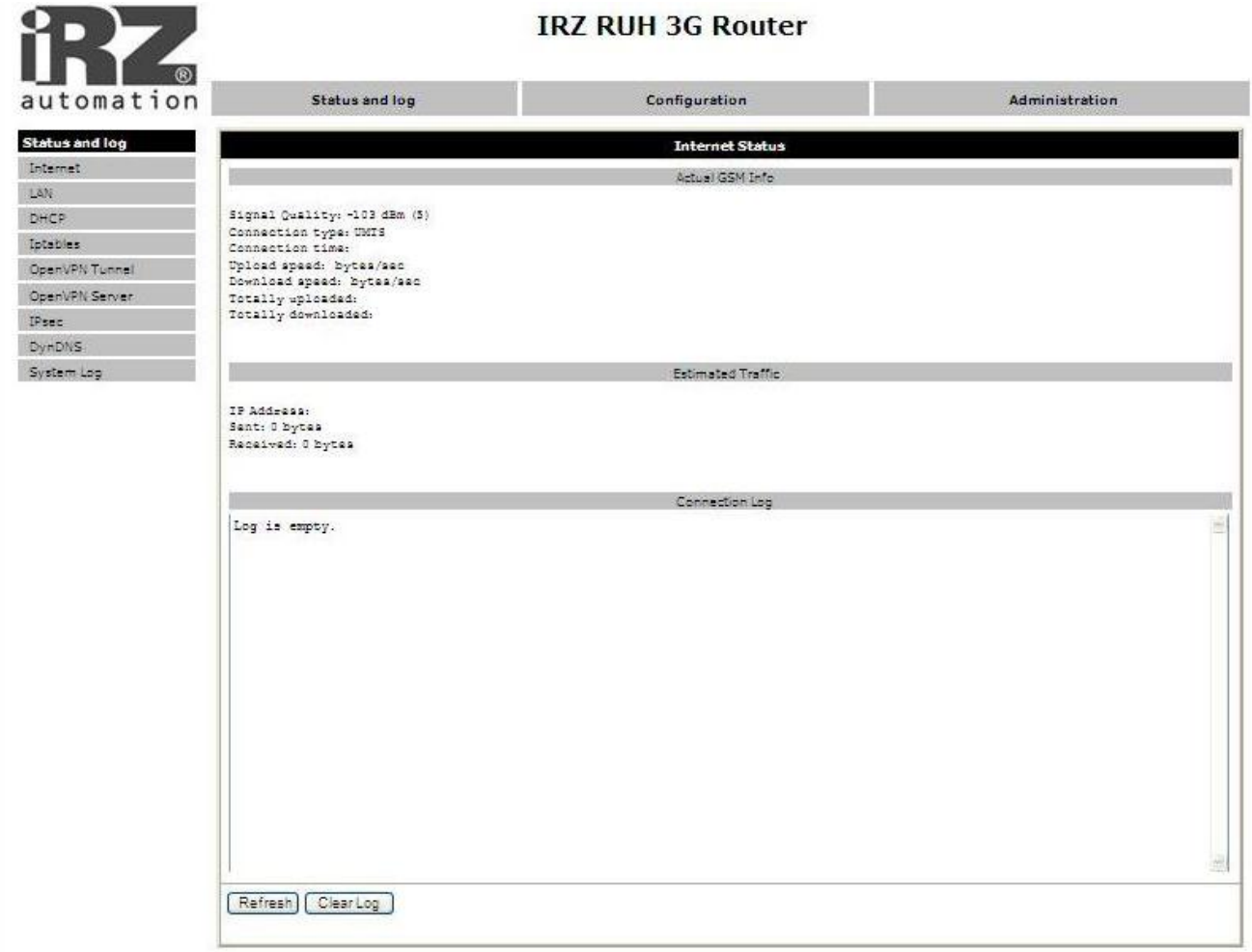
После сброса настроек устройство будет доступно по адресу **192.168.1.1** с именем пользователя **root** и паролем **root.**

4. Описание web-интерфейса

4.1. Status and log

4.1.1. Internet

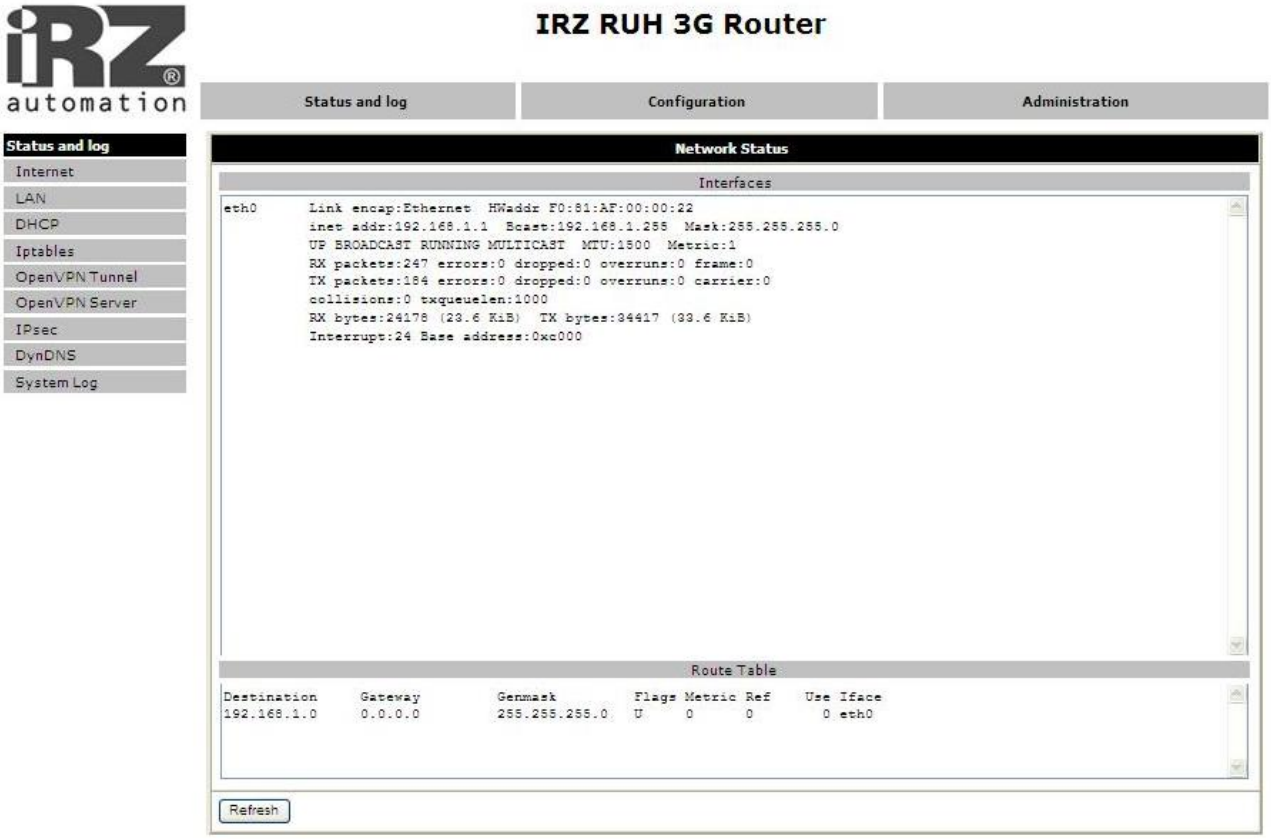
Состояние GSM-сети и интернет соединения.



Где:
Actual GSM Info - информация о GSM сети,
Estimated Traffic- примерный расход трафика за сессию,
Connection Log - журнал установки соединений
Refresh - обновить страницу,
Clear Log - очистить журнал установки соединения.

4.1.2. LAN

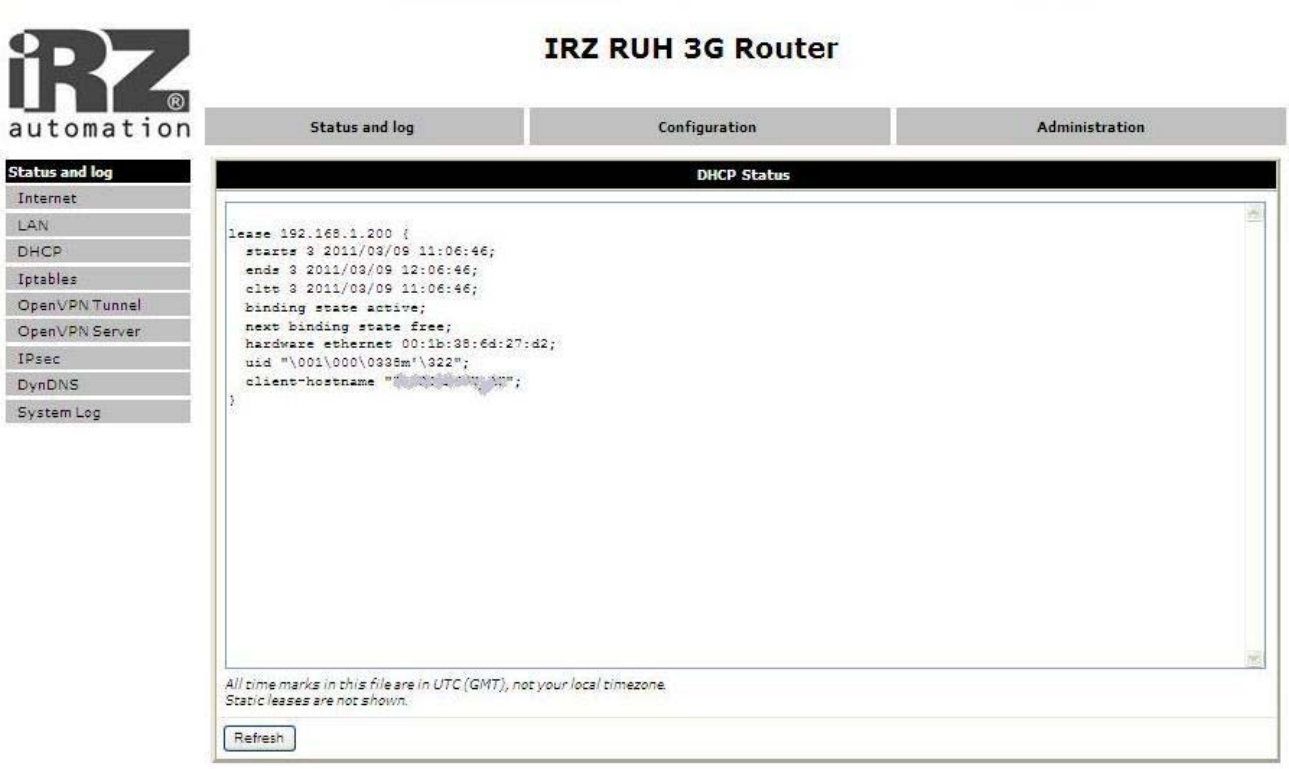
Текущее состояние сетевых подключений и таблица маршрутизации.



Где:
Interfaces - работающие интерфейсы и их состояние,
eth0 - подключение по локальной сети,
ppp0 – UMTS/ EDGE/GPRS подключение,
gre1 - GRE-туннель,
Route table - таблица маршрутизации.

