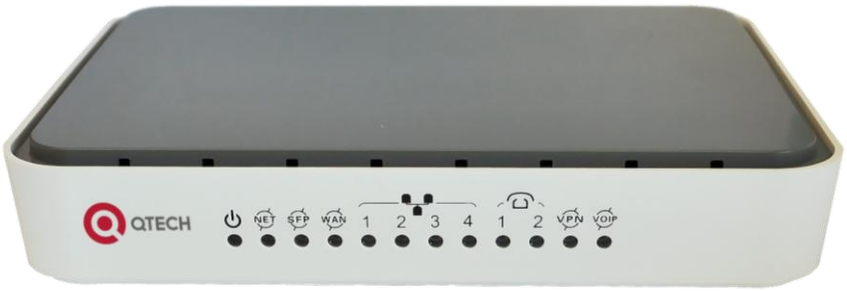
QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ



QFR-300

www.qtech.ru

Оглавление

1. ВВЕДЕНИЕ

Серия гигабитных оптических маршрутизаторов QFR-300 — это отличное решение для волоконно-оптических сетей операторов связи. В серию входят модели QFR-300-4G-2V-W-U и QFR-300-4G-W-U.

В отличие от других устройств маршрутизаторы серии QFR-300 поддерживают функции VPN, VLAN, маршрутизации, брандмауэра и т. д., удовлетворяя требованиям эффективной и безопасной передачи данных. Маршрутизаторы поддерживает стандарты Wi-Fi 802.11b/g/n (до 300 Мбит/с), SFP, гигабитные интерфейсы для сетей WAN и LAN и отвечает всем требованиям для передачи голоса, данных и видео.

1.1 Целевая аудитория

Данное руководство предназначено для технических специалистов, сетевых инженеров и администраторов, занимающихся развертыванием, настройкой и управлением сетями. Описание настроек, представленных в руководстве, актуально для всех версий прошивок, начиная с версии 1.10.

1.2 Внешний вид устройства

Лицевая панель коммутатора представлена на рисунке 1.1, задняя панель устройства изображена на рисунке 1.2 Состояние индикаторов, расположенных на лицевой панели, а также их описание и их обозначения описаны в таблице 1.1

Рисунок 1-1. Лицевая панель маршрутизатора QFR-300-4G2VWU

Рисунок 1-2. Задняя панель маршрутизатора QFR-300-4G2VWU

Таблица 1-1. Описание индикаторов устройства

Индикатор	Цвет	Состояние
PWR	Выключен	Питание устройства выключено
	Горит зеленым	Устройство включено
INTERNET	Выключен	Питание устройства выключено
	Медленно мигает зеленый	Ошибка при авторизации PPPoE соединения
	Горит зеленым	Подключение WAN установлено
SFP	Выключен	Нет оптического сигнала
	Горит зеленым	Есть оптический сигнал, интерфейс готов к работе
WAN	Выключен	Нет соединения
	Мигает зеленым	Идет передача данных
	Горит зеленым	Есть соединение, интерфейс готов к работek
LAN1 - LAN4	Выключен	Нет соединения
	Мигает зеленым	Идет передача данных
	Горит зеленым	Есть соединение, интерфейс готов к работek
Phone1&2	Выключен	Нет регистрации на SIP сервере
	Горит зеленым	Зарегистрирован на SIP сервере
VPN	Выключен	Нет VPN подключения

	Горит зеленым	Установлено VPN подключение
REG	Выключен	Ошибка при регистрации всех подключений
	Горит зеленым	Все подключения зарегистрированы
	Мигает зеленый	Некоторые подключения установлены и не удается зарегистрировать остальныes

На задней панели расположены следующие элементы:

- WAN-порт: поддерживает подключение на скорости 1000/100/10 Мбит/с.
- LAN-порты: поддерживают подключение на скорости 1000/100/10 Мбит/с.
- SFP-порт: поддерживают подключение на скорости 1000/100/10 Мбит/с.
- FXS порты: для подключения аналоговой телефонии.
- POWER: кнопка выключения питания.
- Reset: кнопка сброса устройства на заводские настройки.
- WPS: кнопка включения WPS

2. СПЕЦИФИКАЦИЯ

2.1 Сеть передачи данных

Таблица 2-1 Сеть передачи данных

WAN	1 порт Ethernet-WAN 10/100/1000 Мбит/с, 1 порт SFP 10/100/1000 Мбит/с, 1 порт USB для подключения модема 2G, 3G или 4G
Сеть LAN	4 порта Ethernet 10/100/1000 Мбит/с
Способ доступа к сети WAN	Статический IP-адрес, PPPoE, DHCP
Сетевой интерфейс	Подключение к нескольким провайдерам (MultiWAN), режим моста, 802.1Q
Качество обслуживания (QoS)	MAC/IP-адрес приемника/источника, приложение, DSCP, приоритет пакетов, ограничение полосы пропускания
Маршрутизация	Статическая маршрутизация, маршрутизация на основе правил, DNS-прокси, протокол RIP, перенаправление/запуск портов
Управление внутренними адресами	DHCP-сервер, привязка IP-адресов и MAC-адресов, ретрансляция DHCP
Сетевые протоколы	TCP/IP (IPv4/v6), UDP, RTP, SNTP, NAT, DHCP, DNS, DDNS
VPN	PPTP, L2TP
IP-телевидение	IGMP-прокси / отслеживание пакетов IGMP, мост IP-телевидения

2.2 Беспроводная сеть

Таблица 2-3 Беспроводная сеть

Стандарт	IEEE 802.11b/g/n (2,4 ГГц)
Безопасность	WEP, WPA, WPA2, WPA-PSK, WPA2-PSK
Функции Wi-Fi	WMM, изоляция WLAN от LAN, Multi-SSID (до 4), изоляция точки доступа
Тип антенны	2R2T

2.3 Голосовые характеристики

Голосовые характеристики для модели маршрутизатора QFR-300-4G-2V-W-U.

Таблица 2-4 Голосовые характеристики

Аналоговый интерфейс	2 порта FXS
Кодеки	G.711Alaw, G.711mulaw, G.723, G.729
Протокол	SIP
Факс	T.30/T.38, прозрачный канал передачи для факсов
Биллинг	Обратная полярность
Голосовые функции	Определитель номера, ожидание вызова, перенаправление вызова, переадресация вызова, быстрый набор, трехсторонняя конференция, функция «не беспокоить» (должна поддерживаться оператором)
Аналоговый интерфейс	2 порта FXS
Кодеки	G.711Alaw, G.711mulaw, G.723, G.729
Протокол	SIP
Факс	T.30/T.38, прозрачный канал передачи для факсов

2.4 Брандмауэр и безопасность

Таблица 2-5 Брандмауэр и безопасность

Брандмауэр	IDS и IPS, блокировка ping-запросов / ICMP / IDENT, брандмауэр SPI, ограничение сканирования портов
Управление доступом	Блокировка по URL, IP-адресу, MAC-адресу, типу протокола, порту

2.5 Управление

Таблица 2-6 Управление

Протоколы управления	Командная строка (CLI), SNMP версии 1/2, TR-069, веб-интерфейс
Светодиодные индикаторы	12 светодиодных индикаторов: питание, активность сетей WAN/LAN, телефонная линия
Кнопки управления	Кнопка WPS, кнопка WLAN, выключатель питания, кнопка сброса

2.6 Условия эксплуатации

Таблица 2-7 Условия эксплуатации

Габариты	204 × 151 × 37 мм
Масса нетто	632 г
Питание	12 В пост. тока, 1 А
Диапазон рабочих температур	от 0 до 40 °C, от 32 до 113 °F
Влажность	10–90 %, без конденсации

3. ИНСТРУКЦИЯ ПО НАСТРОЙКЕ

3.1 Авторизация

Для получения доступа к WEB-интерфейсу маршрутизатора, необходимо подключиться к устройству через LAN-порт, после чего ввести в адресной строке браузера IP-адрес (по умолчанию 192.168.10.1) и нажать клавишу Enter. Появится меню, изображенное на рисунке 2.1

Рисунок 3-1. Меню авторизации

3.2 Пункт меню Home

После авторизации на WEB-интерфейсе, в верхней части экрана появится основное меню и откроется страница System status (состояние системы). На странице можно увидеть основную информацию о текущем состоянии маршрутизатора.

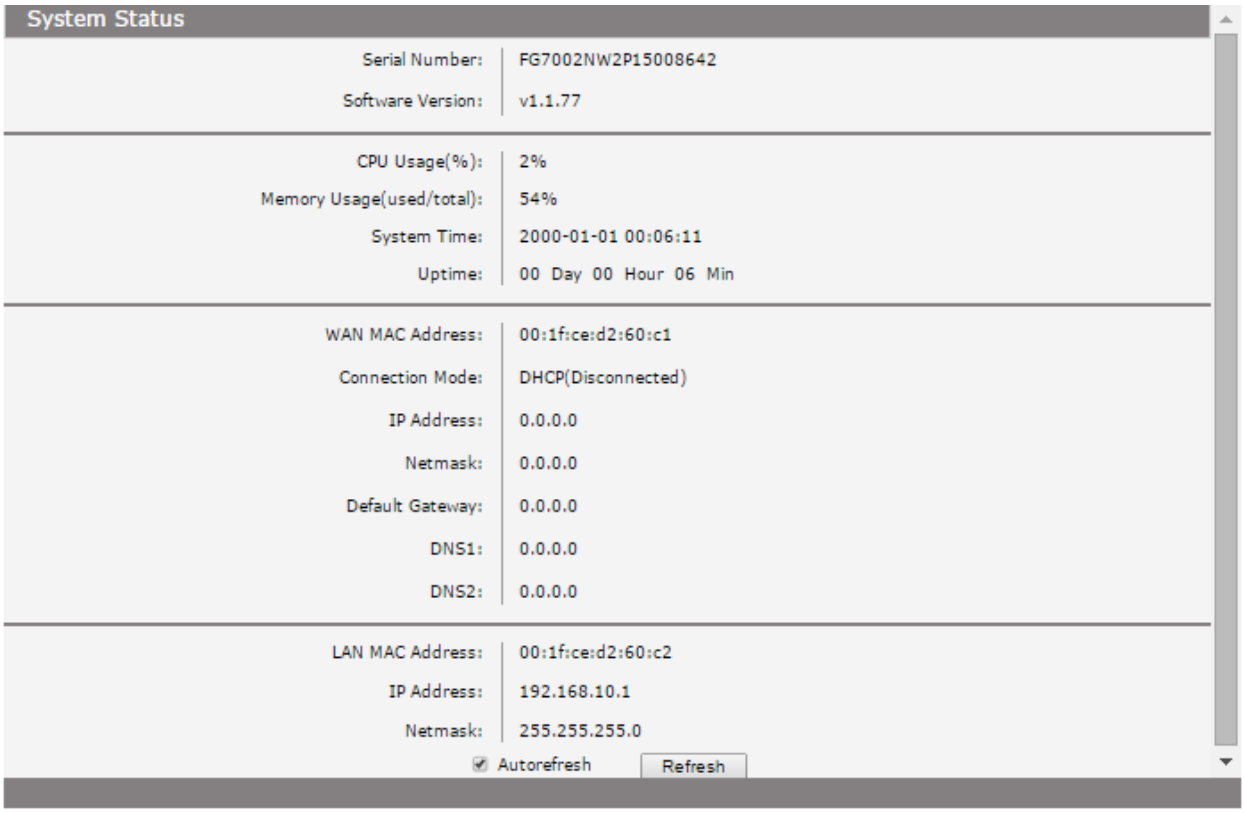


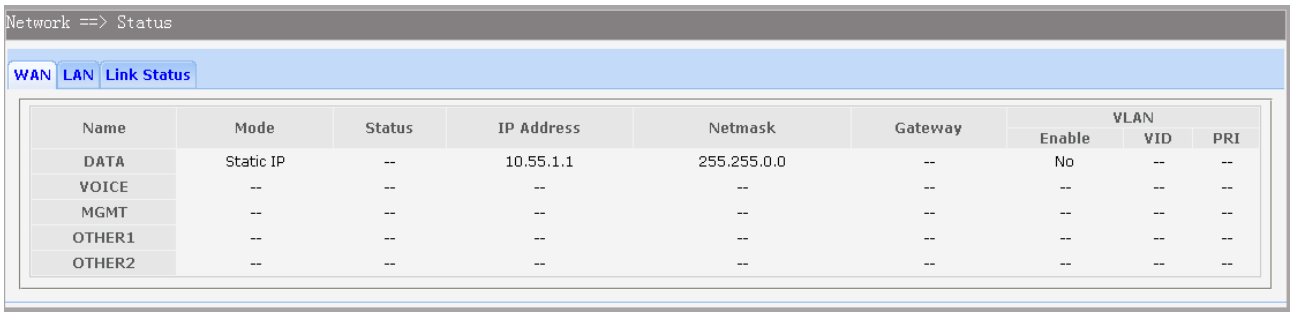
Рисунок 3-2. Состояние системы

3.3 Пункт меню Network Configuration

3.3.1 Состояние сети

3.3.1.1 Состояние WAN

Для просмотра состояния WAN интерфейсов, выберите в меню пункты Network→Status→WAN.



Name	Mode	Status	IP Address	Netmask	Gateway	VLAN		
						Enable	VID	PRI
DATA	Static IP	--	10.55.1.1	255.255.0.0	--	No	--	--
VOICE	--	--	--	--	--	--	--	--
MGMT	--	--	--	--	--	--	--	--
OTHER1	--	--	--	--	--	--	--	--
OTHER2	--	--	--	--	--	--	--	--

Рисунок 3-3. Состояние WAN интерфейсов

3.3.1.2 Состояние LAN

Для просмотра состояния LAN интерфейсов, выберите в меню пункты Network→Status→LAN.

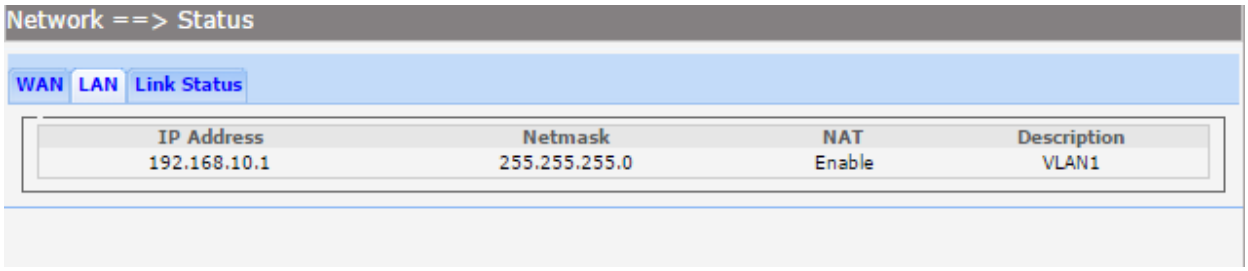


Рисунок 3-4. Состояние LAN интерфейсов

3.3.1.3 Физическое состояние портов

Для просмотра физического состояния портов, выберите в меню пункты Network→Status→Link Status.

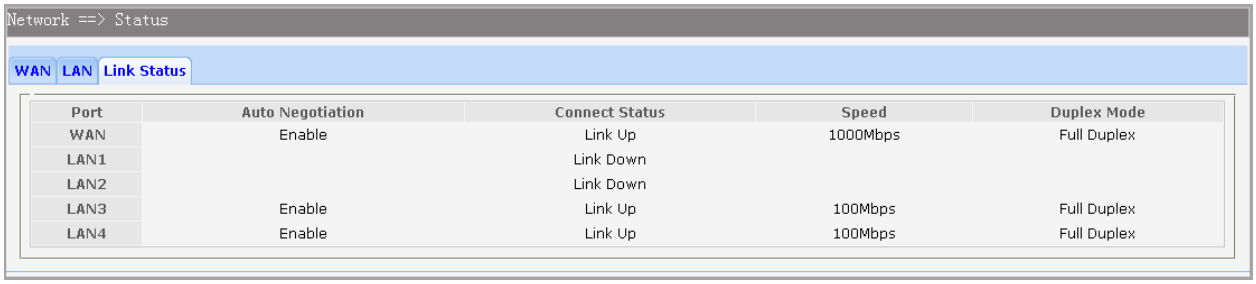


Рисунок 3-5. Физическое состояние портов

3.3.2 Настройка WAN

Маршрутизаторы серии QFR-300 поддерживает работу пяти WAN-интерфейсов: DATA; VOICE; MGMT; OTHER1; OTHER2. Каждый из указанных интерфейсов позволяет использовать различные варианты подключений: статический IP, получение настроек по DHCP, создание PPPoE соединения, создание PPTP соединения, создание L2TP соединения. Для перехода на страницу конфигурации интерфейса, выберите в меню пункты Network→WAN, после чего необходимо нажать на имя интерфейса.

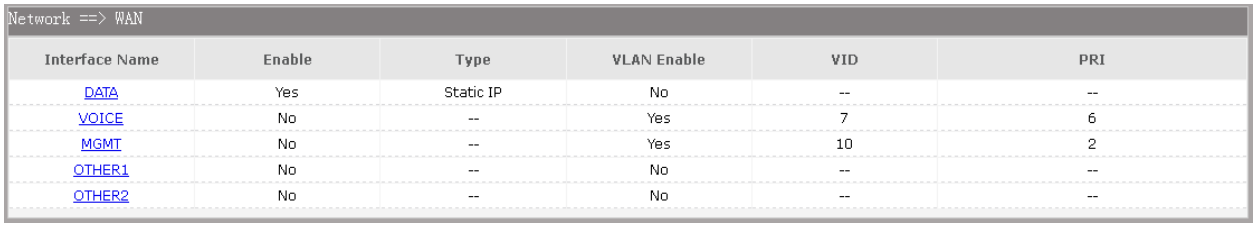


Рисунок 3-6. Меню настройки WAN интрефейсов

3.3.2.1 Настройка статического IP адреса

Если ваш интернет провайдер предоставляет доступ в глобальную сеть, используя статический IP-адрес, необходимо выбрать тип подключения Static IP и выполнить настройки, указанные ниже.

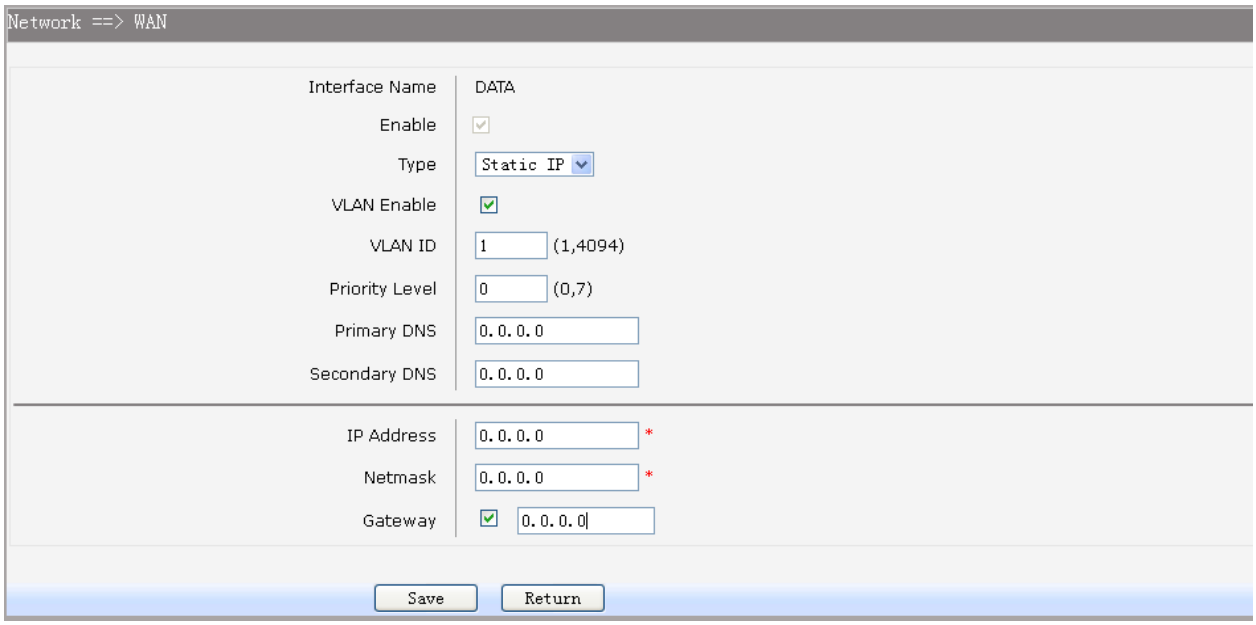


Рисунок 3-7. Настройка статического IP на WAN интерфейсе

Пункты для настройки статического IP-адреса:

- Enable: включает работу интерфейса (интерфейс DATA включен всегда).
- Type: выберите пункт Static IP.
- VLAN Enable: необязательная настройка, включение которой позволяет настроить идентификатор VLAN и выбрать приоритет, для настраиваемого интерфейса.
- VLAN ID: необязательная настройка. Задает идентификатор VLAN для настраиваемого интерфейса.
- Priority level: необязательная настройка. Задает уровень приоритета VLAN для настраиваемого интерфейса.
- Primary DNS: введите адрес DNS сервера.
- Secondary DNS: необязательная настройка. Если в настройках, выданных провайдером указан второй адрес DNS сервера, введите его.
- IP Address: введите IP адрес, согласно настройкам, выданным провайдером.
- Netmask: введите маску подсети, согласно настройкам, выданным провайдером.
- Gateway: введите адрес шлюза, согласно настройкам, выданным провайдером.

3.3.2.2 Настройка соединения по DHCP

Если ваш интернет провайдер предоставляет доступ в глобальную с сеть, используя автоматическое назначение IP-адресов посредством протокола DHCP, необходимо выбрать тип подключения DHCP и выполнить настройки интерфейса, указанные ниже.

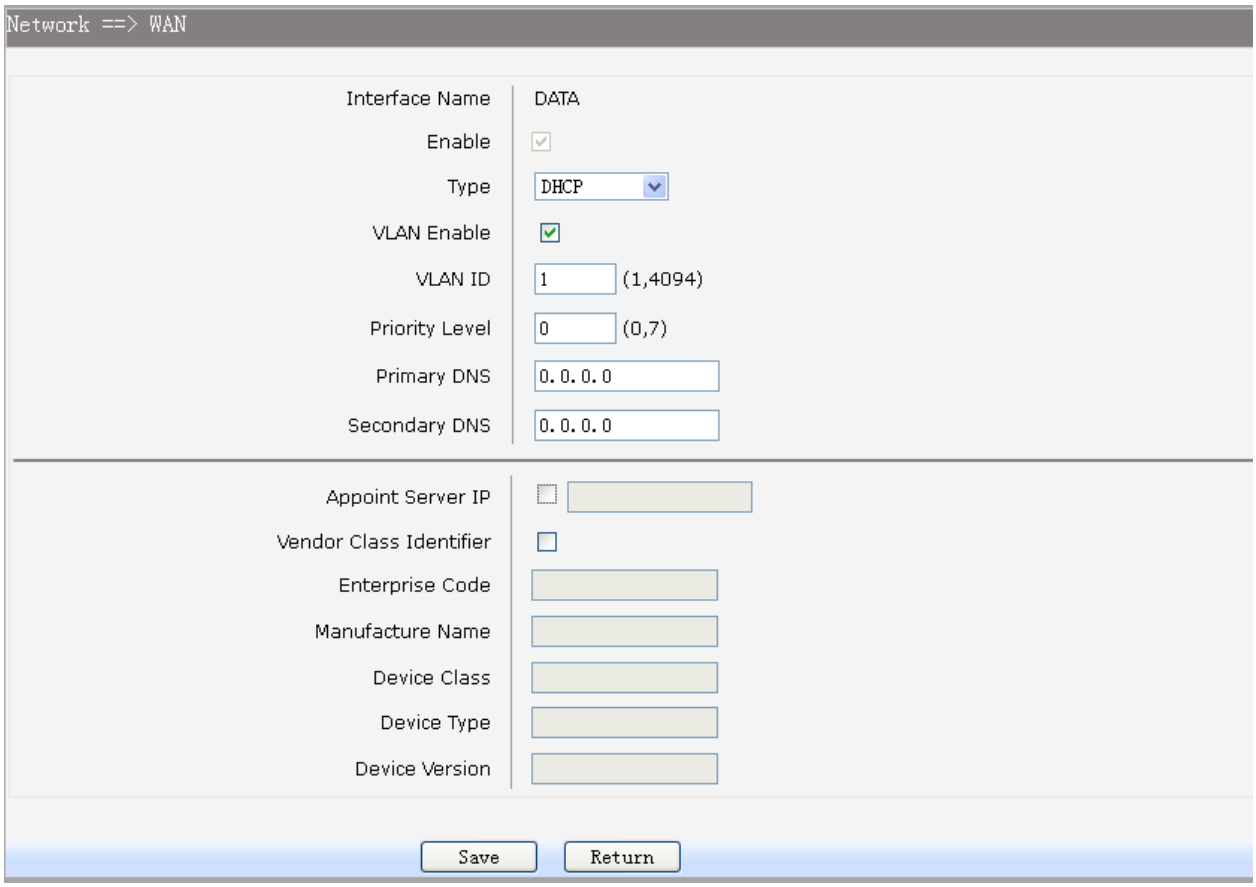


Рисунок 3-8. Настройка DHCP на WAN интерфейсе.

Пункты для настройки интерфейса:

- Enable: включает работу интерфейса (интерфейс DATA включен всегда).
- Type: выберите пункт DHCP
- VLAN Enable: необязательная настройка, включение которой позволяет настроить идентификатор VLAN и выбрать приоритет, для настраиваемого интерфейса.
- VLAN ID: необязательная настройка. Задает идентификатор VLAN для настраиваемого интерфейса.
- Priority level: необязательная настройка. Задает уровень приоритета VLAN для настраиваемого интерфейса.
- Primary DNS: введите адрес DNS сервера, который выдал ваш провайдер.
- Secondary DNS: необязательная настройка.
- Appoint Server IP: необязательная настройка. Если в сети несколько DHCP-серверов, необходимо задать IP-адрес DHCP-сервера вашего провайдера.

- Vendor Class Identifier: необязательная настройка Может использоваться DHCP-клиентом чтобы сообщить DHCP-серверу о производителе и функционале устройства.
- Manufacture Name: необязательная настройка. Настраивается, если включена передача информации в пункте Vendor Class Identifier.
- Device Class: необязательная настройка. Настраивается, если включена передача информации в пункте Vendor Class Identifier.
- Device Type: необязательная настройка. Настраивается, если включена передача информации в пункте Vendor Class Identifier.
- Device Version: необязательная настройка. Настраивается, если включена передача информации в пункте Vendor Class Identifier.

3.3.2.3 Настройка PPPoE соединения

Если ваш интернет провайдер предоставляет доступ в глобальную сеть посредством создания PPPoE соединения, необходимо выбрать тип подключения PPPoE и выполнить настройки, описанные ниже.

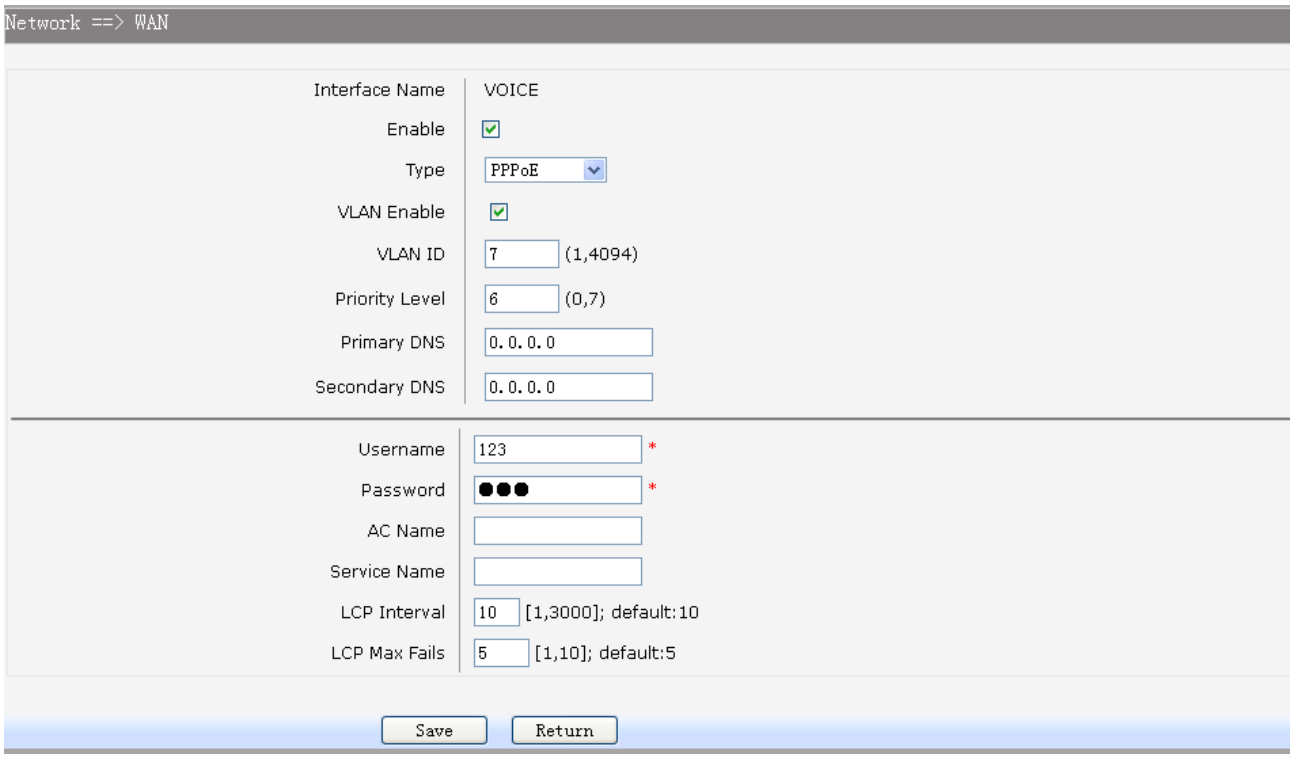


Рисунок 3-9. Настройка PPPoE подключения на WAN интерфейсе

Пункты для настройки PPPoE соединения:

- Enable: включает работу интерфейса (интерфейс DATA включен всегда).
- Type: выберите пункт PPPoE.

- VLAN Enable: необязательная настройка, включение которой позволяет настроить идентификатор VLAN и выбрать приоритет, для настраиваемого интерфейса.
- VLAN ID: необязательная настройка. Задает идентификатор VLAN для настраиваемого интерфейса.
- Priority level: необязательная настройка. Задает уровень приоритета VLAN для настраиваемого интерфейса.
- Primary DNS: введите адрес DNS сервера, который выдал ваш провайдер.
- Secondary DNS: необязательная настройка. Если провайдер указал второй адрес DNS сервера, введите его.
- Username: введите логин, предоставленный провайдером.
- Password: введите пароль, предоставленный провайдером.
- Service Name/AC Name: необязательная настройка. Имя службы и имя концентратора доступа необходимо конфигурировать, если на это в явно виде указал ваш провайдер. В большинстве случаев, это поле можно оставить пустым и PPPoE подключение будет работать.
- LCP Interval: PPPoE соединение посылает эхо запросы LCP через определенный интервал, указанный в данном пункте.
- LCP Max Fails: PPPoE соединение будет считаться разорванным если число эхо запросов LCP, указанных в этом пункте, останутся без эхо-ответа.

3.3.2.4 Настройка L2TP соединения

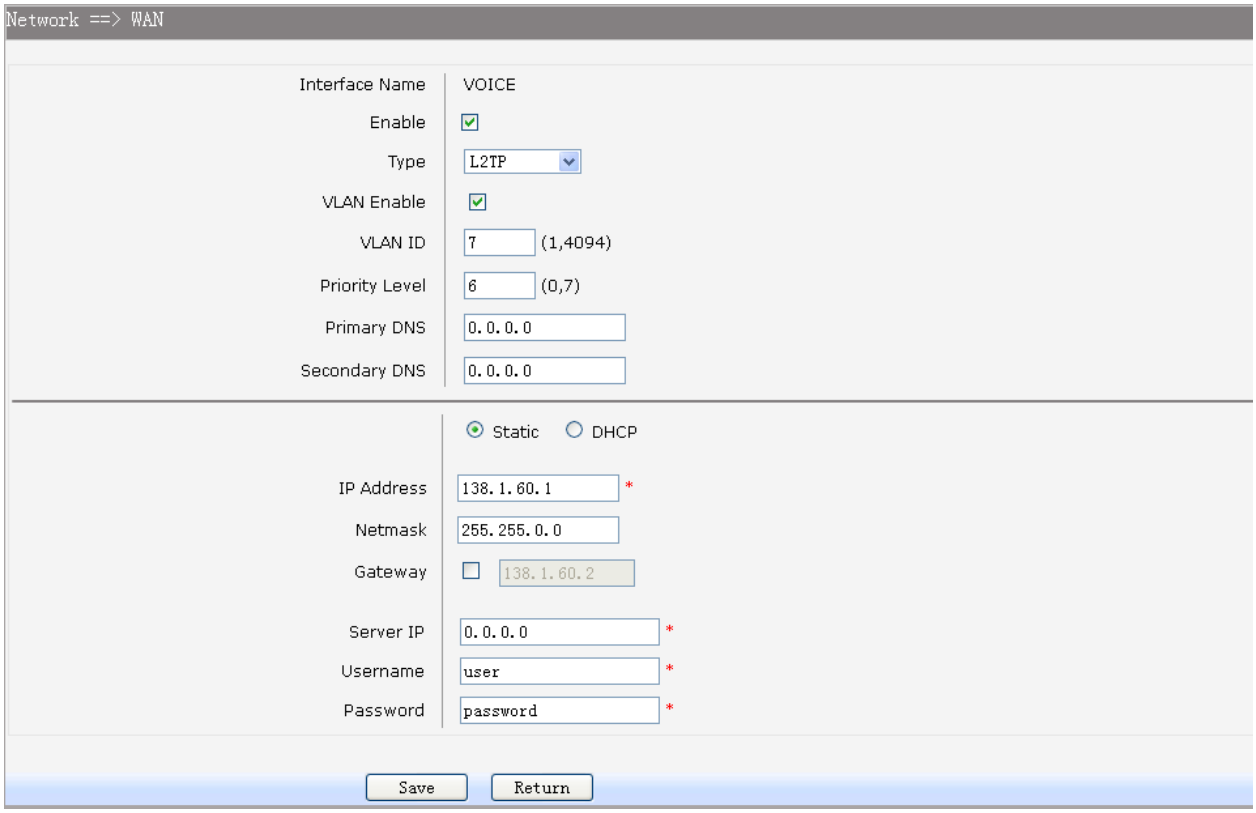


Рисунок 3-10. Настройка L2TP подключения на WAN интерфейсе

Если ваш интернет провайдер предоставляет доступ в глобальную сеть по технологии L2TP, необходимо выбрать тип подключения L2TP и выполнить настройки, представленные ниже:

- Enable: включает работу интерфейса (интерфейс DATA включен всегда).
- Type: выберите пункт L2TP.
- VLAN Enable: необязательная настройка, включение которой позволяет настроить идентификатор VLAN и выбрать приоритет, для настраиваемого интерфейса.
- VLAN ID: необязательная настройка. Задает идентификатор VLAN для настраиваемого интерфейса.
- Priority level: необязательная настройка. Задает уровень приоритета VLAN для настраиваемого интерфейса.
- Primary DNS: введите адрес DNS сервера, который выдал ваш провайдер.
- Secondary DNS: необязательная настройка. Если провайдер указал второй адрес DNS сервера, введите его.
- Username: введите логин, предоставленный провайдером.

- Password: введите пароль, предоставленный провайдером.

В следующих пунктах отражены настройки подключении при использовании двух различных возможных способах подключения: ручная настройка статического IP или автоматическое получение настроек от DHCP-сервера. Если используется статический IP адрес, необходимо настроить следующие пункты:

- IP Address: введите IP адрес, согласно настройкам, выданным провайдером.
- Netmask: введите маску подсети, согласно настройкам, выданным провайдером.
- Gateway: введите адрес шлюза, согласно настройкам, выданным провайдером.

Если подключение получает адрес от DHCP сервера, возможны следующие настройки:

- Appoint Server IP: необязательная настройка. Если в сети несколько DHCP-серверов, необходимо задать IP-адрес DHCP-сервера вашего провайдера.
- Vendor Class Identifier: необязательная настройка Может использоваться DHCP-клиентом чтобы сообщить DHCP-серверу о производителе и функционале устройства.
- Manufacture Name: необязательная настройка.
- Device Class: необязательная настройка.
- Device Type: необязательная настройка.
- Device Version: необязательная настройка.

3.3.2.5 Настройка PPTP соединения

Если ваш интернет провайдер предоставляет доступ в глобальную сеть посредством технологии PPT, необходимо выбрать тип подключения PPTP и выполнить настройки, представленные ниже:

- Enable: включает работу интерфейса (интерфейс DATA включен всегда).
- Type: выберите пункт PPTP.
- VLAN Enable: необязательная настройка, включение которой позволяет настроить идентификатор VLAN и выбрать приоритет, для настраиваемого интерфейса.
- VLAN ID: необязательная настройка. Задает идентификатор VLAN для настраиваемого интерфейса.
- Priority level: необязательная настройка. Задает уровень приоритета VLAN для настраиваемого интерфейса.
- Primary DNS: введите адрес DNS сервера, который выдал ваш провайдер..
- Secondary DNS: необязательная настройка. Если провайдер указал второй адрес DNS сервера, введите его.

- Server IP: введите IP-адрес PPTP сервера, предоставленный провайдером.
- Username: введите логин, предоставленный провайдером.
- Password: введите пароль, предоставленный провайдером.
- Enable Encryption: необязательная настройка. Включает шифрование трафика.

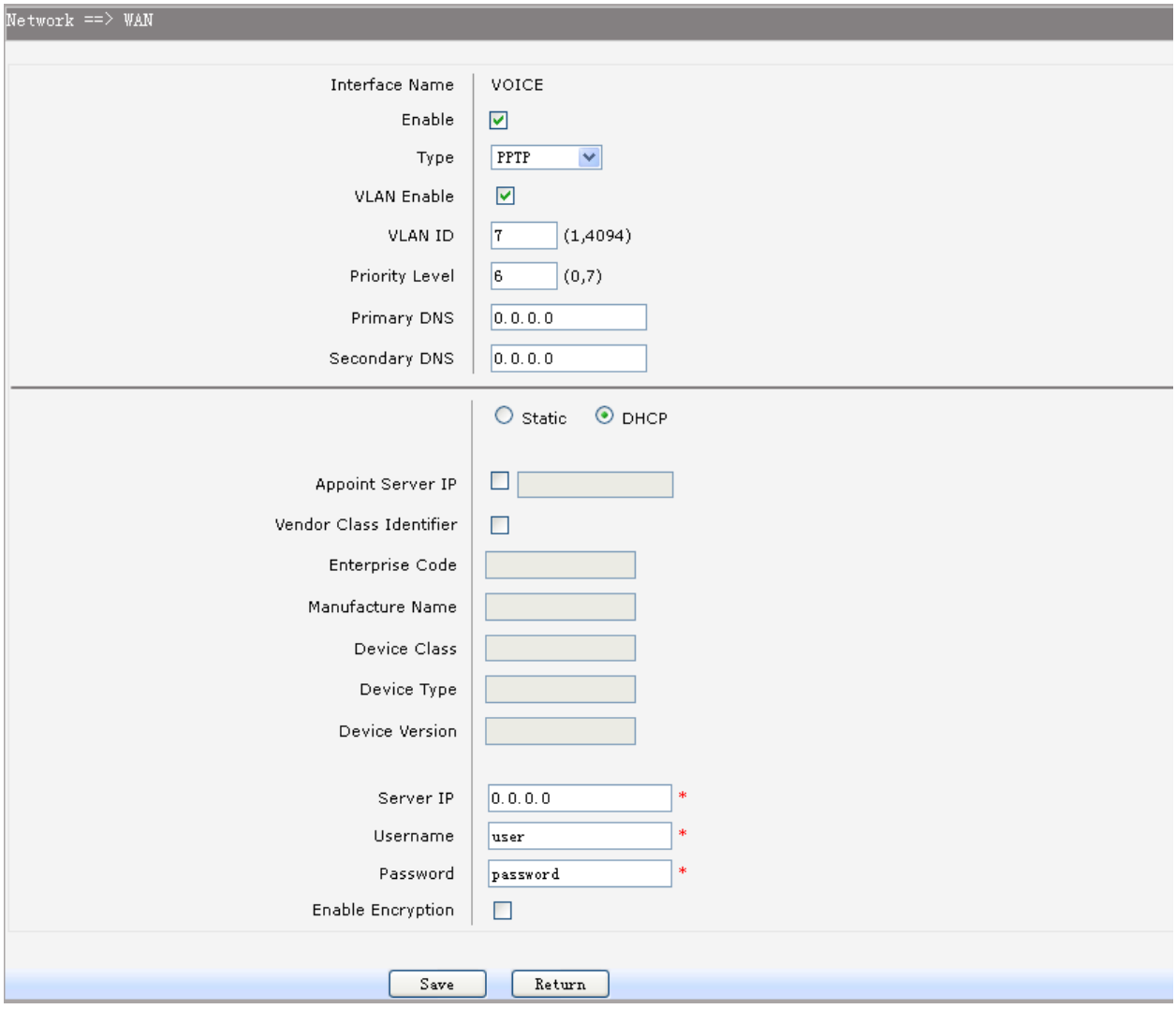


Рисунок 3-11. Настройка PPTP подключения на WAN интерфейсе

В следующих пунктах отражены настройки подключении при использовании двух различных возможных способах подключения: ручная настройка статического IP или автоматическое получение настроек от DHCP-сервера. Если используется статический IP адрес, необходимо настроить следующие пункты:

- IP Address: введите IP адрес, согласно настройкам, выданным провайдером.
- Netmask: введите маску подсети, согласно настройкам, выданным провайдером.

- Gateway: введите адрес шлюза, согласно настройкам, выданным провайдером.

