

# Руководство

по настройке туннелей на роутерах iRZ



## Содержание

<b>1. Введение</b>	<b>3</b>
1.1. Описание документа	3
1.2. Версия встроенного обеспечения	4
1.3. Предупреждения	5
<b>2. PPTP Client</b>	<b>6</b>
<b>3. L2TPv2 Client</b>	<b>8</b>
<b>4. OpenVPN туннели</b>	<b>10</b>
4.1. OpenVPN Layer 2: dev TAP	10
4.2. OpenVPN Layer 3: dev TUN	14
<b>5. GRE туннели</b>	<b>15</b>
5.1. Настройка GRE туннеля уровня L2	15
5.2. Настройка GRE туннеля уровня L3	18
<b>6. IPsec туннели</b>	<b>21</b>
6.1. Настройка IPsec туннеля	21
6.2. Статус IPsec туннеля	25
<b>7. DMVPN / NHRP туннели (только для роутеров серии R4, R2, R50)</b>	<b>27</b>
<b>8. EoIP туннели</b>	<b>30</b>
<b>9. L2TPv3 туннели</b>	<b>32</b>
<b>10. Термины и сокращения</b>	<b>34</b>
<b>11. Контакты</b>	<b>38</b>

# 1. Введение

## 1.1. Описание документа

Данный документ содержит примеры корректной конфигурации сетевых служб PPTP Client, L2TPv2 Client, OpenVPN Tunnel, GRE Tunnels, DMVPN/NHRP, EoIP Tunnels, L2TPv3 Tunnels, IPsec Tunnels в решениях, построенных на базе роутеров iRZ. Для получения информации о работе самих устройств смотрите соответствующее руководство пользователя. Для получения информации о веб-интерфейсе роутеров смотрите документ «Руководство по настройке роутеров iRZ».

## 1.2. Версия встроенного обеспечения

### Актуальная (текущая) версия встроенного ПО

---

- роутеры серии R0: R0-v20.9 (2024-03-22)
  - роутеры серии R2: R2-v20.9 (2024-03-22)
  - роутеры серии R50: R50-v20.9 (2024-03-22)
  - роутеры серии R10(R10, R11): R50-v20.9 (2024-03-22)
-

### 1.3. Предупреждения

Отклонение от рекомендованных параметров и настроек может привести к непредсказуемым последствиям и значительным издержкам как в процессе пусконаладки вычислительного комплекса, так и во время эксплуатации production-версии вычислительного комплекса в реальных условиях.



Прежде чем вносить любые изменения в настройки оборудования, устанавливаемого на объекты, настоятельно рекомендуется проверить работоспособность всех параметров новой конфигурации на тестовом стенде. Также не следует ограничиваться синтетическими тестами, а максимально реалистично воспроизвести условия, в которых будет эксплуатироваться оборудование.

## 2. PPTP Client

Туннель PPTP представлен на роутерах iRZ в виде клиентской части. Для подключения к серверу PPTP необходимо указать адрес сервера в виде IP адреса или его доменного имени, логин и пароль клиентского доступа и выбрать тип аутентификации.

Для сохранения выполненных настроек, используйте кнопку **Save**.



При переходе на другие страницы разделов все выполненные, но не сохраненные настройки будут сброшены!

**Enable PPTP Client**

**Server**

127.0.0.1

**Firewall Zone**

<none>

**Use as default route**

**Username**

username

**Password**

\*\*\*\*\*

**Use MPPE (MS-CHAP-V2 auth)**

**Additional Options**

**Authentication Type**

PAP

**Failover management**

**Ping Address**

Enter address to check connection

**Ping Interval (sec)**

Default 30 seconds

**Ping Attempts**

3 by default

Save

Рис. 1. Пример интерфейса PPTP Client

Для авторизации на сервере представлены следующие распространенные типы аутентификации для PPTP туннеля: EAP, PAP, CHAP и MPPE (MS-CHAP-V2). Значение Any в поле Authentication Type позволяет договариваться с сервером PPTP о методе аутентификации в автоматическом режиме.

### Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет по умолчанию.



Управление маршрутами находится в разделе **Network - Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.
- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
  - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
  - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.



Для включения функции должен быть выбран параметр **Default Route**

### 3. L2TPv2 Client

Туннель L2TP версии 2 на роутерах представлен только в виде клиентской части. Для подключения к удаленному серверу необходимо указать адрес или доменное имя сервера и логин с паролем.