4.1.3. DHCP

Сведения о выданных IP-адресах и их получателях.

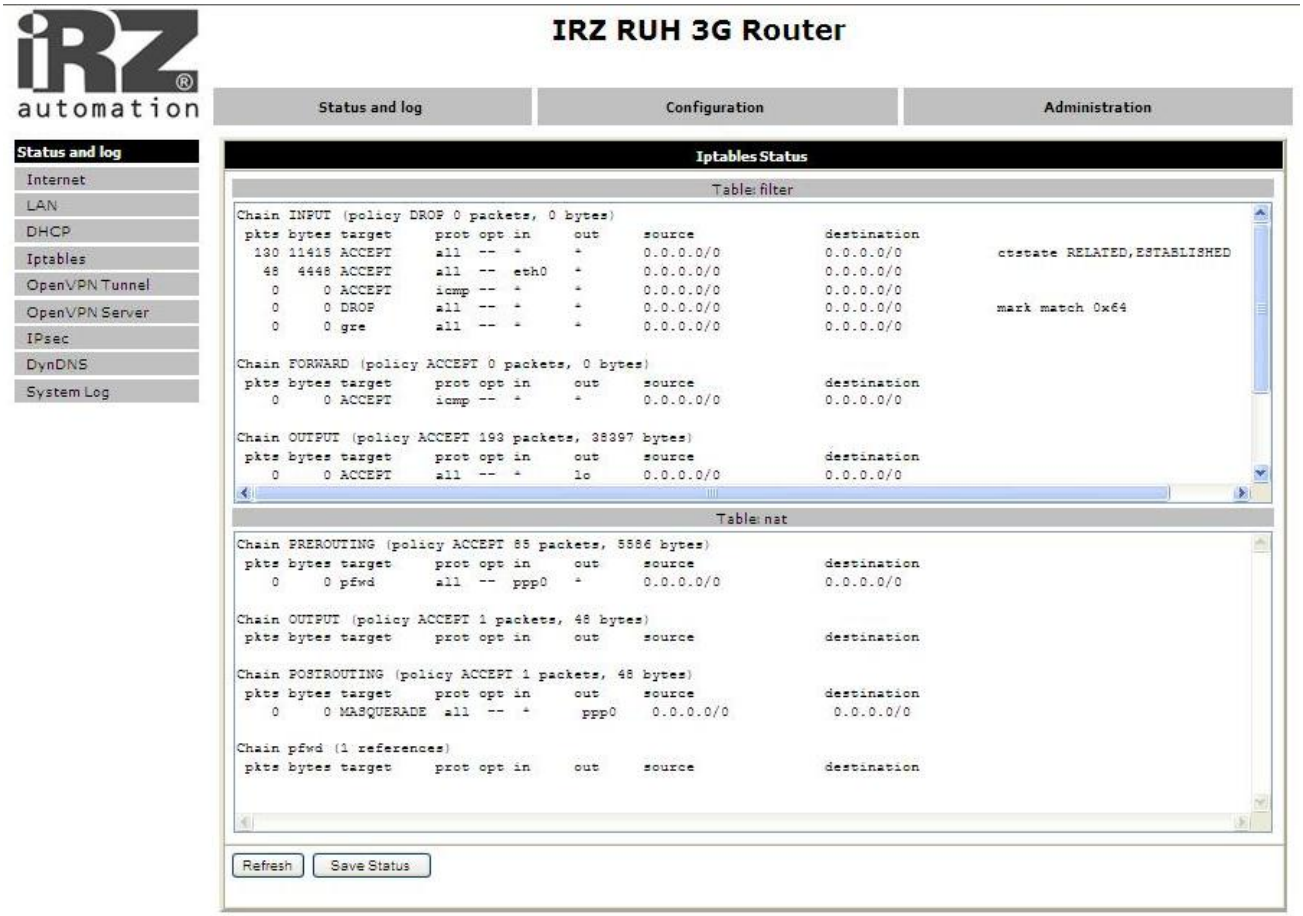


Где:
DHCP Status - текущие DHCP выдачи,
lease - выданный IP-адрес,
starts - дата и время выдачи IP-адреса,
ends - дата и время окончания действия IP-адреса,
hardware ethernet - MAC-адрес устройства.

Обратите внимание, что здесь время указывается в формате UTC. То есть, не учитывается сдвиг для конкретной временной зоны. Таким образом, локальное время для Москвы, например, будет на 3 часа больше (или на 4, если время летнее). Это вызвано особенностями работы DHCP-сервера.

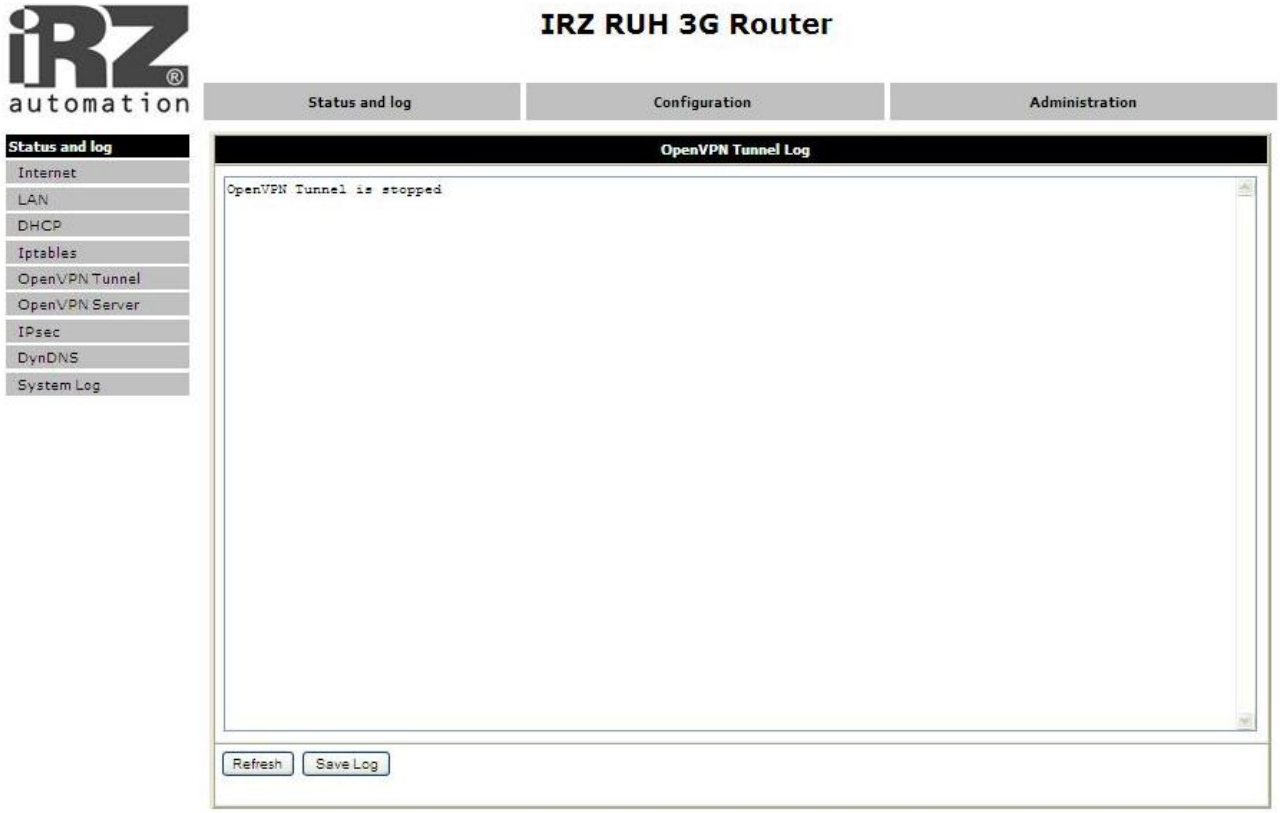
4.1.4. Iptables

Правила Iptables.



Где:
Table filter - правила таблицы filter,
Table nat - правила таблицы nat.