Если подключение получает адрес от DHCP сервера, возможны следующие настройки:

- Appoint Server IP: необязательная настройка. Если в сети несколько DHCP-серверов, необходимо задать IP-адрес DHCP-сервера вашего провайдера.
- Vendor Class Identifier: необязательная настройка Может использоваться DHCP-клиентом чтобы сообщить DHCP-серверу о производителе и функционале устройства.
- Manufacture Name: необязательная настройка.
- Device Class: необязательная настройка.
- Device Type: необязательная настройка.
- Device Version: необязательная настройка.

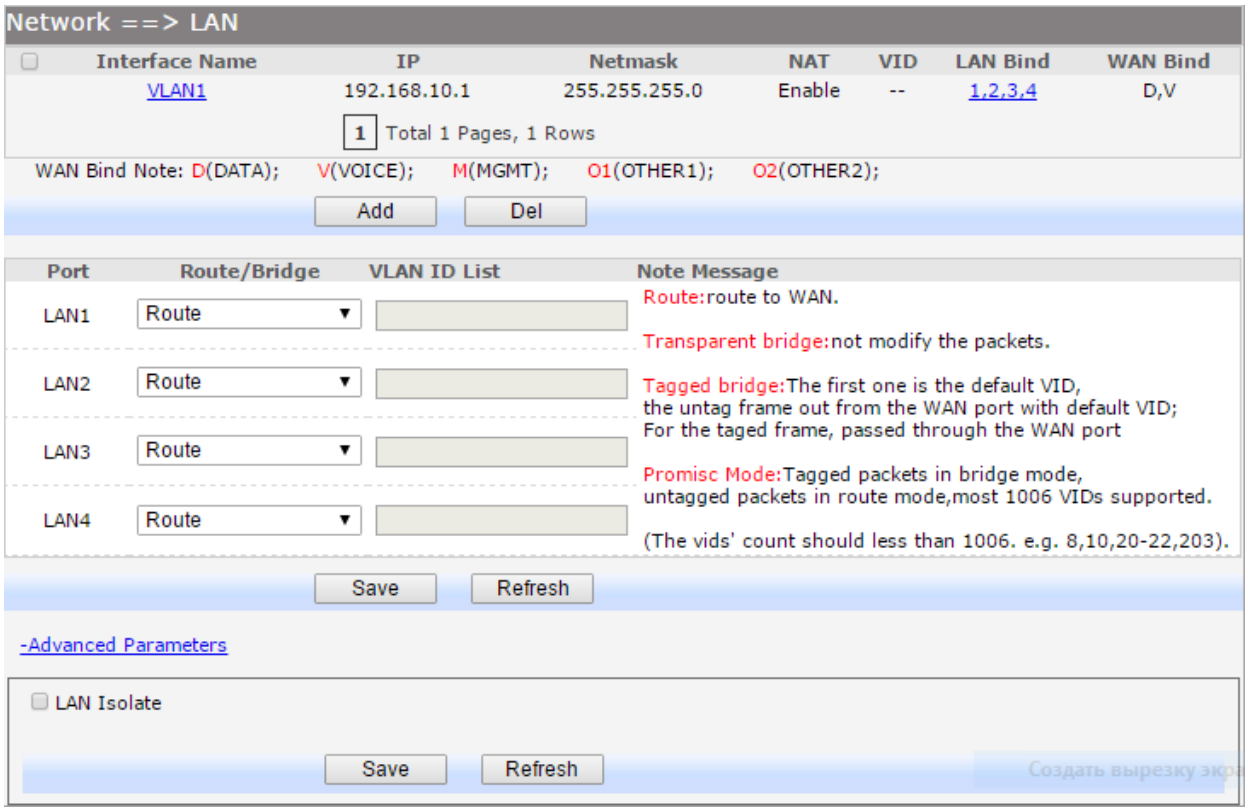


Рисунок 3-12. Меню настройки LAN интерфейсов.

3.3.3 Настройка LAN

Чтобы перейти на страницу конфигурации LAN, выберите в меню пункты Network→LAN. Страница настройки, изображенная на рисунке 2-12, разбита на три части, в зависимости от типа конфигурации.

3.3.3.1 Конфигурация LAN-интерфейса

Для добавления нового интерфейса необходимо нажать кнопку Add. Для удаления интерфейса необходимо его выделить и нажать кнопку Del (интерфейс VLAN1 – интерфейс по умолчанию, его нельзя удалить). Нажмите на имя интерфейса, если вы хотите его настроить. После нажатия на имя интерфейса откроется окно настройки, изображенное на рисунке 2-13.

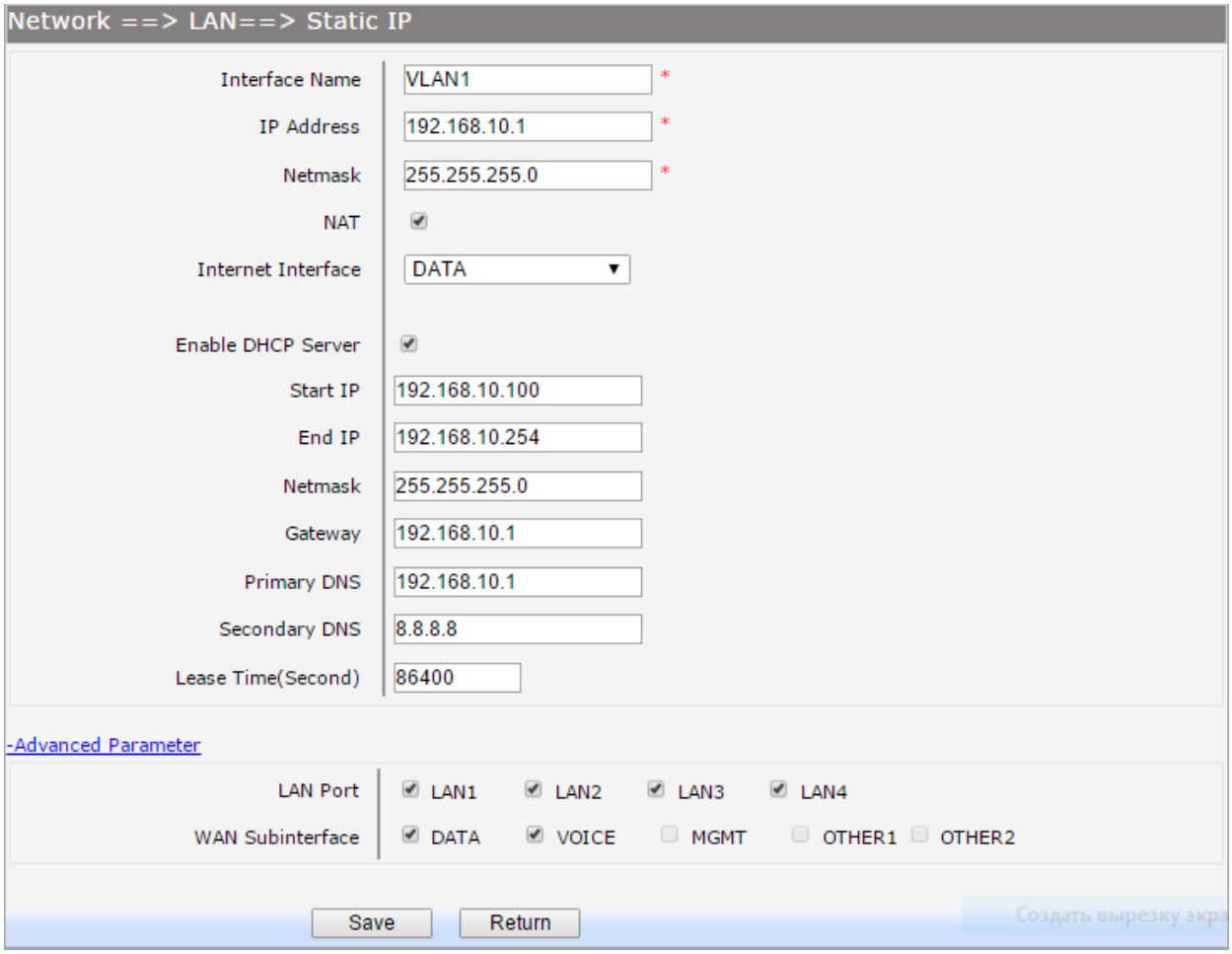


Рисунок 3-13. Настройка интерфейса VLAN1

Пункты для настройки интерфейса представлены ниже:

- Interface Name: имя LAN интерфейса.
- IP Address: введите IP адрес интерфейса.
- Netmask: введите маску подсети для данного интерфейса.
- NAT: необязательная настройка. Включает или отключает механизм преобразования IP адресов NAT.
- Assign NAT IP: необязательная настройка. При использовании настройки, можно назначить адрес для трансляции NAT.

- Enable DHCP Server: необязательная настройка. Включает или отключает DHCP-сервер на интерфейсе.
- Start IP: Настраивается если DHCP-сервер включен. Введите начальный IP-адрес диапазона, из которого DHCP-сервер будет выдавать адреса. IP-адрес должен быть в одной подсети с IP-адресом настраиваемого интерфейса
- End IP: Настраивается если DHCP-сервер включен. Введите последний IP-адрес диапазона, из которого DHCP-сервер будет выдавать адреса. IP-адрес должен быть в одной подсети с IP-адресом настраиваемого интерфейса
- Netmask: Настраивается если DHCP-сервер включен. Введите маску подсети для сети, из которой DHCP-сервер выдает адреса.
- Gateway: Настраивается если DHCP-сервер включен. Введите адрес шлюза, для сети, из которой DHCP-сервер выдает адреса.
- Primary DNS: Настраивается если DHCP-сервер включен. Введите адрес DNS сервера, который будет выдавать DHCP-сервер.
- Secondary DNS: Настраивается если DHCP-сервер включен. Введите адрес вторичного DNS сервера, который будет выдавать DHCP-сервер.
- Lease Time(Second): Настраивается если DHCP-сервер включен. Задается время, на которое DHCP-сервер выдает IP-адрес каждому клиенту. Если клиент не отошлет запроса на продление Lease time, после истечения данного времени IP-адрес будет считаться свободным и может быть назначен другому пользователю.

Дополнительные параметры настройки:

- LAN Port: выберите порты, на которых будет поднят настроенный LAN интерфейс.
- WAN Subinterface: выберите интерфейс WAN, через который трафик из данного LAN интерфейса будет отправляться в WAN сеть.

3.3.3.2 Конфигурация режимов Route/Bridge LAN интерфейса

В средней части меню, представленного на рисунке 2-12, находятся настройки для четырех физических портов: LAN1, LAN2, LAN3, LAN4. Существует несколько режимов работы порта, изменяемых в столбце Route/Bridge:

- Route: трафик маршрутизируется в WAN сеть.
- Transparent bridge: трафик передается без модификации пакетов.
- Tagged bridge: пакеты из LAN сети идут без меток VLAN, пакеты из WAN сети могут пропускаться с меткой VLAN. Поддерживается мост только для одного идентификатора VLAN.
- Promisc Mode: пакеты с метками передаются в режиме моста, пакеты без меток маршрутизируются в WAN сеть. Поддерживается использование пяти VLAN.

Если выбран режим работы Tagged bridge или Promisc Mode в столбце VLAN ID List необходимо будет указать идентификаторы для VLAN.

3.3.3.3 Конфигурация для IPTV

Чтобы перейти на страницу конфигурации дополнительных настроек для IPTV, выберите в меню пункты Network→LAN→Advanced Parameters. Пункты для настройки представлены ниже:

- LAN Isolate: поставьте флажок, чтобы запретить передачу трафика между LAN интерфейсами.
- Auto Bridge: поставьте флажок, чтобы автоматически создавать подключение типа мост для STB- приставок.
- DHCP Vendor ID: задает Vendor ID, используемый в option 60 DHCP.
- IP Address: IP-адрес интерфейса для службы передачи данных STB-приставки.
- Netmask: маска подсети для интерфейса службы передачи данных STB-приставки.
- VID: идентификатор VLAN для IPTV VLAN.
- PRI: уровень приоритета для трафика передаваемого в IPTV VLAN.
- Automatic: поставьте флажок, для автоматического обнаружения идентификатора VLAN, служащего для служебной передачи информации на STB-приставки.

3.3.4 Настройка WLAN

Маршрутизаторы серии QFR-300 поддерживают работу Wi-Fi сети по протоколам 802.11b, 802.11g, 802.11n. Маршрутизатор обеспечивает высокую скорость передачи данных в беспроводной сети между различными мобильными устройствами: ноутбуками, планшетами, телефонами и другими мобильными устройствами.

3.3.4.1 Основные настройки

Чтобы перейти на страницу конфигурации основных настроек беспроводной сети, выберите в меню пункты Network→WLAN→Basic Settings. Откроется страница, изображенная на рисунке 2-14.

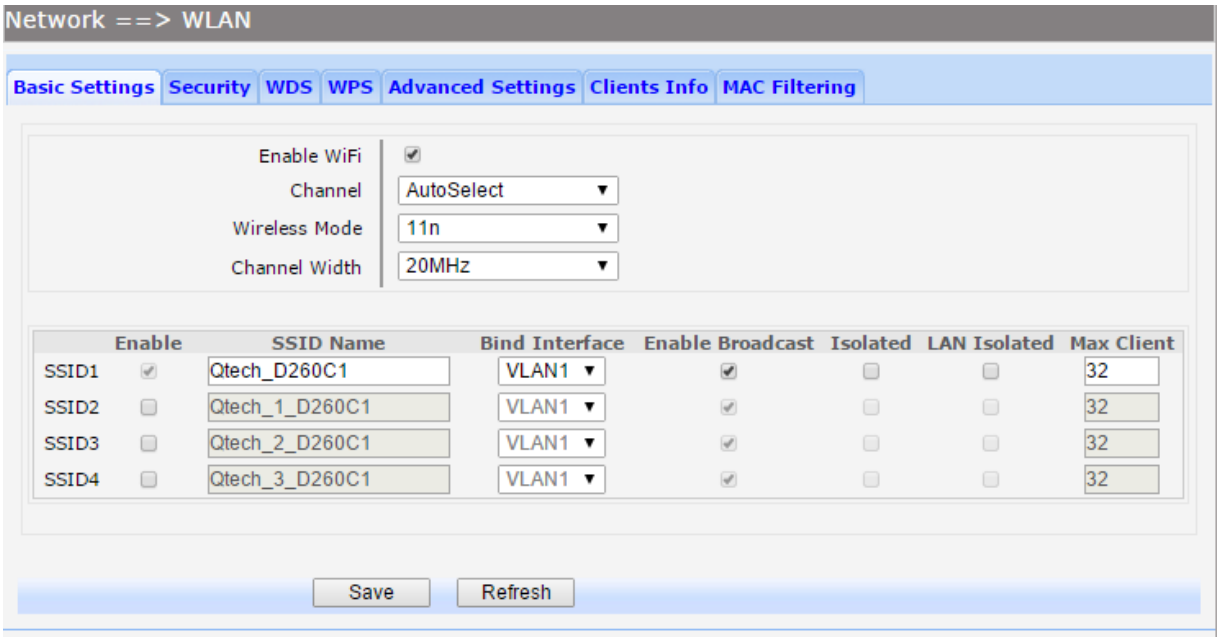


Рисунок 3-14. Конфигурация Wi-Fi. Основные настройки.

Пункты для настройки представлены ниже:

- Enable WiFi: глобальное включение или отключение модуля Wi-Fi на устройстве.
- Channel: поле определяет какой рабочий канал будет использоваться. По умолчанию установлен автоматический выбор канала, при котором Wi-FI модуль выберет лучший канал автоматически. Если вы заметили проблемы в работе Wi-Fi, которые могут быть связаны с помехами от работы Wi-Fi точек, находящихся рядом, можно воспользоваться ручной настройкой канала.
- Wireless Mode: пункт, определяющий режим работы Wi-Fi передатчика:
  - 11b: режим работы для устройств, поддерживающих протокол 802.11b
  - 11g: режим работы для устройств, поддерживающих протокол 802.11g
  - 11n: режим работы для устройств, поддерживающих протокол 802.11n
  - 11b/g: режим работы для устройств, поддерживающих протокол 802.11b или 802.11g
  - 11b/g/n: режим работы для устройств, поддерживающих протокол 802.11b, 802.11g или 802.11n
- Channel Width: позволяет выбрать ширину канала. По умолчанию ширина канала выбирается автоматически в зависимости от клиентов, подключенных к точке доступа.

SSID используется устройствами для идентификации Wi-Fi сети. Маршрутизаторы серии QFR-300 позволяют настраивать до четырех SSID на одном устройстве. В меню,

представленном на рисунке 2-14, представлена таблица со следующими столбцами настройки:

- Enable: поставьте флажок, чтобы включить или выключить SSID. SSID1 отключить нельзя.
- SSID Name: введите имя беспроводной сети. Имя SSID должно быть уникальным среди сетей, находящихся рядом.
- Bind interface: выбор интерфейса LAN с которым будет установлено подключение типа мост.
- Enable Broadcast: Беспроводные клиенты слушают эфир для обнаружения беспроводных сетей. Беспроводные точки доступа, вещая свой SSID в эфир, помогают обнаружить Wi-Fi сеть клиентским устройствам. Поставьте флажок, чтобы устройство транслировало свое имя (SSID) в эфир.
- Isolated: включение или отключение изоляции между клиентами, подключенным к одной беспроводной сети.
- LAN Isolated: включение или отключение изоляции между LAN интерфейсом и SSID.
- Max Client: настройка максимального числа клиентов, которым разрешено подключения к SSID.
- SSID AP Isolated: данная функция позволяет изолировать беспроводные станции сети друг от друга. Беспроводные устройства смогут связывать друг с другом только через маршрутизатор. Для включения функции необходимо поставить флажок, по умолчанию функция отключена.

3.3.4.2 Настройки безопасности Wi-Fi сети

Маршрутизаторы серии QFR-300 поддерживают девять различных режимов безопасности работы Wi-Fi сети, такие как: Open WEP, Shared WEP, WEP Auto, WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK, WPA, WPA2 и WPA/WPA2.

Чтобы перейти на страницу конфигурации режима безопасности беспроводной сети, выберите в меню пункты Network→WLAN→Security. Если вы не хотите использовать настройки безопасности для беспроводной сети, выберите Disabled, но оставлять сесть открытой не рекомендуется по соображениям безопасности.

Для настройки WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK, выберите один из этих типов безопасности сети, после чего загрузится меню, изображенное на рисунке 2-15.

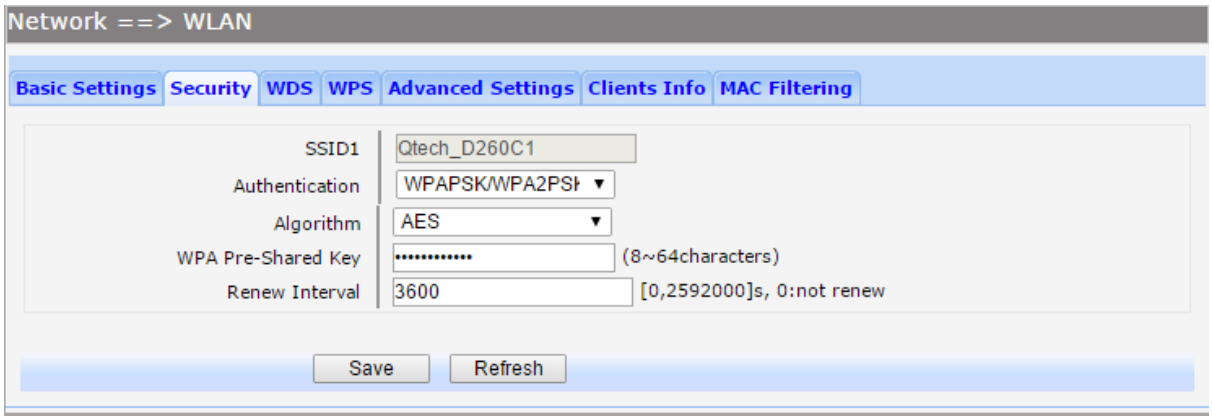


Рисунок 3-15. Настройка безопасности WPAPSK

Пункты для настройки представлены ниже:

- SSID: пункт отображает SSID для которого настраивается настройка безопасности.
- Authentication: настройка метода аутентификации (WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK).
- Algorithm: настройка алгоритма шифрования. При использовании метода аутентификации WPA2-PSK или WPAPSK / WPA2PSK можно выбрать алгоритм шифрования TKIP, AES или TKIP/AES. При использовании метода аутентификации WPA-PSK можно выбрать алгоритм шифрования TKIP или AES.
- WPA Pre-Shared Key: введите ключ безопасности сети длинной от 8 до 64 символов. Данный ключ будет использоваться клиентами при подключении Wi-Fi точке.
- Renew Interval: период обновления ключа, по умолчанию 3600 секунд. Чтобы отключит обновление, необходимо ввести в поле значение 0.

Для настройки Open WEP, Shared WEP, WEP Auto, выберите один из этих типов безопасности сети, после чего загрузится меню, изображенное на рисунке 2-16.

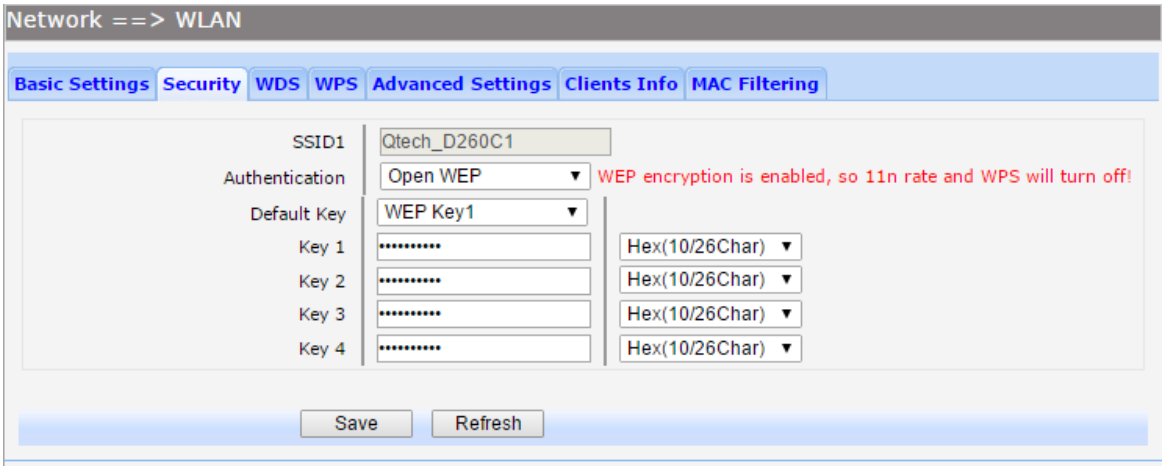


Рисунок 3-16. Настройки безопасности WEP

Пункты для настройки представлены ниже:

- SSID: пункт отображает SSID для которого настраивается настройка безопасности.
- Authentication: выбор метода аутентификации (Open WEP, Shared WEP, WEP Auto)
- Default Key: выберите ключ, который будет использоваться по умолчанию.
- Key: настройка ключа. Можно настроить четыре ключа, но использоваться для авторизации может только один ключ, выбранный пунктом ранее. Формат WEP-ключа не должен превышать более 5 символов ASCII или 10 шестнадцатеричных чисел в 64-битном шифровании, или должен быть ограничен до 13 символов ASCII или 26 шестнадцатеричных чисел в 128-битном шифровании.

Для настройки WPA, WPA2, WPA/WPA2, выберите один из этих типов безопасности сети, после чего загрузится меню, изображенное на рисунке 2-17.

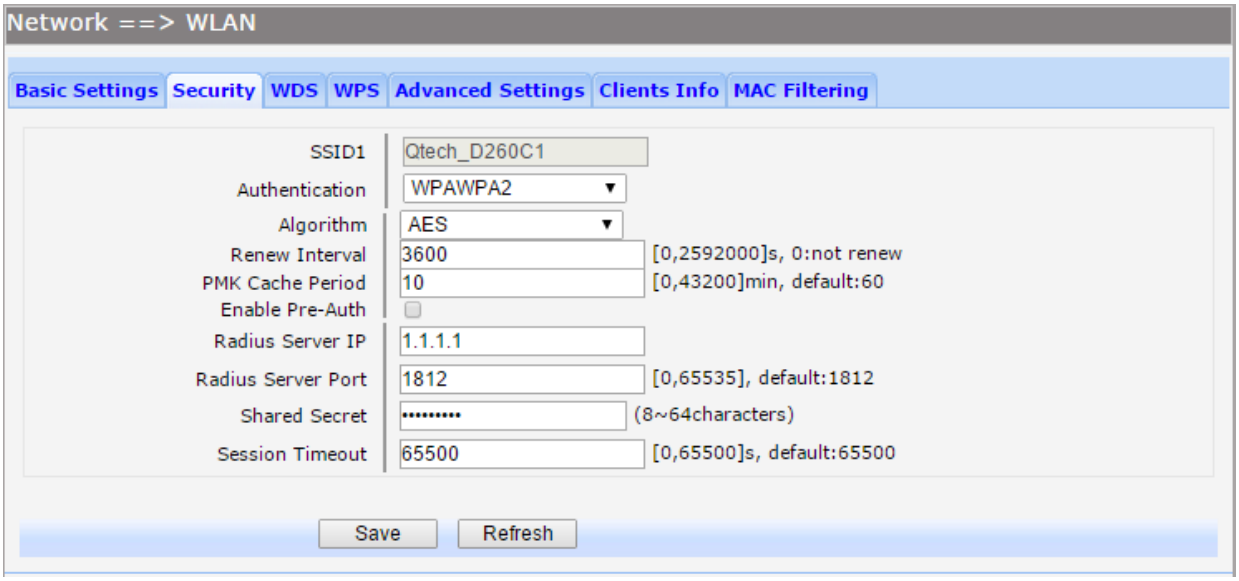


Рисунок 3-17. Настройка безопасности WPA

Пункты для настройки представлены ниже:

- SSID: пункт отображает SSID для которого настраивается настройка безопасности.
- Authentication: настройка метода аутентификации (WPA, WPA2, WPA/WPA2).
- Algorithm: настройка алгоритма шифрования TKIP, AES или TKIP/AES.
- Renew Interval: период обновления ключа, по умолчанию 3600 секунд. Чтобы отключит обновление, необходимо ввести в поле значение 0.
- PMK Cache Period: Установите период хранения WPA2 PMK (парные ключи). PMK Cache управляет списком BSSID и ассоциированными SSID, с которыми устройство идентифицировалось ранее. Этот параметр действителен при выборе метода аутентификации WPA2 или WPA/WPA2.

- Enable Pre-Auth: поставьте флажок для активации передатчика, используемого для идентификации более безопасного и быстрого переключения между точками доступа согласно спецификацией IEEE 802.11i. Этот параметр действителен при выборе метода аутентификации WPA2 или WPA/WPA2. По умолчанию, данный параметр выключен.
- Radius Server IP: введите IP-адрес RADIUS-сервера.
- Radius Server Port: настройка порта, используемого RADIUS-сервером. По умолчанию установлен 1812 в соответствие с требованиями RFC-2138.
- Shared Secret: настройка пароля для RADIUS-сервера.
- Session Timeout: настройка максимальной длительности сеанса (в секундах). Чтобы время длительности не было ограничено введите ноль.

3.3.4.3 WPS

WPS (Wi-Fi Protected Setup) обеспечивает простое соединение беспроводного клиента и беспроводной точки доступа с шифрованием. Это простейший способ создания связи между клиентами беспроводной сети и маршрутизатором. Существует два способа подключения точки доступа и станций с помощью WPS: нажать кнопку конфигурации PBC или используя PIN-код.

Метод подключения с использованием PIN подразумевает, что вы должны знать PIN-код, назначенный в настройках беспроводного клиента.

Метод подключения PBC заключается в нажатии кнопки PBC как на маршрутизаторе (кнопка находится на корпусе устройства), так и на клиенте (обычно виртуальная кнопка в соответствующих настройках), после чего происходит согласование подключения.

Чтобы перейти на страницу конфигурации WPS, выберите в меню пункты Network→WLAN→WPS. Для настройки подключения с использованием PIN-кода, выберите режим PIN, после чего загрузится меню, изображенное на рисунке 2-18

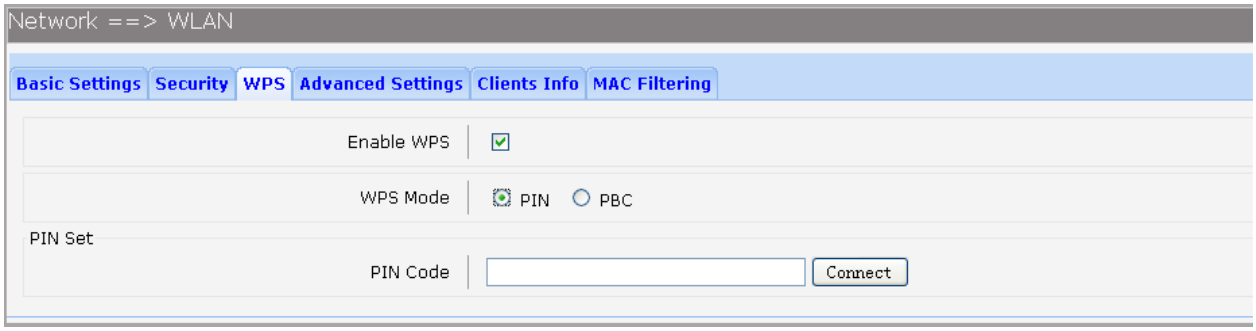


Рисунок 3-18. Настройка Wi-Fi по WPS с использованием PIN-кода

Пункты для настройки представлены ниже:

- Enable WPS: поставленный флажок включает WPS.
- WPS Mode: выбор метода подключения. Выберите режим PIN.

- PIN Code: если выбран режим PIN, введите PIN-код, состоящий из 8 цифр и нажмите кнопку Connect (подключиться).

Для настройки подключения с использованием PBC режима, выберите режим PBC, после чего загрузится меню, изображенное на рисунке 2-19

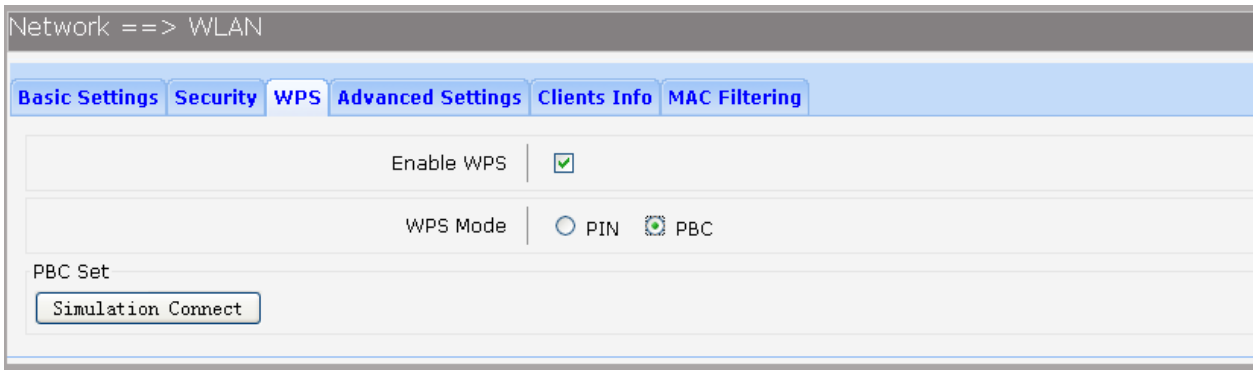


Рисунок 3-19. Настройка Wi-Fi по WPS с использованием PBC

Пункты для настройки представлены ниже:

- Enable WPS: поставленный флажок включает WPS.
- WPS Mode: выбор метода подключения. Выберите режим PBC.
- PBC Set: если выбран режим PBC, нажмите кнопку Simulation Connect.

3.3.4.4 Расширенные настройки

Чтобы перейти на страницу конфигурации расширенных настроек Wi-Fi, выберите в меню пункты Network→WLAN→Advanced Settings.

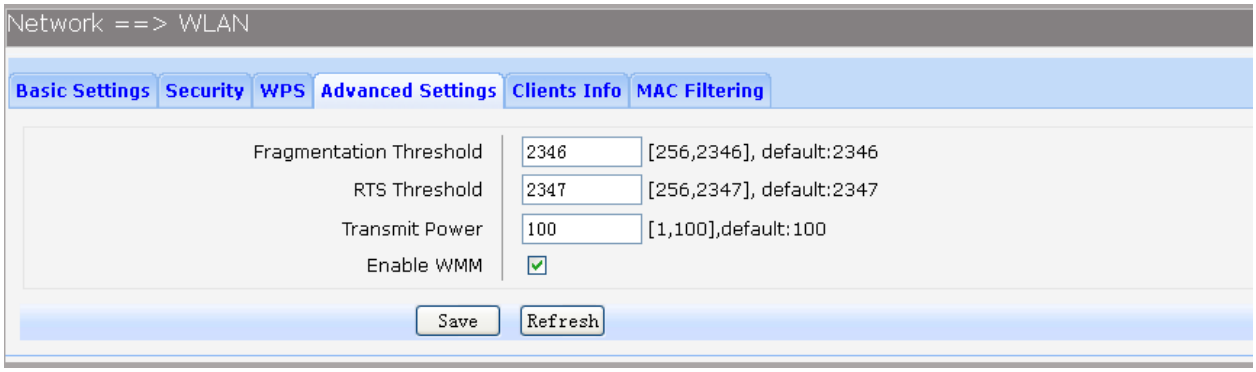


Рисунок 3-20. Расширенные настройки Wi-Fi

Пункты для настройки представлены ниже:

- Fragmentation Threshold: настройка максимального значения не фрагментированного пакета. Значение по умолчанию 2346. Установка низкого уровня порога фрагментации, может привести к снижению производительности сети, из-за чрезмерного роста количества пакетов.

- RTS Threshold: настройка минимального размера пакетов, для которых начнет применяться механизм RTS/CTS. Значение по умолчанию 2347.
- Transmit Power: мощность передатчика в процентах. По умолчанию настроена максимальная мощность.
- Enable WMM: включение или отключение механизма WMM. Этот механизм обеспечивает сетевым пакетам мультимедийных приложений приоритет над сетевыми пакетами данных, позволяя мультимедиа-приложениям работать устойчивее и с меньшим количеством ошибок.

3.3.4.5 Информация о клиентах

Чтобы перейти на страницу просмотра подключенных к Wi-Fi сети клиентов выберите в меню пункты Network→WLAN→Clients Info.

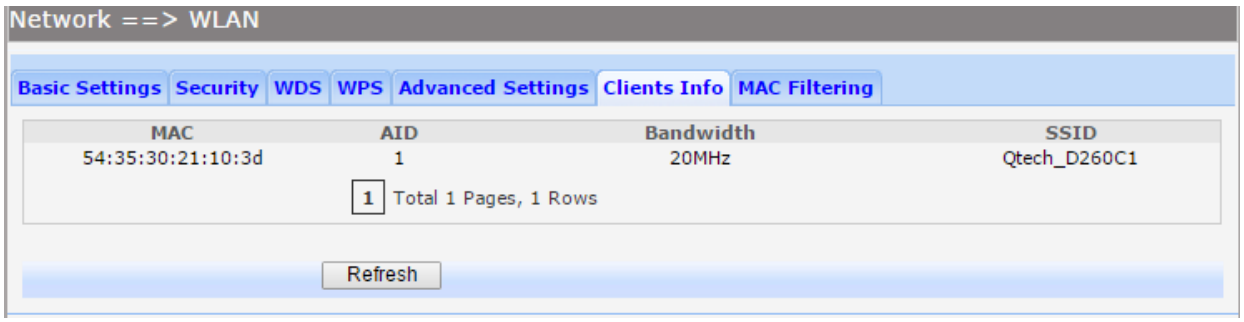


Рисунок 3-21. Просмотр информации о подключенных Wi-Fi клиентах

На странице отображаются все подключенные к маршрутизатору Wi-Fi клиенты и информация о них. Поля представленной на странице информации описаны ниже:

- MAC: MAC-адрес подключенного клиента
- AID: представляет собой 16-битовый идентификатор клиента, назначенный маршрутизатором на время соединения с клиентом.
- Bandwidth: полоса пропускания на которой установлено соединение с клиентом.
- SSID: SSID к которой подключен клиент.

3.3.4.6 Фильтрация по MAC-адресам

Доступ к Wi-Fi сети на маршрутизаторах серии QSW-300 можно контролировать, используя фильтрацию по MAC-адресам. Для настройки фильтрации выберете в меню пункты Network→WLAN→MAC Filtering.

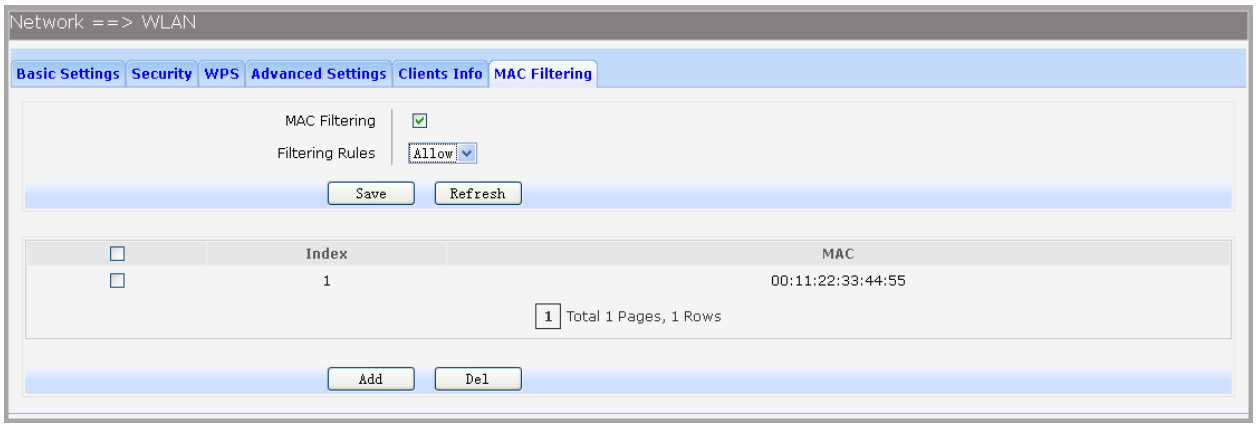


Рисунок 3-22. Просмотр фильтрации по MAC-адресам для Wi-FI сети

Пункты для настройки представлены ниже:

- MAC Filtering: глобальное включение или отключение механизма фильтрации по MAC-адресам для Wi-Fi сети.
- Filtering Rules: возможны два правила фильтрации:
  - Allow: разрешает доступ к маршрутизатору клиентам, чьи MAC-адреса описаны в списке доступа.
  - Permit: запрещает доступ к маршрутизатору клиентам, чьи MAC-адреса описаны в списке доступа.

Чтобы удалить запись о MAC-адресе выберите соответствующую запись и нажмите кнопку Del. Чтобы добавить запись в таблицу, нажмите кнопку Add, после чего откроется меню, изображенное на рисунке 2-23.

MAC-адрес, который необходимо добавить в таблицу фильтрации, необходимо ввести в поле MAC в формате XX:XX:XX:XX:XX, где XX шестнадцатеричная цифра, после чего нажмите кнопку Add. Для удаления выбранного MAC-адреса, выберите соответствующую запись и нажмите кнопку Del.

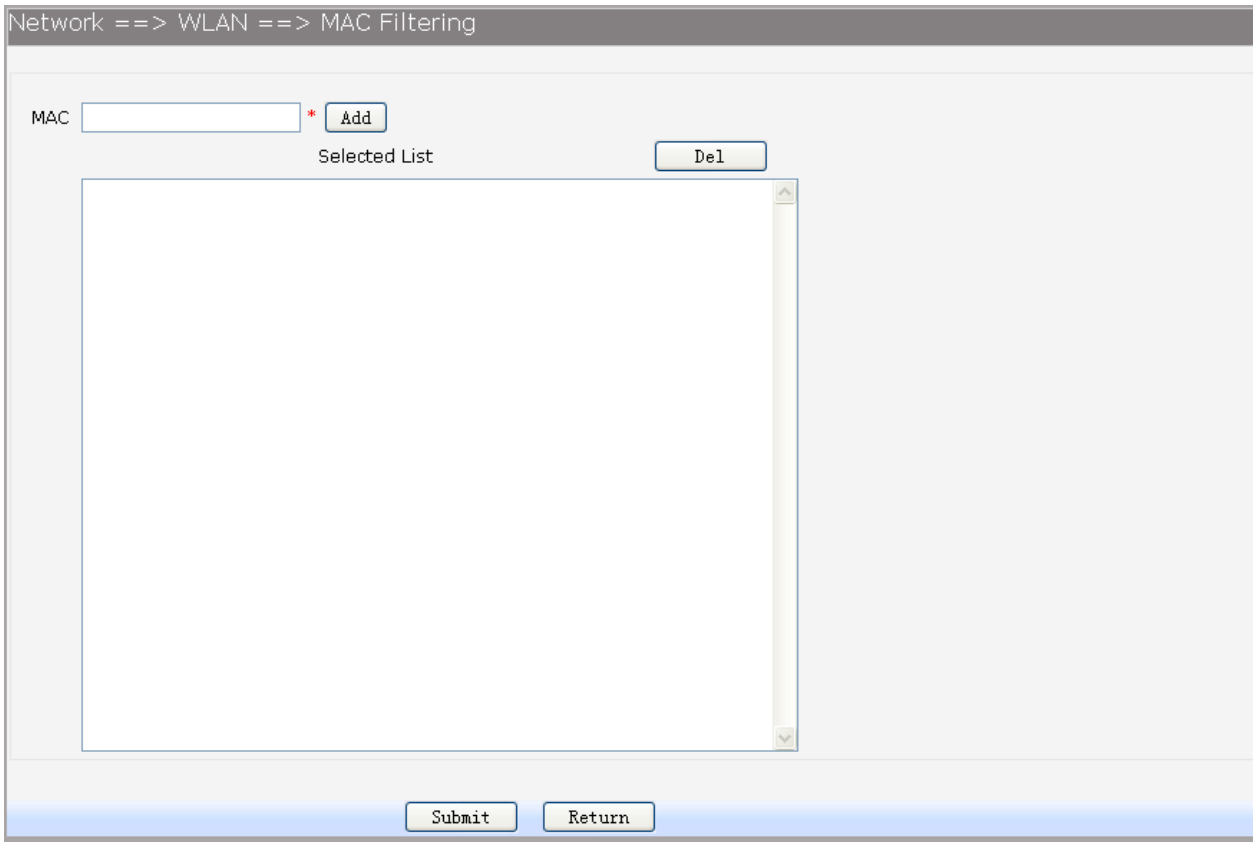


Рисунок 3-23. Добавление MAC-адреса Wi-Fi клиента в таблицу фильтрации

3.3.5 Настройка 3G

Маршрутизаторы серии QSW-300 позволяют подключать 3G модем, используя модем для доступа в глобальную сеть. Чаще всего данный тип подключения используется в качестве резервного канала.