Enable L2TPv2 Client

**Server**

**Firewall Zone**

Use as default route

**Username**

**Password**

Use MPPE (MS-CHAP-V2 auth)

**Additional Options**

Use IPSec Protection

**IPSec Pre-Shared Key**

**Failover management**

<b>Ping Address</b> <input type="text" value="Enter address to check connection"/>	<b>Ping Interval (sec)</b> <input type="text" value="Default 30 seconds"/>	<b>Ping Attempts</b> <input type="text" value="3 by default"/>
---	---	---

Рис. 2. Пример интерфейса L2TPv2 Client



Таблица 1. Поля в разделе L2TPv2 Client

Поле	Описание
Use as default route	Использовать как маршрут по умолчанию. В этом случае роутер будет направлять весь трафик через данный туннель, в таблице маршрутизации маршрут через данный туннель будет приоритетным. Таким образом, остальные WAN интерфейсы (такие как подключение через сотовую сеть или отдельный WAN порт) станут резервными, и переключение с одного WAN порта на другой не будет приводить к разрыву туннеля, то есть его переключению
Use MPPE (MS-CHAP-V2)	Заставит роутер подключаться к серверу L2TP только по указанному протоколу аутентификации
Additional Options	Позволяет прописывать дополнительные опции для работы туннеля
Use IPsec Protection	Дает возможность настроить шифрование туннеля с помощью IPsec. Данный функционал разработан для взаимодействия с сетевым оборудованием Mikrotik. В поле IPsec Pre-Shared Key следует вписать ключ

### Failover management (проверка состояния соединения)

Предусмотрена проверка состояния соединения при помощи отправки ICMP-пакетов (пинга) указанного адреса.

В поле **Ping Address** указывается IP-адрес или доменное имя сервера для проверки работы соединения. Можно указать несколько IP-адресов или доменов через ПРОБЕЛ. В поле **Ping Interval** задается периодичность запуска пинга (в секундах). В поле **Ping Attempts** указывается количество неудачных попыток подряд.

В момент начала отслеживания соединению (маршруту) присваивается приоритет по умолчанию.



Управление маршрутами находится в разделе **Network - Routes**

- Если после отправки ICMP-пакета на сервер поступает ответ, маршрут считается работающим. Никаких дополнительных действий не происходит.
- Если после отправки ICMP-пакета на сервер ответа не поступает, попытка считается неудачной, начинает отсчитываться Ping Attempts. Маршрут переводится в резервный.
  - Если следующая попытка соединения будет удачной, маршруту возвращается исходный приоритет.
  - Если количество неудачных попыток подряд достигнет заданного, интерфейс будет перезапущен и через какое-то время маршрут стартует с приоритетом по умолчанию.



Для включения функции должен быть выбран параметр **Default Route**

## 4. OpenVPN туннели

### 4.1. OpenVPN Layer 2: dev TAP

В данном разделе рассматривается туннель OpenVPN типа Ethernet Bridging.

Этот тип туннеля OpenVPN характеризуется общим адресным пространством между устройствами, а маршрутизаторы, на которых создается OpenVPN, прозрачны для остальных сетевых устройств. Данный туннель создаётся на базе виртуального сетевого интерфейса TAP.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

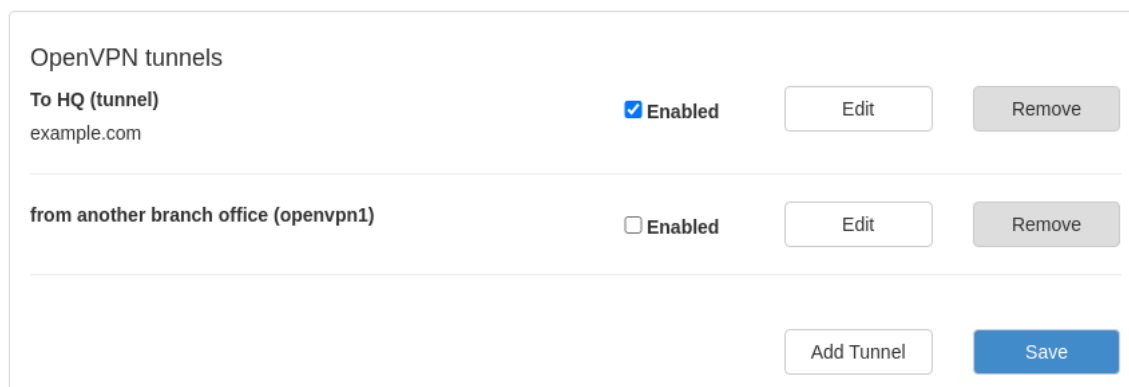


Рис. 3. Пример интерфейса раздела OpenVPN tunnels

Для настройки OpenVPN-туннеля с TAP (Layer 2), в веб-интерфейсе роутера:

1. Зайдите в раздел Network → OpenVPN Tunnel;
2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
3. Выберите в поле Device значение TAP (L2);
4. Настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы ниже).