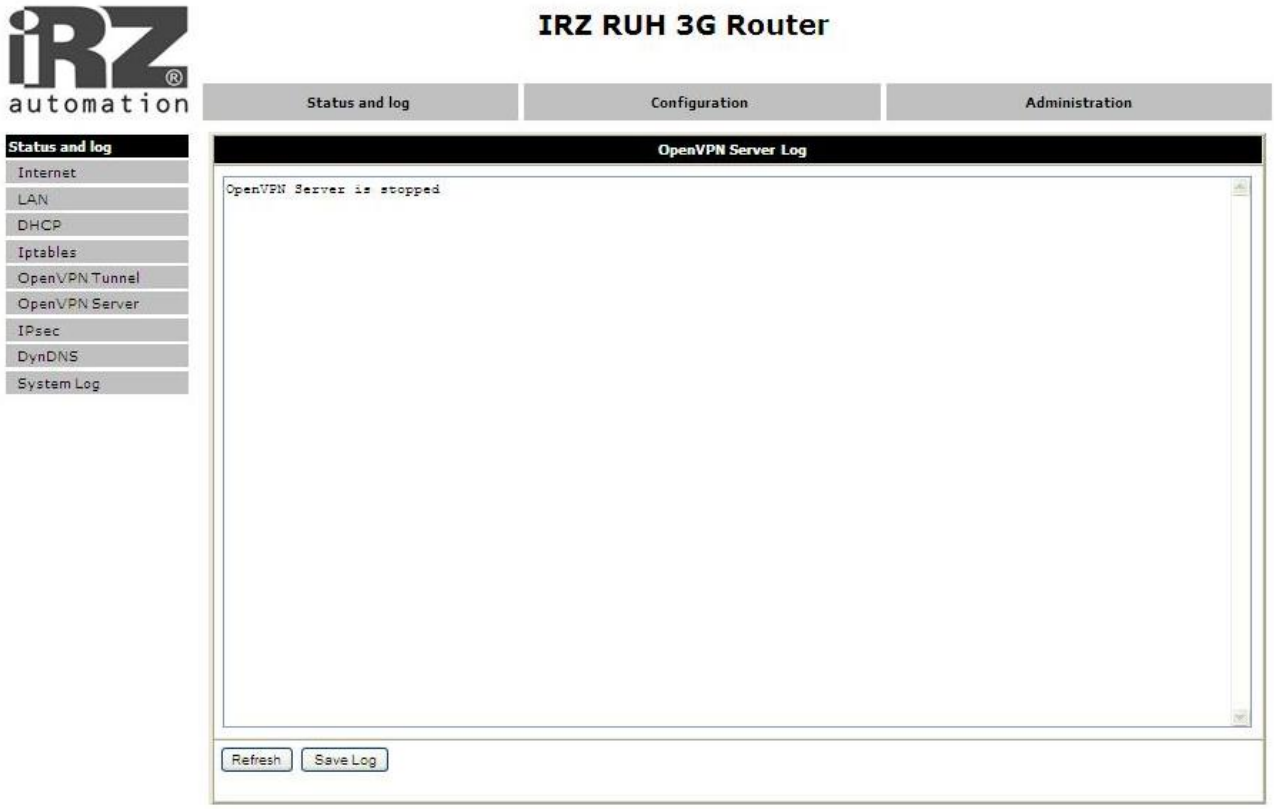
4.1.5. OpenVPN Tunnel



Initialization Sequence Completed - соединение установлено

4.1.6. OpenVPN Server

Журнал сообщений сервера OpenVPN



4.1.7. IPsec

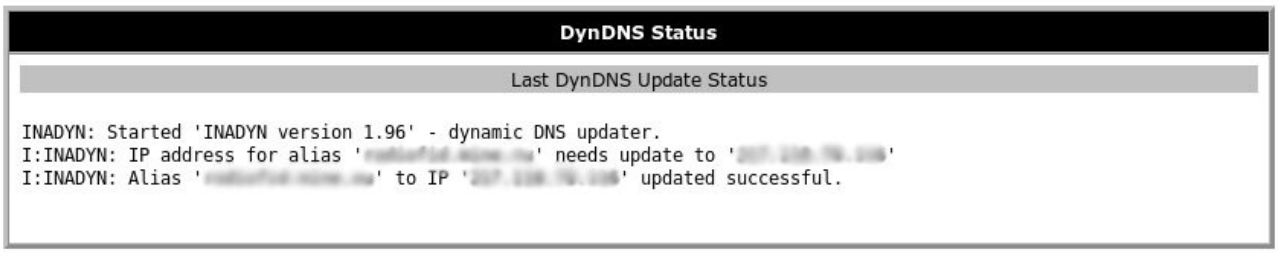
Состояние шифрованного туннеля IPsec.

```
000 "ipsec1": 192.168.1.0/24===85.26.139.166...217.66.146.11===192.168.2.0/24; erouted; eroute owner: #6
000 "ipsec1":     myip=unset; hisip=unset; myup=/etc/init.d/updown; hisup=/etc/init.d/updown;
000 "ipsec1":   ike_life: 3600s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "ipsec1":   policy: PSK+ENCRYPT+TUNNEL+UP; prio: 24,24; interface: ppp0;
000 "ipsec1":   newest ISAKMP SA: #1; newest IPsec SA: #6;
000 "ipsec1":   IKE algorithm newest: AES_CBC_128-SHA1-MODP2048
```

Первая строка отображает конфигурацию туннеля и его состояние: erouted - установлен, unrouted - не установлен. В нижней строке указан используемый алгоритм шифрования.

4.1.8. DynDNS

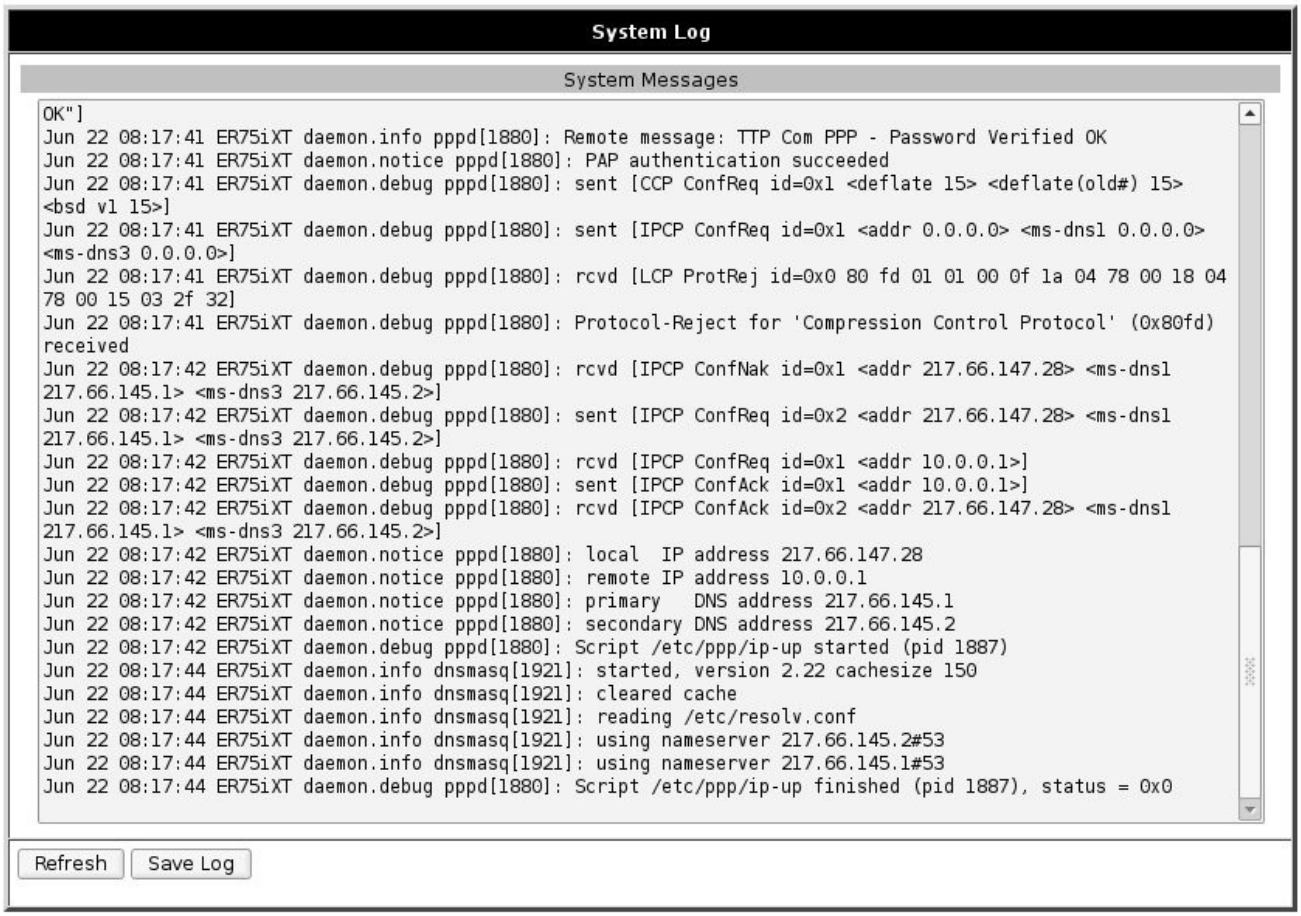
Сведения о результатах обновления IP-адреса в системе DynDNS.



Last DynDNS Update Status - журнал последнего обновления DynDNS

4.1.9. System Log

Журнал сообщений системы.

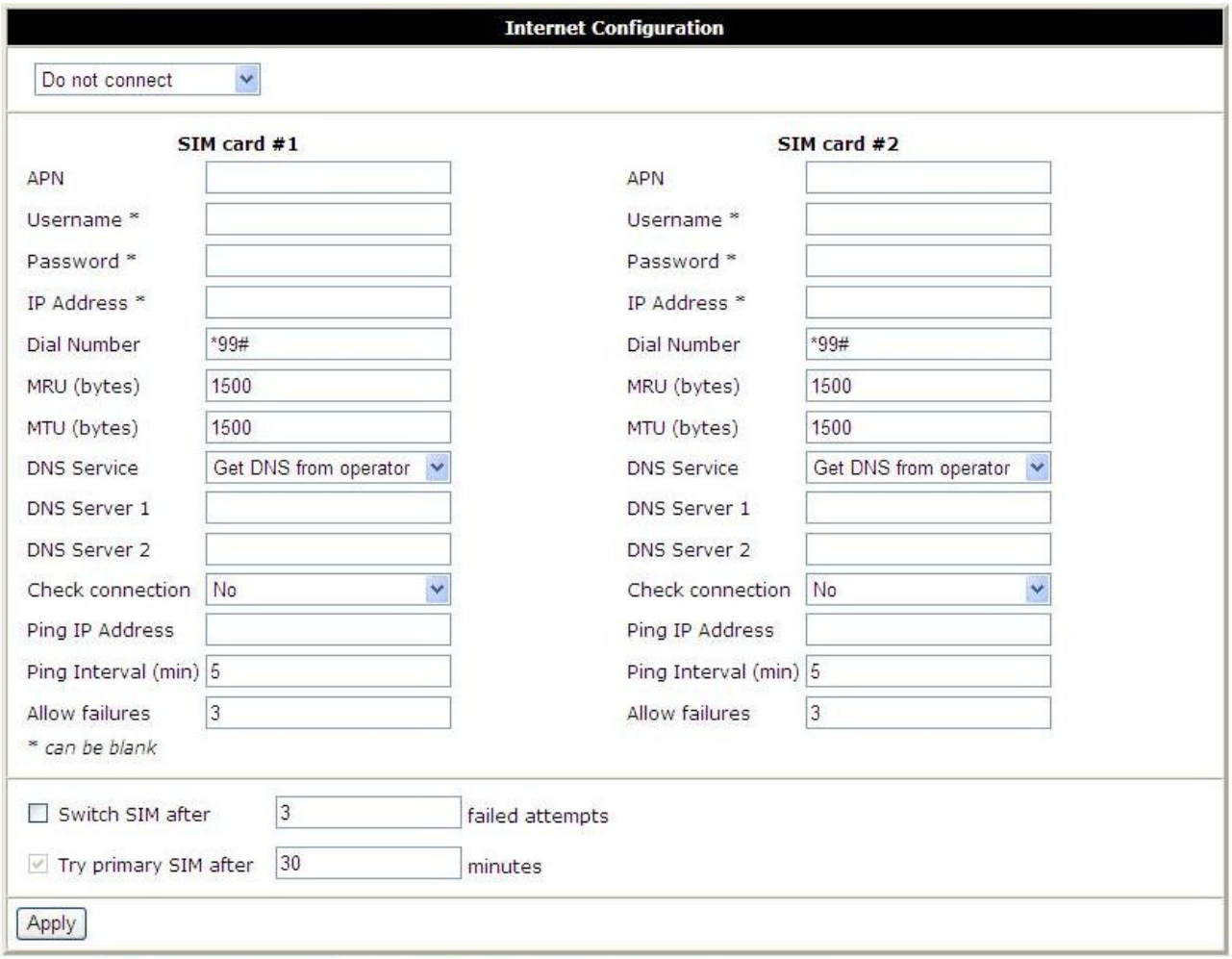


Где:
System Messages - журнал сообщений системы,
Refresh - обновить страницу,
Save Log - сохранить журнал на компьютере.

4.2. Configuration

4.2.1. Internet

Настройка GSM соединения.