При установке 3G модема в USB-порт устройства, система распознает SIM-карту и совершает авторизацию в сети. После успешной авторизации 3G модем будет служить резервным каналом для доступа в глобальную сеть.

3.3.5.1 Основные настройки 3G модема

Для просмотра настроек и конфигурирования 3G модема, выберите в меню пункты Network→3G Modem. Откроется меню основных настроек, изображенное на рисунке 2-24

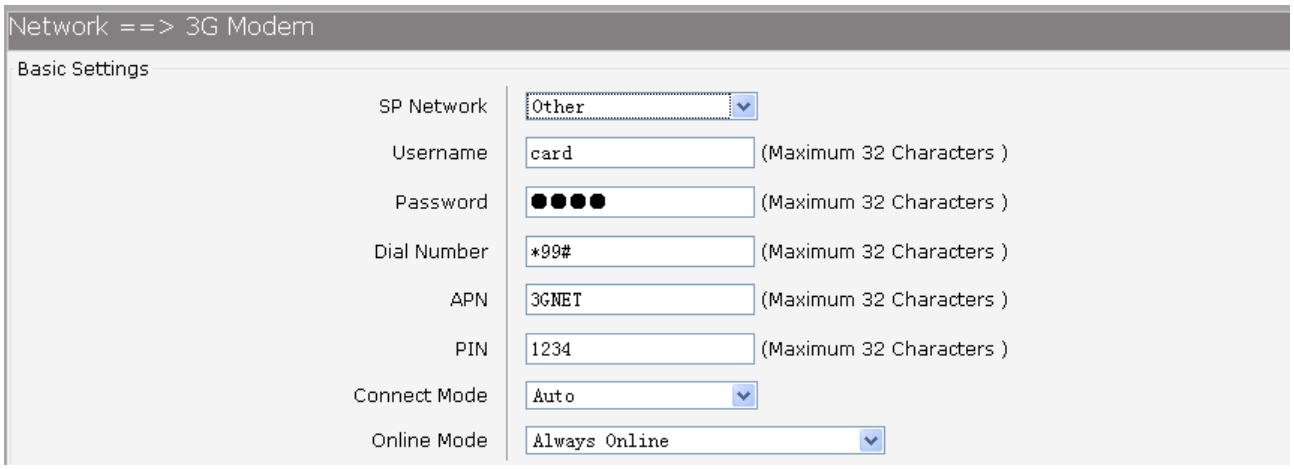


Рисунок 3-24. Основные настройки 3G

Пункты для настройки 3G модема, представлены ниже:

- SP Network: выбор сотового оператора. Если вашего оператора нет в списке, выберите Other.
- Connect Mode: настройка режима подключения (ручной или автоматический).
- Online Mode: настройка режима соединения. Всегда на связи или выход после простоя. Настройка по умолчанию «всегда на связи».

Если выбран пункт Other, при выборе сотового оператора, появятся дополнительные пункты настройки:

- Username: настройка имени пользователя для 3G подключения.
- Password: настройка пароля для 3G подключения.
- Dial Number: настройка номера дозвона.
- APN: настройка APN.
- PIN: некоторые 3G соединения требуют настройки PIN-кода. Уточните информацию у оператора. Если настройка не требуете, оставьте поле пустым.

3.3.5.2 Дополнительные настройки 3G модема

Для настройки дополнительных параметров работы 3G модема, выберите в меню пункты Network→3G Modem→Advanced. Откроется страница, изображенная на рисунке 2-25

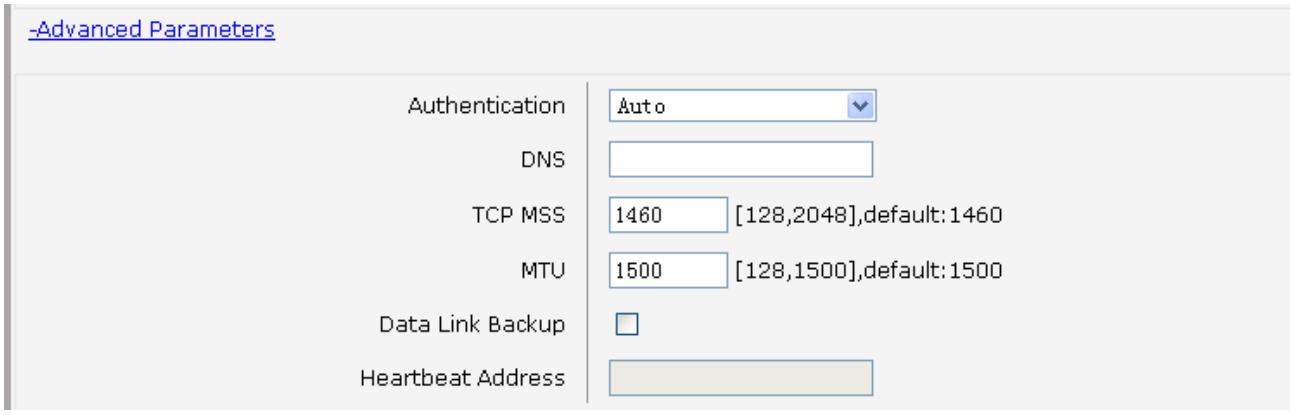


Рисунок 3-25. Дополнительные параметры настройки 3G

Пункты для настройки, представлены ниже:

- Authentication: настройка режима аутентификации (CHAP, PAP, Auto). По умолчанию настроен режим Auto.
- DNS: настройка адреса DNS-серверов. По умолчанию адреса DNS-серверов получаются автоматически.
- TCP MSS: настройка максимального размера пакета TCP-соединения. Рекомендуется оставить значение по умолчанию.
- MTU: настройка MTU. Рекомендуется оставить значение по умолчанию.
- Data Link Backup: если поставлен флажок, то в случае разрыва соединения на WAN-интерфейсе устройства, маршрутизация автоматически переключится на резервный канал, работающий через 3G модем.
- Heartbeat Address: настройка адреса для проверки соединения. При настройках модема 3G по умолчанию, данная настройка не требуется.

3.3.5.3 Состояние работы 3G модема

Для просмотра состояния работы 3G модема, выберите в меню пункты Network→3G Modem→Status. Откроется страница, изображенная на рисунке 2-26.

Рисунок 3-26. Состояние работы 3G

Состояния работы 3G модема описаны ниже:

- Device Status: состояние устройства
- SIM Card Status: указывает состояние SIM-карты.
- Product Name: модель 3G модема.
- Manufacturer Name: производитель 3G модема.
- SP Name: имя сотового оператора.
- Signal Quality: качество сигнала на 3G модеме.
- Connection Status: состояние подключения.

3.3.6 Настройка портов

3.3.6.1 Зеркалирование порта

Зеркалирование порта – технология, позволяющая дублировать пакеты с одного или нескольких портов (порт источника), на другой порт (порт назначения). Как правило, зеркалирование используется для диагностики и анализа пакетов, а также мониторинга и устранения неполадок на сети.

Для настроек зеркалирования выберете в меню пункты Network→Port Management→Port Mirror.

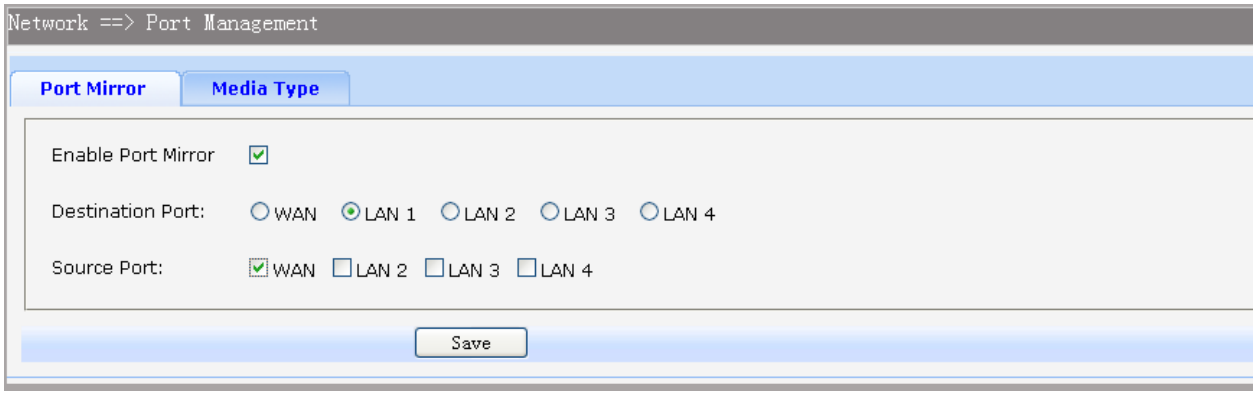


Рисунок 3-27. Настройка зеркалирования портов

Пункты для настройки представлены ниже:

- Enable Port Mirror: включает или выключает механизм зеркалирования.
- Destination Port: порт, на который будут поступать копии пакетов с порта источника.
- Source Port: все пакеты, приходящие на данный порт, будут дублированы и направлены в порт назначения.

3.3.6.2 Настройка скорости работы порта

Для настроек скорости работы пора выберите в меню пункты Network→Port Management→Media Type, откроется меню, изображенное на рисунке 2-28.

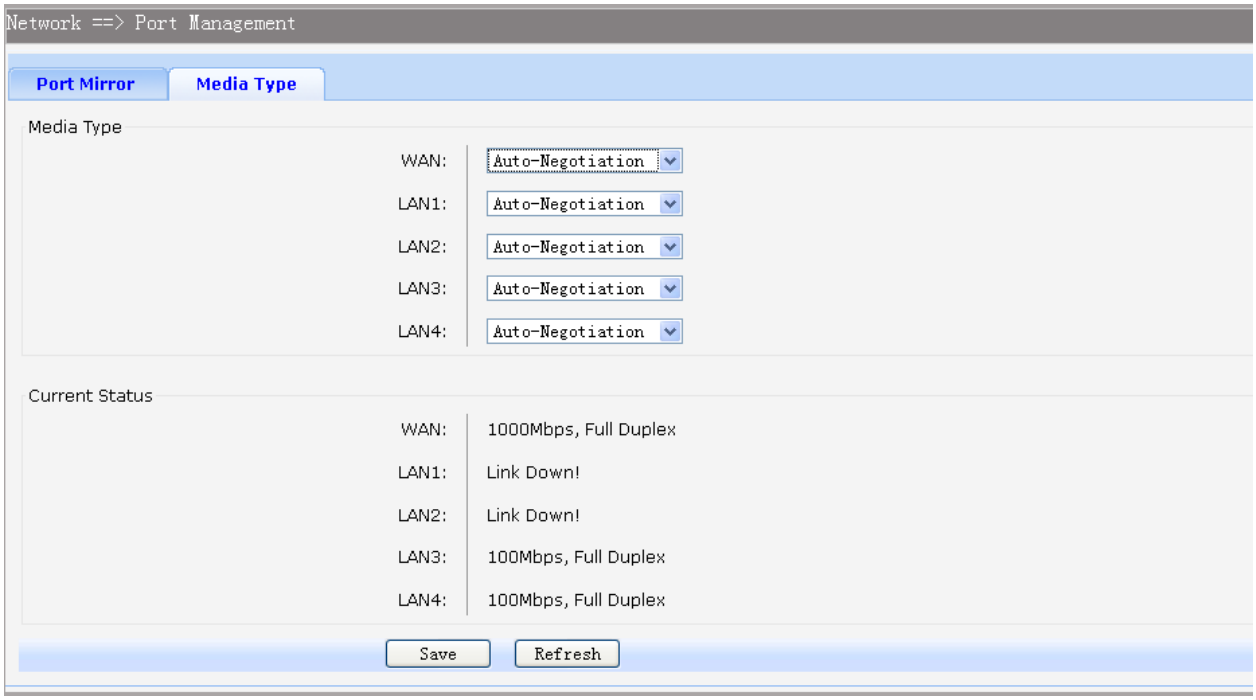


Рисунок 3-28. Настройка скорости порта

Пункты для настройки представлены ниже:

- Media Type: для всех физических портов есть возможность настроить шесть режимов работы: 10 Мбит/с полудуплекс. 10Мбит/с полный дуплекс, 100Мбит/с полудуплекс, 100Мбит/с полный дуплекс, 1000Мбит/с полный дуплекс, авто-согласование (Auto-Negotiation).
- Currect Status: представлена информация по статусу работы всех портов

3.3.6.3 Настройка IPv6

Маршрутизаторы серии QSW-300 поддерживают работу IPv6 протокола. Для настройки IPv6 выберите в меню пункты Network→IPv6, откроется меню, изображенное на рисунке 2-26.

Пункты для настройки WAN интерфейса представлены ниже:

- Enable WAN: если в пункте IP Stack Version выбран пункт IPv4/v6 или IPv6, поставьте флажок для включения протокола IPv6 на WAN интерфейсе.
- Access Mode: выберите режим работы WAN интерфейса: IP или PPP.
- Link-Local Address: настройка локального адреса (Auto или Manual). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.

- Global Unicast Address: настройка глобального адреса (Stateless, Manual или DHCPv6). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.
- Default Gateway Address: настройка адреса шлюза (Stateless или Manual или DHCPv6). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.
- DNS: настройка адреса DNS-сервера (Stateless, Manual или DHCPv6). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.
- Enable DHCP-PD: включение делегирования префикса на WAN интерфейсе.

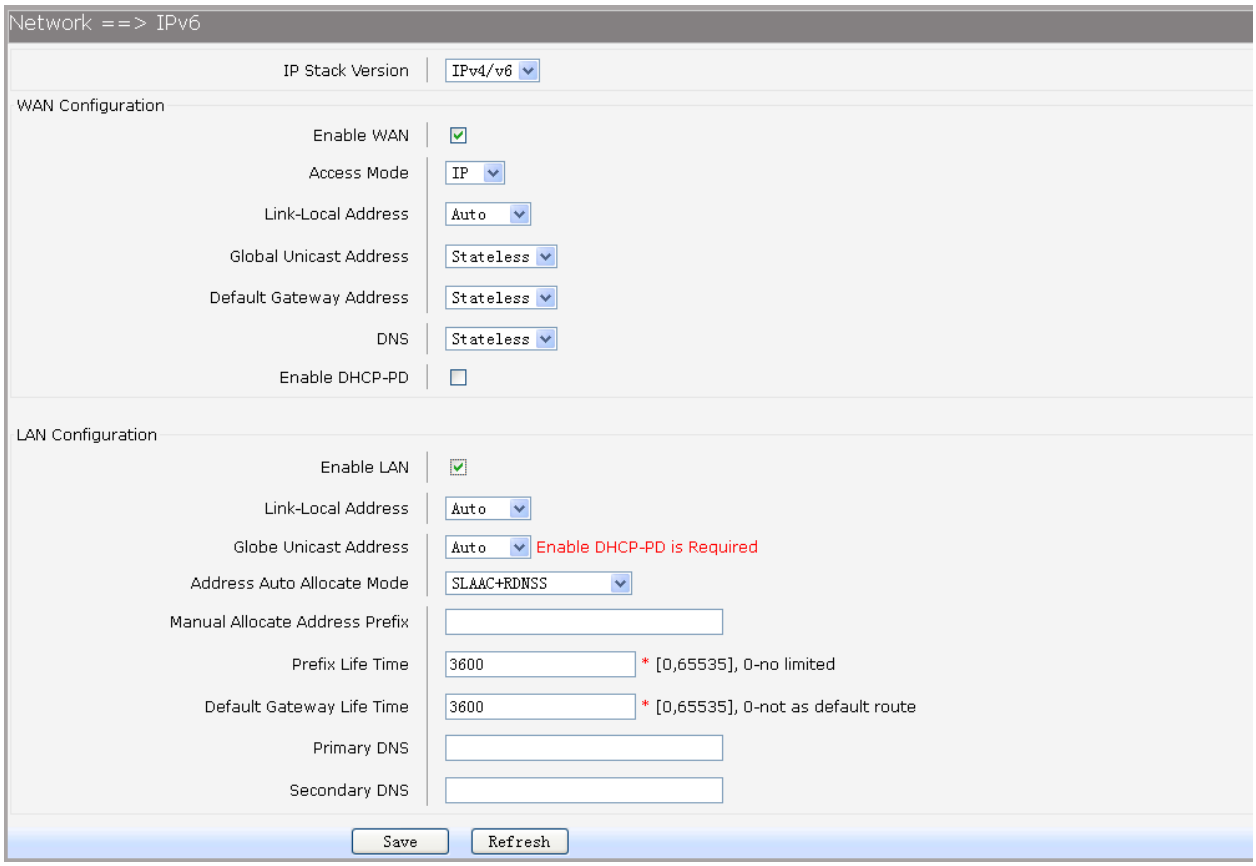


Рисунок 3-29. Настройка IPv6

Пункты для настройки LAN интерфейса представлены ниже:

- Enable LAN: если в пункте IP Stack Version выбран пункт IPv4/v6 или IPv6, поставьте флажок для включения протокола IPv6 на LAN интерфейсе.
- Link-Local Address: настройка локального адреса (Auto или Manual). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.

- Global Unicast Address: настройка глобального адреса (Manual или Auto). Если выбрана ручная настройка (Manual) адреса, его необходимо будет ввести вручную.
- Address Auto Allocate Mode: настройка режима назначения адреса (SLAAC+RDNSS, SLAAC+DHCPv6, DHCPv6).
- Manual Allocate Address Prefix: ручное задание адреса префикса.
- Prefix Life Time: время жизни выдачи префикса, по умолчанию 3600.
- Default Gateway Life time: время жизни адреса шлюза, по умолчанию 3600.
- Primary DNS: введите адрес DNS сервера.
- Secondary введите адрес вторичного DNS-сервера.

3.4 Настройка сервисов

3.4.1 Просмотр состояния сервисов

Вся информация в меню, показывающем текущие состояния сервисов, носит информативный характер и не подлежит редактированию.

3.4.1.1 Информация о работающих сервисах

На странице состояния сервисов показаны все сервисы маршрутизатора и их статус. Для просмотра их состояния, выберите в меню пункты Data Service→Status→Service State.

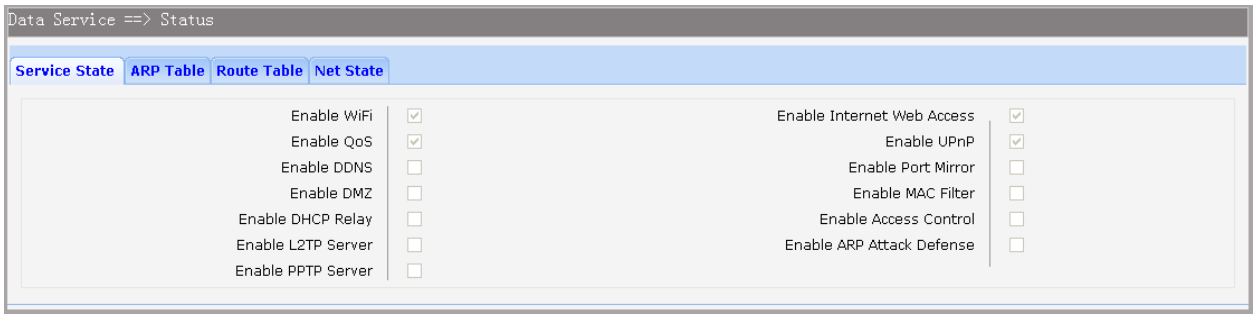


Рисунок 3-30. Информация о работающих сервисах устройства

3.4.1.2 ARP-таблица

Для просмотра ARP-таблицы устройства, выберите в меню пункты Data Service→Status→ARP. Таблица откроется в меню, изображенном на рисунке 2-31.

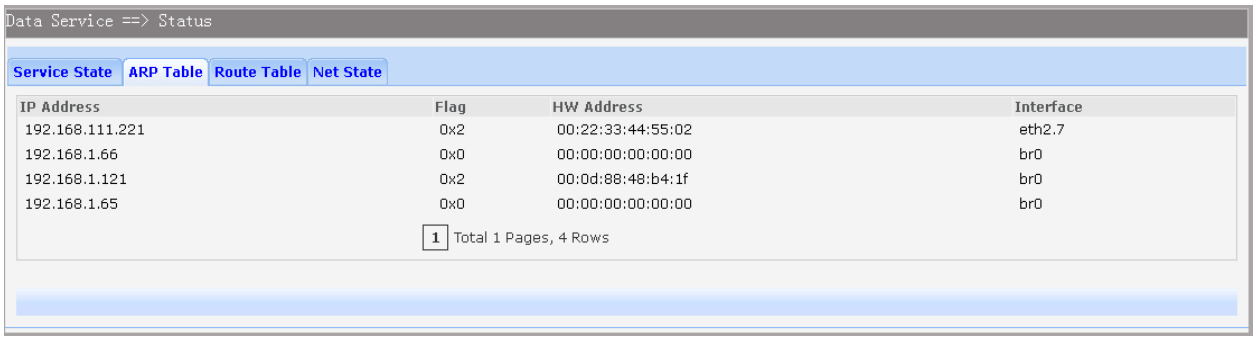


Рисунок 3-31. ARP-таблица

3.4.1.3 Таблица маршрутизации

Для просмотра таблица маршрутизации устройства, выберите в меню пункты Data Service→Status→Route Table. Таблица маршрутизации откроется в меню, изображенном на рисунке 2-32.

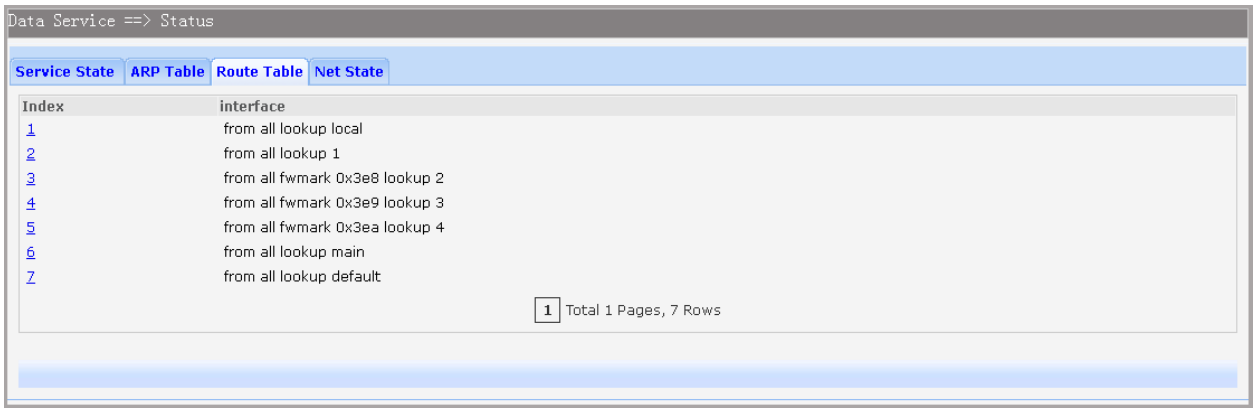


Рисунок 3-32. Таблица маршрутизации

3.4.1.4 Активные соединения

Для просмотра активных соединений устройства, выберите в меню пункты Data Service→Status→Net State. Таблица установленных соединений откроется в меню, изображенном на рисунке 2-33.

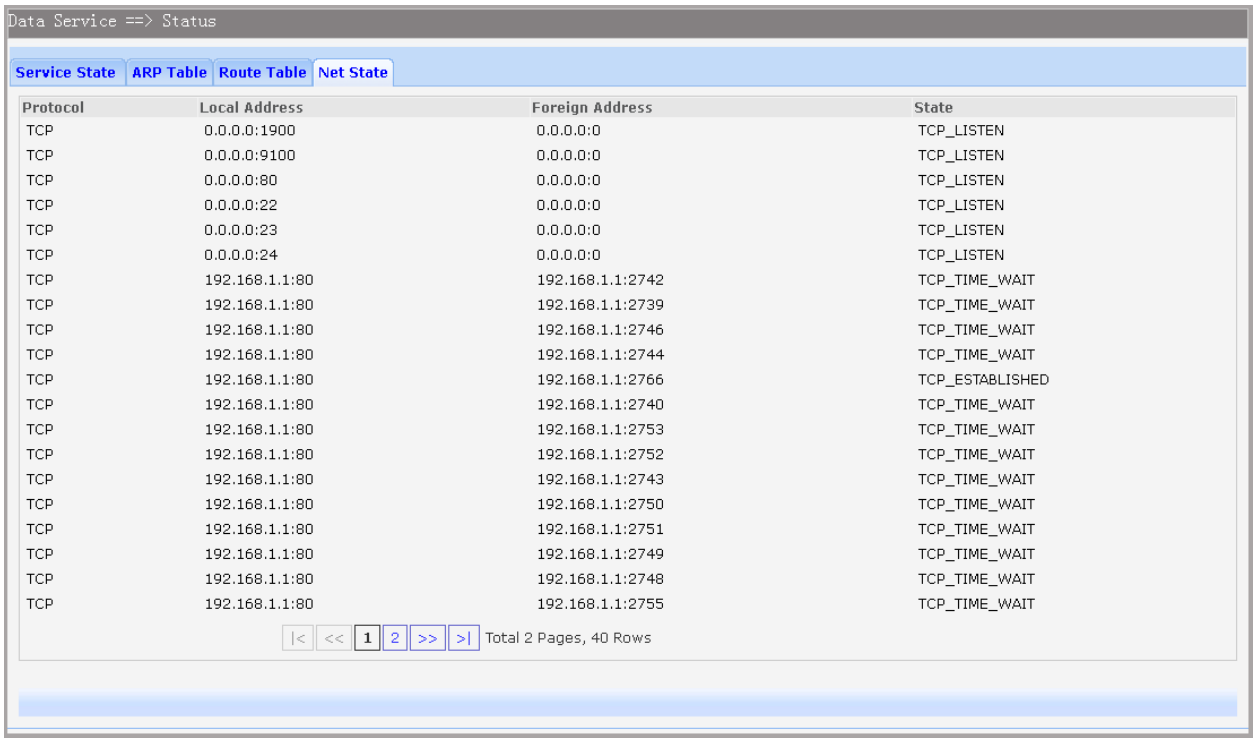


Рисунок 3-33. Активные соединения

3.4.1 Настройка DHCP-сервера

3.4.1.1 Static Address Assign

Может возникнуть необходимость получения клиентом постоянного IP-адреса от DHCP-сервера, который не будет меняться и выдаваться другим устройствам. Для настройки выдачи клиентам определенного IP-адреса, выберите в меню пункты Data Service→DHCP Server→Static Address Assign, откроется меню, изображённое на рисунке 2-34. В открывшимся меню можно посмотреть IP-адреса, назначенные конкретным клиентам, а также добавить новые записи.

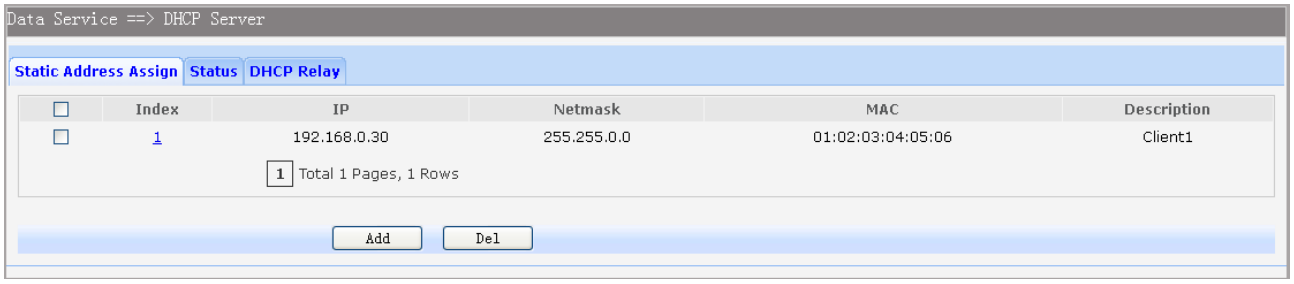


Рисунок 3-34. Просмотр статический записей DHCP-сервера

Для редактирование созданной записи необходимо нажать на номер индекса записи, после чего откроется окно редактирования. Для удаления поставьте флажок напротив соответствующей записи и нажмите кнопку Del. Для добавления новой привязки нажмите кнопку Add, откроется меню добавления новой записи, изображённое на рисунке 2-35.

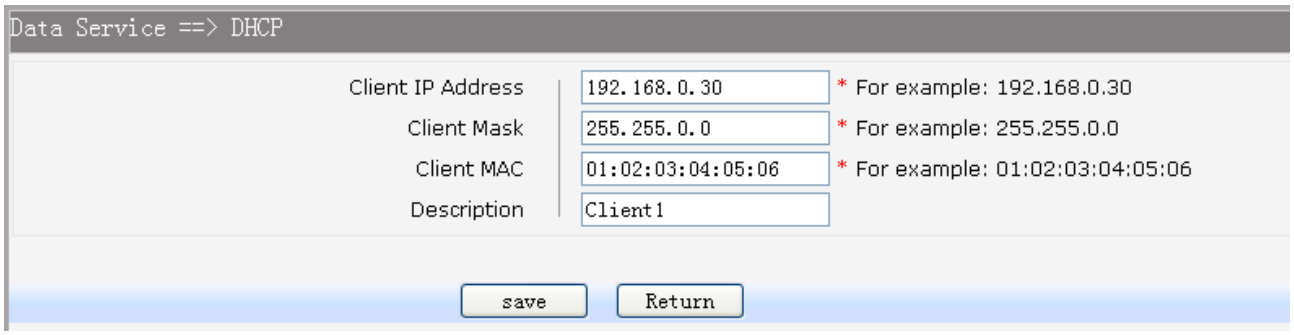


Рисунок 3-35. Меню добавление статической записи

Пункты для настройки представлены ниже:

- Client IP Addres: настройка IP-адреса, зарезервированного для клиента.
- Client Mask: настройка маски подсети.
- Client MAC: настройка MAC-адреса устройства, для которого настраиваете выдачу постоянного IP-адреса.
- Description: описание для настроенной записи привязки.

3.4.1.2 Состояние DHCP-сервера

Для просмотра состояния работы DHCP-сервера, выберите пункты в меню пункты Data Service→DHCP Server→Status, откроется меню с информацией о подключенных клиентах и назначенных адресах.

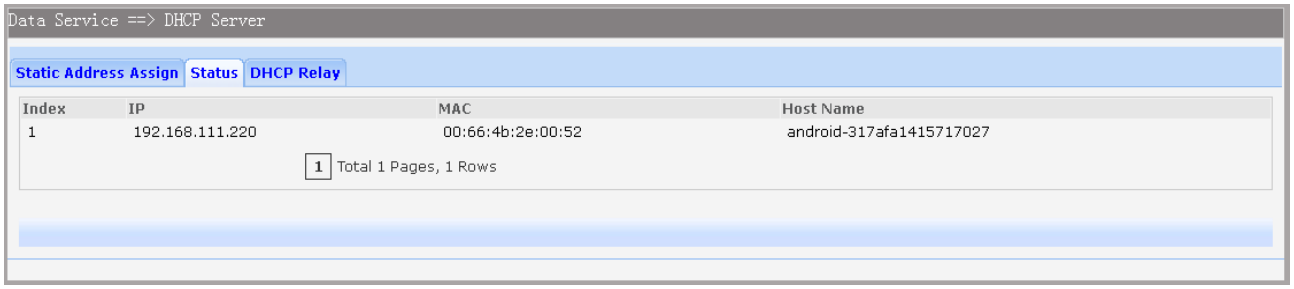


Рисунок 3-36 Таблица DHCP клиентов

3.4.1.3 Механизм DHCP relay

Механизм DHCP relay настраивается на устройстве, называемом DHCP relay агентом. Агент перенаправляет пакеты DHCP между клиентом и сервером, при это клиент и сервер могут находиться в разных подсетях. В отличии пересылки DHCP пакетов при маршрутизации, которая осуществляется прозрачно. Агент, получив DHCP пакет от клиента, генерирует новый DHCP пакет и отправляет его через другой интерфейс серверу. Таким образом, агент слушает запросы клиента и изменяет их, добавляя важную информацию, используемую DHCP-сервером для назначения клиенту выделенного IP-адреса. Когда от DHCP-сервера приходит ответ, агент перенаправляет ответ клиенту. Механизм работы DHCP-relay агента, показана на рисунке 2-37.

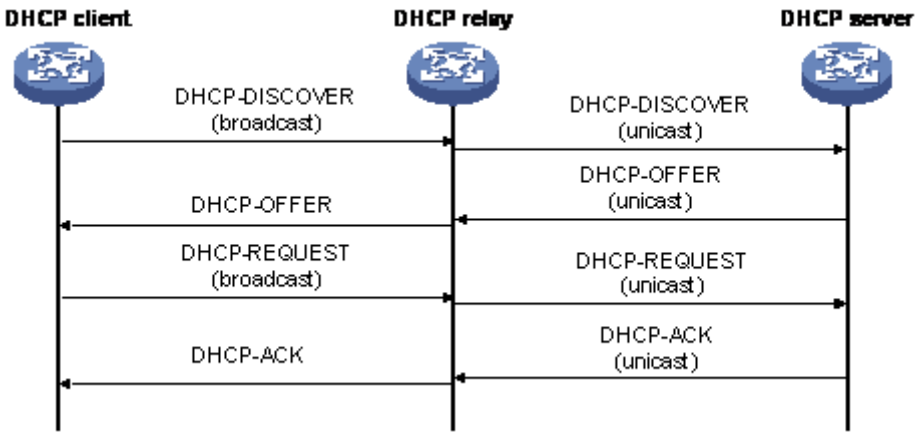


Рисунок 3-37. Механизм работы DHCP relay

Для настройки устройства в качестве агента, выберите пункты меню Data Service→DHCP Server→DHCP Relay.

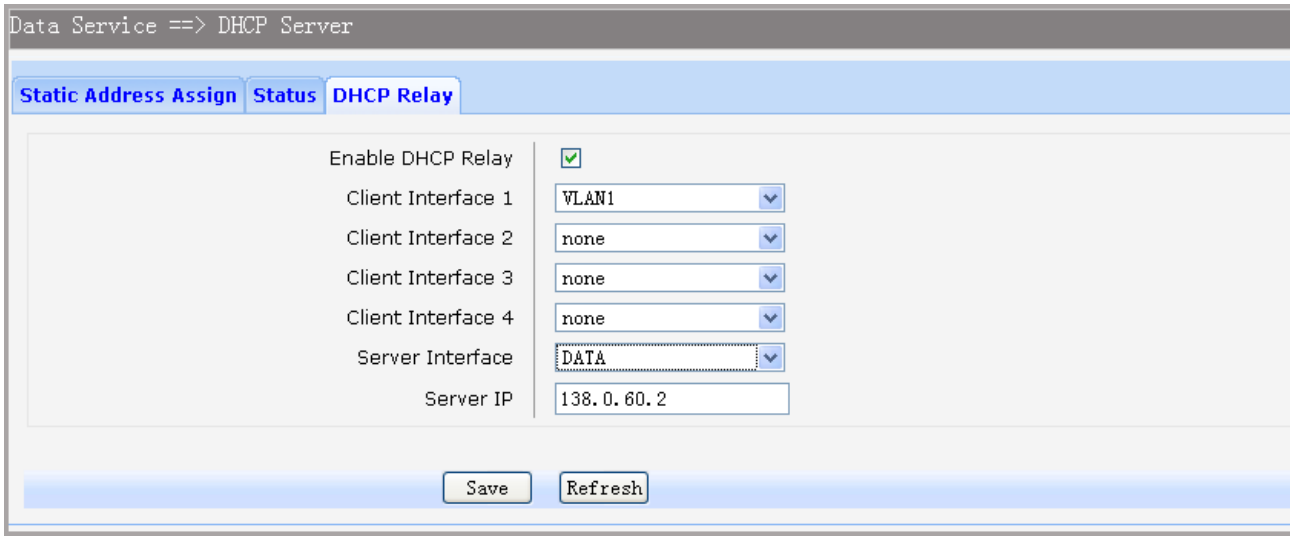


Рисунок 3-38.Настройка DHCP relay

Пункты для настройки представлены ниже:

- Enable DHCP Relay: включение или отключение механизма DHCP relay.
- Client Interface: настройка интерфейсов, которые будут прослушиваться на предмет получения DHCP запросов. Может быть настроено до четырех интерфейсов.
- Server Interface: настройка интерфейса, через который доступен DHCP-сервер.
- Server IP: настройка IP-адреса DHCP сервера.

3.4.2 Настройка NAT

Network Address Translation (NAT) механизм, позволяющий предоставлять множеству устройств доступ в глобальную сеть с одним публичным адресом, позволяя таким образом экономить пространство IPv4 адресов. При прохождении пакета через маршрутизатор механизм NAT меняет информацию о адресе отправителя в IP-пакете, заменяя локальный IP-адрес устройства на публичный.

3.4.2.1 Основные настройки NAT

Для настройки механизма NAT на устройстве, выберите в меню пункты Data Service→NAT Config→Basic Settings.

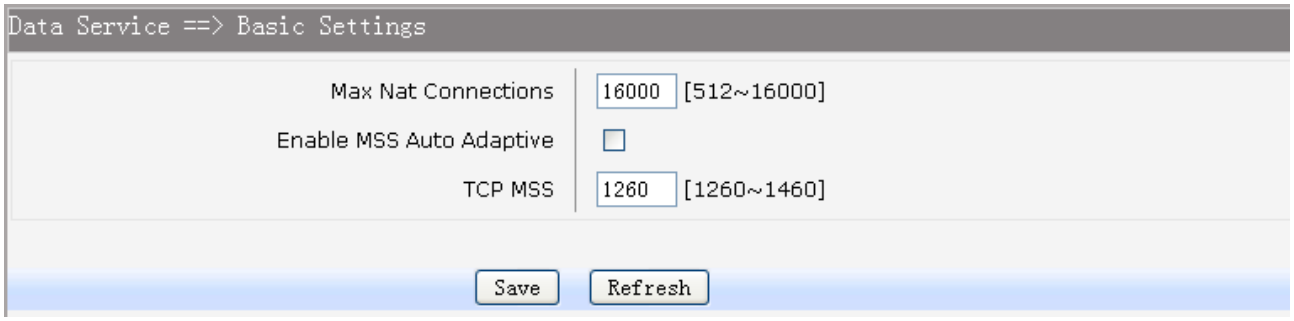


Рисунок 3-39 Настройка NAT

Пункты для настройки представлены ниже:

- Max Nat Connections: определяет максимальное число NAT трансляций.
- Enable MSS Auto Adaptive: включает или выключает автоматическое определение максимального размера сегмента.
- TCP MSS: Если не включено автоматическое определение максимального размера сегмента, данный пункт позволяет настроить его значение вручную.

3.4.2.2 Настройка PAT

Механизм преобразования адресов позволяет заменять один локальный адрес на один публичный, таким образом расходуется большое количество публичных IPv4 адресов, для решения этой проблемы был разработан механизм PAT (Port address translation). PAT позволяет преобразовать несколько локальных IP-адресов в один публичный. Для того, чтобы различать трансляции с разных локальных IP-адресов в один публичный, PAT использует уникальные номера портов для каждого транслируемого соединения, заменяя в отправляемом пакете как IP-адрес источника, так и номер порта. Для настройки механизма PAT, выберите в меню пункты Data Service→NAT Config→PAT Settings.

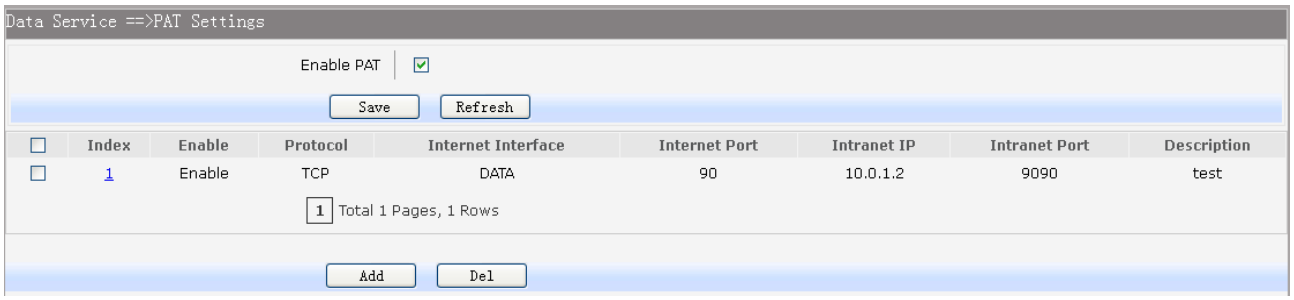


Рисунок 3-40. Просмотр настроек PAT

Пункт Enable PAT включает или отключает работу механизма PAT. Если необходимо поменять настройки созданной трансляции нажмите на ее индекс. Для удаления записи трансляции, поставьте флажок напротив удаляемых записей и нажмите кнопку Del. Для добавления новой записи, нажмите кнопку Add, после нажатия кнопки откроется окно, изображённое на рисунке 2-41.