Edit tunnel: Unnamed (tunnel)

---

**Description**

**Device** **Transport Protocol**

TAP (L2) UDP

**Remote Address** **Port**

IP or domain name 1194

**Authentication Method** **Add to Bridge or Create New**

None none

**Tunnel IP** **Tunnel Mask**

**Remote Subnet** **Remote Subnet Mask** **Remote Gateway**

**Ping Interval** **Ping Timeout**

**LZO Compression**

No

**Additional Config**

Рис. 4. Пример конфигураций OpenVPN. Настройка OpenVPN

Таблица 2. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Поля	Описание
Description	Описание и имя туннеля. Это же имя отображается во всех остальных настройках роутера (например, в разделе Firewall)
Device	Выбор виртуального интерфейса
Transport Protocol	Выбор транспортного протокола: <ul style="list-style-type: none"> <li>• UDP;</li> <li>• TCP Server;</li> <li>• TCP Client.</li> </ul>

Таблица 2. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Remote Address	IP-адрес удаленного сетевого устройства (указывается если <b>Transport Protocol = UDP</b> или <b>TCP Client</b> )
Port	Номер порта, через который будет работать туннель
Authentication Method	Метод авторизации
<b>Advanced Settings:</b>	<i>Нажмите на строчку Show advanced settings, чтобы открыть доступ к настройкам</i>
Add to Bridge or Create New	Создание моста с локальными интерфейсами роутера
Ping Interval	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы туннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-туннель, если ответ от удаленного устройства не будет получен
LZO Compression	<p>Режим сжатия данных, проходящих через туннель:</p> <ul style="list-style-type: none"> <li>• No — отсутствие сжатия данных</li> <li>• Always — всегда сжимать данные</li> <li>• Adaptive — адаптивное сжатие данных, режим по умолчанию</li> <li>• None — не указан тип сжатия данных</li> </ul>
Tunnel IP	IP-адрес туннеля на данном устройстве
Tunnel Mask	Маска IP-адреса туннеля на данном устройстве
Remote Subnet	IP-адрес удаленной сети (на другом конце туннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце туннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце туннеля)

Поле **Additional Config** позволяет указывать дополнительные параметры для создания туннеля. Пункты и их расшифровка, которые указываются в данном поле, можно посмотреть на

официальном сайте OpenVPN по адресу: <https://openvpn.net/index.php/open-source/documentation/howto.html#server>.

## 4.2. OpenVPN Layer 3: dev TUN

В данном разделе рассматривается туннель OpenVPN типа Routing.

Данный тип туннеля OpenVPN характеризуется маршрутизацией пакетов между сетями на разных концах туннеля, находящимися за сетевыми устройствами, и устанавливающими туннель между собой. Данный вид туннеля создается на базе виртуального сетевого интерфейса TUN.

Всего четыре варианта настройки туннеля, различающиеся по методу аутентификации:

- без аутентификации (Authentication method: None);
- с аутентификацией по общему ключу (Authentication method: Shared secret);
- в роли сервера OpenVPN (Authentication method: TLS Server);
- в роли клиента OpenVPN (Authentication method: TLS Client).

При этом необходимо учитывать, что туннель может работать по двум сетевым протоколам: UDP и TCP. Для протокола TCP есть возможность работать по методу сервера, когда роутер ожидает подключения извне, так и по методу клиента, когда роутер инициирует подключение с другим сетевым устройством.

Для настройки OpenVPN-туннеля с TUN (Layer 3), в веб-интерфейсе роутера:

1. Зайдите в раздел Network → OpenVPN Tunnel;
2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
3. Выберите в поле Device значение TUN (L3);
4. Настройте остальные параметры на странице в зависимости от требуемой конфигурации.