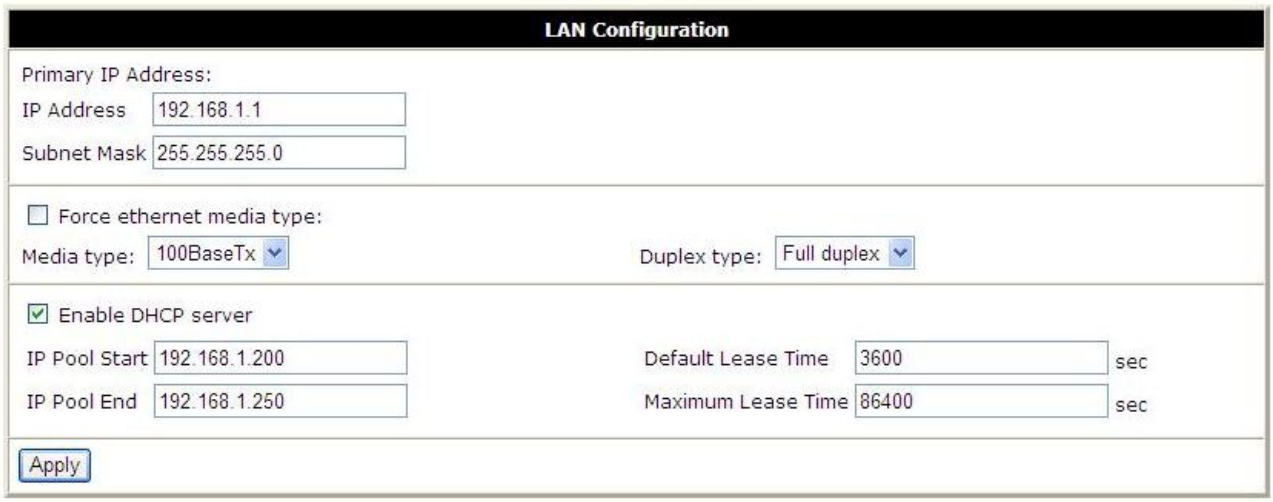
Где:
Do not connect/Connect using SIM 1/Connect using SIM 2 – выбор сим-карты при запуске,
SIM card #1 - параметры подключения для SIM-карты №1,
SIM card #2 - параметры подключения для SIM-карты №2,
APN - имя точки доступа,
Username* - имя пользователя,
Password* - пароль,
IP Address* - сетевой адрес (если требуется оператором),
Dial Number - команда установки интернет-соединения,
MRU - максимальный размер принятого пакета,
MTU - максимальный размер переданного пакета,
DNS service - настройка DNS-сервиса (не использовать/получить адрес DNS-сервера от оператора/ использовать указанный DNS-сервер),

Check GPRS connection – не проверять/проверять наличие соединения,
Ping IP Address - адрес, с которым проверяется соединение,
Ping Interval - интервал проверки,
Allow failures - допустимое количество неудачных проверок,
Switch SIM cards on failure - переключаться на другую SIM-карту при ошибке соединения
Switch SIM after X failed attempts - переключать SIM-карту после X неудачных попыток
Try primary SIM after XX minutes - Переходить на основную SIM-карту после XX минут работы на резервной.
Apply - применить настройки

* - поле может быть пустым.

4.2.2. LAN

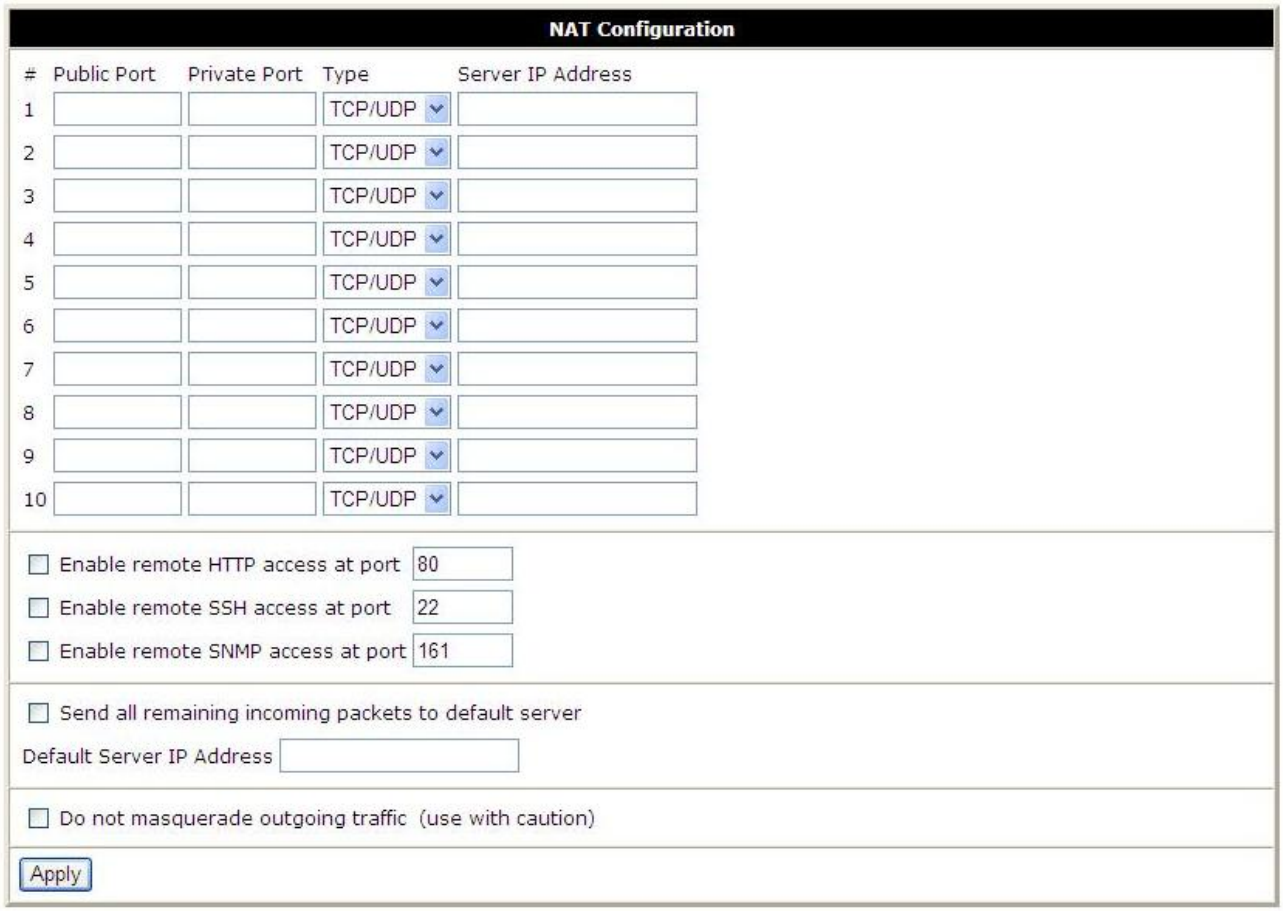
Настройка подключения к локальной сети и DHCP-сервера.



Где:
IP Address - IP адрес роутера,
Subnet Mask - маска подсети,
Enable DHCP server - включить DHCP-сервер,
IP Pool Start - начало диапазона выдаваемых адресов,
IP Pool End - конец диапазона выдаваемых адресов,
Default Lease Time - срок аренды адреса по-умолчанию,
Maximum Lease Time - максимальный срок аренды адреса,
Apply - применить настройки.

4.2.3. Port Forwarding

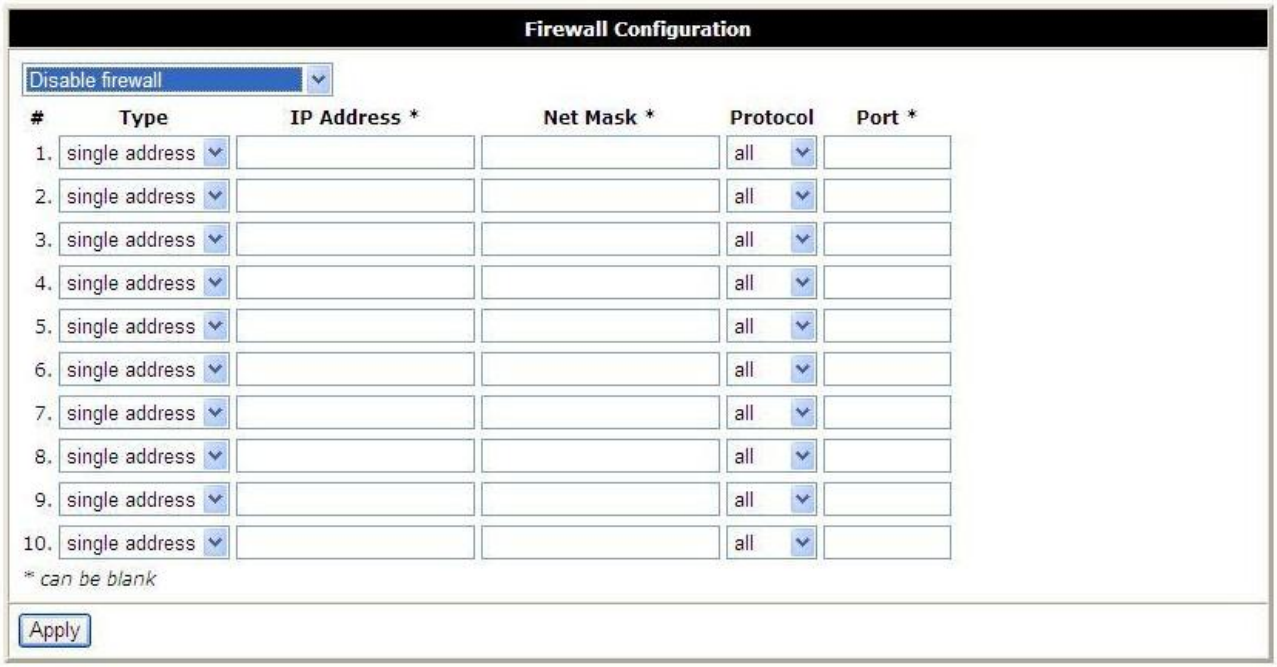
Предоставление компьютерам из сети Интернет доступа к серверу, расположенному в локальной сети.



Где:
Public Port - порт, доступный из сети Интернет,
Private Port - порт сервера в локальной сети,
Type - тип протокола: TCP или UDP,
Server IP Address - IP-адрес сервера,
Enable remote HTTP access - разрешить доступ к web-интерфейсу роутера через интернет на указанный порт,
Send all remaining incoming packets to default server - отправлять все остальные входящие пакеты на сервер по умолчанию,
Default Server IP Address - адрес сервера по умолчанию,
Do not masquerade outgoing traffic - отключить маскарадинг исходящего трафика,
Apply - применить настройки.

4.2.4. Firewall

Брандмауэр ограничивает доступ к указанным сетевым ресурсам.