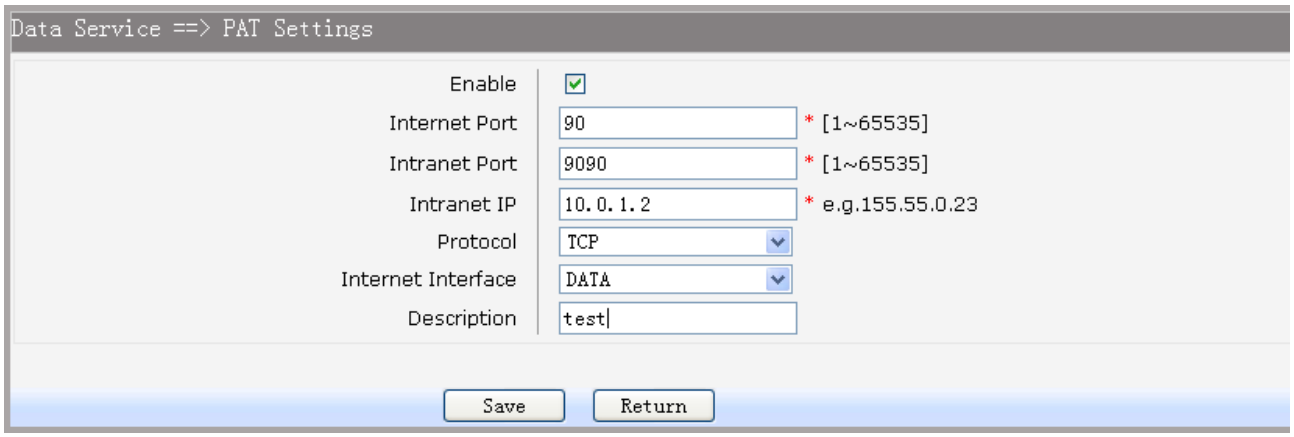


Рисунок 3-41. Добавление или изменение статической PAT записи

Пункты для настройки представлены ниже:

- Enable: включение или отключение настраиваемой PAT-трансляции.
- Internet Port: настройка порта, используемый для предоставления услуг доступа из внешней сети. Все запросы из интернета к этому порту, будут переадресованы на внутренний порт.
- Intranet Port: настройка внутреннего порта, используемого сервисом для доступа из локальной сети.
- Intranet IP: настройка локального IP-адреса, запросы на который будут переадресовываться из внешней сети.
- Protocol: настройка используемого протокола транспортного уровня (TCP или UDP).
- Internet Interface: настройка интерфейса, используемого для получения запросов из внешней сети.

- Description: настройка описания записи созданной PAT-трансляции.

3.4.2.3 Настройка DMZ

DMZ (демилитаризованная зона) представляет собой логический сегмент сети, в котором содержатся общедоступные сервисы, отделяемые в целях безопасности от остальных устройств локальной сети. Целю DMZ является добавление дополнительного уровня безопасности в локальной сети, позволяющего минимизировать ущерб в случае атаки на один из общедоступных сервисов. Злоумышленник из глобальной сети будет имеет прямой доступ только к оборудованию в DMZ. Для настройки DMZ на устройстве, выберите в меню пункты Data Service→NAT Config→DMZ Settings. Откроется страница, изображенная на рисунке 2-42.

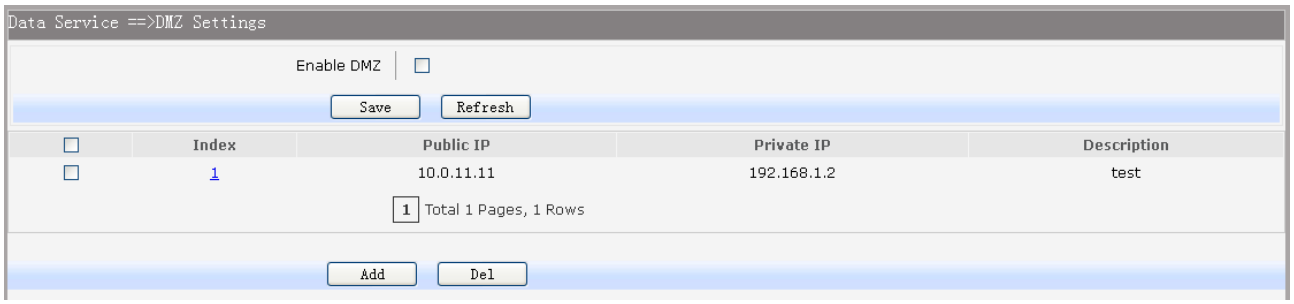


Рисунок 3-42. Просмотр настроек DMZ

Поставьте флажок в пункте Enable DMZ, если хотите включить работу DMZ на устройстве. Для редактирования созданной записи нажмите на ее индекс. Для удаления записи необходимо поставить флажок в соответствующей строке таблице и нажать кнопку Del. Для добавления новой записи нажмите кнопку Add.

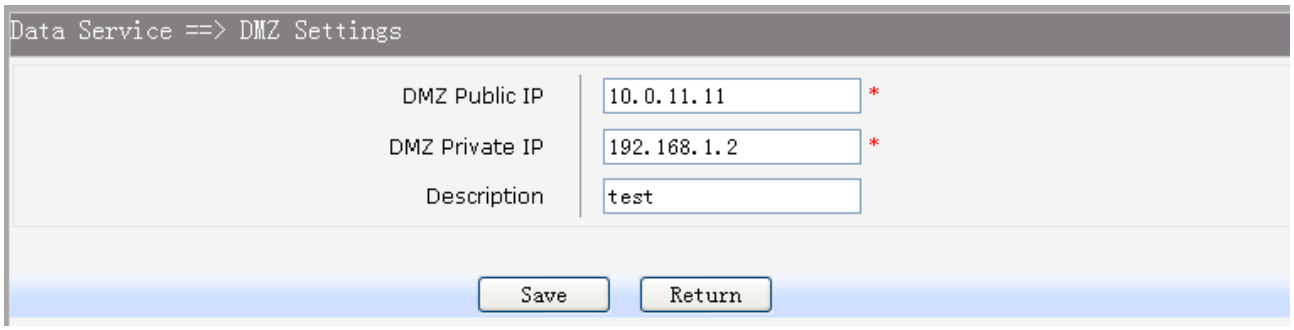


Рисунок 3-43. Настройка DMZ

Пункты для настройки DMZ представлены ниже:

- DMZ Public IP: настройка публичного IP-адреса для DMZ записи.
- DMZ Private IP: настройка локального IP-адреса для DMZ записи.
- Description: добавление описания записи.

3.4.2.4 Настройка ALG

Application-level gateway (ALG) компонент NAT, который понимает некоторые протоколы прикладного уровня и при прохождении через него пакетов этого протокола модифицирует их таким образом, что находящиеся за NAT пользователи могут пользоваться протоколом. Для настройки шлюза прикладного уровня (ALG) выберите в меню пункты Data Service→NAT Config→ALG Settings. Откроется меню настройки, изображённое на рисунке 2-44.

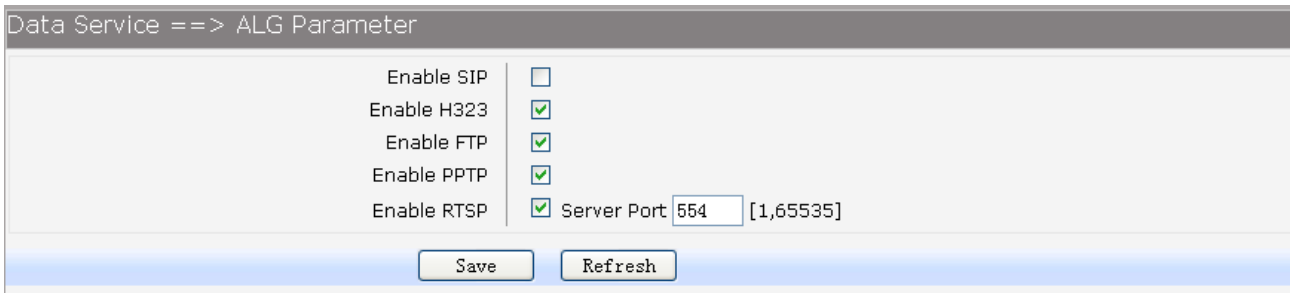


Рисунок 3-44. Настройка ALG

Пункты для настройки ALG представлены ниже:

- Enable SIP:включение или отключение SIP ALG.
- Enable H323: включение или отключение функции, позволяющей корректно работать клиенту Microsoft NetMeeting при подключении через NAT.
- Enable FTP: включение или отключение функции, позволяющей FTP клиентам взаимодействовать с сервером через NAT.
- Enable PPTP: Включение или отключение PPTP ALG.
- Enable RTSP: Включение или отключение RTSP ALG.

3.4.3 Настройка сетевого экрана

3.4.3.1 Настройка защиты от сетевых атак

При включении функции защиты от сетевых атак, маршрутизаторы серии QSW-300 могут анализировать пакеты и предотвращать различного рода атаки, такие как сканирование портов, защита от флуда различными типами трафика и защиту от других проблем, вызываемых вредоносным трафиком. Для перехода к настройкам защиты от сетевых атак, выберите в меню пункты Data Service→Firewall Config→Attack Defense. Откроется окно, изображенное на рисунке 2-45.

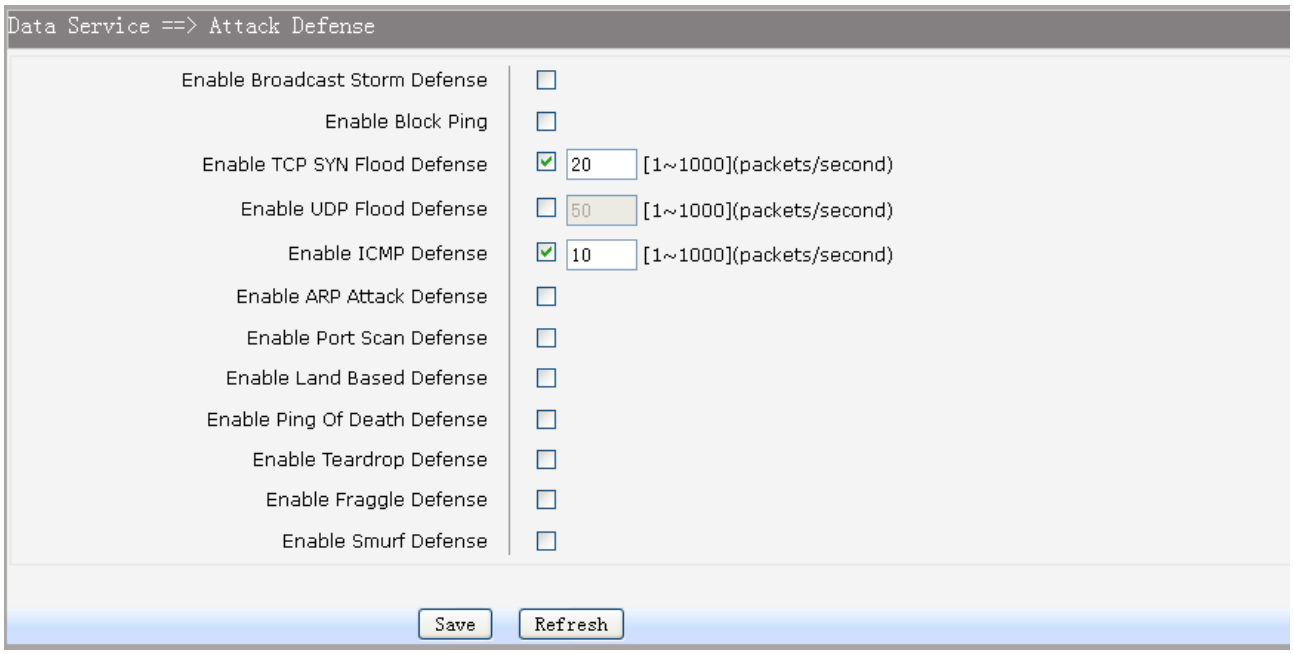


Рисунок 3-45. Настройка защиты от сетевых атак

Пункты настройки защиты от сетевых атак представлены ниже:

- Enable Broadcast Storm Defense: включение или отключение функции защиты от широковещательных штормов.
- Enable Block Ping включение или отключение блокирования PING пакетов.
- Enable TCP SYN Flood Defense: включение или отключение функции защиты от TCP SYN атак. Настраивается максимальное число TCP пакетов с SYN запросами, которое будет пропускать устройство.
- Enable UDP Flood Defense: включение или отключение функции защиты от UDP флуда. Настраивается максимальное число UDP пакетов, которое будет пропускать устройство.
- Enable ICMP Defense: включение или отключение функции защиты от большого числа ICMP-запросов. Настраивается максимальное число ICMP пакетов, которое будет пропускать устройство
- Enable ARP Attack Defense: включение или отключение механизма защиты от ARP-атак.
- Enable Port Scan Defense: включение или отключение механизма предотвращения сканирования портов.
- Enable Land Based Defense: включение или отключения механизма защиты от Land атаки. Land атака заключается в передаче на открытый порт клиента TCP-пакета с установленным флагом SYN, причем исходный адрес и порт такого пакета равны адресу и порту атакуемого клиента. Это приводит к тому, что клиент пытается

установить соединение сам с собой, в результате чего сильно возрастает загрузка процессора и может произойти зависание, перезагрузка системы клиента.

- Enable Ping Of Death Defense: включение или отключение механизма защиты от Ping of death атаки.
- Enable Teardrop Defense: включение или отключение механизма защиты от Teardrop атаки.
- Enable Fraggle Defense: включение или отключение механизма защиты от Fraggle атаки. Атака Fraggle является разновидностью Smurf атаки, используются UDP пакеты. Принцип действия этой атаки следующий: на седьмой порт жертвы отправляются широковещательные запросы, затем подменяется ip-адрес злоумышленника на ip-адрес клиента, который получает множество ответных сообщений
- Enable Smurf Defense: включение или отключение механизма защиты от Smurf атаки. Атака осуществляется большим количеством ICMP-запросов на адрес клиента.

3.4.3.2 Меню Service Type

Меню Service Type позволяет настроить записи, определяющие диапазон портов, используемых на странице контроля доступа клиентов (Internet Access-Ctrl page). Для перехода в меню, выберите в меню пункты Data Service→Firewall Config→Service Type.

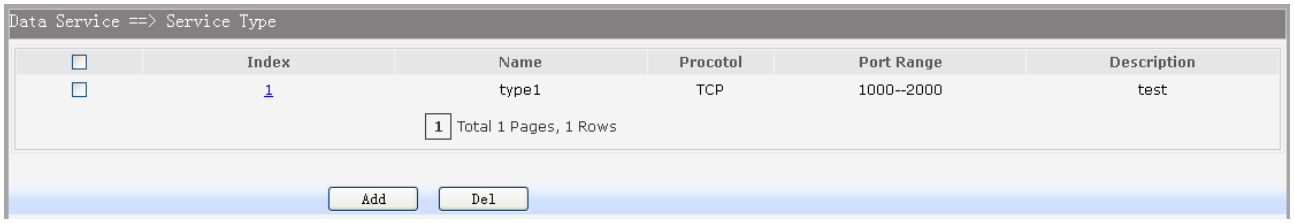


Рисунок 3-46. Просмотре настроек Service Type

Для редактирования записи, нажмите на её индекс, откроется окно редактирования, изображенное на рисунке 2-47. Для удаления записи, выберите сиротствующую запись и нажмите кнопку Del. Для добавления новой записи, нажмите кнопку Add.

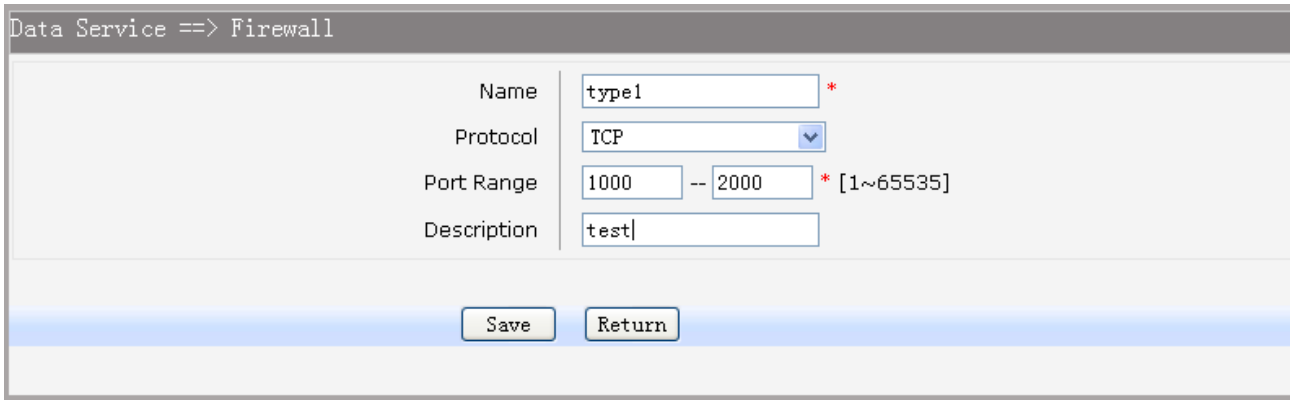


Рисунок 3-47. Окно конфигурации Service Type

Пункты для настройки представлены ниже:

- Name: имя записи, которое будет отображаться в списке на странице, изображенной на рисунке 2-48.
- Protocol: настройка протокол (TCP, UDP, ICMP).
- Port Range: настройка диапазона портов протоколов.
- Description: настройка описания записи.

3.4.3.3 Настройка контроля доступа к глобальной сети

3.4.3.3.1 Настройка доступа

Для перехода в меню настроек доступа, выберите пункты в меню Data Service→Firewall Config→Internet Access-Ctrl→Access. Откроется окно, изображенное на рисунке 2-48.

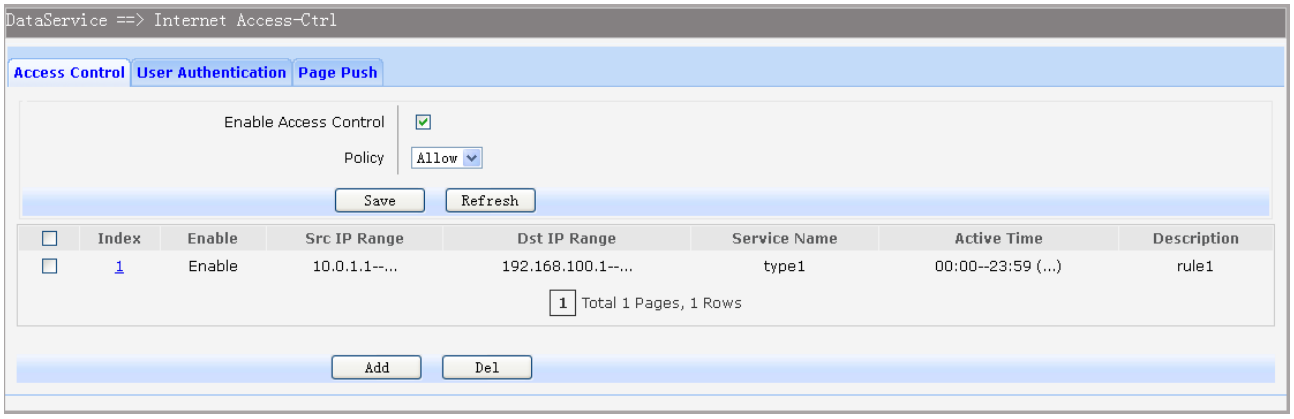


Рисунок 3-48. Просмотр записей контроля доступа

Пункты для настройки представлены ниже:

- Enable Access Control: включение или отключение контроля доступа для WAN-интерфейса.
- Policy: настройка политики контроля доступа (Allow или Deny). Если выбрать Allow, все пакеты будут разрешены, кроме отраженных в записях на странице. При выборе правила Deny, все пакеты будут запрещены, за исключением отраженных в записях, указанных на странице.

Для настройки созданной записи, нажмите на её индекс. Для удаления записи, поставьте флажок напротив соответствующей записи и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add, откроется окно, изображенное на рисунке 2-49.

Пункты для настройки представлены ниже:

- Action: политика для правила (Allow или Deny).

- Enable Rule: включение или отключение правила. Description: настройка описания записи.
- Source IP Range: настройка диапазона IP-адресов источников пакетов.
- Destination IP Range: настройка диапазона IP-адресов назначения.
- Service Name: применение списка Service Type.
- Active Time: настройка времени, когда правило работает.
- Active Day: настройка дней недели, в которые правило работает.

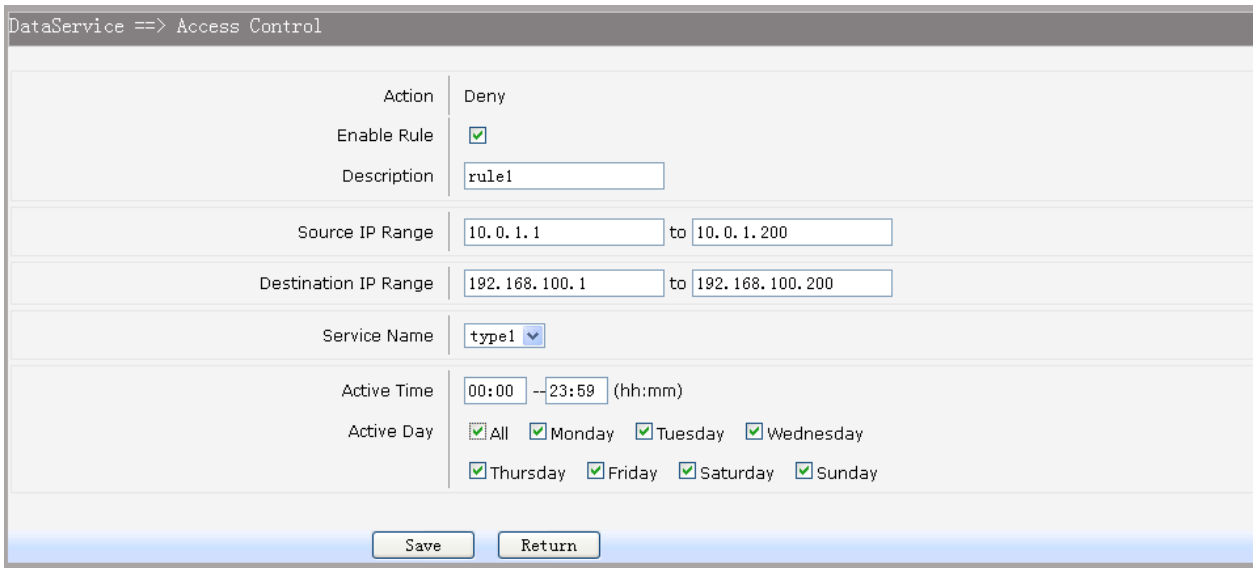


Рисунок 3-49 Добавление или редактирование записи контроля доступа

3.4.3.3.2 Авторизация пользователей

Маршрутизаторы серии QFR-300 позволяют настроить авторизацию доступа в сеть для пользователей (по имени и паролю). Для настройки авторизации пользователей, выберите в меню пункты Data Service→Firewall Config→Internet Access-Ctrl→User Authentication. Откроется окно, изображенное на рисунке 2-50.

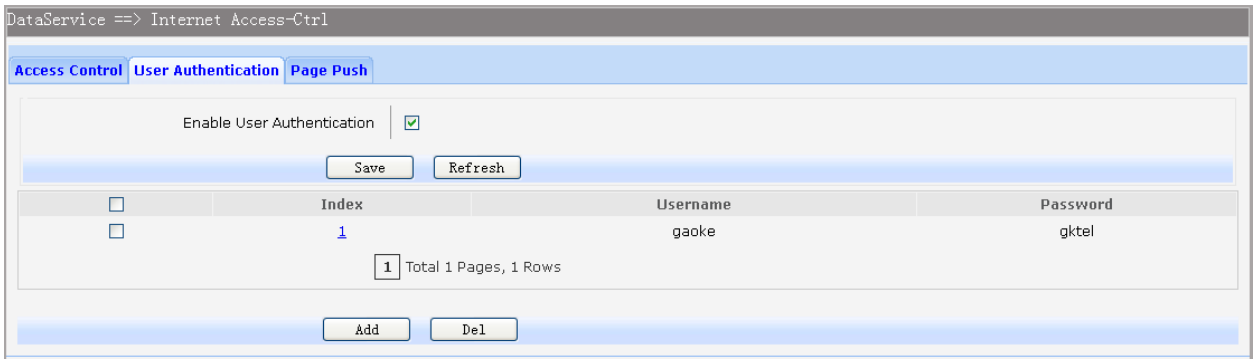


Рисунок 3-50 Просмотр списка пользователей

Пункт Enable User Authentication глобально включает или отключает глобальную авторизацию пользователей в сети. Если авторизация включена, то доступ в сеть смогут получить только пользователи, которые отражены в списке ниже.

Для редактирования записей пользователей в списке доступа нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add, откроется окно, изображенное на рисунке 2-51.

Пункты для настройки записи представлены ниже:

- Username: настройка имени пользователя.
- Password: настройка пароля.
- Auth Mode: Настройка режима авторизации.
  - Allow Multi-PC Access: режим разрешающий доступ в интернет по учетной записи пользователя с нескольких компьютеров.
  - Allow One PC Access: режим разрешающий доступ в интернет пользователю только с одного компьютера.
  - Allow Special IP Access: режим разрешающий доступ в сеть пользователю при заходе с устройства с определённым IP-адресом.
  - Allow Special MAC Access: режим разрешающий доступ в сеть пользователю при заходе с устройства с определённым MAC-адресом.

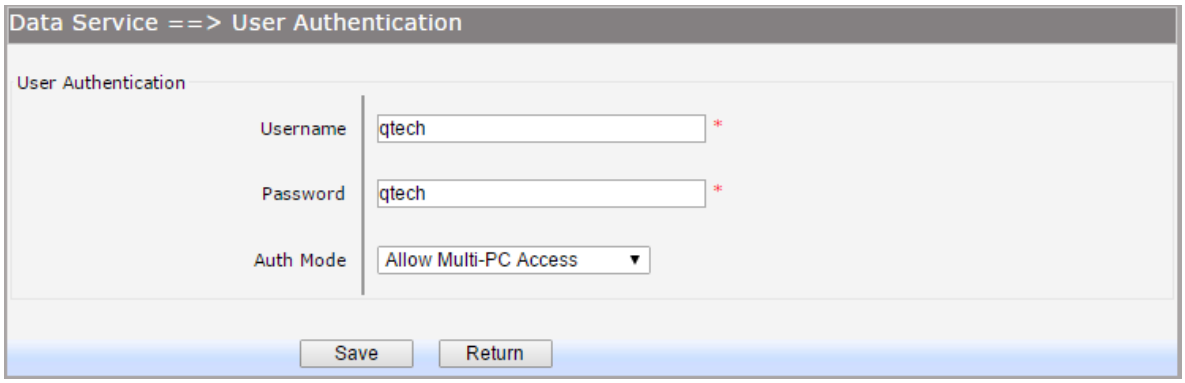


Рисунок 3-51. Настройка и редактирование записи аутентификации пользователя

3.4.3.3.3 Настройка HTTP Page push

Режим HTTP Page push позволяет переадресовать пользователя на определенную страницу при первом подключении к сети интернет через браузер. Для настройки выберите пункты в меню Data Service→Firewall Config→Internet Access-Ctrl→Page. Откроется окно, изображенное на рисунке 2-52.

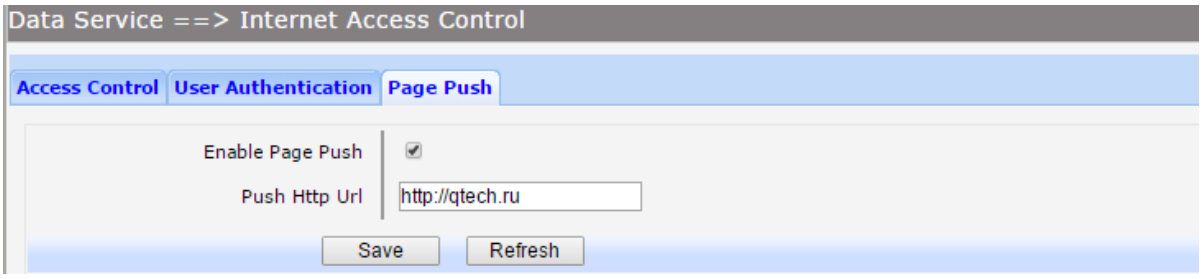


Рисунок 3-52. Настройка HTTP Page Push

Пункт Enable Page Push включает переадресацию пользователя на заданную в пункте Push Http Url.

3.4.3.4 Настройка контроля доступа к устройству

3.4.3.4.1 Настройка контроля WEB доступа

Для настройки контроля доступа по WEB, выберите в меню пункты Data Service→Firewall Config→Netword Access-Ctrl→WEB. Откроется окно, изображенное на рисунке 2-53.

Пункты для настройки записи представлены ниже:

- HTTP Port: настройка порта, используемого для доступа по HTTP.
- HTTPS Port: настройка порта, используемого для доступа по HTTPs.

Подменю Internet Web Access позволяет ограничить доступ из внешней сети на WEB-интерфейс устройства. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к WEB-интерфейсу устройства можно будет подключиться из внешней сети.
- IP Limit: включение режима, ограничивающего доступ к WEB-интерфейсу.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ на WEB-интерфейс. Используется если включен режим, ограничивающий доступ.
- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ на WEB-интерфейс. Используется если включен режим, ограничивающий доступ.

Подменю Intranet Web Access позволяет ограничить доступ из локальной сети на WEB-интерфейс устройства. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к WEB-интерфейсу устройства можно будет подключиться из локальной сети.
- IP Limit: включение режима, ограничивающего доступ к WEB-интерфейсу.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ на WEB-интерфейс. Используется если включен режим, ограничивающий доступ.
- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ на WEB-интерфейс. Используется если включен режим, ограничивающий доступ.

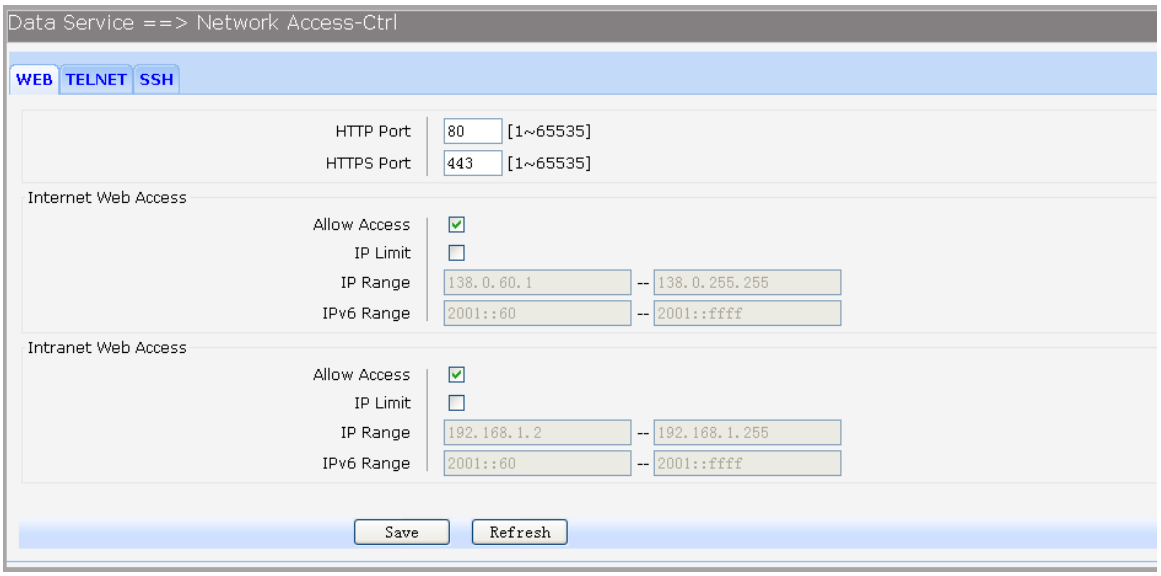


Рисунок 3-53. Настройка WEB доступа

3.4.3.4.2 Настройка контроля доступа по telnet протоколу

Для настройки контроля доступа по telnet протоколу, выберите в меню пункты Data Service→Firewall Config→Netword Access-Ctrl→Telnet. Откроется окно, изображенное на рисунке 2-54.

Пункт Port позволяет настроить порт, который будет прослушивать устройство для создания telnet соединения.

Подменю Internet Telnet Access позволяет ограничить telnet подключения к устройству из внешней сети. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к устройству можно будет подключиться из внешней сети.
- IP Limit: включение режима, ограничивающего доступ по telnet.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ по telnet на устройство. Используется если включен режим, ограничивающий доступ.
- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ по telnet на устройство. Используется если включен режим, ограничивающий доступ.

Подменю Intranet Telnet Access позволяет ограничить telnet подключения к устройству из локальной. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к устройству можно будет подключиться из локальной сети.
- IP Limit: включение режима, ограничивающего доступ по telnet.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ по telnet на устройство. Используется если включен режим, ограничивающий доступ.

- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ по telnet на устройство. Используется если включен режим, ограничивающий доступ.

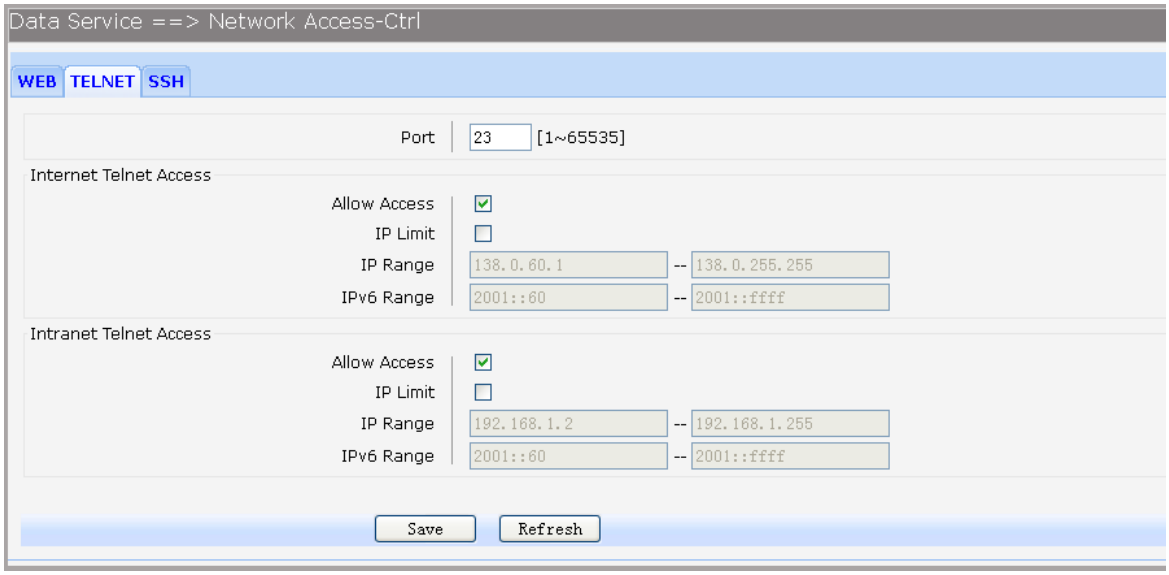


Рисунок 3-54. Настройка доступа по telnet

3.4.3.4.3 Настройка контроля доступа по ssh протоколу

Для настройки контроля доступа по ssh, выберите в меню пункты Data Service→Firewall Config→Network Access-Ctrl→SSH. Откроется окно, изображенное на рисунке 2-55.

Пункт Port позволяет настроить порт, который будет прослушивать устройство для создания ssh соединения.

Подменю Internet SSH Access позволяет ограничить ssh подключения к устройству из внешней сети. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к устройству можно будет подключиться из внешней сети.
- IP Limit: включение режима, ограничивающего доступ по ssh.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ по ssh на устройство. Используется если включен режим, ограничивающий доступ.
- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ по ssh на устройство. Используется если включен режим, ограничивающий доступ.

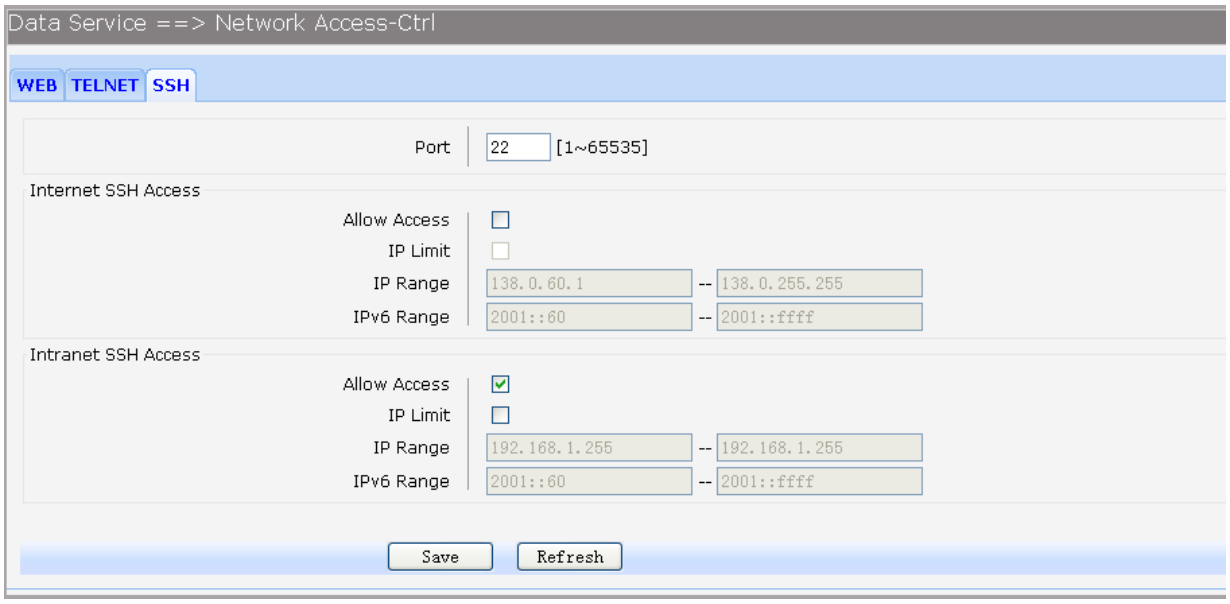


Рисунок 3-55. Настройка доступа по ssh

Подменю Intranet SSH Access позволяет ограничить ssh подключения к устройству из локальной. Пункты для настройки представлены ниже:

- Allow Access: настройка доступа. Если разрешен, к устройству можно будет подключиться из локальной сети.
- IP Limit: включение режима, ограничивающего доступ по ssh.
- IP Range: настройка диапазона IP-адресов, с которых разрешен доступ по ssh на устройство. Используется если включен режим, ограничивающий доступ.
- IPv6 Range: настройка диапазона IPv6-адресов, с которых разрешен доступ по ssh на устройство. Используется если включен режим, ограничивающий доступ.

3.4.3.5 Политики фильтрации доступа во внешнюю сеть

3.4.3.5.1 Настройка фильтрации WEB-страниц по ключевым словам

Для настройки политик фильтрации WEB-страниц, выберите в меню пункты Data Service→Firewall Config→ Filter Strategy→Keyword Filter. Откроется окно, изображенное на рисунке 2-56.

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add.

Пункты для настройки представлены ниже:

- Keyword Filter: глобальное включение политики фильтрации WEB-страниц по словам.
- Policy: настройка политики фильтрации (Deny или Allow). Разрешающая или запрещающая политика для записей фильтрации по словам.

Для экспорта политик фильтрации нажмите кнопку Export и выберите место куда сохранить файл. Для загрузки политик из файла, нажмите кнопку Browse, выберите файл с политиками на вашем ПК и нажмите кнопку Import.

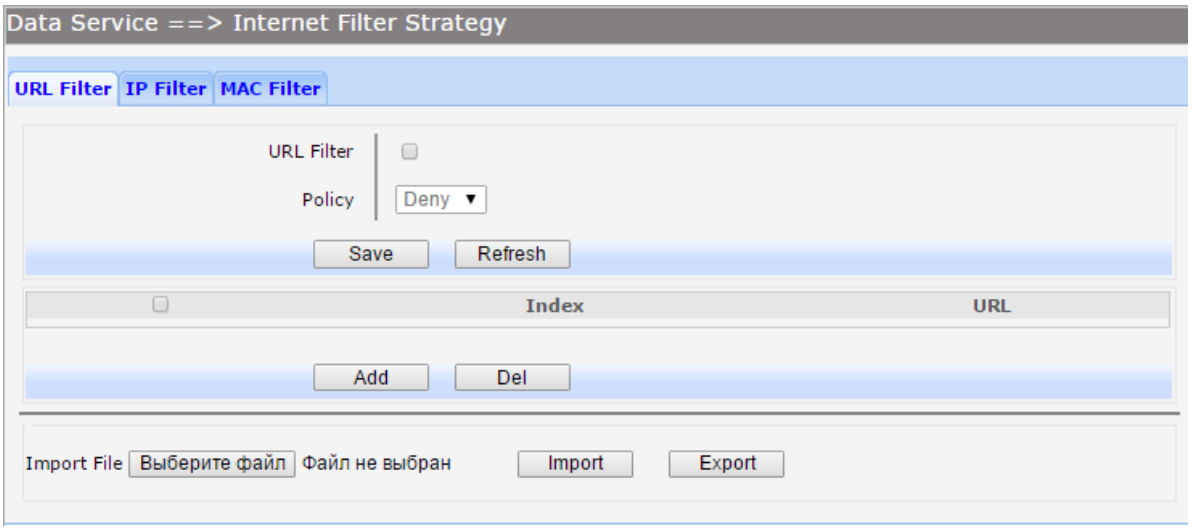


Рисунок 3-56. Настройка фильтрации по ключевым словам

3.4.3.5.2 Настройка фильтрации по IP-адресу

Для настройки политик доступа к внешним ресурсам клиентам, с определенными локальными IP-адресами, выберите в меню пункты Data Service→Firewall Config→ Filter Strategy→IP Filter. Откроется окно, изображенное на рисунке 2-57.

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add.