## 5. GRE туннели

### 5.1. Настройка GRE туннеля уровня L2

В примерах настройки используется следующая схема сети:

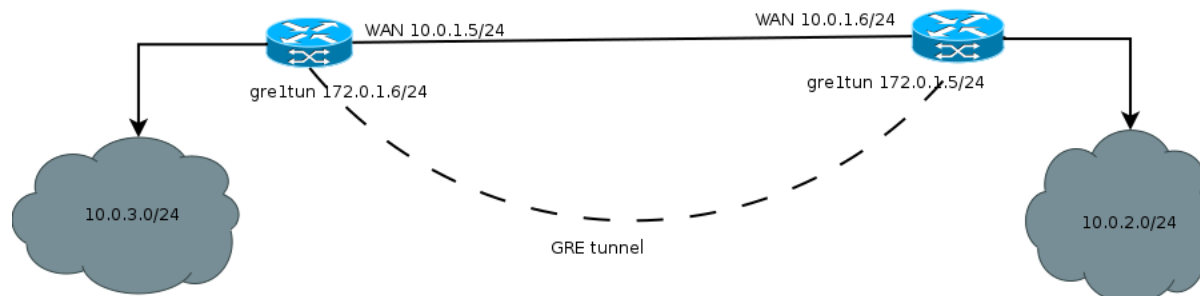


Рис. 5. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L2, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел **Network** → **Local Network**;
2. Укажите IP-адрес локального пользователя в поле **IP**;
3. Укажите маску сети в поле **Mask**;

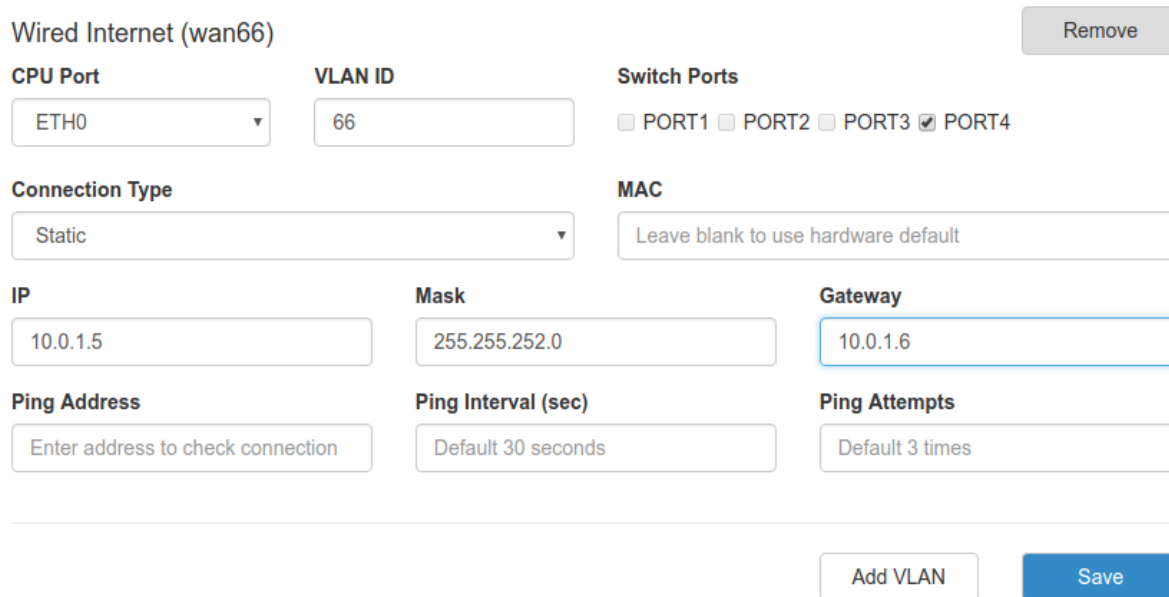
Local Network (lan)			Remove
<b>CPU port</b>	<b>VLAN ID</b>	<b>Switch Ports</b>	
ETH0	1	<input checked="" type="checkbox"/> PORT1 <input checked="" type="checkbox"/> PORT2 <input checked="" type="checkbox"/> PORT3 <input type="checkbox"/> PORT4	
<b>IP</b>	<b>Mask</b>	<b>MAC</b>	
10.0.3.1	255.255.255.0	f0:81:af:00:8f:64	
			Add VLAN
			Save

Рис. 6. Примеры конфигураций Local Network. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. следующий рисунок):