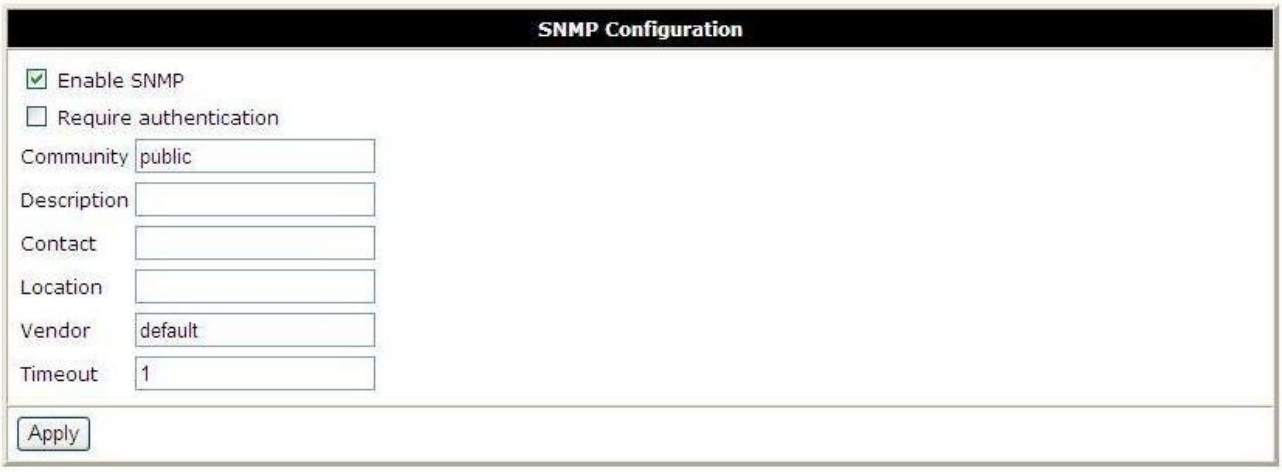


Где:
Disable firewall/Disable specified, allow others – выбор фильтрации разрешения доступа к указанным хостам,
Type: single address - указанный адрес, any любой,
IP Address - IP-адрес источника
Protocol - протокол (все, tcp, udp, icmp)
Port - порт назначения
Apply - применить настройки

* - поле может быть пустым.

4.2.5. SNMP

Сервис для удалённого наблюдения за состоянием устройства.



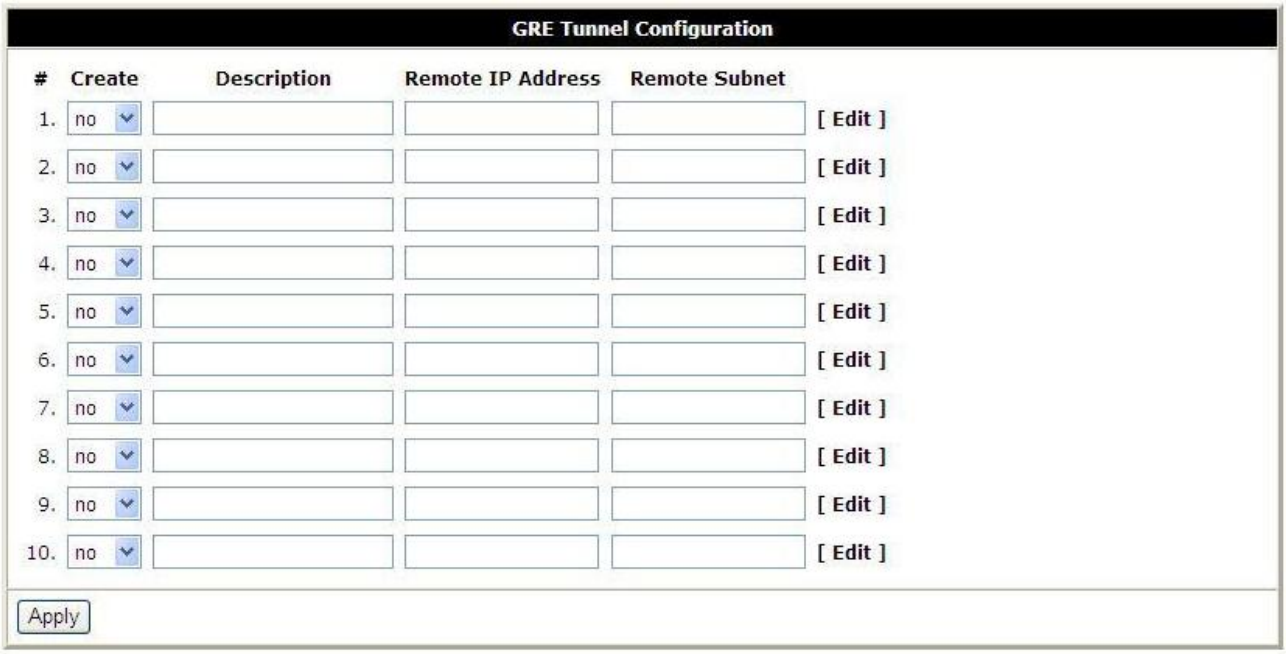
Где:
Enable SNMP - включить сервис SNMP,
Require authentication - требовать аутентификацию (протокол 2c),
Community - имя сообщества,
Description - описание устройства,
Contact - информация о владельце,
Location – местонахождение,
Vendor – производитель,
Timeout - период обновления статистики,
Apply - применить настройки.

Обратите внимание: по техническим причинам не допускается использовать пробелы в текстовых полях. Все поля являются необязательными — нужные значения будут подставлены автоматически.

4.2.6. GRE

С помощью GRE-туннеля можно объединить две физически разделённые локальные сети в одну логическую. Внимание: данные передаются в открытом виде!

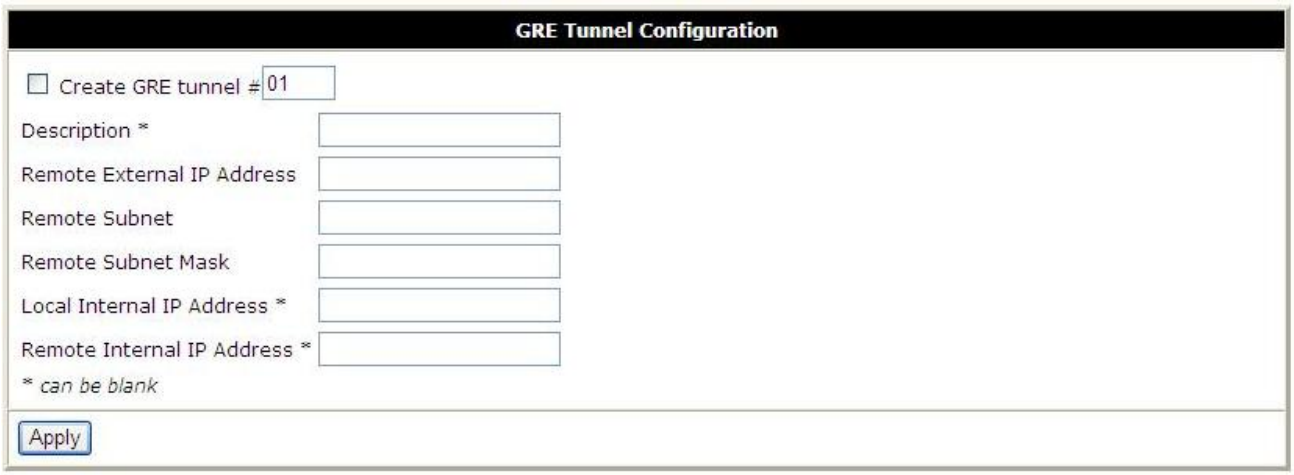
Сводная таблица туннелей:



Где:
- номер туннеля,
Create - создать туннель: yes – да, no – нет,
Description - краткое описание,
Remote IP Address - адрес удалённой машины,
Remote Subnet - удалённая сеть,
Edit - редактировать настройки туннеля
Apply - применить настройки

На этой странице вы можете включить или выключить отдельные туннели или перейти на страницу настроек одного из туннелей.

Страница настройки туннеля



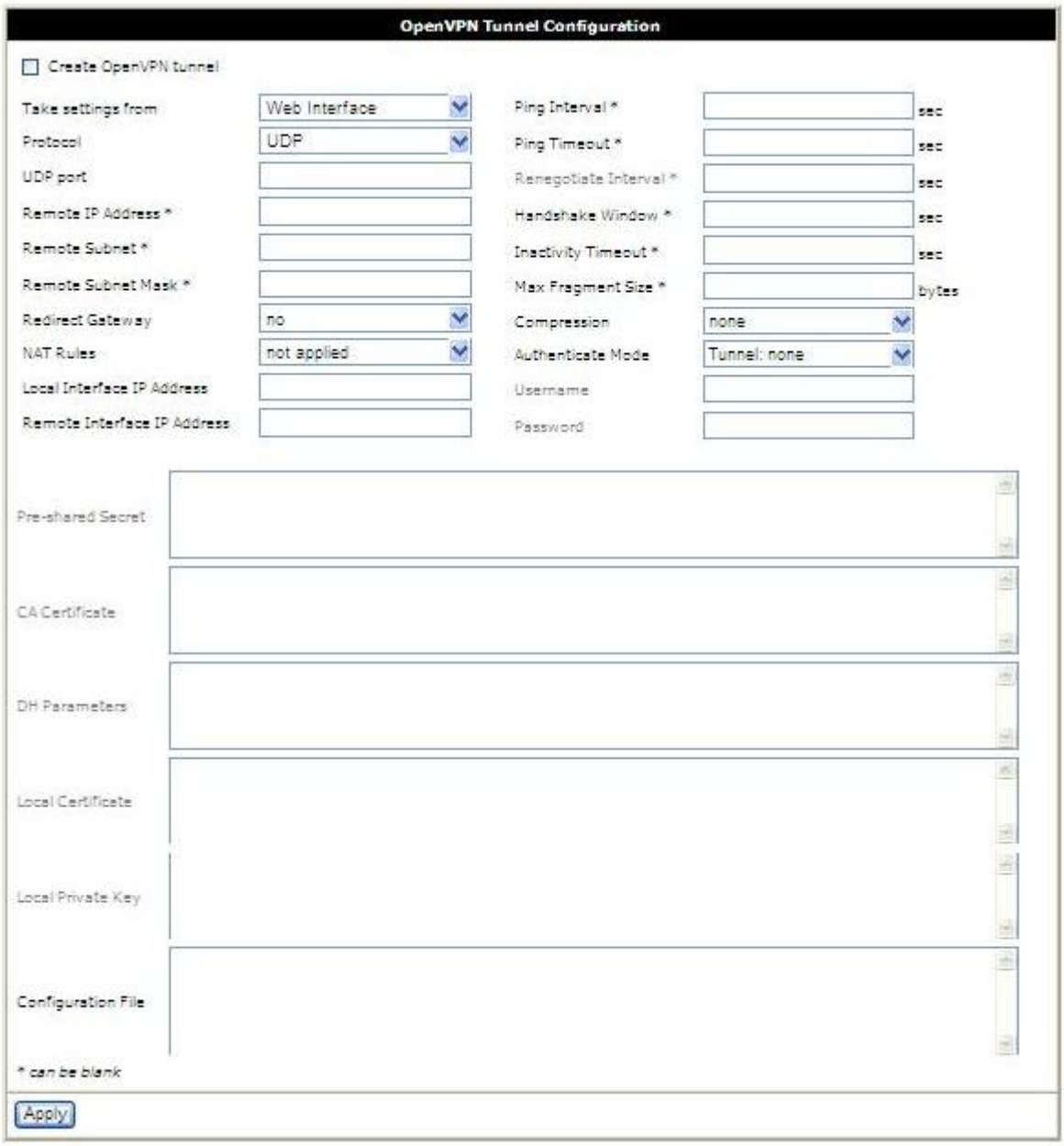
Где:
Create GRE tunnel #01 - создать GRE-туннель №1
Description - краткое описание туннеля
Remote External IP Address - внешний IP адрес удалённой сети
Remote Subnet - удалённая сеть
Remote Subnet Mask - маска удалённой сети
Local Internal IP Address - локальный внутренний IP адрес
Remote Internal IP Address - удалённый внутренний IP адрес
Apply - применить настройки.