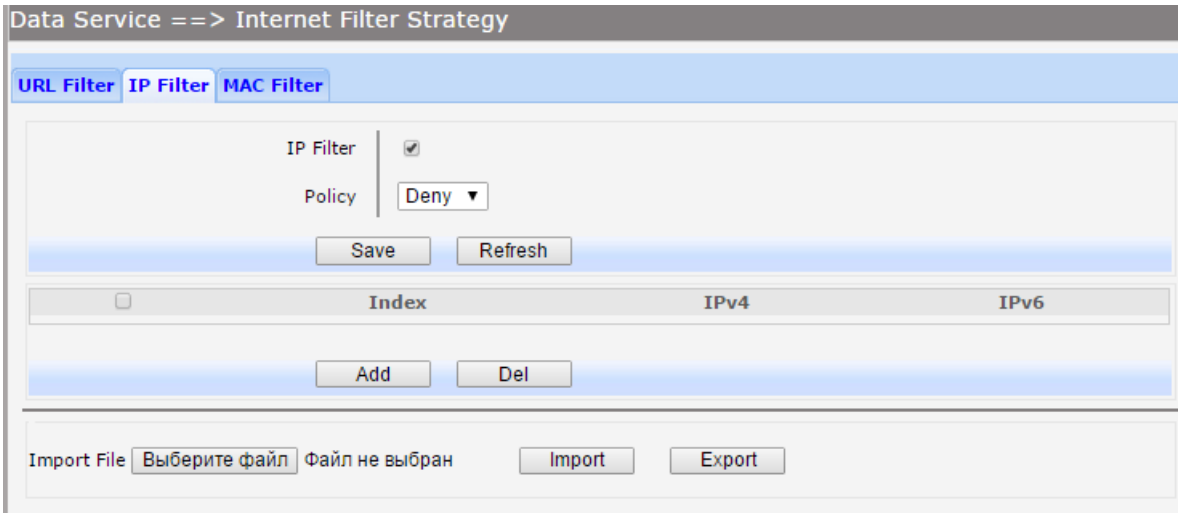


Рисунок 3-57 Настройка фильтрации по IP-адресам

Пункты для настройки представлены ниже:

- IP Filter: глобальное включение политики фильтрации по IP-адресам.
- Policy: настройка политики фильтрации (Deny или Allow). Разрешающая или запрещающая политика для доступа во внешнюю сеть локальным клиентам.

Для экспорта политик фильтрации нажмите кнопку Export и выберите место куда сохранить файл. Для загрузки политик из файла, нажмите кнопку Browse, выберите файл с политиками на вашем ПК и нажмите кнопку Import.

3.4.3.5.3 Настройка фильтрации по MAC-адресу

Для настройки политик доступа к внешним ресурсам клиентам, с определенными MAC-адресами, выберите в меню пункты Data Service→Firewall Config→ Filter Strategy→MAC Filter. Откроется окно, изображенное на рисунке 2-58.

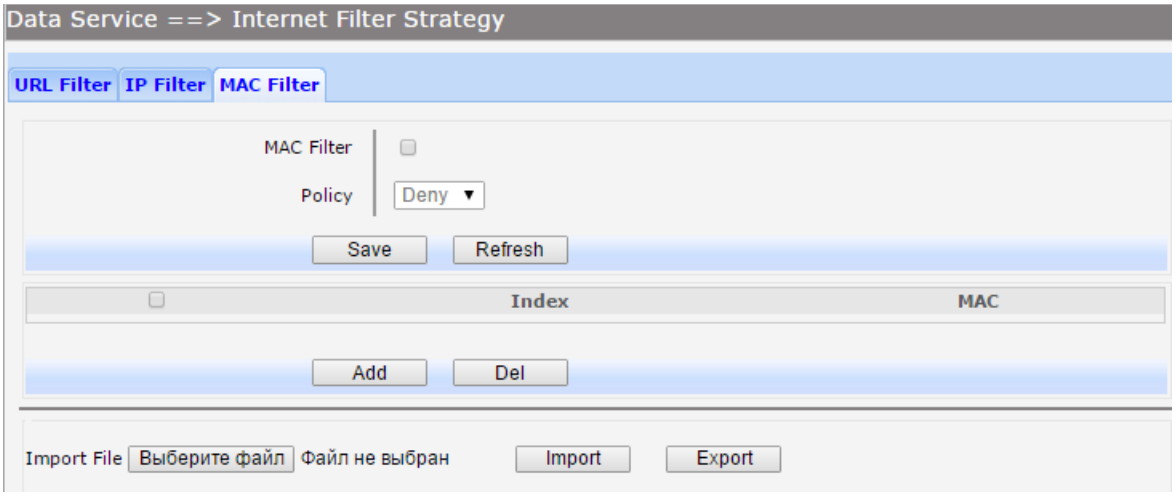


Рисунок 3-58. Настройка фильтрации по MAC-Адресам

Пункты для настройки представлены ниже:

- MAC Filter: глобальное включение политики фильтрации по MAC-адресам.
- Policy: настройка политики фильтрации (Deny или Allow). Разрешающая или запрещающая политика для доступа во внешнюю сеть локальным клиентам.

Для экспорта политик фильтрации нажмите кнопку Export и выберите место куда сохранить файл. Для загрузки политик из файла, нажмите кнопку Browse, выберите файл с политиками на вашем ПК и нажмите кнопку Import.

Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add, откроется окно, изображенное на рисунке 2-59.

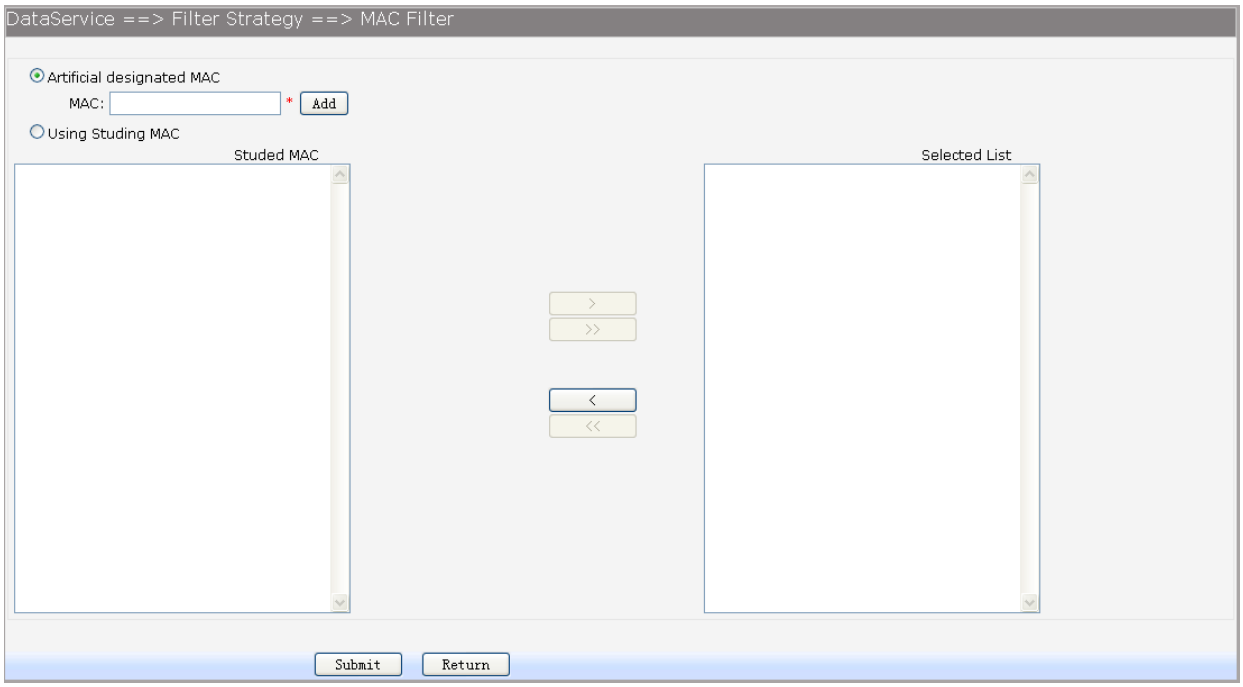


Рисунок 3-59. Добавление записи MAC-адреса в таблицу фильтрации

Есть два способа добавления MAC-адресов:

- Artificial designated MAC: настройка MAC-адресов вручную. Для этого введите MAC-адрес устройства, после чего нажмите кнопку Add.
- Using Studying MAC: включение механизма изучения MAC-адресов, в меню Studed MAC отобразится список изученных устройством адресов. Для добавления их в список фильтрации выберите MAC-адрес, нажмите кнопку “>”, после чего примените изменения, нажав кнопку Sumbit.

3.4.3.6 Настройка IP и MAC Binding

Функция IP и MAC Binding позволяет контролировать доступ клиентов во внешнюю сеть на основе их MAC-адреса и IP-адреса. Для настройки выберите в меню пункты Data Service→Firewall Config→IP&MAC. Откроется окно, изображенное на рисунке 2-60.

Есть два способа добавления MAC-адресов:

- Можно вручную ввести IP-адрес в поле IP, MAC-адрес в поле MAC и нажать на кнопку Add Item.
- В списке Scan List выбрать соответствующую запись и нажать кнопку “>”.

Для сохранения результатов добавления записей нажмите кнопку Save.

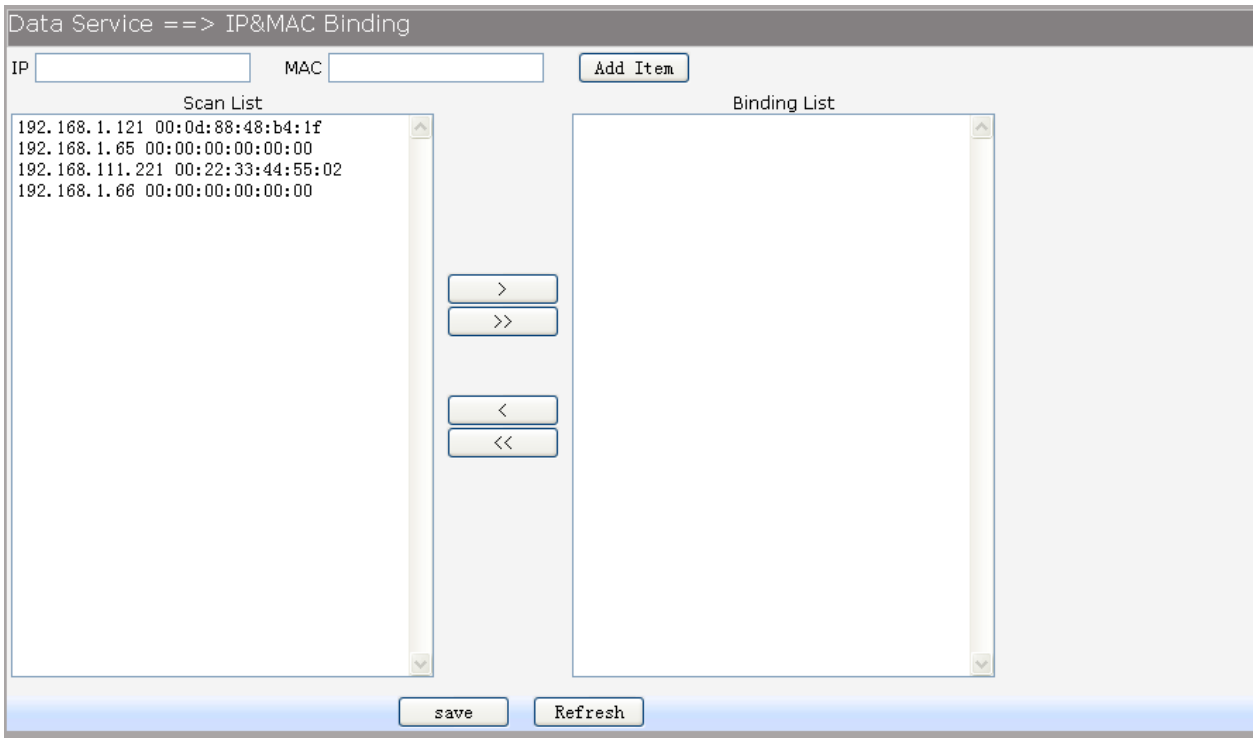


Рисунок 3-60. Настройка IP и MAC Binding

3.4.4 Настройка QoS

3.4.4.1 Основные настройки

Функция QoS, работающая по протоколу 802.1p включена по умолчанию. Маршрутизаторы серии QSW-300 поддерживают четыре очереди приоритетов. Для настройки выберите в меню пункты Data Service→QoS→Basic. Откроется окно, изображенное на рисунке 2-61.

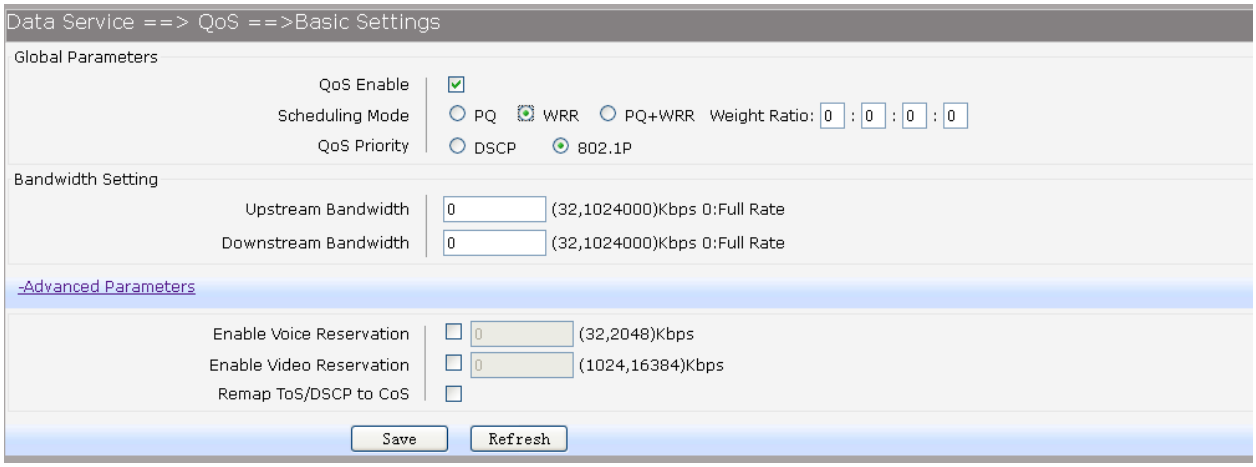


Рисунок 3-61.

Пункты для настройки, представленные в подменю Global Parameters, представлены ниже:

- QoS Enable: глобальное включение или отключение функционала QoS.
- Scheduling Mode: настройка режимов планировщика QoS

  ○ PQ: режим приоритетной очереди PQ. Пакеты, входящие в систему, сначала классифицируется по видам трафика, затем отправляются в соответствующие очереди. В первую очередь отправляются пакеты с высшим приоритетом.

  ○ WRR: режим взвешенных справедливых очередей WRR. Входящий трафик делится на несколько классов, для каждого из которых ведется отдельная очередь пакетов. Каждой очереди назначается вес (Weight Ratio), на основании этого веса назначается процент пропускной способности, гарантируемый данному классу трафика.

  ○ PQ+WRR: для трафика с высшим приоритетом используется режим PQ, для остального трафика режим WRR.

- QoS Priority: настройка приоритетов зависимости от выбранной политики QoS.

  ○ DSCP: значения приоритетов очередей при выборе политики приоритетов DSCP указаны в таблице 2-1.

  ○ 802.1p: значения приоритетов очередей при выборе политики приоритетов 802.1P указаны в таблице 2-2

Таблица 3-1. Приоритеты DSCP

Значение приоритета DSCP	Приоритет очереди (3 максимальный)
0-15	Очередь 0
16-31	Очередь 1
32-47	Очередь 2
48-64	Очередь 3

Таблица 3-2. Приоритеты 802.1P

Значение приоритета 802.1p	Приоритет очереди (3 максимальный)
0-1	Очередь 0
2-3	Очередь 1
4-5	Очередь 2
6-7	Очередь 3

Пункты для настройки, представленные в подменю Bandwidth Parameters, представлены ниже:

- Upstream Bandwidth: настройка полосы пропускания для исходящего трафика.
- Downstream Bandwidth: настройка полосы пропускания для входящего трафика.

Пункты для настройки, представленные в подменю Advanced Parameters, представлены ниже:

- Enable Voice Reservation: включения резервирования и настройка полосы пропускания, зарезервированной для голосового трафика.
- Enable Video Reservation: включения резервирования и настройка полосы пропускания, зарезервированной для видео трафика.
- Remap ToS/DSCP to CoS: Функция позволяет заменять в пакетах теги 802.1p на теги DSCP для исходящего трафика. Соотношения приоритетов представлены в таблице 2-3.

Таблица 3-3 Соотношения приоритетов при перемаркировки тегов.

Значение приоритета DSCP	Значение приоритета 802.1p
0-7	0
8-15	1
16-23	2
24-31	3
32-39	5
40-47	5
48-55	6
56-63	7

3.4.4.2 Настройка ограничения скорости порта

Функция Rate Limit позволяет ограничивать скорость на LAN портах для различных типов пакетов. Для настройки выберите в меню пункты Data Service→QoS→Port Rate Limit. Откроется окно, изображенное на рисунке 2-62.

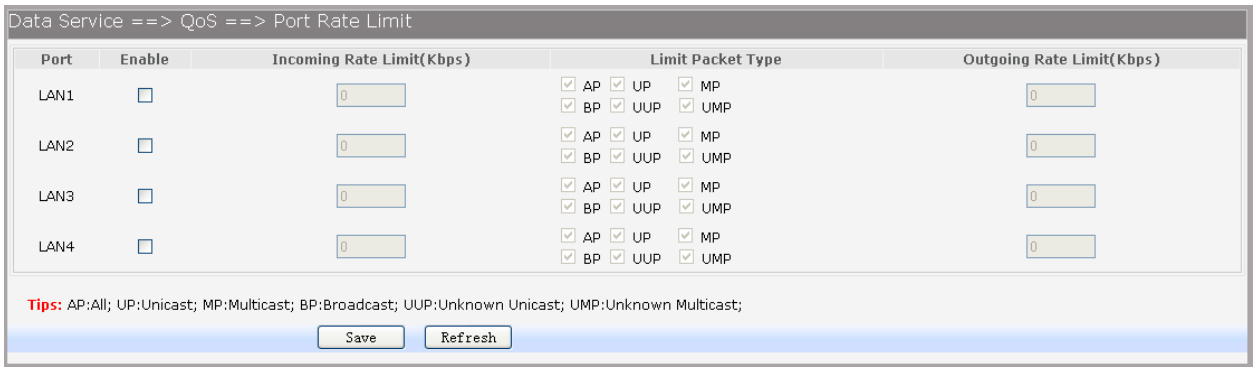


Рисунок 3-62. Настройка ограничения скорости порта

Пункты для настройки представлены ниже:

- Port: LAN порт для которого осуществляется настройка.
- Enable: включение или отключение работы механизма Rate Limit на LAN порту.
- Incoming Rate Limit: настройка максимальной полосы пропускания для входящего трафика (полоса пропускания настраивается кратной 32 Кбит/с).
- Limit Packet Tape: выбор типа пакетов, для которых будет ограничена полоса пропускания.
- Outgoing Rate Limit: настройка максимальной полосы пропускания для исходящего трафика (полоса пропускания настраивается кратной 32 Кбит/с).

3.4.4.3 Настройка ограничения скорости потока

Для настройки ограничений скорости потока, выберите в меню пункты Data Service→QoS→Port Rate Limit.

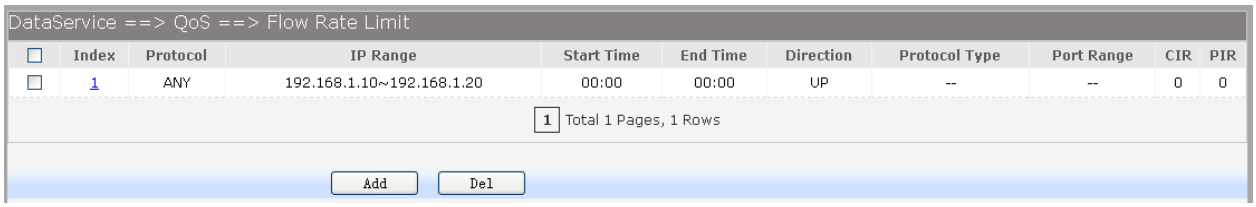


Рисунок 3-63. Просмотр записей настроек ограничения скорости потоков

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-64.

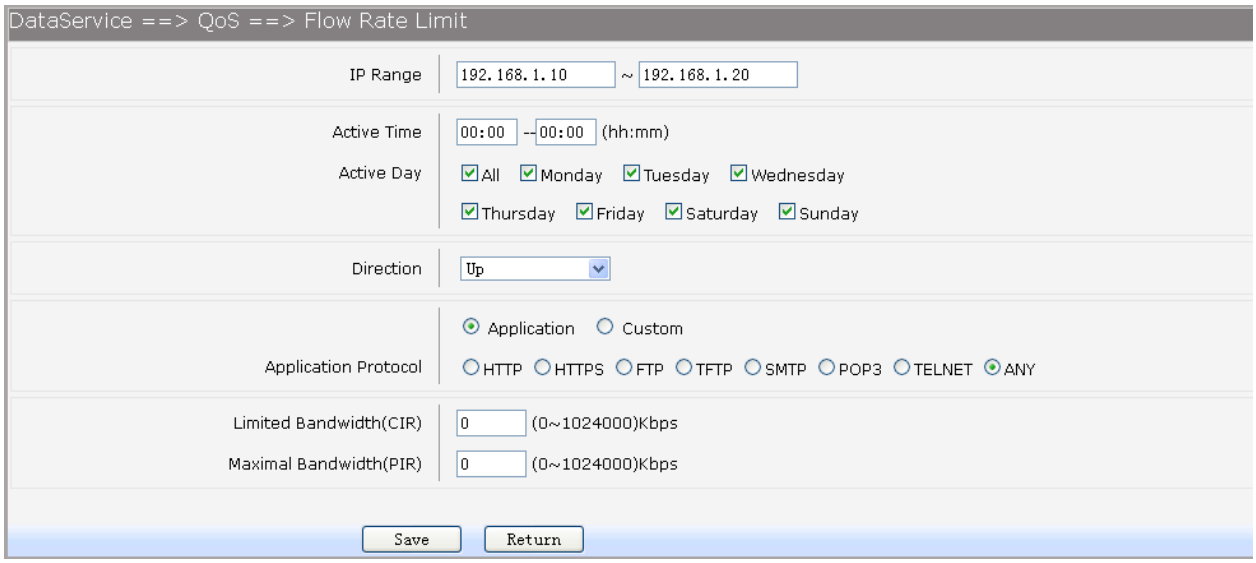


Рисунок 3-64. Настройка ограничения скорости потока

Пункты для настройки представлены ниже:

- IP Range: настройка диапазона IP-адресов локальной сети, для которых будет ограничиваться скорость потока.
- Active Time: настройка времени действия правила. Если не настроено, правило будет работать постоянно.
- Active Day: настройка дней действия правила. Если не настроены, правило будет работать постоянно.
- Direction: выбор режима работы:
  - UP: правило ограничения скорости применяется для исходящего трафика.
  - DOWN: правило ограничения скорости применяется для входящего трафика.
  - Bidirectional: правило применяется для входящего и исходящего трафика.
- Application: режим ограничивающий скорость пропускания для определенных протоколов
  - Application Protocol: выбор протоколов, для которых будет применятся правило ограничения скорости потока.
- Custom: режим ограничивающий скорость соединений установленных на настроенные в ручную порты. При выборе данного режима откроется дополнительное меню, изображенное на рисунке 2-65.
  - Protocol Type: настройка протокола (TCP или UDP).
  - Port Range: настройка диапазона портов.

- Limited Bandwidth (CIR): ограничение гарантированной полосы пропускания.
- Maximal Bandwidth (PIR): ограничение максимальной полосы пропускания.

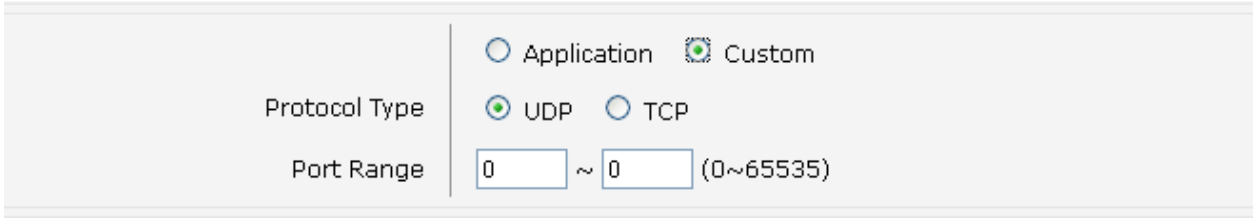


Рисунок 3-65. Настройка портов для правила ограничения скорости потока

3.4.4.4 Настройка QoS для различных сервисов

Устройство поддерживает перемаркировку приоритетов для QoS, в зависимости от типа услуг. Для настройки, выберите в меню пункты Data Service→QoS→Service.

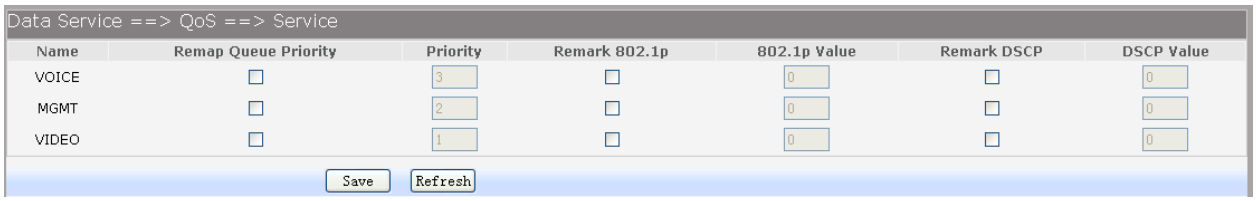


Рисунок 3-66. Меню QoS Service

Пункты для настройки представлены ниже:

- Name: имя сервиса.
- Remap Queue Priority: поставьте флажок для перемаркировки очереди QoS.
- Priority: настройка приоритета (от 0 до 3. 3 максимальный).
- Remark 802.1p: поставьте флажок для перемаркировки приоритета на 802.1p.
- 802.1p Value: значение приоритета 802.1p.
- DSCP Value: поставьте флажок для перемаркировки приоритета на DSCP.

3.4.4.5 Настройка ACL

Для просмотра настроенных ACL, выберите в меню пункты Data Service→QoS→ACL.

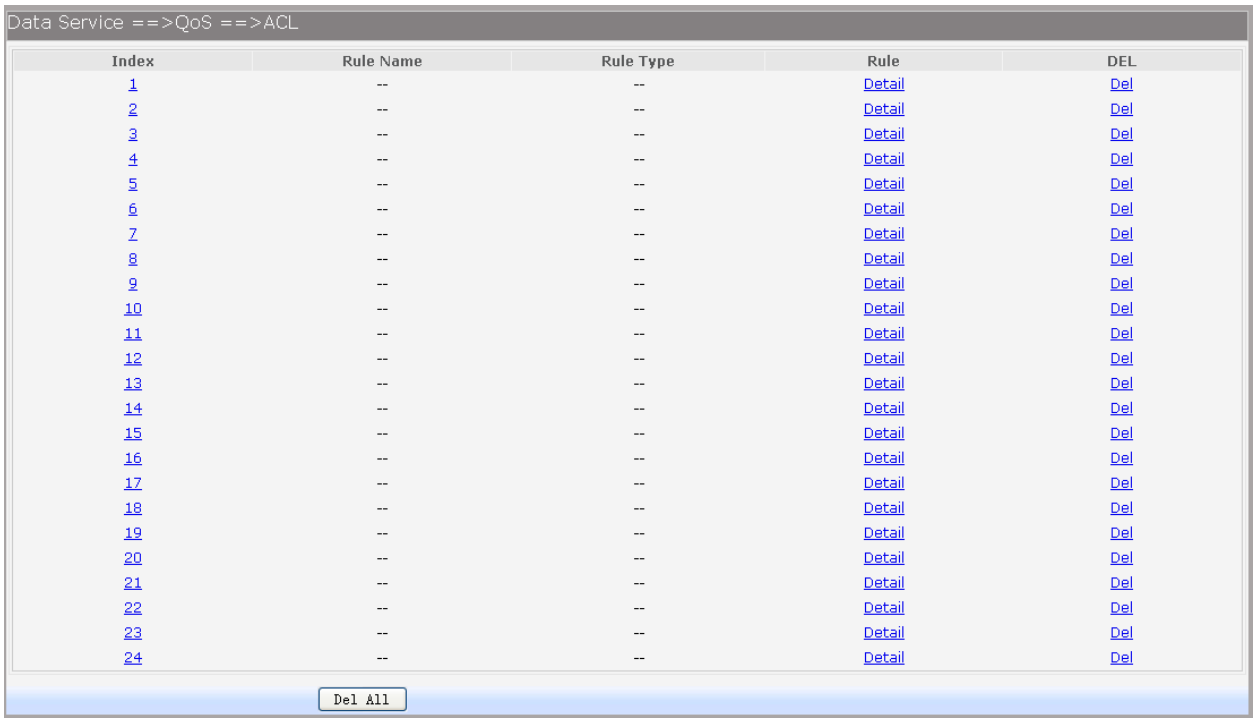


Рисунок 3-67. Просмотр настроенных ACL.

Для удаления записи ACL нажмите на Del, напротив соответствующей записи. Для настройки записи нажмите на её индекс или на Detail. Откроется окно, изображенное на рисунке 2-68.

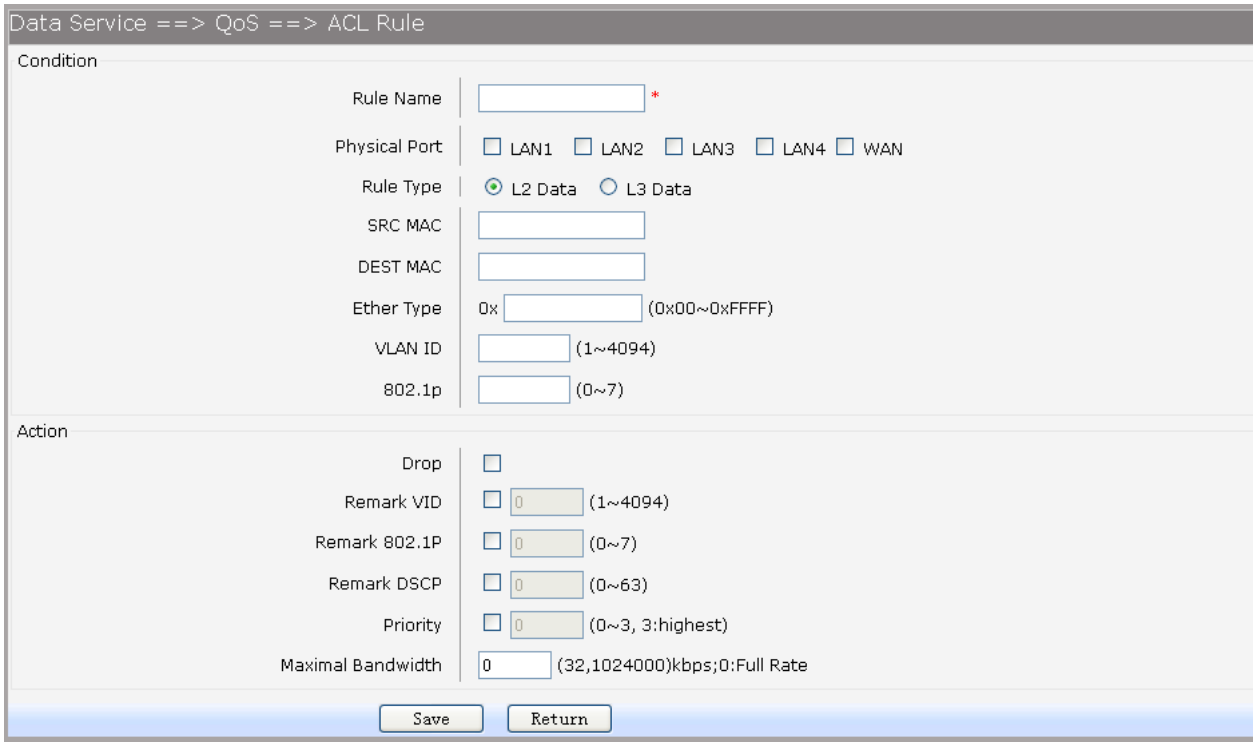


Рисунок 3-68. Настройка записи ACL

Пункты для настройки представлены ниже:

- Rule Name: имя правила.
- Physical Port: выбор порта, на который будет применятся ACL.
- Rule type: выбор режима работы правила (L2 или L3).

Если выбран режим L2, пункты настройки для выбора параметров анализируемых пакетов будут следующие:

- SRC MAC: настройка MAC-адреса.
- DEST MAC: настройка MAC-адреса назначения.
- EtherType: настройка EtherType.
- VLAN ID: настройка идентификатора VLAN.
- 802.1p: настройка приоритета.

Если выбран режим L3, пункты настройки для выбора параметров анализируемых пакетов представлены на рисунке 2-69 и описаны ниже:

- Src IP/Netmask: настройка IP-адреса и маски подсети (например, 192.168.10.1/255.255.255.0) источников.
- Dest IP/Netmask: настройка IP-адреса и маски подсети устройств, которым предназначен пакет.
- Protocol: выбор протокола (ICMP, UDP, TCP или другой протокол передаваемый по IP)
- L4 Src Port: настройка диапазона портов источников.
- L4 Dest Port: настройка диапазона портов назначения.

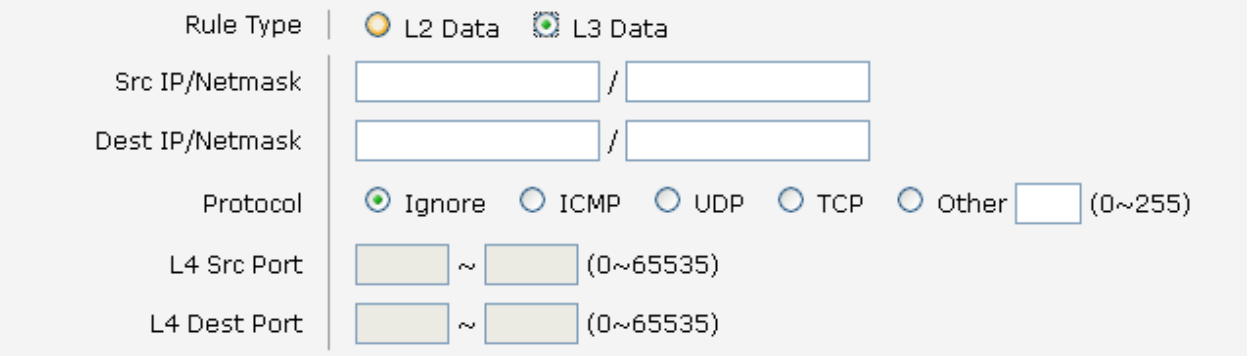


Рисунок 3-69. Настройка ACL для L3 пакетов

В подменю Action представлены следующие пункты настройки:

- Drop: отбросить пакеты описанные ACL.

- Remark VID: поменять идентификатор VLAN для пакетов описанных ACL.
- Remark 802.1p: поменять приоритет 802.1p для пакетов описанных ACL.
- Remark DSCP: поменять приоритет DSCP для пакетов описанных ACL.
- Priority: поменять очередь для пакетов описанных ACL.
- Maximal Bandwidth: ограничить максимальную полосу пропускания для пакетов описанных ACL.

3.4.5 Настройка DDNS

Служба DDNS применяется для назначения постоянного доменного имени любому сетевому устройству с динамическим IP-адресом. Это может быть IP-адрес, полученный по DHCP или при PPPoE-соединении. Другие устройства в Интернете могут устанавливать соединение с этой машиной по доменному имени и даже не знать, что IP-адрес изменился. Для просмотра настроек DDNS, выберите в меню пункты Data Service→DDNS.

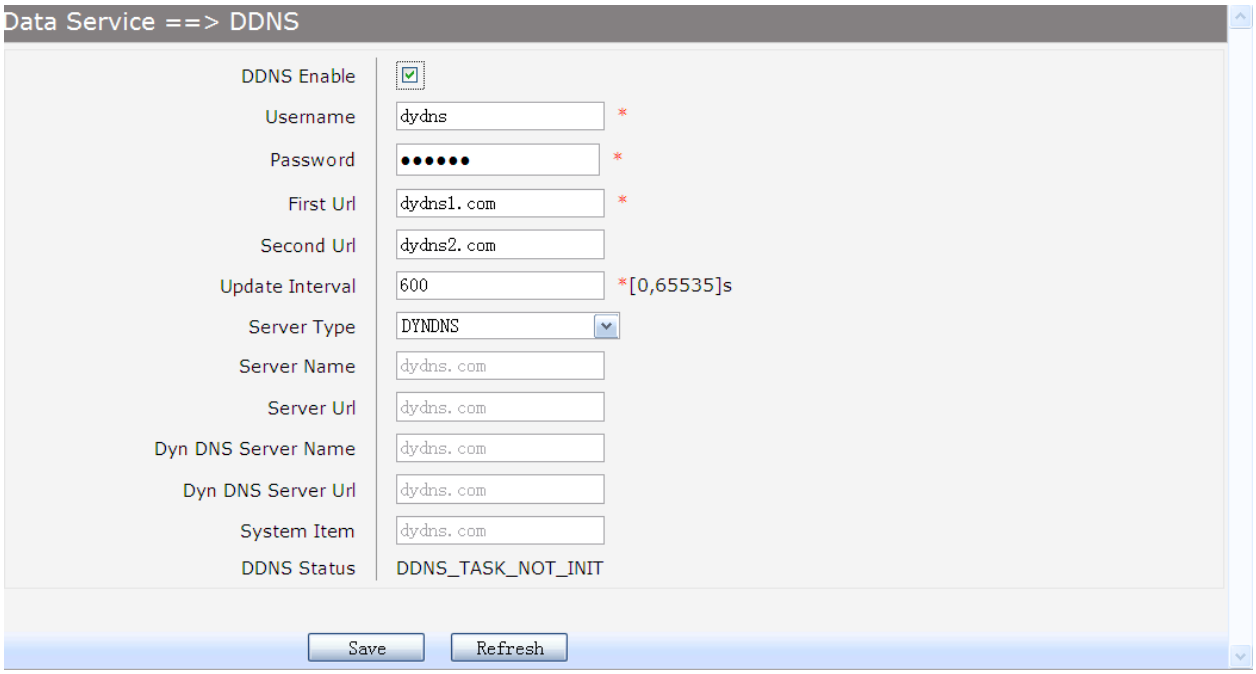


Рисунок 3-70. Настройка DDNS

Пункты для настройки представлены ниже:

- DDNS Enable: включение или отключение сервис DDNS.
- Username: настройка имени пользователя от аккаунта DDNS.
- Password: настройка пароля от аккаунта DDNS.
- First Url: имя домена, которое зарегистрировано у DDNS провайдера.

- Seconf Url: вторичное имя домена, которое зарегистрировано у DDNS провайдера (если применимо).
- Update Interval: настройка времени обновления. Настраивается в зависимости от времени обновления внешнего IP-адреса.
- Server Type: выбор DDNS-сервера.
    - DYDNS: для сервера dydnns.org
    - FREEDNS: для сервера freedns.afraid.org
    - ZONE: для сервера zoneedit.com
    - NOIP: для сервера no-ip.com
    - 3322: для сервера 3322.org
    - CUSTOM: для других серверов DDNS, требуется ручная настройка параметров.
- DDNS Status: пункт меню отражающий состояние DDNS-сервера.

Если в пункте меню Service Type, выбран пункт Custom, потребуются дополнительные настройки:

- Server Name: имя сервера устройства.
- Server Url: URL-адрес сервера устройства.
- Dyn DNS Server Name: настройка имени DDNS сервера.
- Dyn DNS Url: настройка URL-адреса DDNS севера.
- System Item: настройка обозначения в системе.

Для сохранения внесенных изменений нажмите кнопку Save.

3.4.6 Настройка VPN

Виртуальная частная сеть (VPN) – это общее название технологии, обеспечивающей одно или несколько соединений поверх других существующих сетей, включая Интернет. С ростом популярности сети интернет, возникает все больше необходимости передавать данные между локальными сетями и при этом иметь надежную возможность их защиты от изменений или прочтения. Технология VPN разработана с учетом этих требований и гарантирует надежный канал связи с защитой передаваемых данных, через общедоступные сети общего пользователя. Для этого VPN создает туннель, для установления соединения между двумя конечными точками. Туннель позволяет обеспечить безопасность данных с помощью проверки подлинности и шифрования данных. Типичная топология VPN-сети изображена на рисунке 2-71.

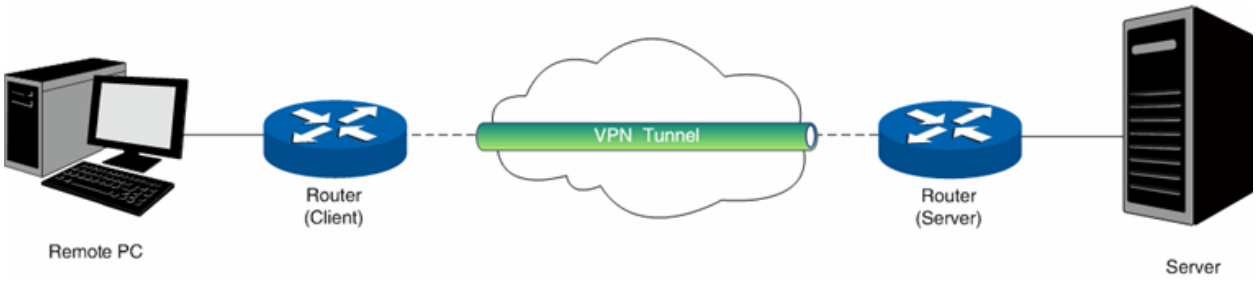


Рисунок 3-71. Топология VPN-сети.

Пакеты, передаваемые в туннеле, инкапсулируются и де-инкапсулируются на маршрутизаторах. Таким образом туннель позволяет передавать в содержимом пакета информацию второго уровня (L2TP или PPTP).

3.4.6.1 Настройка PPTP-сервера

VPN-туннель устанавливающий соединение на втором уровне создается посредством L2TP или PPTP протоколов. Оба этих протока инкапсулируют своим пакеты, добавляя к пакету дополнительный заголовок посредством PPP протокола. Таблица 2-4 показывает разницу между L2TP и PPTP протоколами.

Таблица 3-4. Сравнение L2TP и PPTP

Протокол	Среда передачи	Тип туннеля	Длина заголовка	Авторизация
PPTP	IP сети	Один туннель	Не менее 6 байт	Не поддерживается
L2TP	IP сети по UDP	Множество туннелей	Не менее 4 байт	Поддерживается

Для настройки PPTP-сервера, выберите в меню пункты Data Service→VPN →PPTP Server.

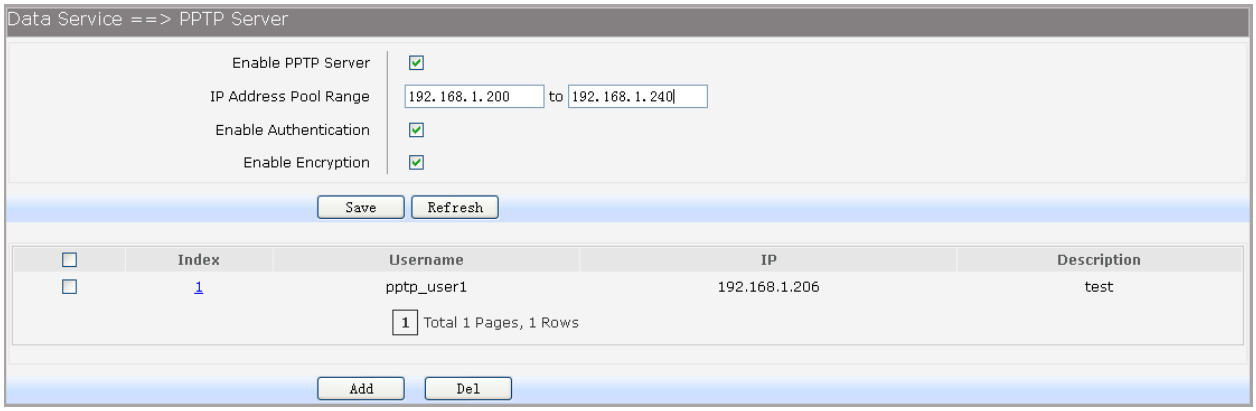


Рисунок 3-72. Настройка PPTP-сервера

Пункты для настройки представлены ниже:

- Enable PPTP Server: включение или отключение PPTP-сервера

- IP Address Pool Range: настройка пула IP-адресов. Первый адрес пула не должен быть больше последнего, диапазоны не должны перекрываться друг с другом.
- Enable Authentication: настройка проверки подлинности при создании туннеля.
- Enable Encryption: настройка шифрования туннеля. Если стоит флажок будет использоваться метод шифрования MPPE.

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-73.

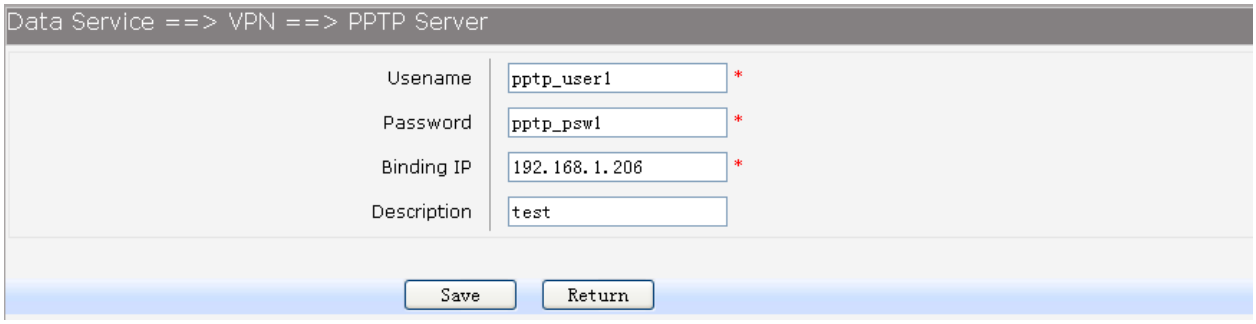


Рисунок 3-73. Создание или редактирование учетной записи PPTP-клиента.

Пункты для настройки представлены ниже:

- Username: настройка имени пользователя для создания PPTP-туннеля. Имя пользователя должно быть одинаковым на сервере и клиенте.
- Password: настройка пароля пользователя для создания PPTP-туннеля. Пароль должен быть одинаковым на сервере и клиенте.
- Binding IP: настройка IP-адреса для подключения к PPTP-серверу.
- Description: настройка описания учетной записи.

3.4.6.2 Настройка L2TP-сервера

Для настройки L2TP-сервера, выберите в меню пункты Data Service→VPN →L2TP Server.

Пункты для настройки представлены ниже:

- Enable L2TP Server: включение или отключение L2TP-сервера
- Local IP: настройка локального IP-адреса сервера.
- IP Address Pool Range: настройка пула IP-адресов. Первый адрес пула не должен быть больше последнего, диапазоны не должны перекрываться друг с другом.
- Enable Authentication: настройка проверки подлинности при создании туннеля. Если проверка включена, необходимо ввести секретный ключ.
- Enable Debug: включение режима отладки L2TP-туннеля.

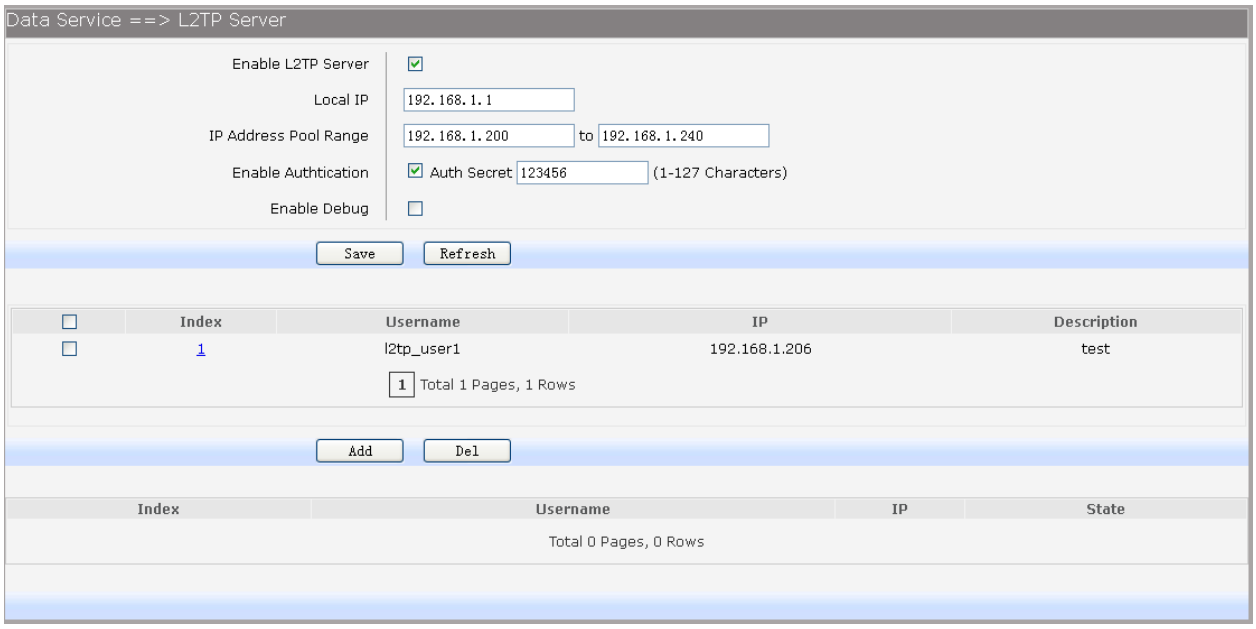


Рисунок 3-74. Настройка L2TP-сервера.

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-75.

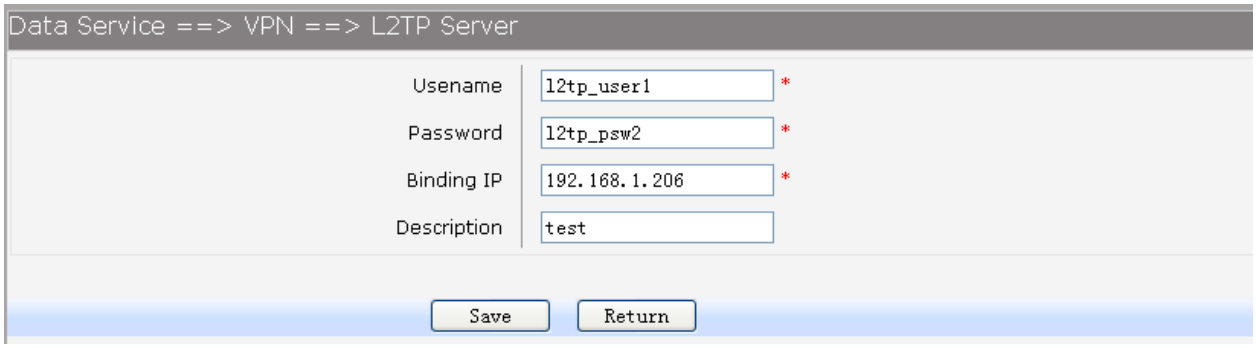


Рисунок 3-75. Создание или редактирование учетной записи L2TP-клиента.

Пункты для настройки представлены ниже:

- Username: настройка имени пользователя для создания L2TP-туннеля. Имя пользователя должно быть одинаковым на сервере и клиенте.
- Password: настройка пароля пользователя для создания L2TP-туннеля. Пароль должен быть одинаковым на сервере и клиенте.
- Binding IP: настройка IP-адреса для подключения к L2TP-серверу.
- Description: настройка описания учетной записи.

3.4.7 Настройка маршрутизации

3.4.7.1 Статическая маршрутизация

3.4.7.1.1 Маршрутизация IPv4

Для настройки IPv4 маршрутизации, выберите в меню пункты Data Service→Routing→Static Route→IPv4.

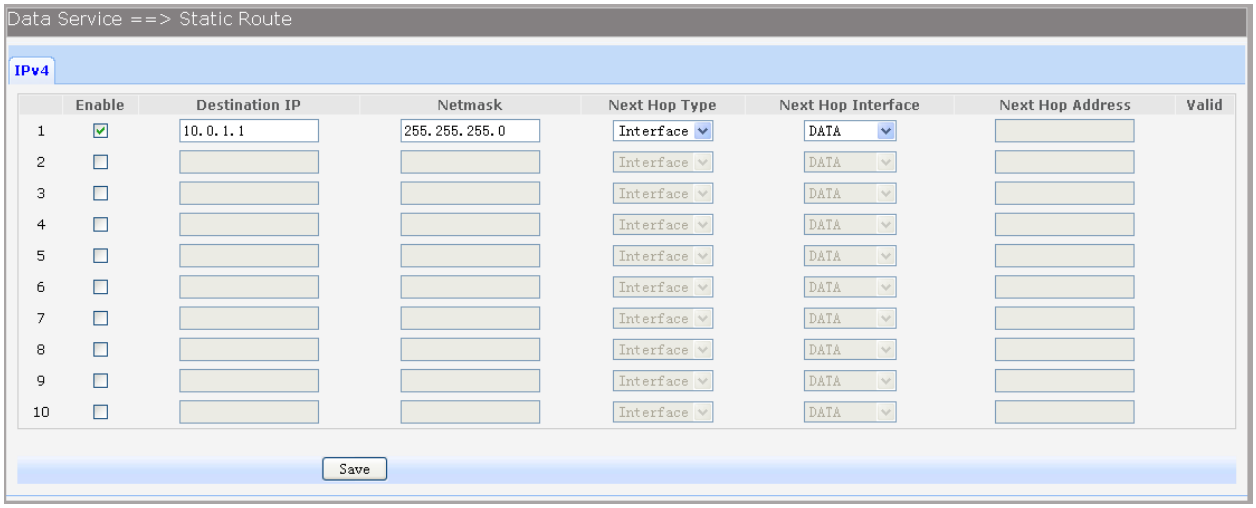


Рисунок 3-76. Настройка IPv4 маршрутизации

Пункты для настройки представлены ниже:

- Enable: поставьте флажок для включения и настройки нового статического маршрута или отключения действующего.
- Destination IP: настройка IP-адреса назначения.
- Netmask: настройка маски подсети для сети назначения.
- Next Hop Type: Next hop interface или Next hop address.
- Next Hop Interface: настройка интерфейса, через который пойдет маршрут на следующий хоп.
- Next Hop Address: настройка IP-адреса следующего хопа для маршрута.
- Valid: показывает статус маршрута.

3.4.7.1.2 Маршрутизация IPv6

Если меню IPv6 маршрутизации скрыто, значит, не включена работа IPv6 стека, настройки стека описаны в главе 2.3.6.3 настоящего руководства. Для настройки IPv6 маршрутизации, выберите в меню пункты Data Service→Routing→Static Route→IPv6.

Конфигурация маршрутизации IPv6 более простая, нежели IPv4. Для включения статического маршрута достаточно поставить флажок и задать длину префикса, эквивалентную маске сети в протоколе IPv4.

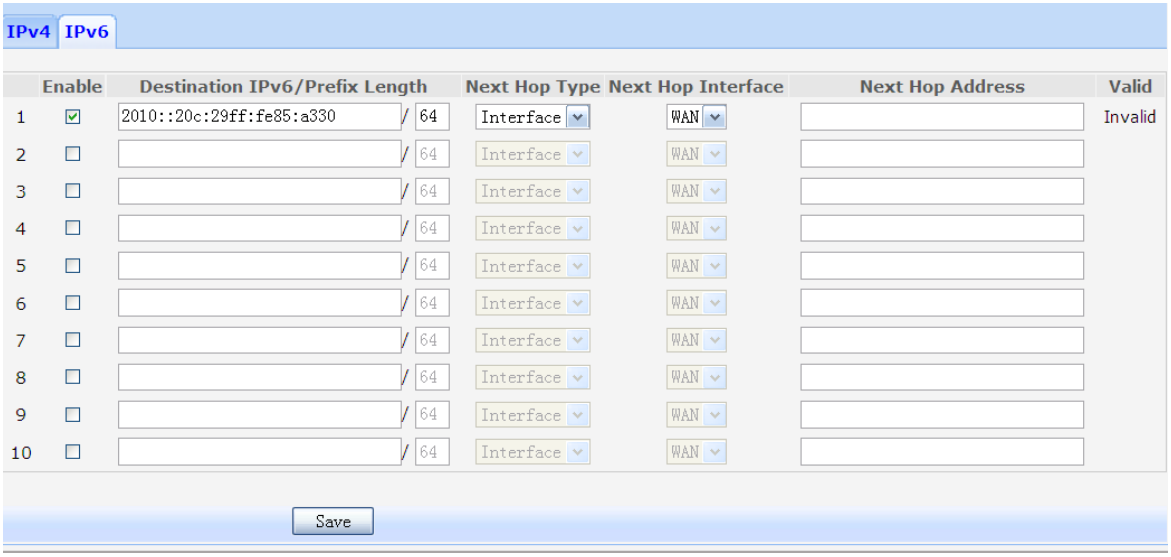


Рисунок 3-77. Настройка IPv6 маршрутизации

3.4.7.2 Настройка политик маршрутизации

Для настройки выберите в меню пункты Data Service→Routing→Policy Route.

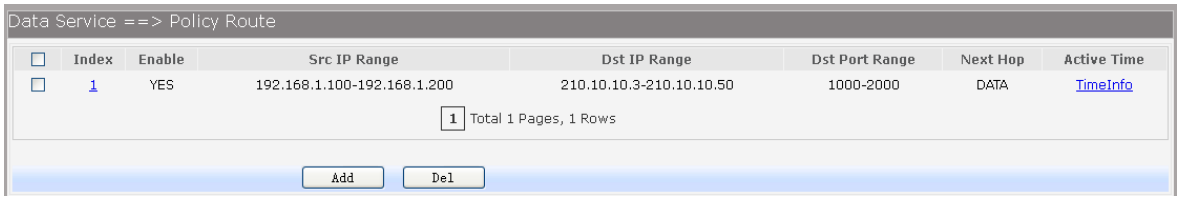


Рисунок 3-78. Просмотр политик маршрутизации

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-79.

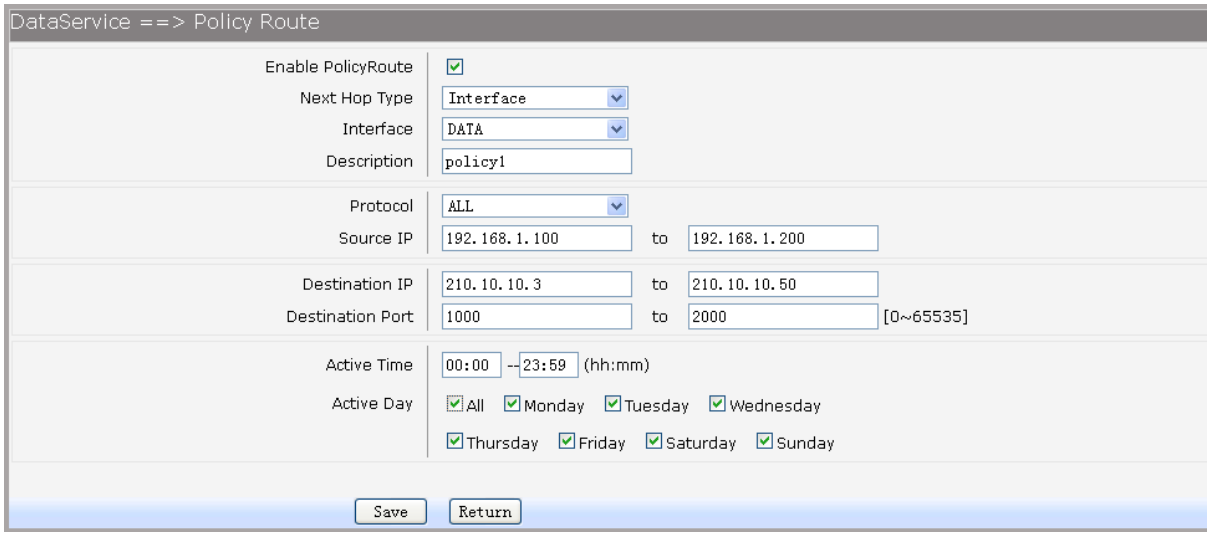


Рисунок 3-79. Добавление или редактирование записи политики маршрутизации

Пункты для настройки представлены ниже:

- Enable PoliceRoute: включение или отключение политики.
- Next Hop Type: interface или address.
- Interface: настройка интерфейса, через который пойдет маршрут на следующий хоп.
- Address: настройка IP-адреса следующего хопа для маршрута.
- Description: описание политики.
- Protocol: настройка протокола на который распространяется политика (TCP, UDP или ALL).
- Source IP: настройка пула адресов источника.
- Destination IP: настройка пула адресов назначения.
- Destination port: настройка пула портов назначения.
- Active Time: время работы политики.
- Active Day: настройка дней работы политики.

3.4.7.3 Настройка RIP

RIP один из самых простых и старых дистанционно-векторных протоколов маршрутизации, который оперирует хопами в качестве метрики маршрутизации. Для настройки выберите в меню пункты Data Service→RIP→RIP Service.

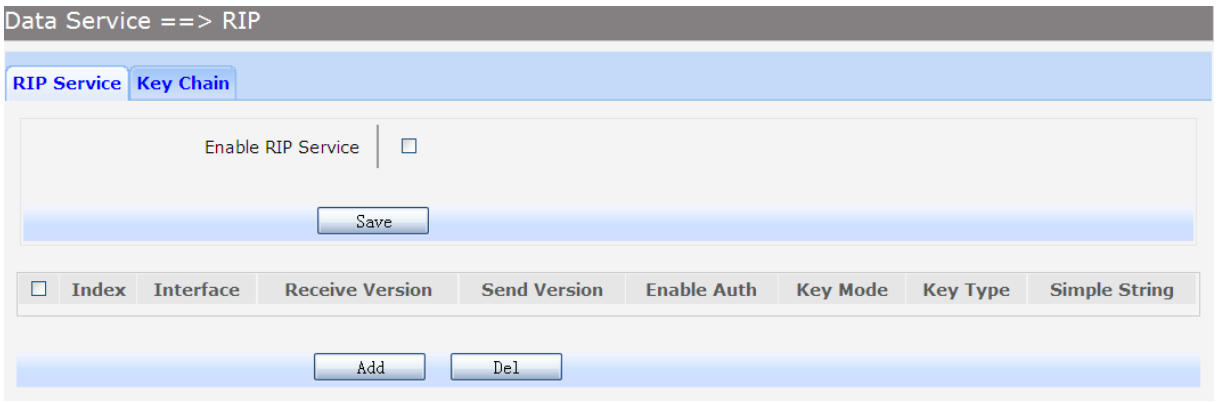


Рисунок 3-80. Настройка RIP

Поставьте флажок напротив Enable RIP Service для глобального включения RIP маршрутизации. Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-81.

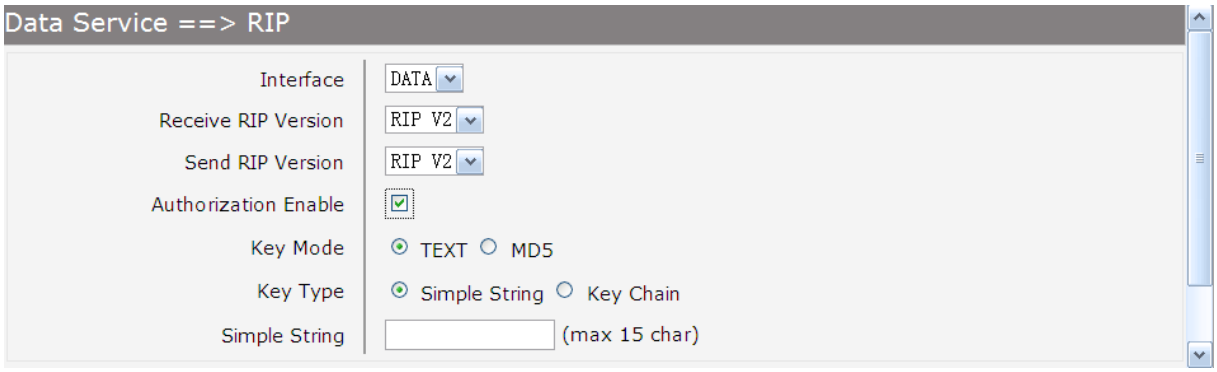


Рисунок 3-81. Создание или редактирование RIP маршрутизации

Пункты для настройки представлены ниже:

- Interface: настройка интерфейса.
- Receive RIP Version: настройка версии протокола для получения служебных пакетов (RIPv1 или RIPv2).
- Send RIP Version: настройка версии протокола для отправки служебных пакетов (RIPv1 или RIPv2).
- Authorization Enable: включение авторизации.
- Key Mode: настройка метода шифрования ключа (TEXT или MD5)
- Key Type: настройка ключа Simple String или Key Chain.
- Simple String: если выбран режим Simple String в пункте Key Type, введите строку, которая будет использоваться в качестве ключа.

Для настройки Key Chain авторизации выберите в меню пункты Data Service→RIP→Key Chain.

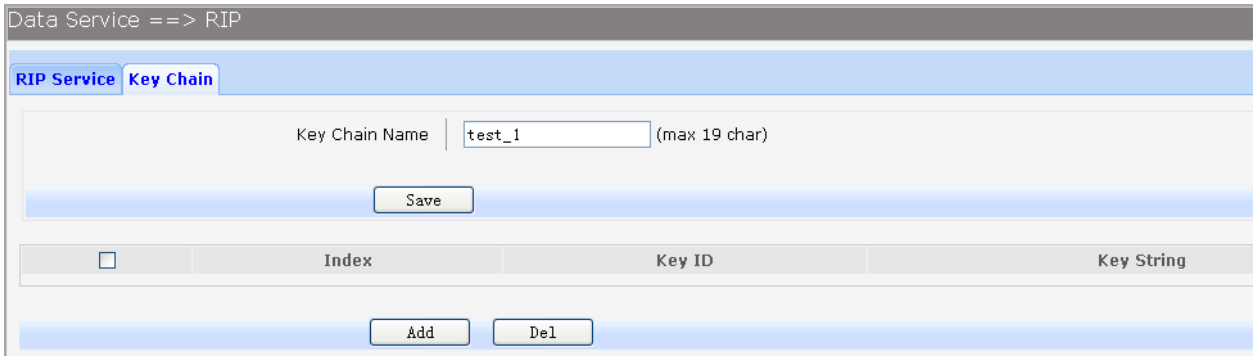


Рисунок 3-82. Просмотр настроек Key Chain авторизации

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-83.

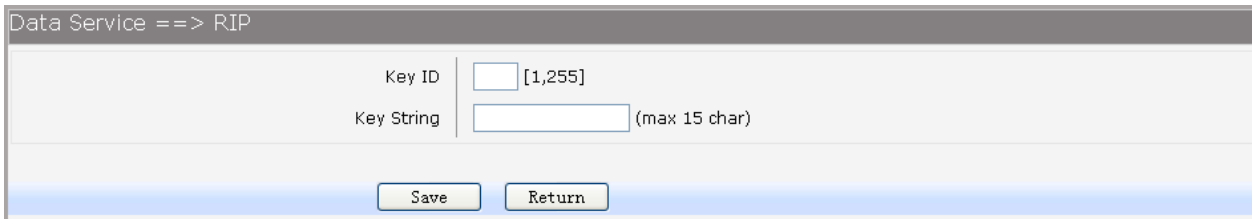


Рисунок 3-83. Добавление или редактирование записей Key Chain

Пункты для настройки представлены ниже:

- Key ID: настройка ID.
- Key String: настройка ключа.

3.4.8 Дополнительные настройки

3.4.8.1 Настройка UPnP

UPnP это технология соединения между персональными компьютерами и интеллектуальными устройствами, установленными, дома (телевизор, приставки, телефоны, планшеты и др.). UPnP обеспечивает автоматическое подключение подобных устройств друг к другу и их совместную работу в сетевой среде, позволяя:

- Просматривать семейные фотографии с помощью телевизора.
- Смотреть домашнее видео.
- Прослушивать музыку по всему дому.

DLNA набор стандартов, позволяющих устройствам в домашней сети передавать и принимать различный мультимедиа контент. Устройства, которые поддерживают спецификацию DLNA, могут настраиваться и объединяться в сеть в автоматическом режиме.

Для настройки параметров UPnP, выберите в меню пункты Data Service→Advanced Parameters→UPnP Parameter.

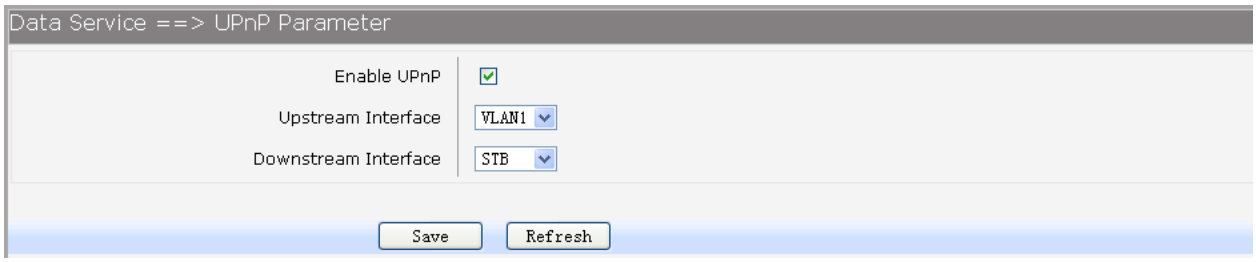


Рисунок 3-84. Настройка UPnP

Пункты для настройки представлены ниже:

- Enable UPnP: глобально включение или отключение функции UPnP.
- Upstream Interface: настройка интерфейса, подключенного к DLNA серверу.

- Downstream Interface: настройка интерфейса, подключенного к DLNA клиенту.

3.4.8.2 Настройка мультикаста

Для настройки IGMP Proxy, выберите в меню пункты Data Service→ Multicast.

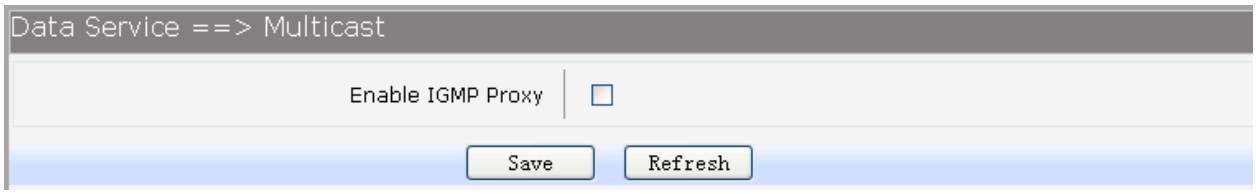


Рисунок 3-85. Настройка мультикаста

Для включения механизма IGMP Proxy, используемого для IPTV, необходимо поставить флажок напротив пункта Enable IGMP Proxy и нажать кнопку Save.

3.4.8.3 Настройка USB-хранилища

Функция организации USB хранилища позволяет обмениваться файлами по FTP или Samba протоколу. Для настройки выберите в меню пункты Data Service→USB Storage.

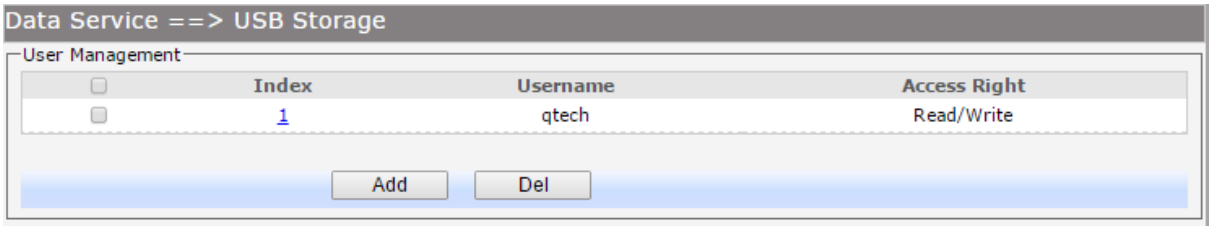


Рисунок 3-86. Просмотр конфигурации пользователей хранилища

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-87.

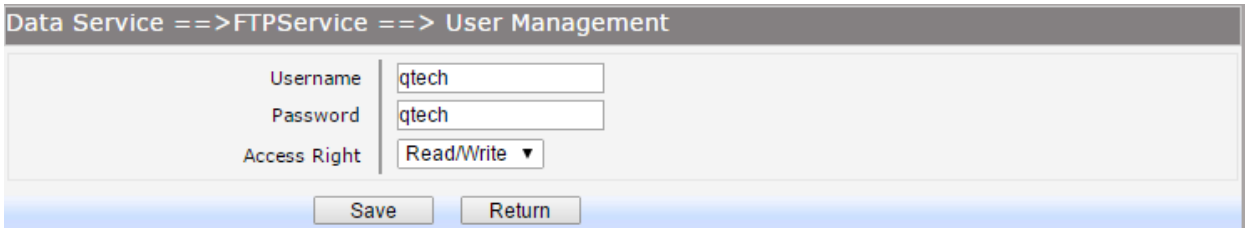


Рисунок 3-87. Добавление или редактирование записей пользователей хранилища

Пункты для настройки представлены ниже:

- Username: настройка имени пользователя.
- Password: настройка пароля для пользователя.
- Access Right: настройка прав доступа для пользователя (Read или Read/Write).

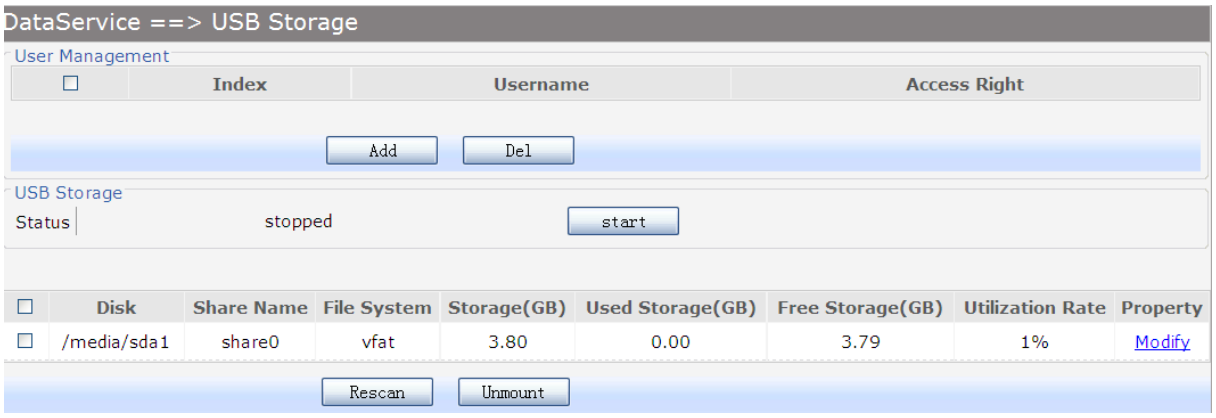


Рисунок 3-88. Просмотр USB-хранилища.

Для сканирования разделов USB нажмите кнопку Rescan. Для отключения хранилища нажмите кнопку Unmount. Для начала работы сервисов FTP и Samba нажмите на кнопку Start. Для настроек доступа пользователям к разделам хранилища нажмите Modify напротив соответствующего раздела, откроется окно, изображенное на рисунке 2-89.

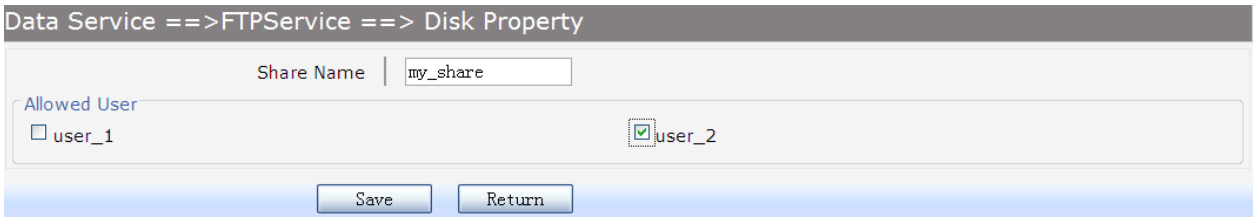


Рисунок 3-89. Настройки раздела хранилища

Пункты для настройки представлены ниже:

- Share name: настройка имени сервера.
- Allowed User: настройка пользователей, которым разрешен доступ к хранилищу. Поставьте флажки для разрешения пользователю доступа к хранилищу.

3.5 Настройка VoIP

Настройки, описанные в данной главе, относятся к настройкам для маршрутизатора модели QFR-300-4G-2V-W-U, имеющего 2 FSX-порта и поддерживающего работу VoIP.

3.5.1 Настройка сервиса SIP

SIP (Session Initiation Protocol) – протокол установления сеанса, описывающий способ установления и завершения сеансов для обмена мультимедийным содержимо поверх IP-сетей. Для настройки выберите в меню пункты VOIP Service→SIP Service. Откроется окно, изображенное на рисунке 2-90.

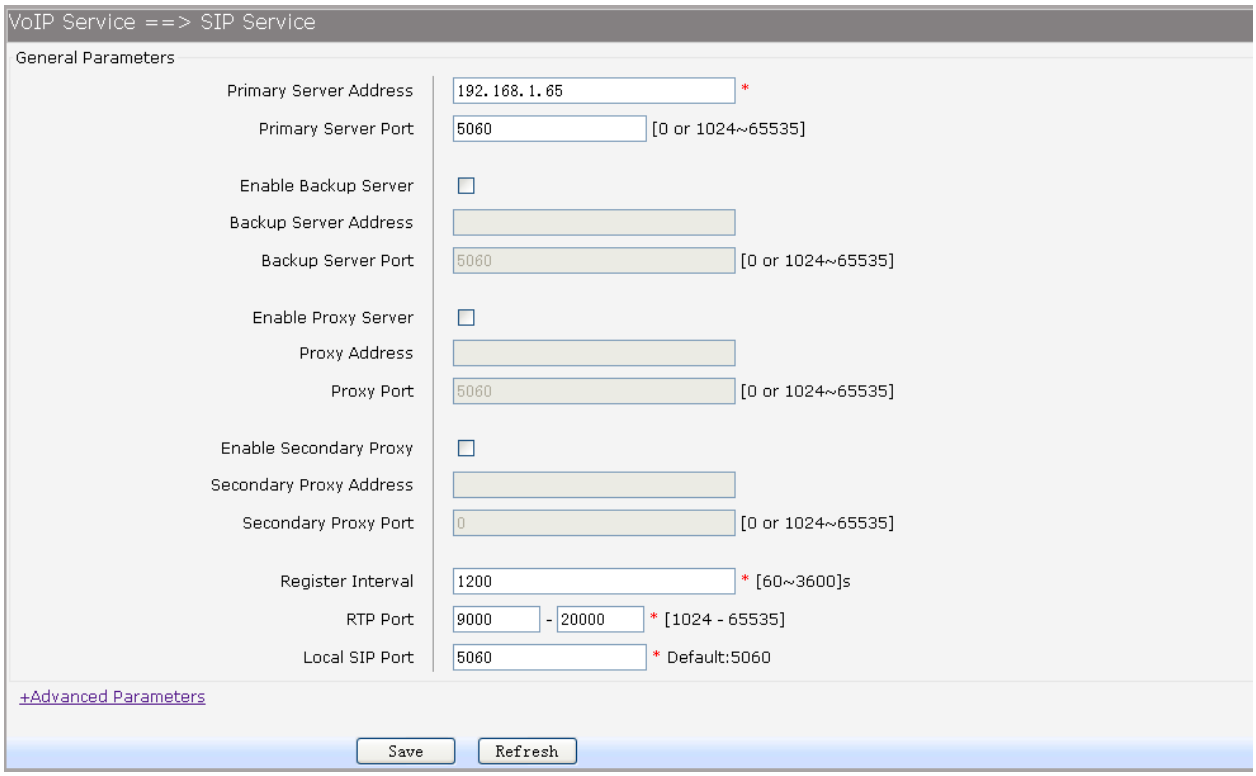


Рисунок 3-90. Настройка основных параметров сервиса SIP.

Пункты для настройки представлены ниже:

- Primary Server Address: имя домена или IP-адрес SIP сервера.
- Primary Server Port: порт сервера.
- Enable Backup Server: включение или отключение резервного SIP сервера.
- Backup Server Address: имя домена или IP-адрес резервного SIP сервера.
- Backup Server Port: порт резервного сервера.
- Enable Proxy Server: включение или отключение прокси-сервера.
- Proxy Address: имя домена или IP-адрес прокси-сервера.
- Proxy Port: порт прокси-сервера.
- Enable Secondary Proxy: включение или отключение резервного прокси-сервера.
- Secondary Proxy Address: имя домена или IP-адрес резервного прокси-сервера.
- Secondary Proxy Port порт резервного прокси-сервера.
- Register Interval: настройка интервала через который SIP UA посылает сообщения о перерегистрации.
- RTP Port: пул портов для RTP соединений.

- Local SIP Port: локальный порт для SIP соединений.

Для просмотра и настроек дополнительных параметров нажмите на +Advanced Parameters, откроется страница, изображенная на рисунке 2-91.

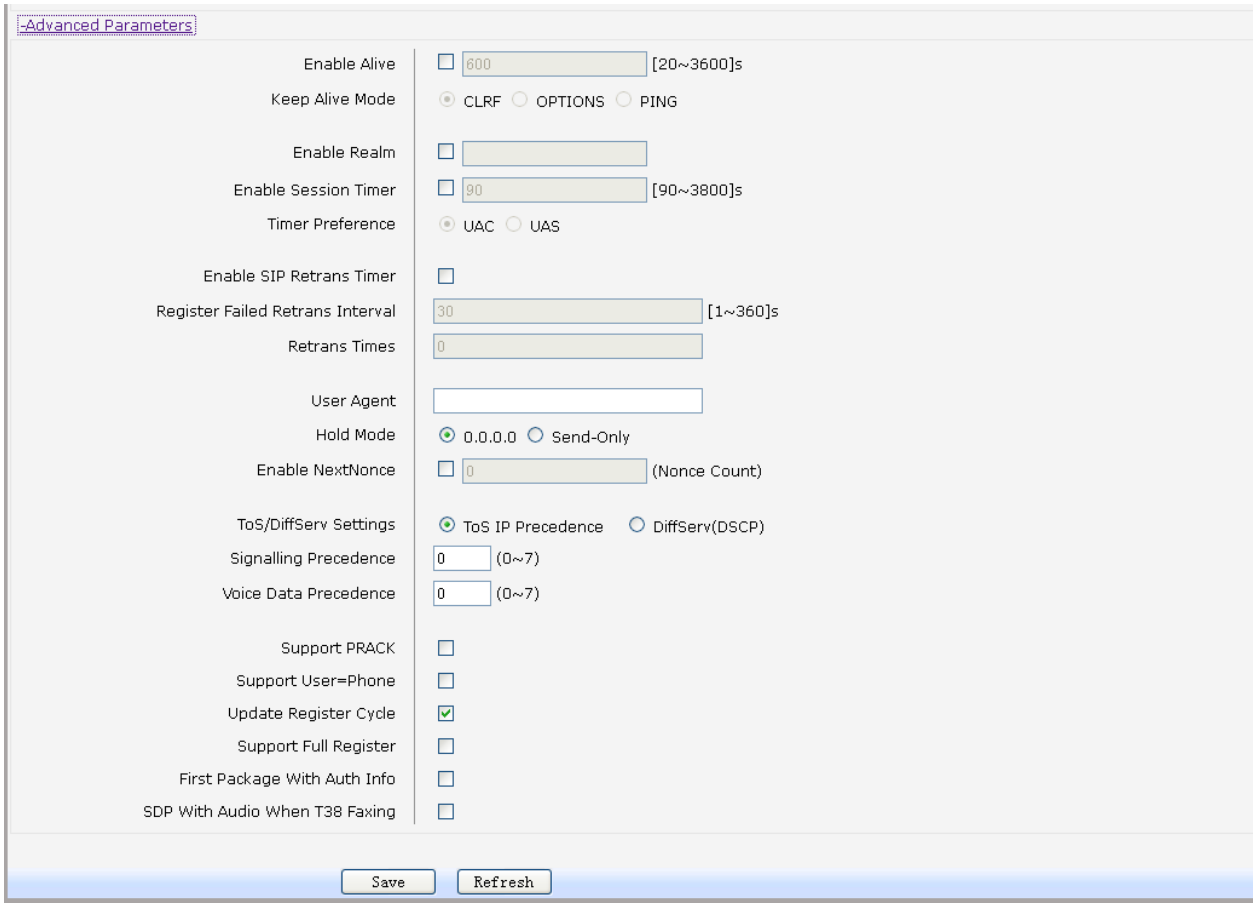


Рисунок 3-91. Настройка дополнительных параметров SIP-сервиса

Пункты для настройки представлены ниже:

- Enable Alive: включение отправки keep-alive пакетов после успешной регистрации на SIP-сервере.
- Keep Alive Mode: настройка режима отправки keep-alive пакетов (CLRF, OPTIONS или PING).
- Enable Realm: включение отправки сигнальных SIP пакетов содержащих информацию realm.
- Enable Session Timer: включение или отключения режимов обновления сессии и настройка времени для режимов (доступны режимы UAC или UAS).
- Enable SIP Retrans Timer: настройка включения режима, начинающего повторную инициализацию сессии при неудаче регистрации на SIP-сервере. Пункт включает

настройки интервалов, через которые будет происходить повторная инициализации сессии.