* - поле может быть пустым.

Поля **Local Internal IP Address** и **Remote Internal IP Address** используются при объединении только двух устройств в разных сетях.

4.2.7. OpenVPN Tunnel

OpenVPN — защищённый туннель между двумя устройствами.



Где:
Create OpenVPN tunnel - создать туннель OpenVPN
Take settings from - брать настройки из:

- Web Interface - веб-интерфейса,
- Configuration File - файла настройки,

Protocol – протокол:

- UDP - рекомендуется (требует оба внешних IP-адреса),
- TCP server - для устройства с внешним IP-адресом,

- TCP client - для устройства без внешнего IP-адреса,

UDP Port - номер порта UDP,
Remote IP Address - удалённый IP адрес,
Remote Subnet - удалённая сеть,
Remote Subnet Mask - маска удалённой сети,
Redirect Gateway - заменить шлюз по умолчанию:

- no – нет,
- yes – да,

NAT Rules - правила NAT:

- no applied - не применять,
- applied – применять,

Local Interface IP Address - адрес локального виртуального интерфейса,
Remote Interface IP Address - адрес удалённого виртуального интерфейса,
Ping Interval - интервал проверки (в секундах),
Ping Timeout - период ожидания ответа (в секундах),
Renegotiate Interval - интервал пересоединения (в секундах),
Handshake Window - максимальный интервал обмена ключами при установке соединения,
Inactivity Timeout - завершать соединение при отсутствии активности в течение заданного интервала,
Max Fragment Size - максимальный размер фрагмента,
Compression – сжатие:

- none- нет,
- LZO - по алгоритму LZO,

Authenticate Mode - метод аутентификации:

- Tunnel: none - Туннель: нет,
- Tunnel: pre-shared secret - Туннель: по ключу,
- Tunnel: X.509 certificate (client) - Туннель: по сертификату X.509 (клиент),
- Tunnel: X.509 certificate (server) - Туннель: по сертификату X.509 (сервер),
- Client: username/password - Клиент: по имени и паролю,
- Client: X.509 certificate - Клиент: по сертификату X.509,

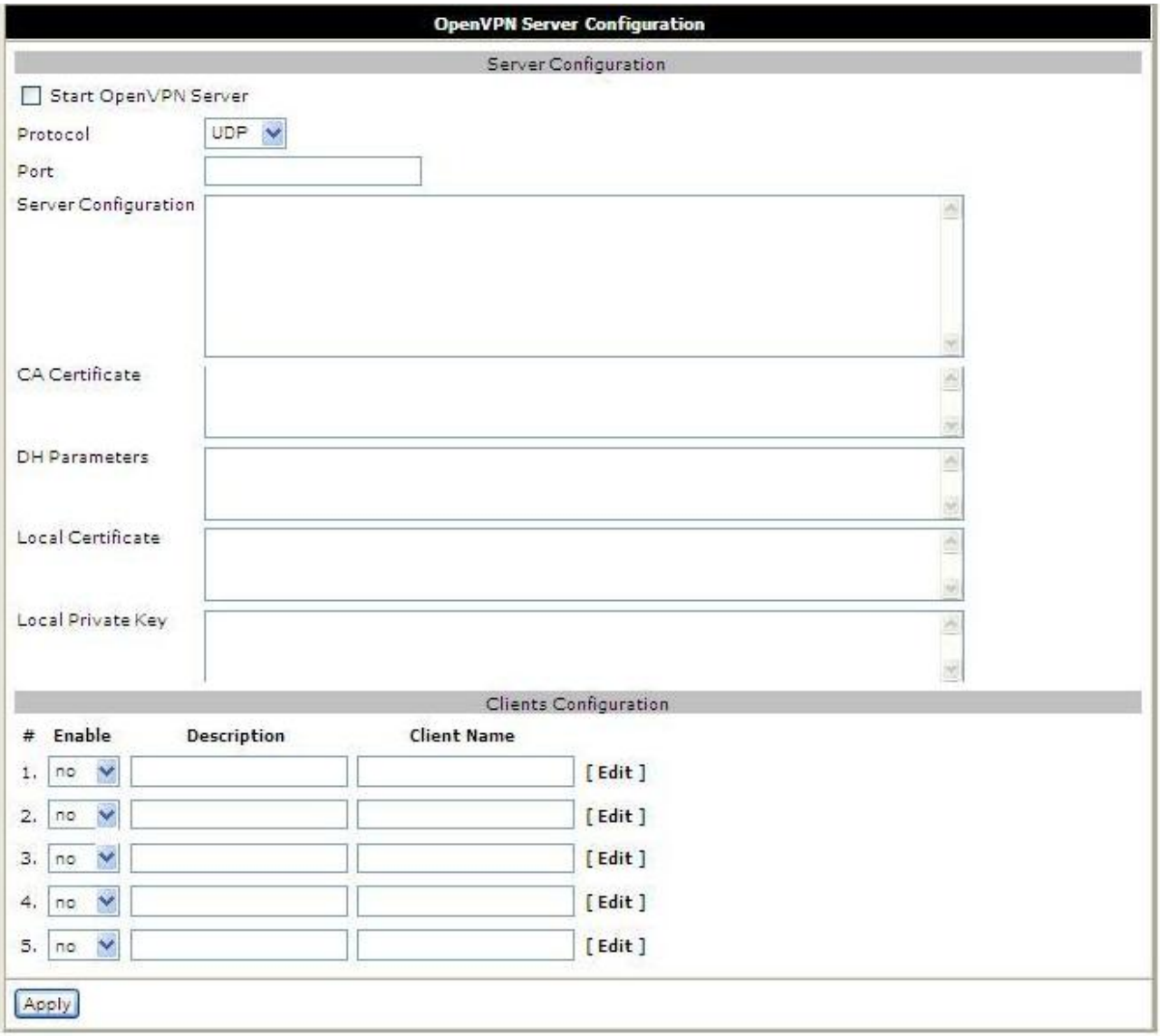
Username - имя пользователя,
Password – пароль,
Pre-shared Secret - ключ для аутентификации,
CA Certificate - корневой сертификат,
DH Parameters - параметры алгоритма Diffie-Hellman
Local Certificate - личный сертификат,
Local Private Key - личный секретный ключ,
Configuration File - поле для ввода файла настройки,
Apply - применить настройки

* - поле может быть пустым

Подробное руководство по настройке туннеля OpenVPN можно найти на нашем сайте в разделе «Поддержка».

4.2.8. OpenVPN Server

OpenVPN сервер позволяет принимать соединения от OpenVPN клиентов.

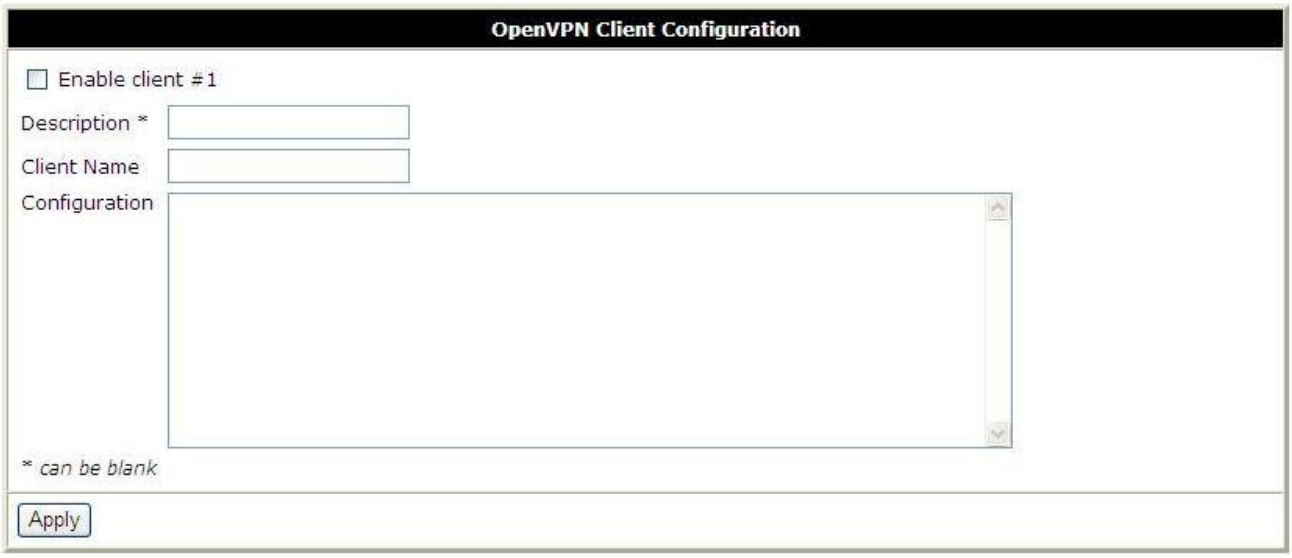


Где:
Server Configuration - настройки сервера,
Start OpenVPN Server - запустить сервер OpenVPN,
Protocol - протокол (TCP или UDP),
Port - порт,
Server Configuration - конфигурация сервера,
CA Certificate - корневой сертификат,
DH Parameters - параметры алгоритма Diffie-Hellman,
Local Certificate - локальный сертификат,
Local Private Key - локальный ключ,
Clients Configuration - настройки клиентов,
- номер клиента,
Enable – разрешить/не разрешить соединение,

Description - краткое описание,
Client Name - имя клиента,
Edit - редактировать настройки клиента,
Apply - применить изменения.

Настройка сервера аналогична настройке сервера OpenVPN на компьютере, за исключением того, что параметры dev, port и proto указывать не нужно.

Страница настройки клиента.

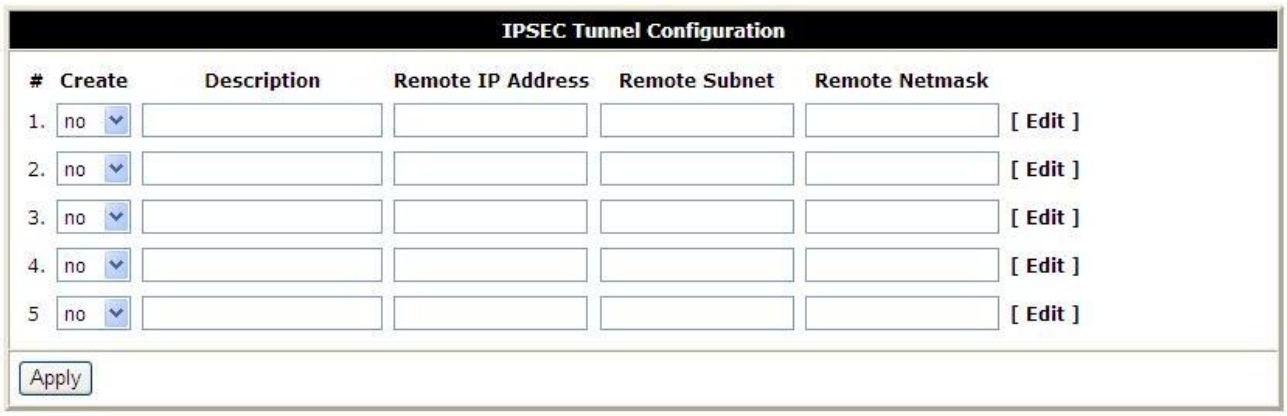


Где:
Enable client #1 - разрешить клиента №1,
Description - краткое описание,
Client Name - имя клиента,
Configuration - конфигурация клиента,
Apply - применить изменения.