- User Agent: включение добавления в сигнальный пакет информации о User Agent.
- Hold Mode: настройка параметра call hold в сигнальном пакете.
- Enable Next Nonce: включение SIP пакетов с nonce информацией.
- Support PRACK: включение или отключение предварительного ответа.
- Support User=Phone: включение или отключение отправки сигнальных SIP-пакетов с информацией User = Phone.
- Update Register Cycle: включение или отключение регистрации на основе ответов от сервера об обновлении срока регистрации.
- Support Full Register: включение или отключение режима полной регистрации.
- First Package With Auth Info: включение отправки первого регистрационного пакета с информацией об аутентификации.
- SDP With Audio When T38 Faxing: включение передачи сигнальных пакетов факса по протоколу T38 с аудиоинформацией.

3.5.1.1 Настройка пользователей

Для настройки выберите в меню пункты VOIP Service→User→User.

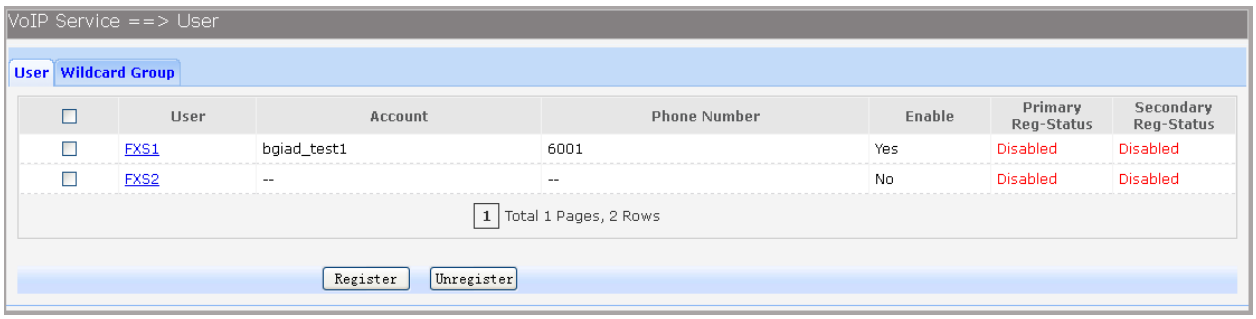


Рисунок 3-92. Настройка пользователей.

Нажмите кнопку Register для запуска регистрации на SIP-сервере. Нажмите кнопку Unregister для отмены регистрации на SIP-сервере. Для редактирования записи пользователя нажмите на соответствующего пользователя в столбце User. Откроется окно, изображенное на рисунке 2-93.

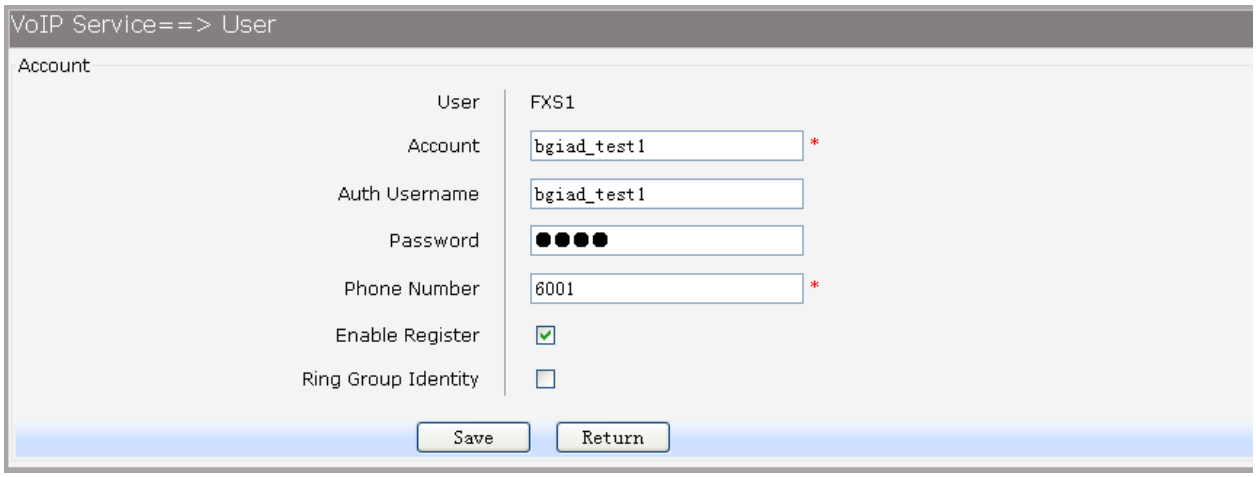


Рисунок 3-93. Настройка пользователя

Пункты для настройки представлены ниже:

- Account: имя аккаунта на SIP-сервере.
- Auth Username: имя пользователя аккаунта на SIP-сервере.
- Password: пароль для аккаунта.
- Phon Number: номер абонентской линии.
- Enable Register: включение регистрации аккаунта.
- Ring Group Identity: настройка телефона для одой сервисной группы.

3.5.1.2 Настройка групп

Для настройки выберите в меню пункты VOIP Service→User→Wildcard Group.

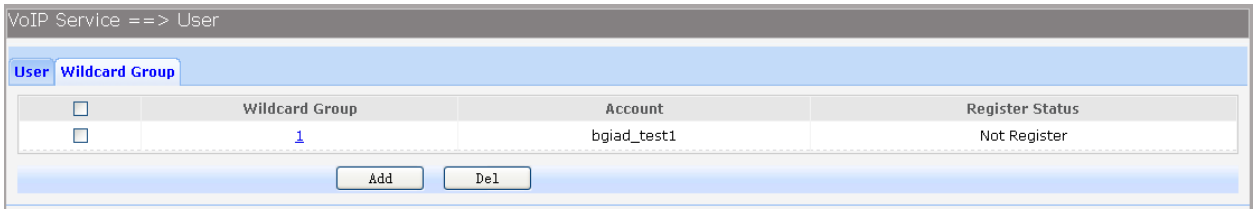


Рисунок 3-94. Настройка групп,

Для редактирования записей нажмите на соответствующий индекс редактируемой записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-95. Для включения групповой регистрации поставьте флажок в пункте Enable Group Register и нажмите клавишу Save.

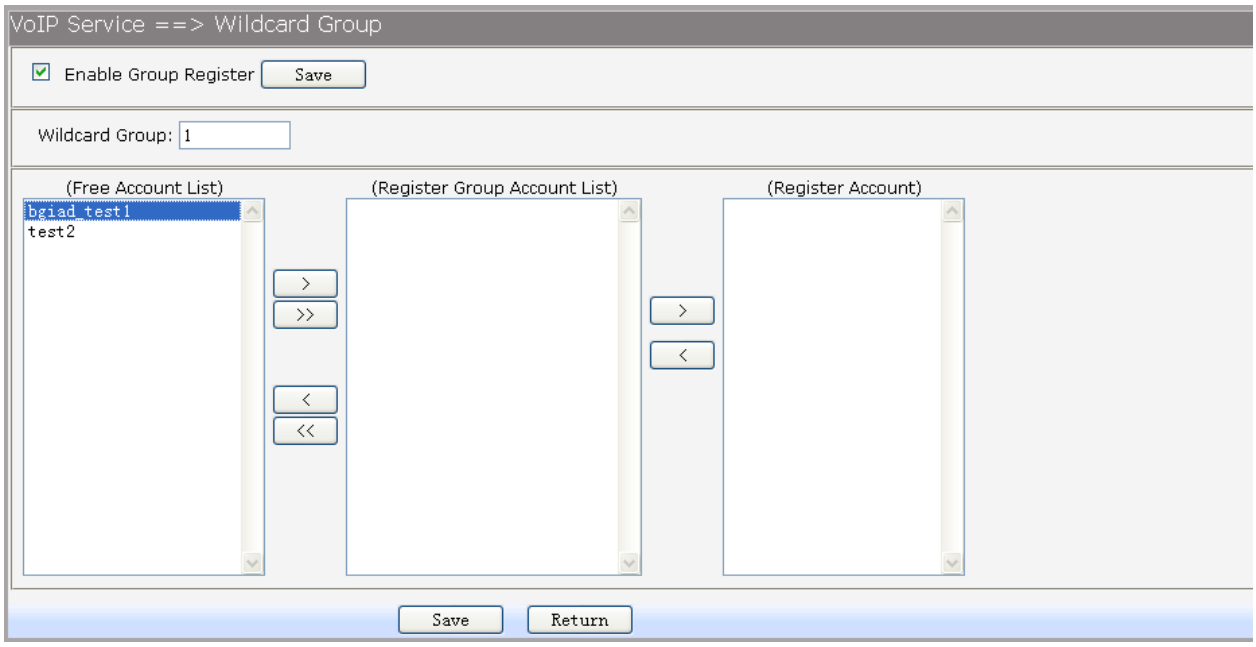


Рисунок 3-95. Добавление или настройка групп

3.5.1.3 Дополнительные настройки пользователей

Для просмотра дополнительных настроек пользователя, выберите в меню пункты VOIP Service→Supplementary.

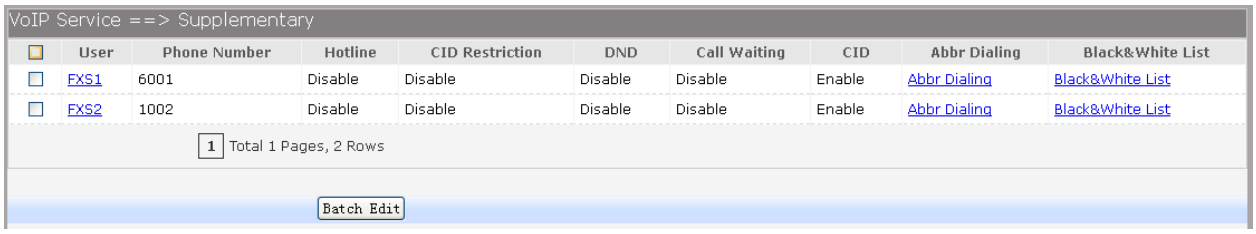


Рисунок 3-96. Просмотр дополнительных настроек пользователей

Для редактирования записей нажмите на соответствующее имя пользователя. Откроется окно, изображенное на рисунке 2-96.

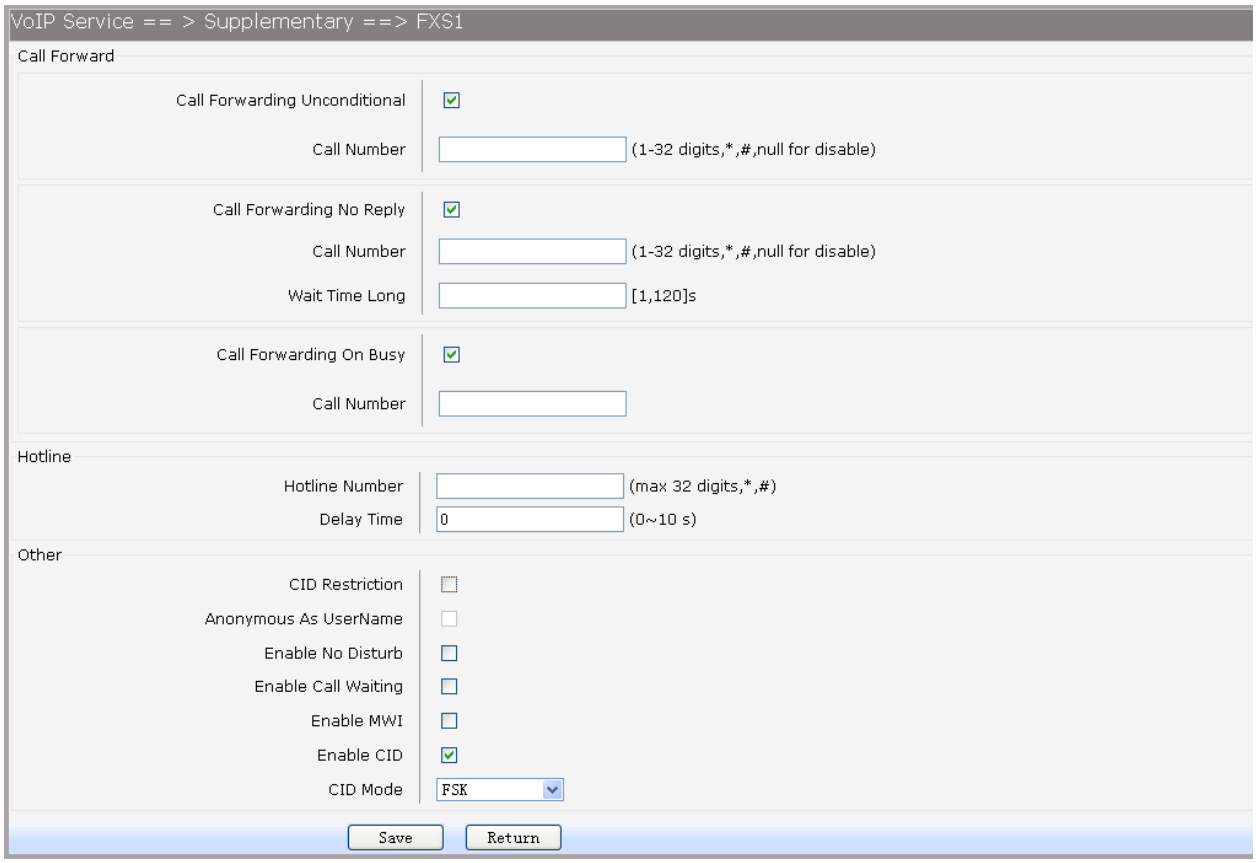


Рисунок 3-97. Редактирование дополнительной конфигурации

Пункты для настройки представлены ниже:

- Call Forwarding Unconditional: включение или отключение безусловной переадресации. Если механизм включен, введите номер для переадресации. Для этого введите *57*номер телефона#. Вызов будет переадресован на указанный норме. Отключить переадресацию можно набрав #57#.
- Call Forwarding No Reply: включение или отключение переадресации при не ответе. Если механизм включен, введите номер для переадресации. Для этого введите *41*номер телефона#. Вызов будет переадресован на указанный норме. Отключить переадресацию можно набрав #41#. Пункт Wait Time Long настраивает интервал, через который вызов будет переадресован.
- Call Forwarding On Busy: включение или отключение переадресации при занятой линии. Если механизм включен, введите номер для переадресации. Для этого введите *40*номер телефона#. Вызов будет переадресован на указанный норме. Отключить переадресацию можно набрав #40#.
- Hotline Number: настройка функции номера горячий линии. Для выключения функции оставьте поле пустым.
- Delay Time: настройка времени задержки горячей линии.

- CID Restriction: включение или отключение ограничения CID.
- Enable No Distrub: включение или отключении функции не беспокоить, позволяющей блокировать входящие вызовы.
- Enable Call Waiting: включение или отключение функции ожидания вызова. Если при разговоре поступит новый вызов, прозвучит звуковой сигнал.
- Enable MWI: включение или отключение функции MWI.
- Enable CID: включение или отключение отправки информации CID на телефон.
- CID Mode: настройка режима CID (FSK или DTMF).

Настройка сокращенного набора номера позволяет хранить выбранные телефонные номера для легкого и быстрого набора. Каждый номер может быть набран с помощью одного или двух символьного префикса. Сохраненные номера могут содержать до 32 символов. Если вы хотите добавить или удалить сокращенные номера набора нажмите Abbr. Dialing. откроется окно, изображенное на рисунке 2-98.

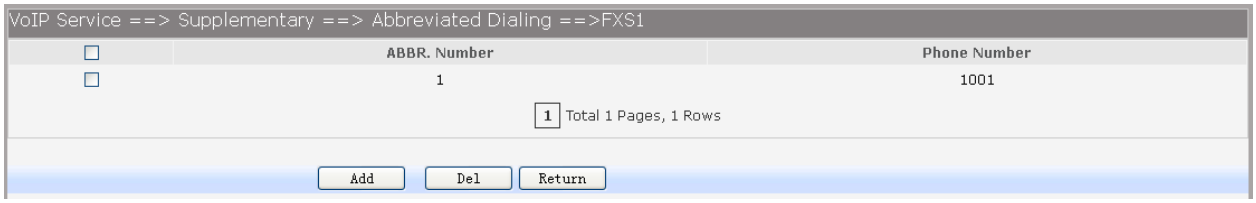


Рисунок 3-98. Просмотр списка коротких номеров

В столбце ABBR.Number представлен короткий номер, в столбце Phone Number номер который будет вызван при наборе короткого номера. Для удаления короткого номера, выберите запись и нажмите кнопку Del. Для добавления номера нажмите кнопку Add.

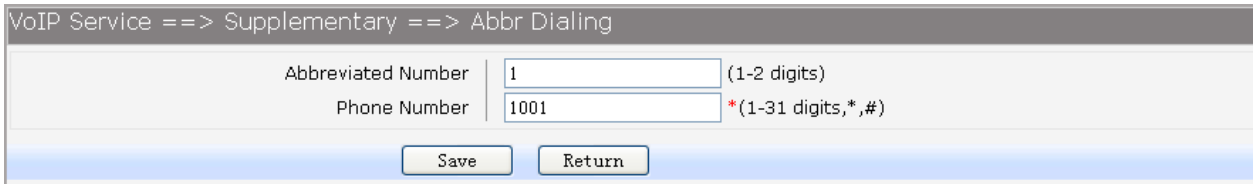


Рисунок 3-99. Настройка короткого номера

Для настройки списка черных/белых номеров нажмите на Black&White List.

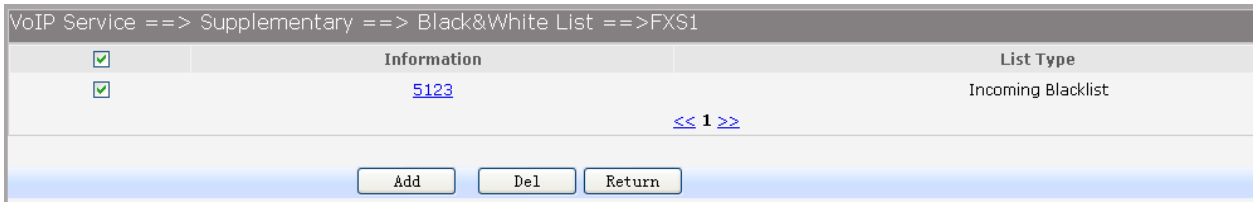


Рисунок 3-100. Список черных/белых номеров

Для редактирования записей нажмите на соответствующий индекс в столбце Information. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add.

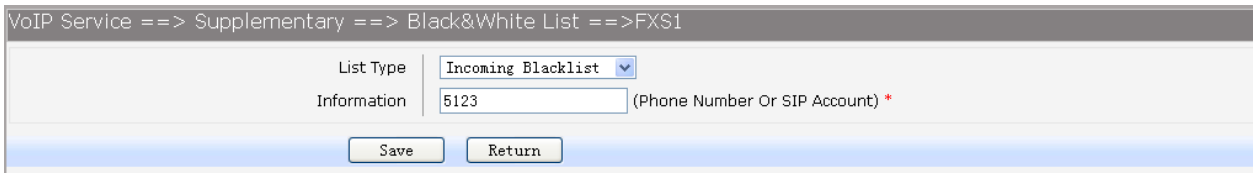


Рисунок 3-101. Добавление и редактирование списка черных/белых номеров

Пункты для настройки представлены ниже:

- List Type: выберите режим работы настраиваемой записи (Incoming Blacklist, Incoming Whitelist, Outgoing Blacklist, Outgoing Whitelist).
- Information: введите номер телефона или SIP-аккаунта.

3.5.2 Настройка параметров кодеков

Интервал пакетизации определяет минимальную задержку «из конца в конец». В более длинных пакетах под заголовок отводится относительно меньшая часть байтов, но они вызывают большую задержку и делают потери пакетов более значимыми. Для настройки параметров пакетизации, выберите в меню пункты VOIP Service→Codec Parameters.

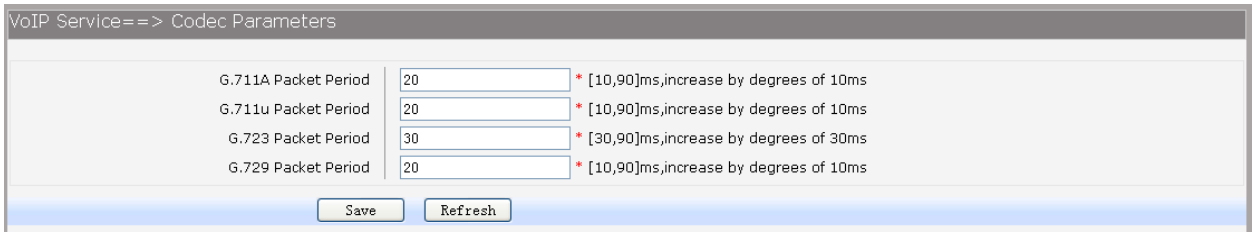


Рисунок 3-102. Настройка интервала пакетизации.

Пункты для настройки представлены ниже:

- G.711A Packet Period: настройка интервала пакетизации для кодека G.711A.
- G.711u Packet Period: настройка интервала пакетизации для кодека G.711.
- G.723 Packet Period: настройка интервала пакетизации для кодека G.723.
- G.729 Packet Period: RTP настройка интервала пакетизации для кодека G.729.

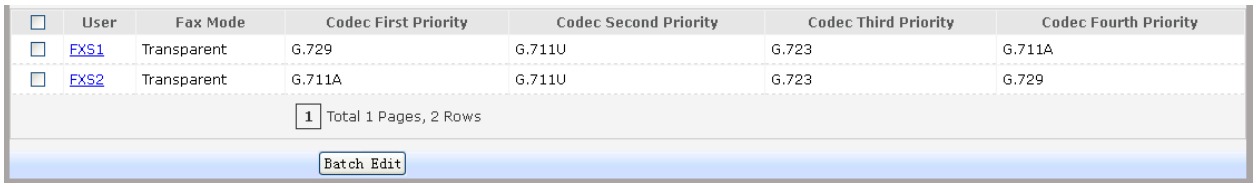


Рисунок 3-103 Просмотр используемых кодеков

Для редактирования режима отправки факса или приоритета кодеков для пользователей, нажмите на запись пользователя. Откроется окно, изображенное на рисунке 2-104.

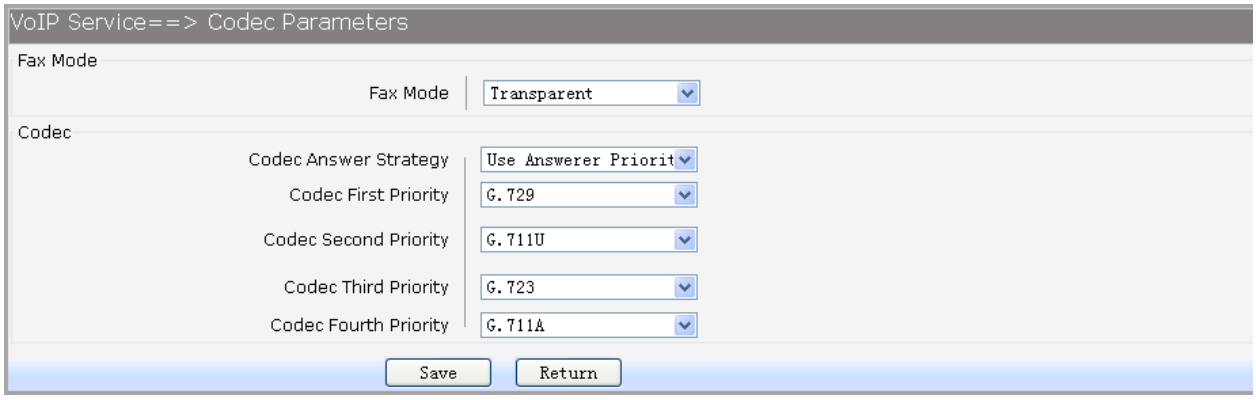


Рисунок 3-104. Настройка режима работы факса и приоритетов кодеков

Пункты для настройки представлены ниже:

- Fax Mode: выбор режима работа факса (Transparent, T38 или VBD).
- Codec Answer Strategy: предусмотрено два режима работы
  - Use Answerer Priority: выбор кодека происходит на основе настроенных приоритетов кодеков.
  - Use Offerer Priority: решение о выборе кодека происходит на основе приоритета настроенного у абонента.
    - Code Priority: пункты настройки приоритетов кодеков доступны, если ранее выбран пункт Use Answerer Priority.

3.5.3 Настройка параметров DSP

Для настройки параметров DSP, выберите в меню пункты VOIP Service→DSP Parameters. Откроется окно, изображенное на рисунке 2-105.

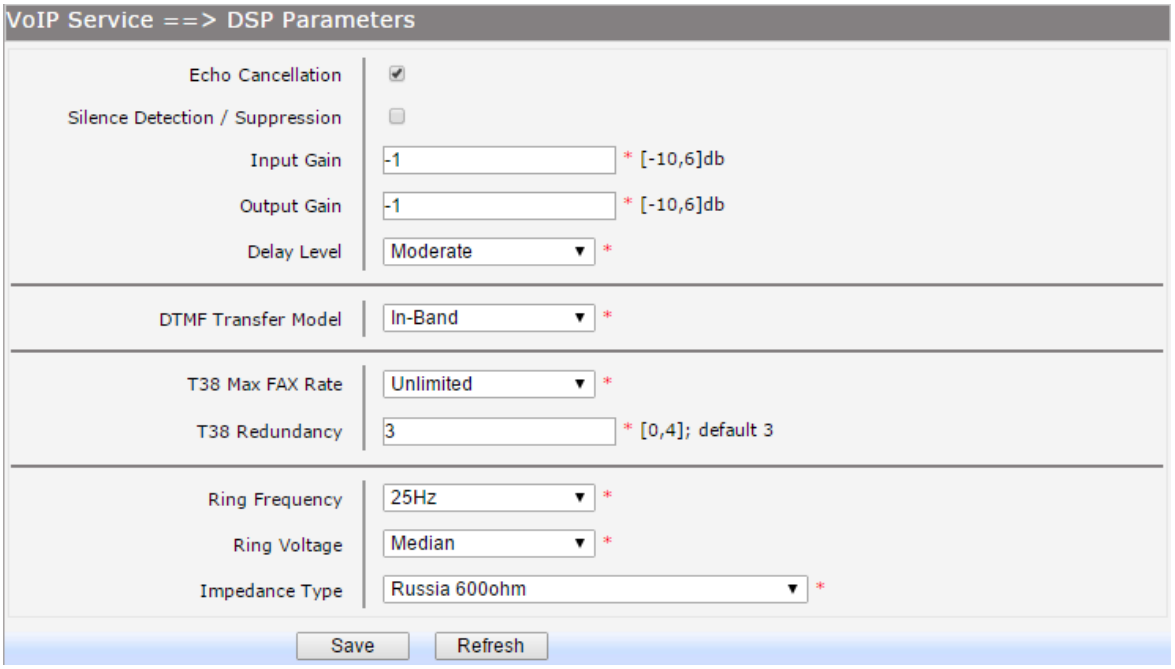


Рисунок 3-105. Настройка параметров DSP

Пункты для настройки представлены ниже:

- Echo Cancellation: включение или отключения механизма подавления эха.
- Silence Detection/Suppression: включение или отключение механизма шумоподавления.
- Input Gain: настройка значения входного усиления.
- Output Gain: настройка значений выходного усиления.
- Delay Level: настройка уровня задержки. (Minimum, Smaller, Moderate, Larger, Maximum).
- DTMF Transfer Model: настройка режима передачи (In-Band, INFO, RFC2833).
- RFC2833 Load Type: настройка полезной нагрузки. Пункт доступен если выбран режим передачи RFC2833.
- T38 Max FAX Rate: настройка скорости при использовании факса по протоколу T38 (Unlimited, 2400bps, 4800bps, 7200bps, 9600bps, 12000bps, 14400bps).
- T38 Signaling Redundancy: настройка избыточности сигнала T38.
- T38 Data Redundancy: настройка избыточности передаваемых данных по протоколу T38.
- Ring Frequency: частота звонка (20Hz, 25Hz).
- Impedance Type: настройка стандарта сопротивления.

3.5.4 Настройка плана нумерации (Digit Map)

План нумерации определяет будет ли номер отправлен SIP приложением. Используется для определения достаточно ли пользователь ввел цифр для совершения вызова на разрешенные номера. Если количество введенных пользователем цифр соответствует количеству, определенному в плане, вызов будет совершен. В противном случае, вызов будет сброшен по истечению таймаута ввода номера. Если число введённых цифр совпадает с планом нумерации, вызов будет сразу же совершен, если количество меньше, то устройство продолжает ждать ввода дополнительных цифр. Символы, используемые для составления плана нумерации представлены в таблице 2-5.

Таблица 3-5. Символы плана нумерации

Символ	Описание символа
0 до 9	Цифры разрешенные в плане нумерации
X	Универсальная маска, означающая любую цифру, исключая символы “*” и “#”
*	Знак звездочки
#	Знак решетки
-	Символ ставится между диапазоном значений
[]	Квадратные скобки указывают на диапазон номеров
.	Символа “.” используется для описания номеров произвольной длинны
|	Символ таймаута Inter-digit
T	Символ завершения таймаута Inter-digit
S	Символ Short таймаута, ставиться в середине описания номера.

Например, распишем представленный план нумерации:

8XXXXXXX|1[0-24]0|2[18].3|3XXSXX|[0-9*#][0-9*#][0-9*#].#|[0-9*#].T

- 8XXXXXXX - описывает номера, начинающиеся с 8 и содержащие 8 символов.
- 1[0-24]0 – описывает номера 100, 110, 120 и 140.
- 2[18].3 – описывает номера которые начинаются на 2 и заканчиваются на 3, они могут произвольной длины и содержать 1 или 8 после первой цифры (23, 213, 2183).
- 3XXSXX – описывает номера, начинающиеся с 3 длинна которых может 3 или 5 символов. Если истечет таймаут Short при наборе между 3 и 4 цифрой, будет отправлен номер из 3 символов.

- [0-9*#][0-9*#][0-9*#].# - описывает номера заканчивающиеся # и длинной не менее 2 символов.
- [0-9*#].T – описывает номера с любым количеством символов, номер будет набираться пока не истечет таймаут Inter-digit

Для настройки плана нумерации, выберите в меню пункты VOIP Service→Digitmap. Откроется страница, изображенная на рисунке 2-106.

Пункты для настройки представлены ниже:

- Enable: включение или отключения плана номеров.
- Short Timer: настройка Short таймаута.
- Digit Map: настройка правила плана номеров.

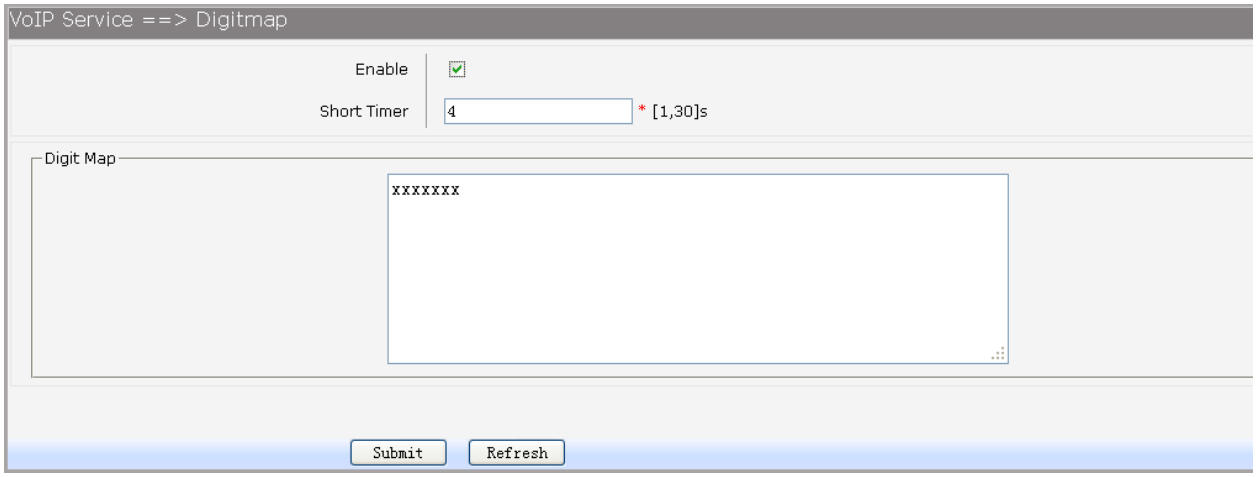


Рисунок 3-106. Настройка плана номеров.

3.5.5 Настройка тонового сигнала

Для настройки выберите в меню пункты VOIP Service→Signal Tone. Откроется окно, изображенное на рисунке 2-107.

Пункт Tone Type позволяет выбрать стандартные настройки. Если требуется пользовательская настройка частоты сигналов, необходимо поставить флажок в пункте User Defined Enable, напротив настройки соответствующего тонового сигнала (dial tone, busy tone, ring back tone).

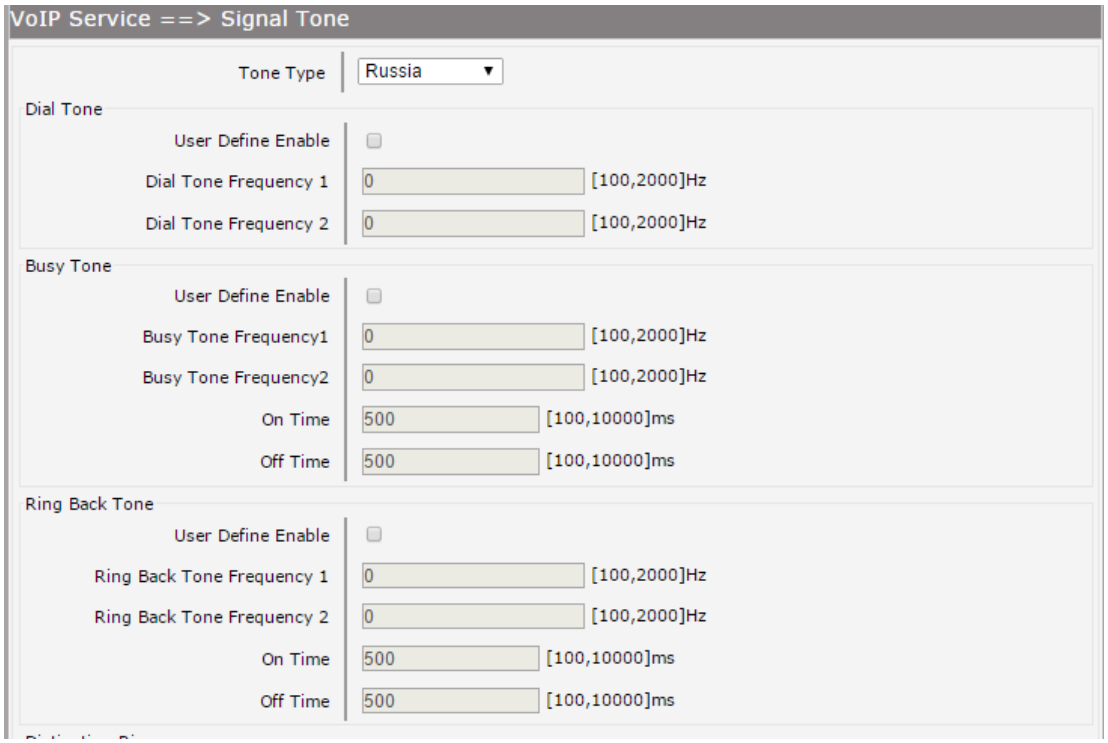


Рисунок 3-107. Настройка тонового сигнала.

3.5.6 Настройка параметров FXS

Для настройки параметров FXS выберите в меню пункты VOIP Service→FXS Parameters. Откроется окно, изображенное на рисунке 2-108.

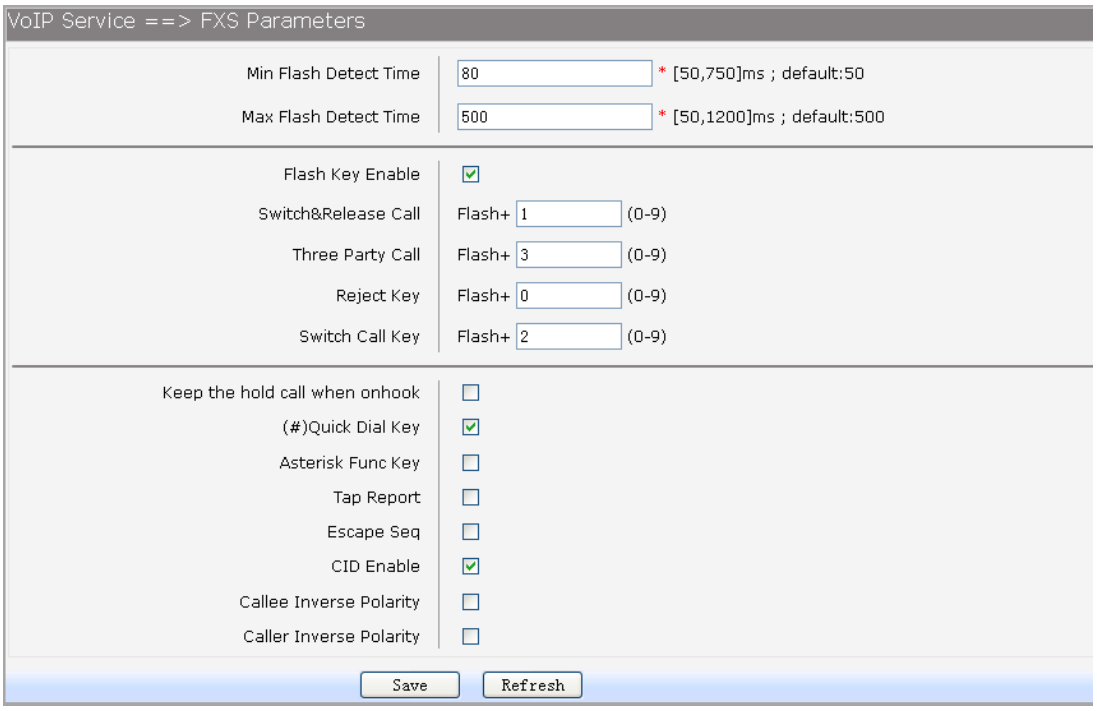


Рисунок 3-108. Настройка FXS

Пункты для настройки представлены ниже:

- Min Flash Detect Time: настройка минимального времени обнаружения нажатия кнопки Flash.
- Max Flash Detect Time: настройка максимального времени обнаружения нажатия кнопки Flash.
- Flash Key Enable: включение или отключение режима обнаружения нажатий цифровых кнопок, после нажатия кнопки Flash.
- Switch&Release Call: настройка символа. При нажатии Flash+символ произойдет прием вызова и перевод его режим Hold.
- Three Party Call: настройка символа. При нажатии Flash+символ произойдет включение конференцсвязи.
- Reject Key: настройка символа. При нажатии Flash+символ произойдет отклонение вызова.
- Switch Call Key: настройка символа. При нажатии Flash+символ произойдет перевод активного вызова в режим Hold и восстановление вызова, находящегося в режим Hold.
- Keep the hold call when onhook: включение функции уведомления пользователя о том, что есть еще один вызов в режиме Hold.
- (#)Quick Dial Key: настройка немедленной отправки номера после нажатия клавиши решетка “#”.
- Asterisk Func Key: включение использование клавиши звездочка “*” в качестве Flash клавиши.
- Tap Report: включение отправки события на сервер, если нажата клавиша Flash
- Escape Seq: включение использование специальных символов при отправке DTMF.
- CID Enable: глобальное включение или отключение Caller ID.

3.5.7 Настройка Centrex

Для управления вызовами на номера, настроенные на одном устройстве, вызов с которых осуществляется друг на друга, выберите в меню пункты VOIP Service→Centrex. Для глобального включения функции поставьте флажок напротив пункта Enable Centrex.

Группа поиска (hunt group), это группа добавочных номеров, которая может одновременно принимать несколько вызовов, поступающих на один номер телефона. Когда вызов поступает на групповой номер, устройство ищет свободный добавочный номер в группе и соединяет вызов с этим добавочным номером. Группы поиска имеют свой номер телефона, который называют групповым номером. Группы поиска делятся на порядковые, альтернативные и параллельные.

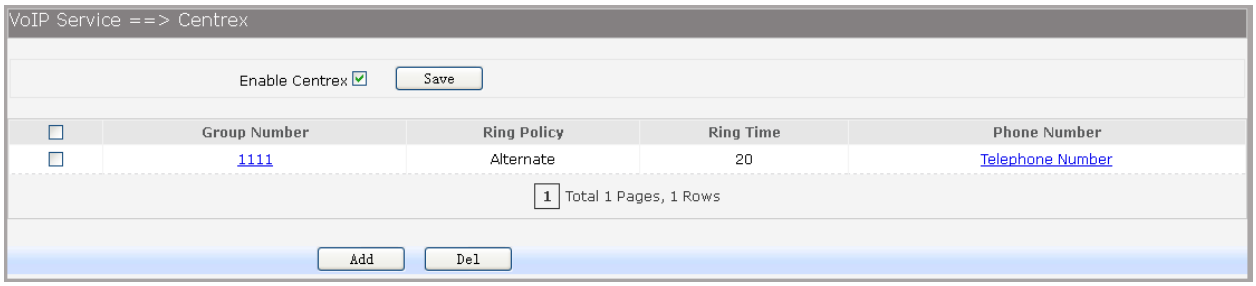


Рисунок 3-109. Настройка Centrex

В порядковой (Ordinal) группе вызов с группового номера передается на первый добавочный номер в списке. В альтернативной (Alternate) группе будет задействован последний номер в списке (номер на который дольше всего не поступало вызовов). В параллельной (Parallel) группе поиска, вызов поступит на все добавочные номера одновременно.

Для редактирования записей группового номера нажмите на соответствующий Group Number. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add. Откроется окно, изображенное на рисунке 2-110.

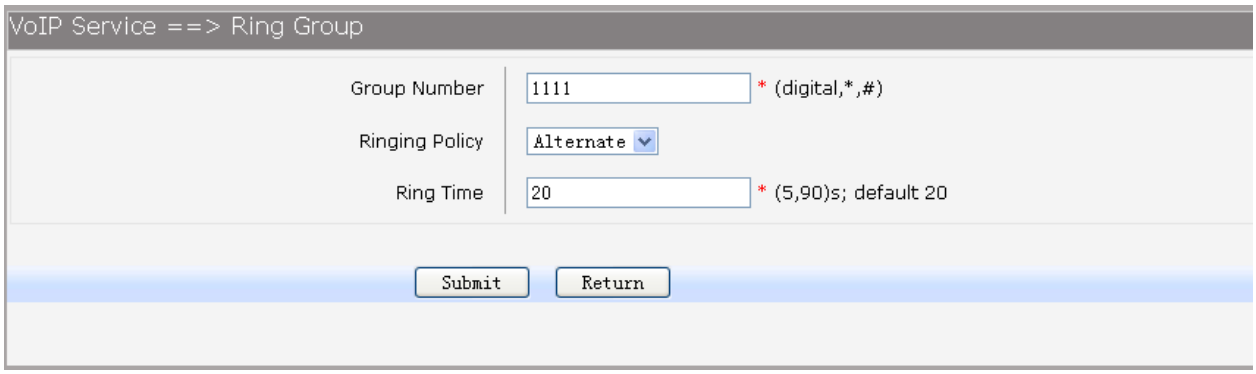


Рисунок 3-110. Настройка группового номера.

Пункты для настройки представлены ниже:

- Groupe Nimber: настройка номера группы.
- Ringing Policy: настройка политики работы группы поиска (Alternate, Ordinal, Parallel).
- Ring Time: настройка времени звонка для каждого пользователя.

Для применения настроек, нажмите кнопку Sumbit, после чего можно будет добавлять телефонные номера в группу поиска. Для этого нажмите на Telephone number, откроется окно с доступными номерами. Пометьте флажком номер и нажмите клавишу Add.

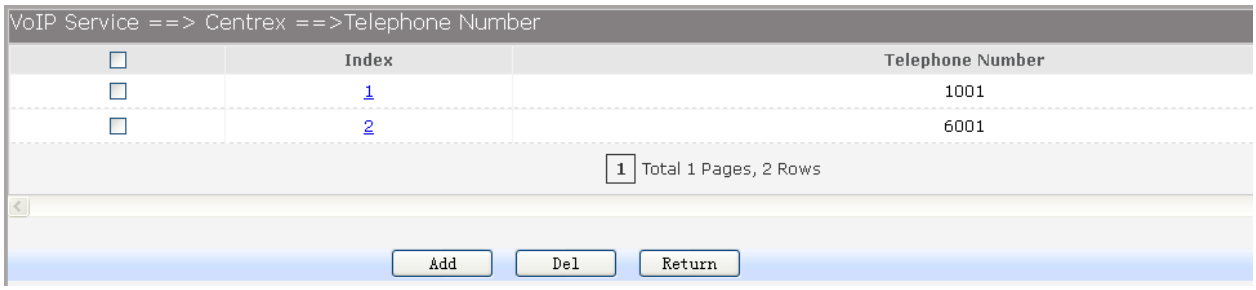


Рисунок 3-111. Добавление номера в группу поиска.

3.5.8 Настройка телефонной книги

Для настройки телефонной книги выберите в меню пункты VOIP Service→Phone Book.

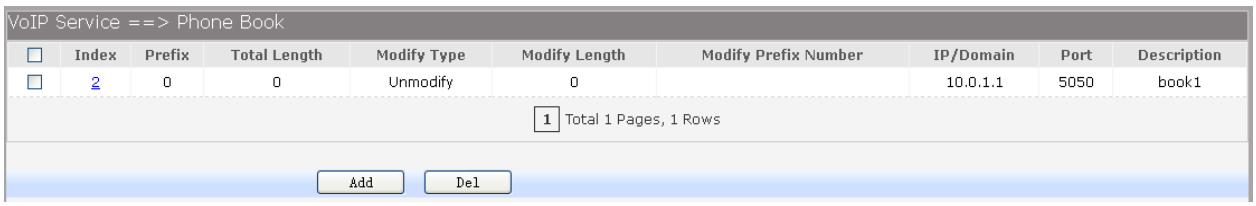


Рисунок 3-112. Настройка телефонной книги

Для редактирования записей нажмите на соответствующий индекс записи. Для удаления записи, выберите запись и нажмите кнопку Dell. Для добавления записи нажмите кнопку Add, откроется окно, изображенное на рисунке 2-113.

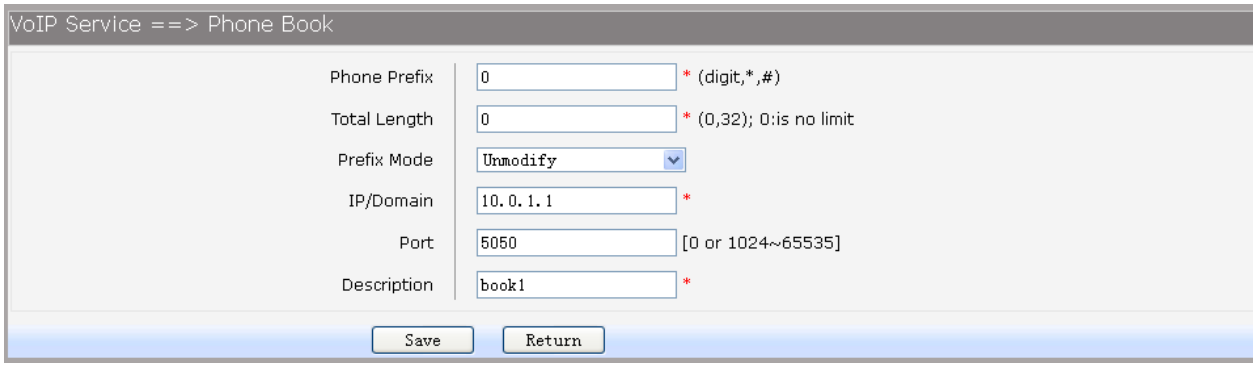


Рисунок 3-113. Добавление записи в телефонную книгу

Пункты для настройки представлены ниже:

- Phone Prefix: настройка префикса для телефонной книги.
- Total Length: длинна номера, которую ожидает устройство перед отправкой.
- Prefix Mode: режим обработки номера префикса (Unmodify, Remove, Add, Modify).
- IP/Domain: настройка имени домена или IP-адреса сервера назначения.
- Port: настройка порта на сервере назначения.
- Description: настройка имени правила.

3.6 Системные настройки

3.6.1 Настройка времени

Для ручной настройки системного времени, выберите в меню пункты Data Service→Time Management и выберите Manual Configuration. Откроется страница, изображенная на рисунке 2-114.

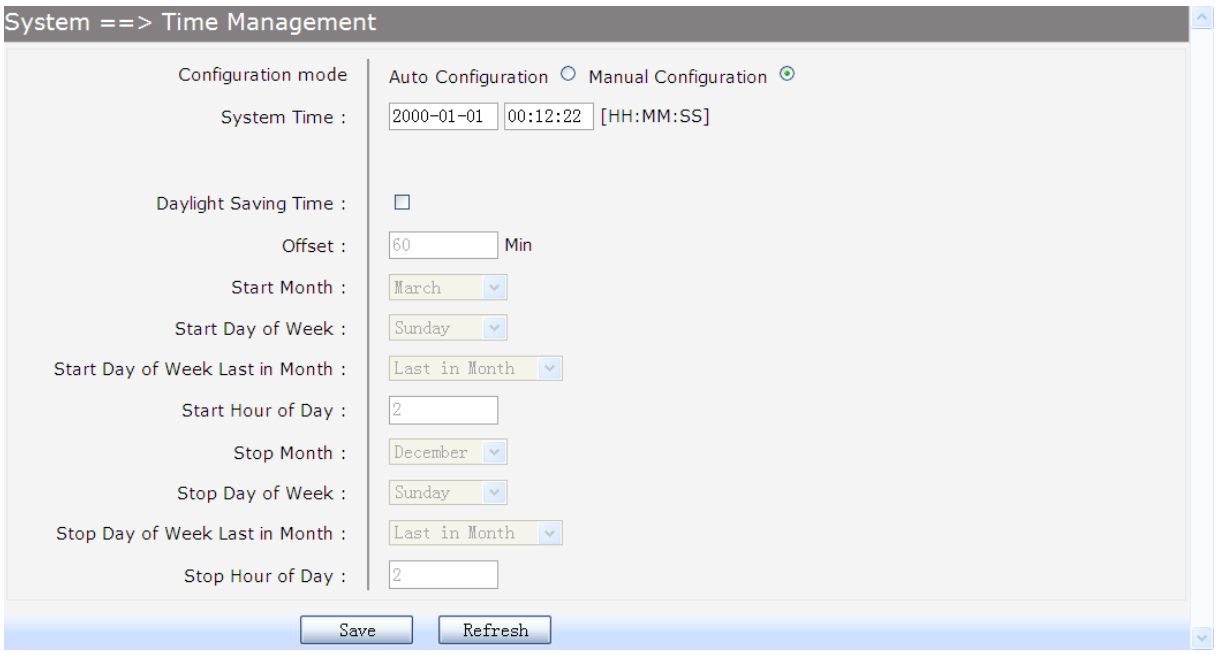


Рисунок 3-114. Ручная настройка времени

Пункты для настройки представлены ниже:

- Configuration mode: режим настройки (Auto Configuration или Manual Configuration). По умолчанию требуется ручная настройка.
- System Time: настройка времени.
- Daylight Saving Time: включение или отключения режима перехода на летнее время.
- Offset: настройка сдвига времени при переходе на летнее время.
- Start Month: настройка месяца перехода на летнее время.
- Start Day of Week: настройка дня недели для перехода на летнее время.
- Start Day of Week Last in Month: настройка недели дня перехода на летнее время (первая неделя месяца, вторая неделя месяца, третья неделя месяца, последняя неделя месяца).
- Start Hour of Day: настройка часа, в который осуществляется переход времени.
- End Month: настройка месяца перехода на стандартное время.

- End Day of Week: настройка дня недели для перехода на стандартное время.
- End Day of Week Last in Month: настройка недели дня перехода на стандартное время (первая неделя месяца, вторая неделя месяца, третья неделя месяц, последняя неделя месяца).
- End Hour of Day: настройка последнего часа летнего времени.

Для автоматической настройки системного времени выберите пункт Auto Configuration, откроется страница, изображенная на рисунке 2-115.

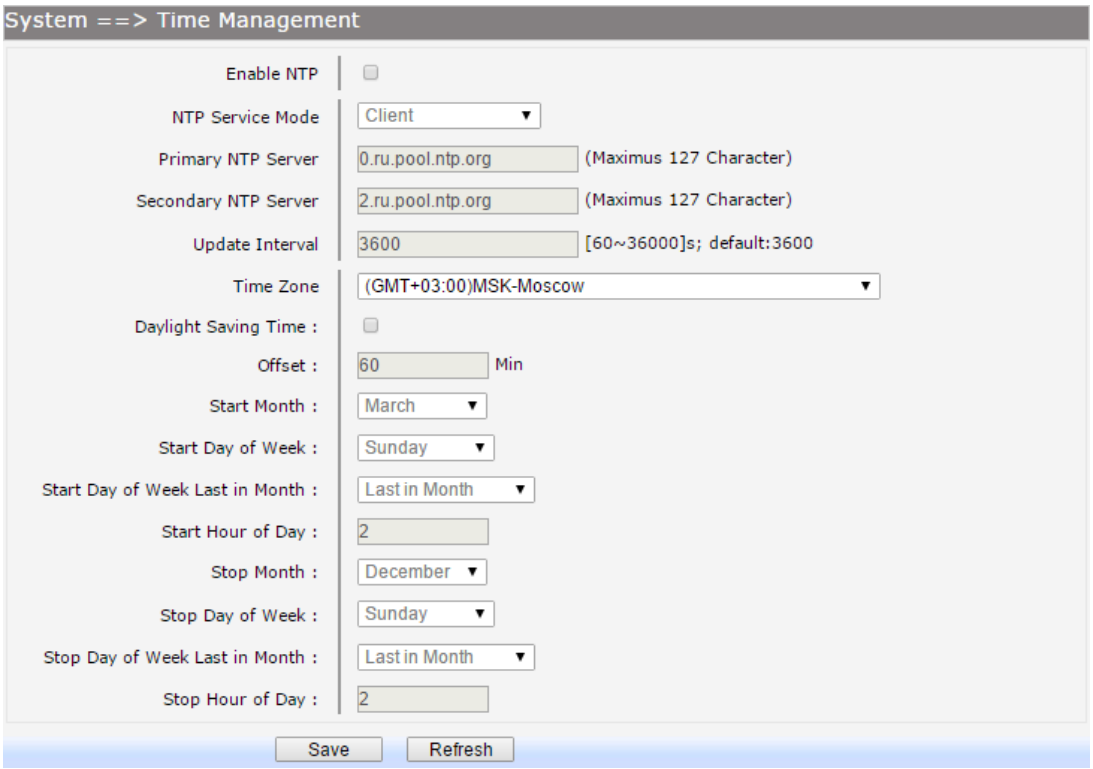


Рисунок 3-115. Автоматическая настройка времени

Пункты для настройки представлены ниже:

- Enable NTP: включение или отключение работы протокола NTP.
- NTP Service Mode: настройка режима работы устройства (клиент или сервер).
- Primary NTP Server: настройка адреса основного NTP сервера для NTP клиента устройства.
- Second NTP Server: настройка вторичного адреса NTP сервера для NTP клиента устройства.
- Time Zone: настройка временной зоны.
- Update Interval: настройка времени частоты обновления информации по NTP-протоколу.

3.6.2 Настройка обновлений

3.6.2.1 Обновление прошивки

Прошивку устройства можно обновить через WEB-интерфейс, для этого необходимо выполнить два шага:

- Выбрать в меню пункт System→Upgrade, указать путь к файлу прошивки на вашем компьютере, после чего нажать кнопку Upgrade. Обновление займет несколько минут.
- После загрузки прошивка автоматически установится, для завершения установки необходимо перезагрузить устройство, выбрав в мерю пункты System→Reboot, после чего нажать кнопку Reboot для перезагрузки устройства.

3.6.2.2 Операции с конфигурацией устройства

3.6.2.2.1 Обновление конфигурации из файла

Конфигурацию устройства можно обновить через WEB-интерфейс, для этого необходимо выполнить два шага:

- Выбрать в меню пункт System→Upgrade, указать путь к файлу конфигурации на вашем компьютере, после чего нажать кнопку Upgrade. Обновление займет несколько секунд.
- Для применения настроек загруженной конфигурации необходимо перезагрузить устройство, выбрав в мерю пункты System→Reboot, после чего нажать кнопку Reboot для перезагрузки устройства.

3.6.2.2.2 Сохранение конфигурации в файл

Конфигурацию устройства можно экспортировать в файл, для этого нажмите "Export Configuration File" выберите директорию на компьютере и имя файла конфигурации.

3.6.3 Перезагрузка системы

Для перезагрузки устройства выберите в меню пункты System→Reboot, после чего нажмите кнопку Reboot.

3.6.4 Восстановление заводских параметров

Для сброса устройства к заводским параметрам или загрузки начальной конфигурации, выберите в меню пункты System→Backup/Restore. Откроется страница, изображенная на рисунке 2-116.

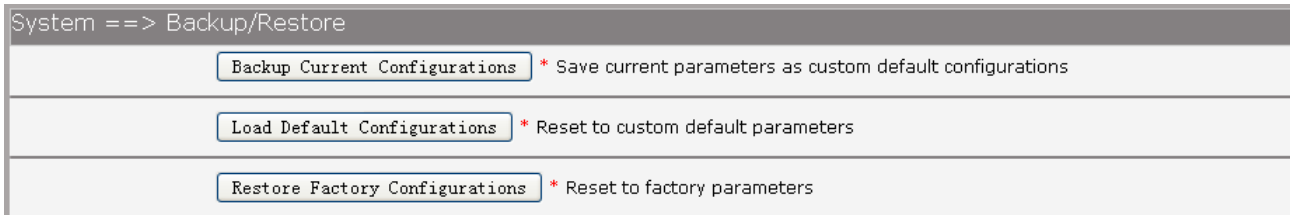


Рисунок 3-116. Восстановление настроек устройства

Пункты для настройки представлены ниже:

- Backup Current Configurations: сохранение настроек пользователя как настроек по умолчанию.
- Load Default Configurations: сброс настроек устройства к настройкам по умолчанию.
- Restore Factory Configurations: сброс настроек устройства до заводских параметров.

3.6.5 Диагностика соединения

3.6.5.1 Утилита Ping

Для проверки соединения с помощью утилиты Ping, выберите в меню пункты System→Diagnostic→Ping. Откроется страница, изображенная на рисунке 2-117.

Для запуска утилиты введите в поле Ping имя домена или IP-адрес узла, соединение с которым диагностируется. В поле Ping Count вводится количество отправляемый пакетов. После задания параметров, нажмите кнопку Start. Для остановки диагностики нажмите кнопку Stop. Результат диагностики будет выведен на экран в окне Result. Для обновления результатов нажмите кнопку Refresh.

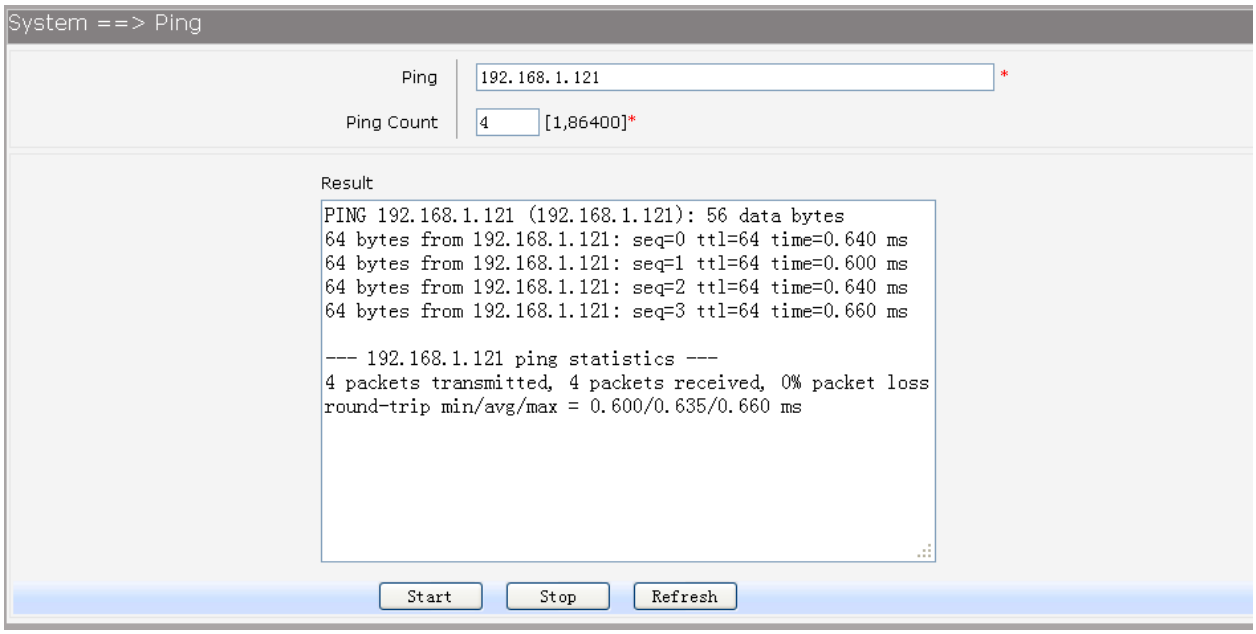


Рисунок 3-117. Утилита Ping

3.6.5.2 Утилита tcpdump.

Утилита tcpdump позволяет перехватывать и анализировать сетевой трафик. Для запуска утилиты выберите в меню пункты System→Diagnostic→Tcpdump. Откроется страница, изображенная на рисунке 2-118.

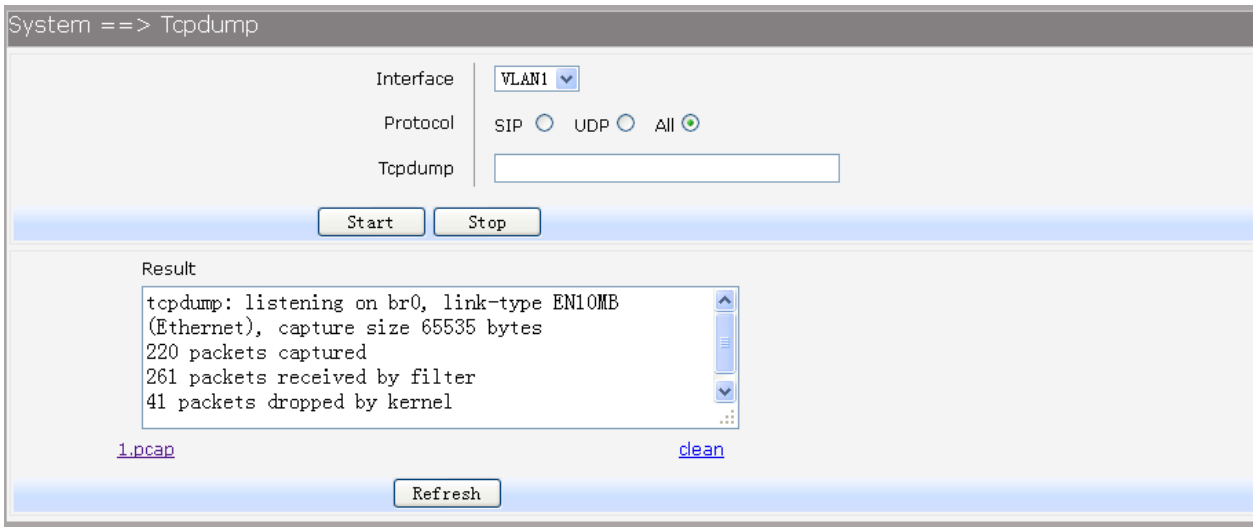


Рисунок 3-118. Утилита tcpdump

Пункты для настройки утилиты представлены ниже:

- Interface: выбор интерфейса на котором будут перехватываться пакеты.
- Protocol: выбор типа перехватываемых пакетов.
- Tcpdump: настройка опцией tcpdump.

После задания параметров, нажмите кнопку Start. Для остановки диагностики нажмите кнопку Stop. Результат диагностики будет выведен на экран в окне Result. Для загрузки файла с перехваченными пакетами нажмите на *.pcap. Для удаления файлов с перехваченными пакетами нажмите clean. Для обновления результатов нажмите кнопку Refresh.

3.6.5.3 Тестирование скорости WAN

Для тестирования скорости загрузки и отдачи на WAN-интерфейсе, выберите в меню пункты System→Diagnostic→WAN Speed Test. Откроется страница, изображенная на рисунке 2-119.

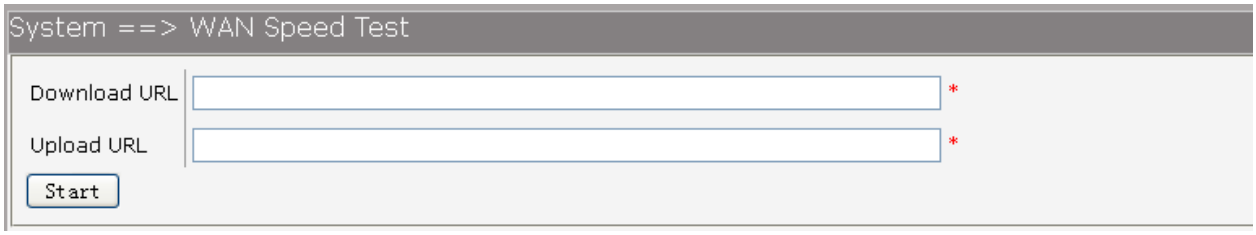


Рисунок 3-119. Тестирование скорости WAN-интерфейса.

Для тестирования скорости необходимо вставить ссылку на файл в соответствующий пункт:

Download URL: тестирование скорости загрузки.

Upload URL: тестирование скорости отдачи.

После задания параметров нажмите на кнопку Start, для начала тестирования.

3.6.6 Настройка учетных записей

Для изменения пароля по умолчанию для пользователей системы, выберите в меню пункты System→User Management. Откроется страница, изображенная на рисунке 2-120.

Выберите пользователя, пароль которого хотите поменять. Новый пароль необходимо ввести в поле New Passwrod, в поле Confirm Password новый пароль вводится еще раз для подтверждения, после чего нажимаете кнопку Save.

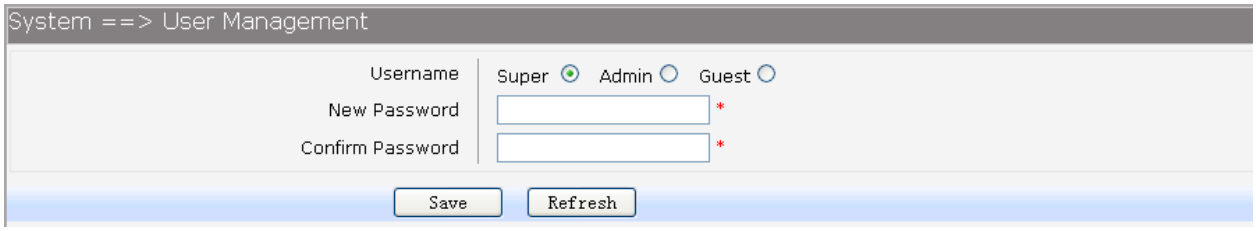


Рисунок 3-120

3.6.7 Настройка журнала событий

Для настройки журнала событий выберите в пеню пункты System→System Log→Log Config. Откроется окно, изображенное на рисунке 2-121.

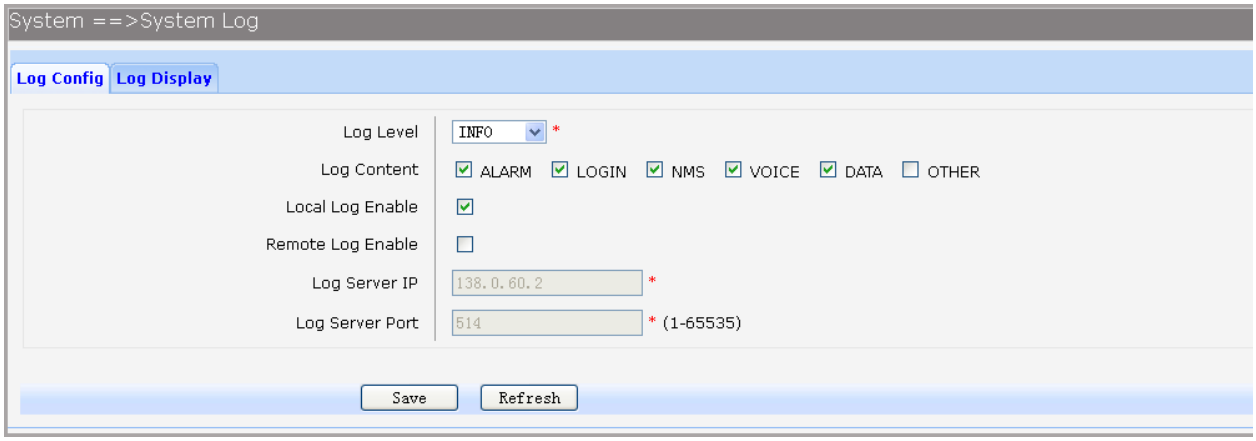


Рисунок 3-121. Настройка журнала событий.

Пункты для настройки представлены ниже:

- Log Level: уровень журналирования событий.
- Log Content: настройка типа журналируемых сообщений. Только сообщения настроенных типов будут сохранятся в журнале или отправляться на SysLog сервер.
- Local Log Enable: включение или отключение функции локального ведения журнала событий.

- Remote Log Enable: включение или отключение функции удаленного протоколирования событий. Если функция включена, записи событий будут отправятся на удаленный сервер.
- Log Server IP: настройка IP-адреса удаленного SysLog-сервера.
- Log Server Port: настройка порта удаленного SysLog-сервера.

Для просмотра журнала событий выберите в меню пункты System→System Log→Log Display. Откроется окно, изображенное на рисунке 2-122.

Для экспорта журнала событий в файл, нажмите кнопку Export. Для отчистки журнала нажмите кнопку Clear. Для обновления страницы журнала событий нажмите кнопку Refresh.

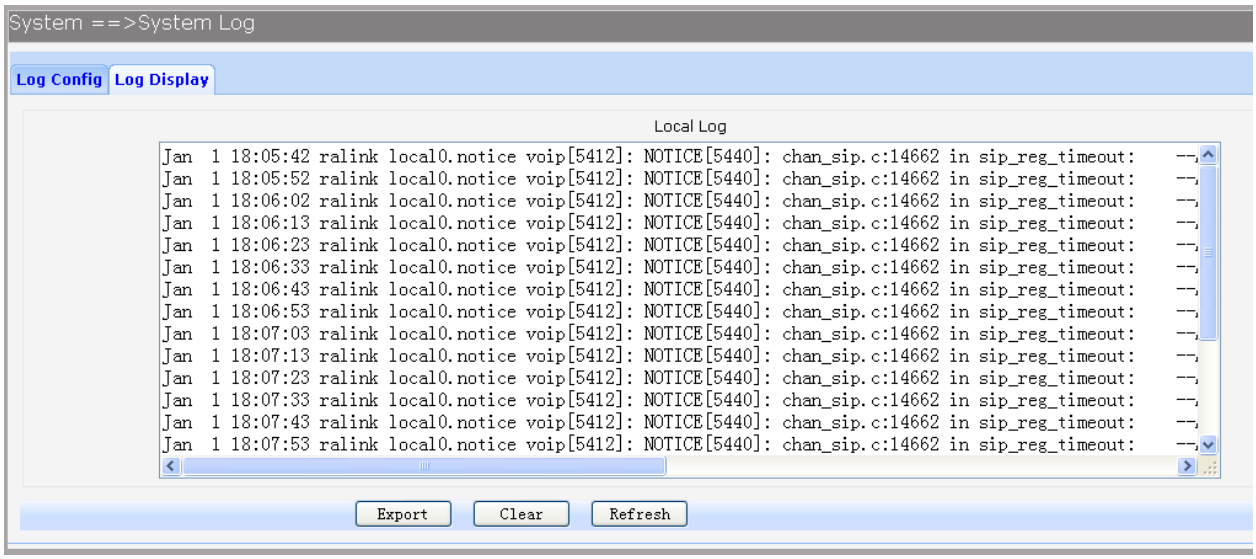


Рисунок 3-122. Просмотр журнала событий

3.6.8 Настройка TR069

TR-069 это спецификация, описывающая протокол CWMP (CPE WAN management protocol). Протокол CWMP предназначен для удалённого управления абонентским оборудованием через глобальную сеть. CWMP передаёт данные с использованием протокола SOAP. Согласно спецификации, на территории провайдера должен находиться сервер ACS (auto configuration server) в задачи которого входят организация взаимодействия с оборудованием клиентов, обработка запросов от устройств. CWMP позволяет выполнять такие функции как, начальная настройка устройства при его загрузке и внесение изменений в настройки уже работающего устройства, удалённое обновление прошивки, удалённый доступ к журналу событий, удаленная диагностика устройства и другим функциям.

Для настройки TR069 выберите в меню пункты System→TR069. Откроется окно, изображенное на рисунке 2-123.

Пункты для настройки представлены ниже:

- Serial Number: серийный номер устройства, информация только для чтения.
- Enable: включение или отключение работы протокола RT069.
- ACS Address: настройка IP-адреса ACS-сервера.
- ACS Port: настройка порта ACS-сервера.
- ACS Server Name: настройка имени TR069 сервера ACS.
- SSL Enable: включение или отключение использования протокола SSL.
- Schedular Send Inform: Включение или отключения функции отправки информации на ASC сервер. Если функция включена, необходимо настроить время, через которое будет отправляться информация.
- Single Account Enable: включение или отключение аккаунта TR069.
- TR069 Account: настройка имени пользователя, используемого для авторизации на ASC-сервере.
- TR069 password: настройка пароля, используемого для авторизации на ASC сервере.
- Connection Request Auth: настройка запроса аутентификации к устройству со стороны ASC сервера.
- Connection Request Username: настройка имени пользователя, используемого ACS сервером при аутентификации на устройстве.
- Connection Request Password: настройка пароля, используемого ACS сервером при аутентификации на устройстве.
- CPE Server Name: настройка имени сервера, используемого ACS при подключении к CPE.
- CPE Port: настройка порта, к которому будет подключатся ACS сервер.
- Status: состояние подключение к ACS серверу. Ъ
- Fail Reason: показывает причину по которой ACS сервер отклонил подключение.

Для сохранения настроек нажмите кнопку Save.

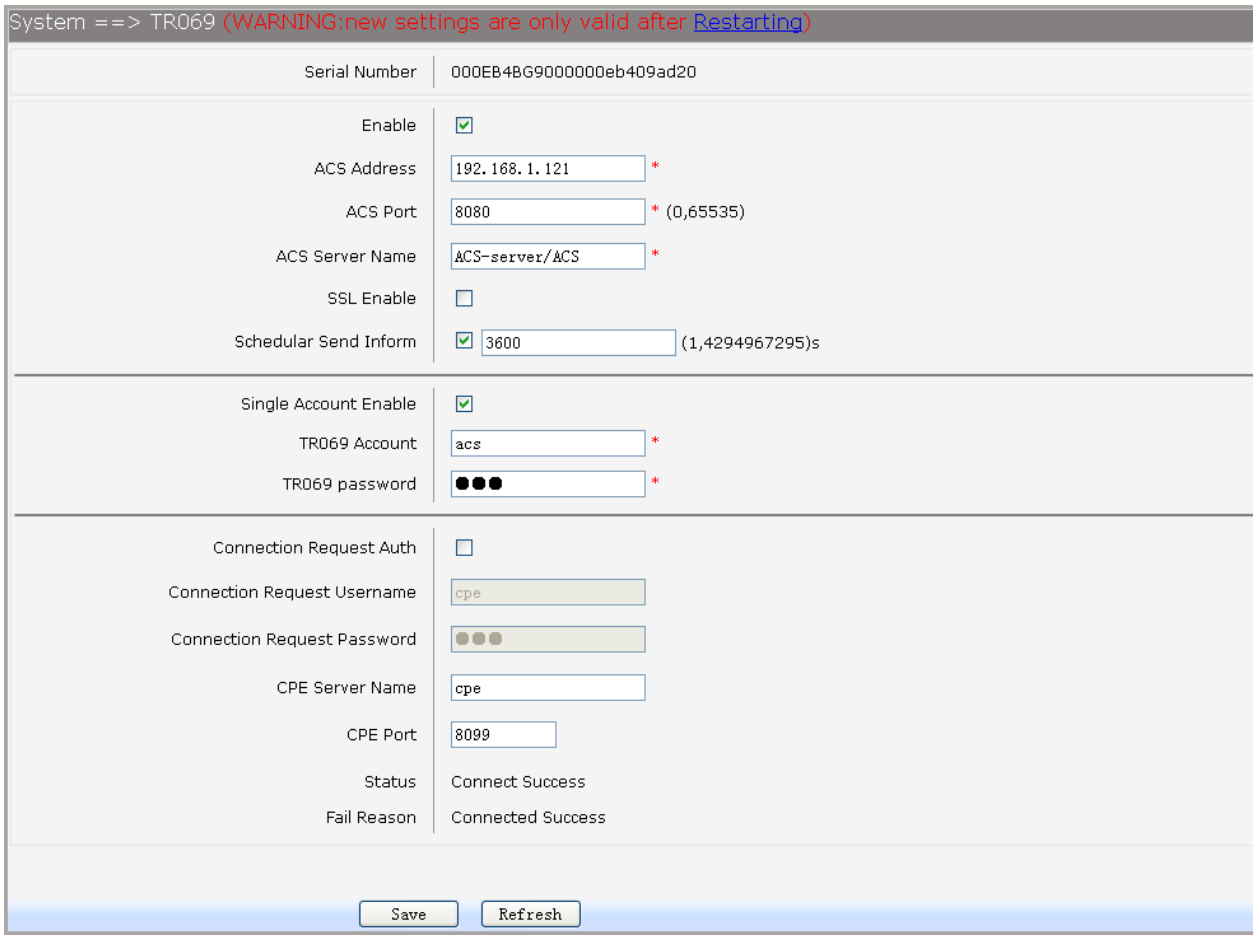


Рисунок 3-123. Настройка TR069

3.6.9 Настройка SNMP

Для настройки SNMP выберите в меню пункты System→SNMP. Откроется окно, изображенное на рисунке 2-124.

- Пункты для настройки представлены ниже:

- Register Enable: включение или отключение функции отправки SNMP сообщений на удаленный сервер.
- Server Address or Domain: настройка имени домена или IP-адреса сервера.
- Server Port: настройка порта сервера.
- TRAP Message Interval: настройка интервала между TRAP сообщениями.
- Regional Identifier: настройка регионального идентификатора.
- Device Identifier: настройка идентификатора устройства.
- Enable Double Register Server: включение или отключение отправки SNMP сообщений на резервный сервер.
- Backup Server Address or Domain: настройка имени домена или IP-адреса резервного сервера.
- Backup Server Port: настройка порта резервного сервера.

- Registration Status: состояние подключения к SNMP-серверу.

Для сохранения настроек нажмите кнопку Save.

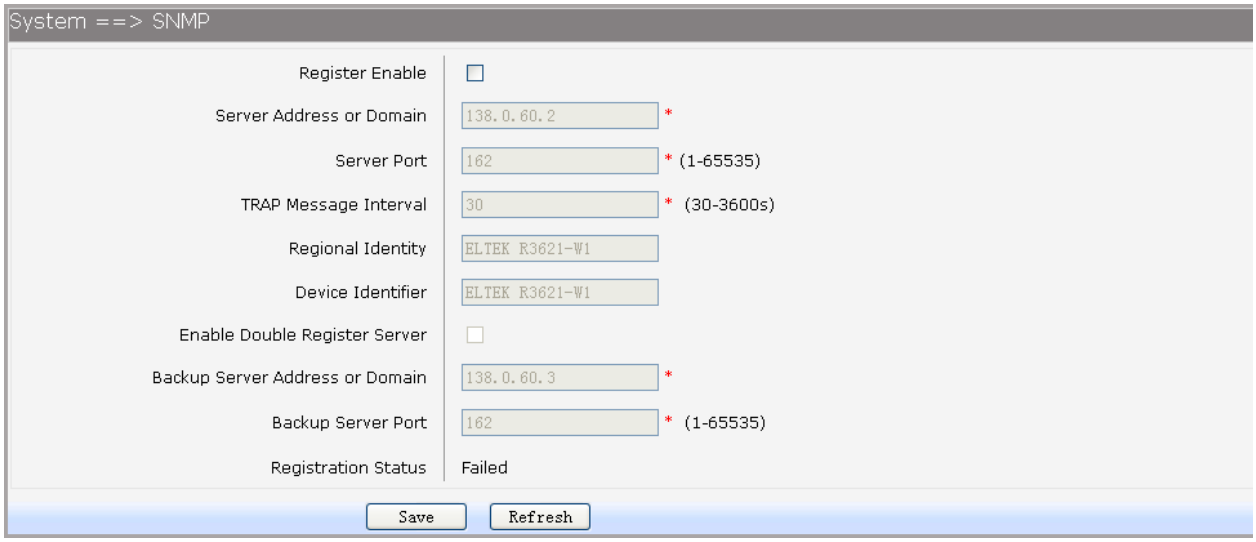


Рисунок 3-124. Настройка SNMP

3.6.10 Настройка прав доступа для пользователей системы

Для настройки прав доступа пользователям системы необходимо зайти на WEB-интерфейс в режиме супер-пользователя и выбрать пункты в меню System→User Access Right.

Рисунок 3-125. Просмотр пользователей

Для изменения прав пользователя нажмите на detail. Откроется меню, изображенное на рисунке 2-126. Для разрешения доступа к определенным настройкам поставьте флажки напротив необходимых пунктов в меню.

3.7 Сохранение настроек

Для сохранения и применения некоторых настроек в системе требуется нажатия пункта Apply. При необходимости данного действия выводится сообщение, изображенное на рисунке 2-127.

Рисунок 3-126. Настройка прав доступа для пользователей системы

Рисунок 3-127. Сохранение настроек