* - поле может быть пустым

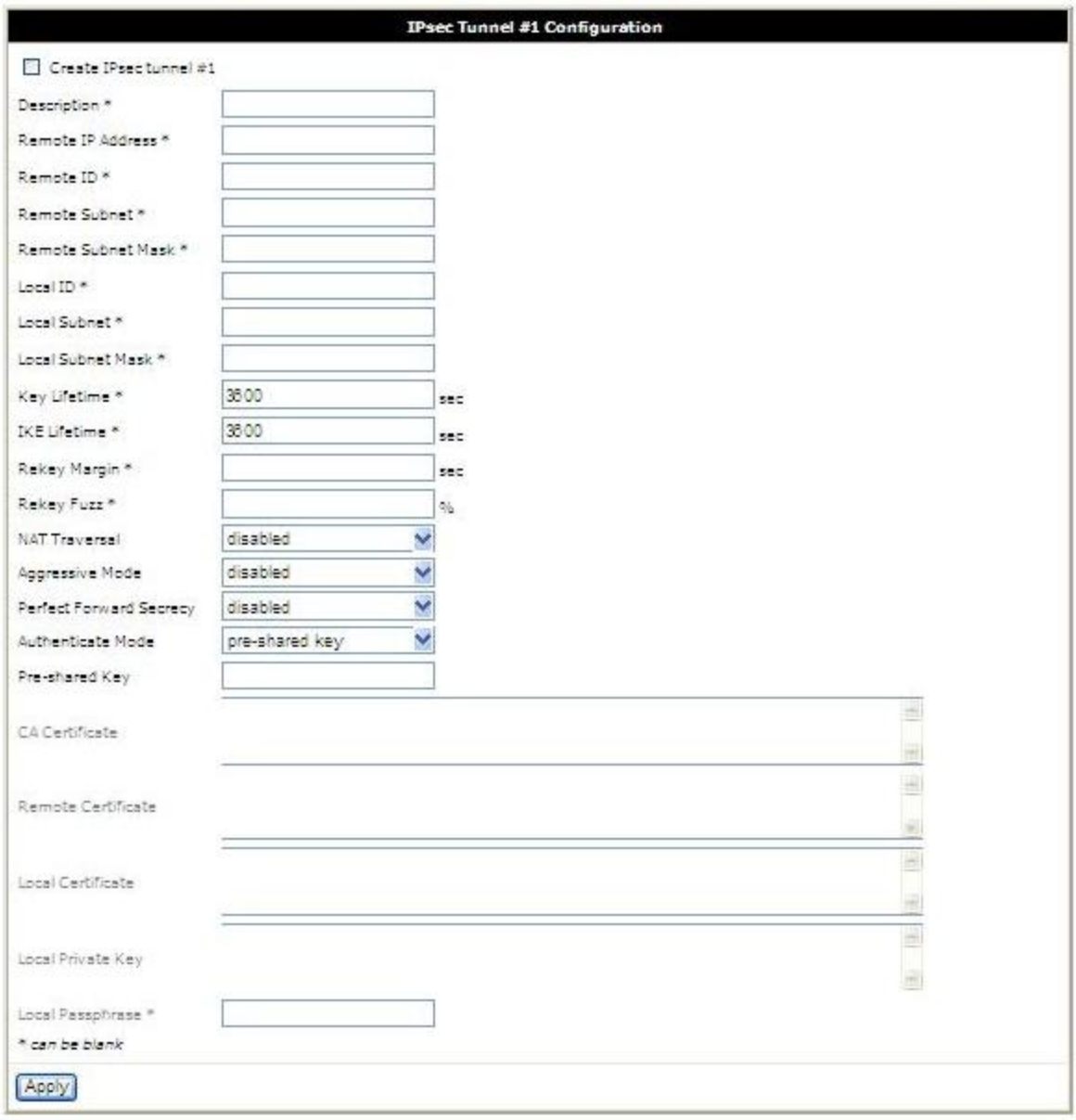
4.2.9. IPsec

IPsec туннель соединяет две сети через зашифрованный канал.



Где:
- номер туннеля,
Create - создать туннель IPsec,
Description – краткое описание,
Remote IP Address - удалённый IP адрес,
Remote Subnet - удалённая подсеть,
Remote Subnet Mask - маска удалённой подсети,
Edit - редактировать настройки клиента,
Apply - применить изменения.

Страница настройки клиента.



Где:
Create IPsec Tunnel #1- создать туннель IPsec №1,
Description – краткое описание,
Remote IP Address - удалённый IP адрес,
Remote ID - удалённый идентификатор,
Remote Subnet - удалённая подсеть,
Remote Subnet Mask - маска удалённой подсети,
Local ID - локальный идентификатор,
Local Subnet - локальная подсеть,
Local Subnet Mask - маска локальной подсети,
Key Lifetime - время жизни ключа,
IKE Lifetime - время жизни IKE соединения,
Rekey Margin - опережение переинициализации,
Rekey Fuzz - случайная добавка к опережению,

NAT Traversal - прохождение через NAT:
- disabled – запрещено,
- enabled – разрешено,

Aggressive Mode - агрессивный режим:
- disabled – запрещено,
- enabled – разрешено,

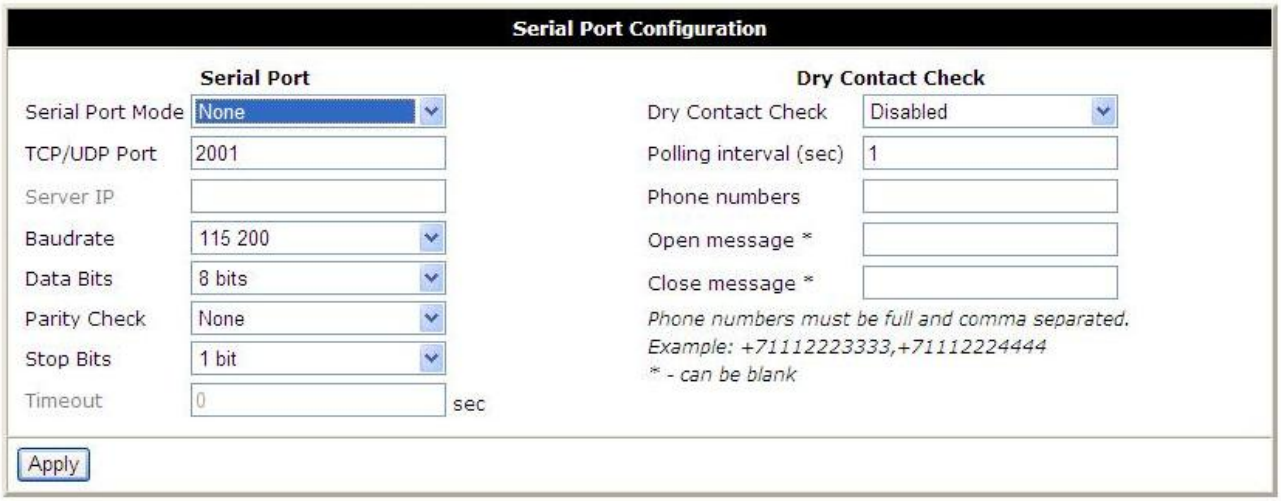
Authenticate Mode - режим аутентификации:
- pre-shared key - общий ключ,
- X.509 certificate - сертификат X.509,

Pre-shared Key - общий ключ,
CA Certificate - корневой сертификат,
Remote Certificate - удалённый сертификат,
Local Certificate - локальный сертификат,
Local Private Key - локальный ключ,
Local Passphrase - локальная парольная фраза,
Apply - применить изменения.

* - поле может быть пустым

4.2.10. Serial Port

Параметры доступа к внешнему последовательному порту.



Где:
Serial Port Mode - режим доступа к последовательному порту,

- None- нет доступа,
- Telnet (TCP) - через Telnet (протокол TCP),
- Raw Data (TCP) - двоичные данные (протокол TCP),
- Tunnel Server (UDP) - сервер туннеля (протокол UDP),
- Tunnel Client (UDP) - - клиент туннеля (протокол UDP),

TCP/UDP Port - порт для подключения (TCP или UDP),
Server IP - IP адрес сервера (только в режиме клиента туннеля),
Baudrate - скорость передачи данных,
Data Bits - количество бит данных,
Parity Check - проверка чётности,

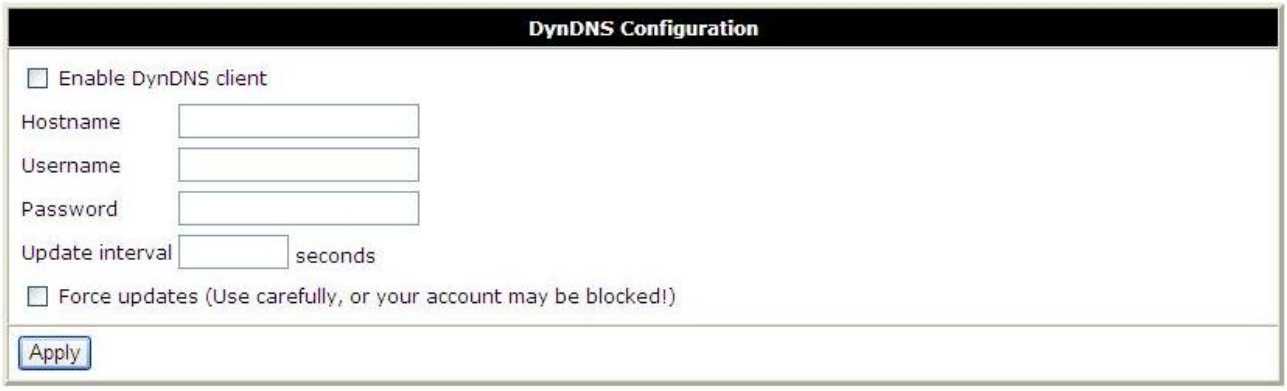
- None – нет,
- Even – чётность,
- Odd – нечётность,

Stop Bits - количество стоп-бит,
Timeout - время ожидания, (только в режимах Telnet и Raw Data)
Apply - применить настройки

Подробное руководство по настройке последовательного порта можно найти на нашем сайте в разделе «Поддержка».

4.2.11. DynDNS

Позволяет назначить доменное имя компьютеру с внешним динамическим IP-адресом.

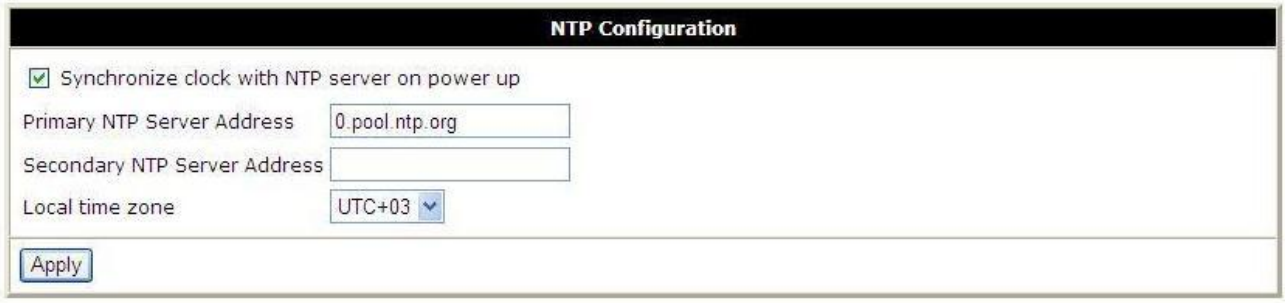


Где:
Enable DynDNS client - включить клиента DynDNS,
Hostname - доменное имя,
Username - имя пользователя,
Password – пароль,
Apply - применить настройки.

Обратите внимание: чтобы использовать сервис DynDNS, необходимо зарегистрироваться на сайте http://www.dyndns.com.

4.2.12. NTP

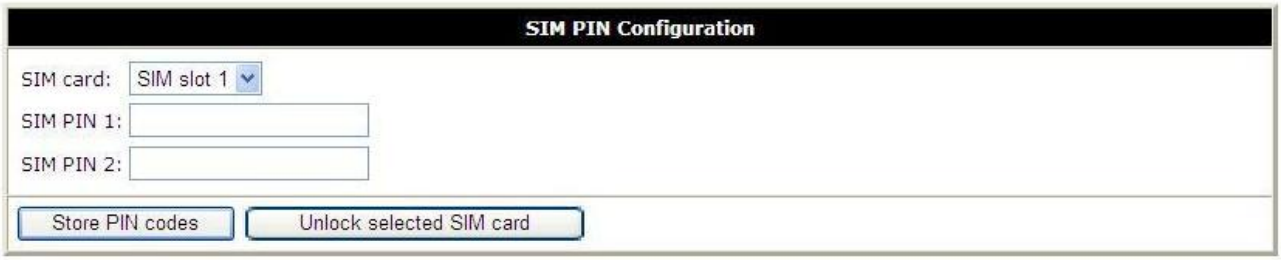
Синхронизация часов роутера с сервером точного времени через интернет.



Где:
Synchronize clock with NTP server on power up - синхронизировать часы при запуске,
Primary NTP Server Address - адрес первого NTP сервера,
Secondary NTP Server Address - адрес второго NTP сервера,
Local time zone - местный часовой пояс,
Apply - применить настройки.

4.2.13. PIN

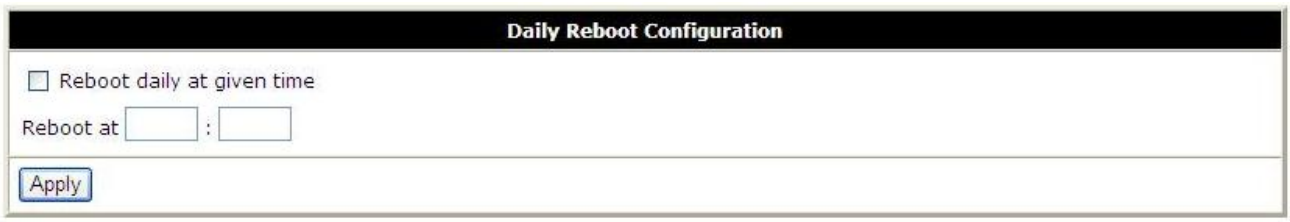
Разблокирование карты, защищённой PIN-кодом.



Где:
SIM card - выбор SIM-карты отключения PIN-кода,
SIM PIN 1 - PIN-код для 1-й SIM-карты,
SIM PIN 2 - PIN-код для 2-й SIM-карты,
Store PIN codes - запомнить PIN-коды,
Unlock selected SIM card - отключить проверку PIN-кода для выбранной SIM-карты.

4.2.14. Daily Reboot

Ежедневная перезагрузка в указанное время.

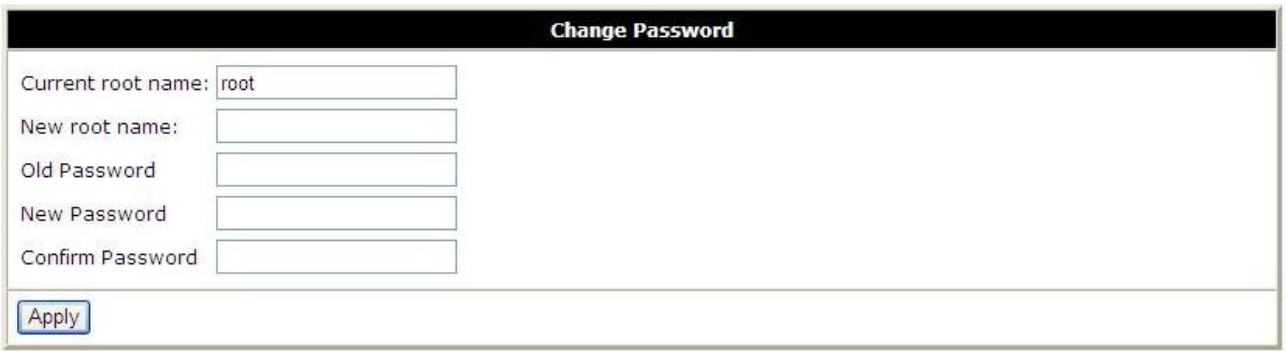


Где:
Reboot daily at given time - перезагружаться ежедневно в указанное время,
Reboot at - время перезагрузки (ЧЧ:ММ),
Apply - применить настройки.

4.3. Administration

4.3.1. Change Password

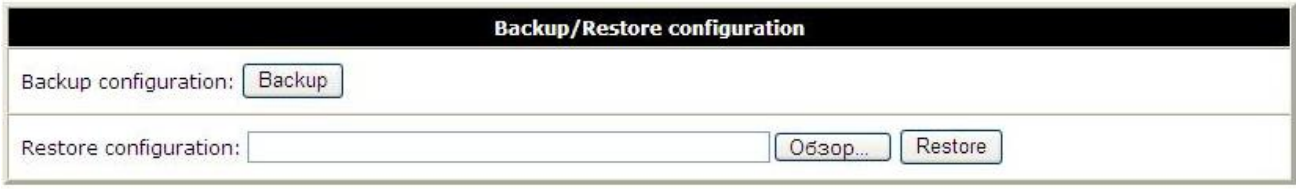
Установка пароля для доступа к web-интерфейсу и консоли, смена имени администратора.



Где:
Current root name - текущее имя администратора,
New root name - новое имя администратора,
Old Password - старый пароль,
New Password - новый пароль,
Confirm Password - повтор нового пароля,
Apply - применить настройки.

4.3.2. Backup/Restore

Сохранение и восстановление настроек роутера.



Где:
Backup - сохранить конфигурацию на компьютере,
Обзор… - выбор файла сохранённой конфигурации,
Restore - восстановление конфигурации.

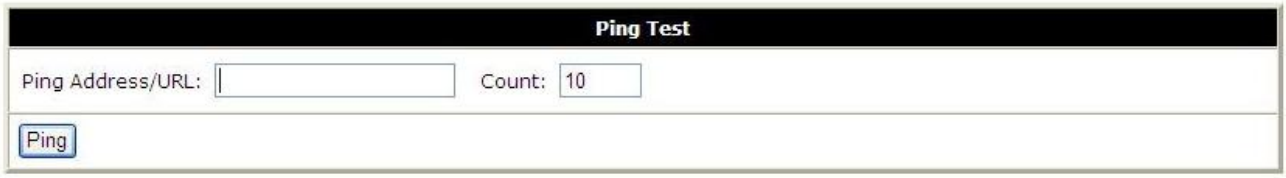
4.3.3. Set Real Time clock

Синхронизировать внутренние часы с сервером точного времени или установить время вручную.

Где:
Current date and time - текущие дата и время,
NTP Server Address - адрес сервера для синхронизации часов,
Enter manually - ввести вручную,
Year - Month – Day - Год - Месяц – День,
Hours : Minutes : Seconds - Часы : Минуты : Секунды,
Apply - применить настройки.

4.3.4. Ping Test

Проверка подключения к интернету.



Где:
Ping Address/URL – адрес,
Count – количество попыток,
Ping – старт проверки.

4.3.5. Startup Script

Скрипт запускается при включении устройства и позволяет проводить дополнительные настройки.

Где:
Run script at startup - выполнить скрипт после запуска,
#!/bin/sh - скрипт обязательно должен начинаться с указания интерпретатора,
Save Script - сохранить скрипт.

4.3.6. IP-Up Script

Скрипт запускается при подключении к интернету и позволяет проводить дополнительные настройки.

Где:
Run script when connected - выполнить скрипт после подключения устройства к интернету,
#!/bin/sh - скрипт обязательно должен начинаться с указания интерпретатора,
Save Script - сохранить скрипт.

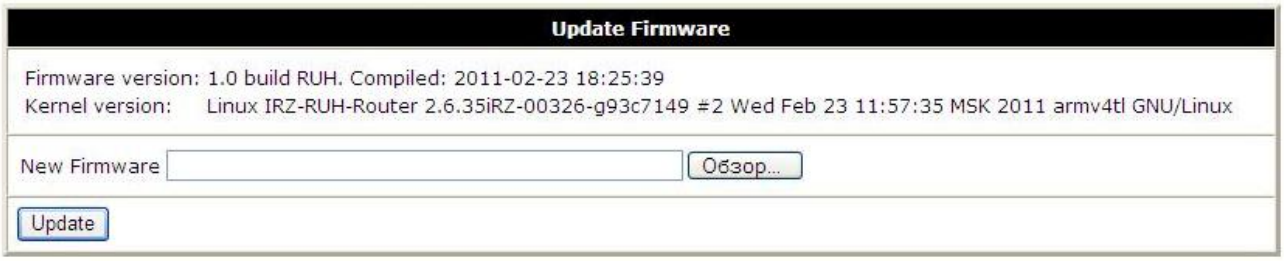
4.3.7. IP-Down Script

Скрипт запускается после отключения устройства от интернета и позволяет проводить дополнительные настройки.

Где:
Run script when disconnected - выполнить скрипт после отключения устройства от интернета,
#!/bin/sh - скрипт обязательно должен начинаться с указания интерпретатора,
Save Script - сохранить скрипт.

4.3.8. Update Firmware

Обновление внутреннего программного обеспечения роутера.



Где:
Firmware Version - текущая версия внутренней программы,
Обзор... - выбор файла с новой версией программы,
Update - выполнить обновление .

4.3.9. Reboot

Перезагрузка роутера, сброс в заводские настройки.

Где:
Reset configuration to defaults – при перезагрузке вернуть настройки по умолчанию,
The reboot process will take about 60 seconds to complete - процесс перезагрузки займёт около 60 секунд
Reboot - выполнить перезагрузку.

5. Поддержка

Новые версии документации и программного обеспечения для роутера можно найти на сайте компании «Радиофид» http://radiofid.ru.