4. Зайдите в раздел **Network** → **Wired Internet**;

5. Укажите тип подключения в поле **Connection Type** (**Static** – статический адрес, **DHCP** – адрес



Wired Internet (wan66) Remove

**CPU Port**  **VLAN ID**  **Switch Ports**  
 PORT1  PORT2  PORT3  PORT4

**Connection Type**  **MAC**

**IP**  **Mask**  **Gateway**

**Ping Address**  **Ping Interval (sec)**  **Ping Attempts**

Add VLAN Save

Рис. 7. Примеры конфигураций Wired Internet. Настройка WAN

Далее необходимо настроить GRE-туннель (см. следующий рисунок):

6. Зайдите в раздел **VPN/Tunnels** → **GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите локальный интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается **L2**);
12. Выберите с каким **LAN** интерфейсом будет создан bridge или задайте отдельную сеть для GRE- туннеля, выбрав значение в поле **Add to Bridge or Create New** (если значение = **LAN**, то дополнительных настроек не требуется, если значение = **<new network>**, то необходимо будет указать IP-адрес пользовательского интерфейса в поле **Tunnel IP** и маску сети в поле **Tunnel Mask**);
13. Выберите к какой зоне **Firewall** необходимо отнести туннель (к зоне **Lan** или зоне **WAN**), выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services** → **Firewall**);
14. При необходимости укажите ключ туннеля — **GRE key** (данный пункт чаще всего необходим если вы устанавливаете несколько таких туннелей с одним удаленным узлом).
15. При необходимости поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.



## Create new GRE

### Name

### Local Address

### Remote Address

### Network Type

### Add to Bridge or Create New

### Tunnel IP

### Tunnel Mask

### GRE key

### Firewall Zone

**Don't Fragment packets**

Рис. 8. Примеры конфигураций GRE. Настройка GRE-туннеля

## 5.2. Настройка GRE туннеля уровня L3

В примерах настройки используется следующая схема сети:

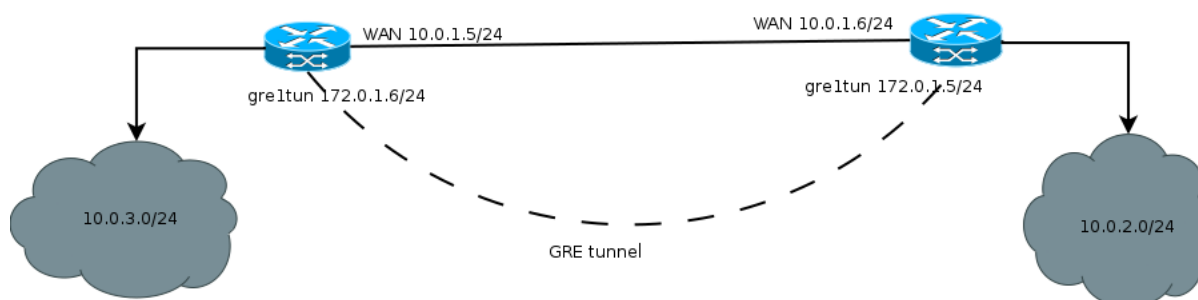


Рис. 9. Примеры конфигураций GRE. Схема сети

Для настройки GRE-туннеля уровня L3, в веб-интерфейсе роутера (см. рисунок ниже):

1. Зайдите в раздел Network → Local Network;
2. Укажите IP-адрес локального пользователя в поле IP;
3. Укажите маску сети в поле Mask;

Local Network (lan)			Remove
<b>CPU port</b>	<b>VLAN ID</b>	<b>Switch Ports</b>	
ETH0	1	<input checked="" type="checkbox"/> PORT1 <input checked="" type="checkbox"/> PORT2 <input checked="" type="checkbox"/> PORT3 <input type="checkbox"/> PORT4	
<b>IP</b>	<b>Mask</b>	<b>MAC</b>	
10.0.3.1	255.255.255.0	f0:81:af:00:8f:64	
<b>Add VLAN</b>			<b>Save</b>

Рис. 10. Примеры конфигураций GRE. Настройка локальной сети

Далее необходимо настроить WAN-порт роутера (см. рисунок ниже):

4. Зайдите в раздел Network → Wired Internet;

5. Укажите тип подключения в поле Connection Type (Static – статический адрес, DHCP – адрес получаемый по DHCP);

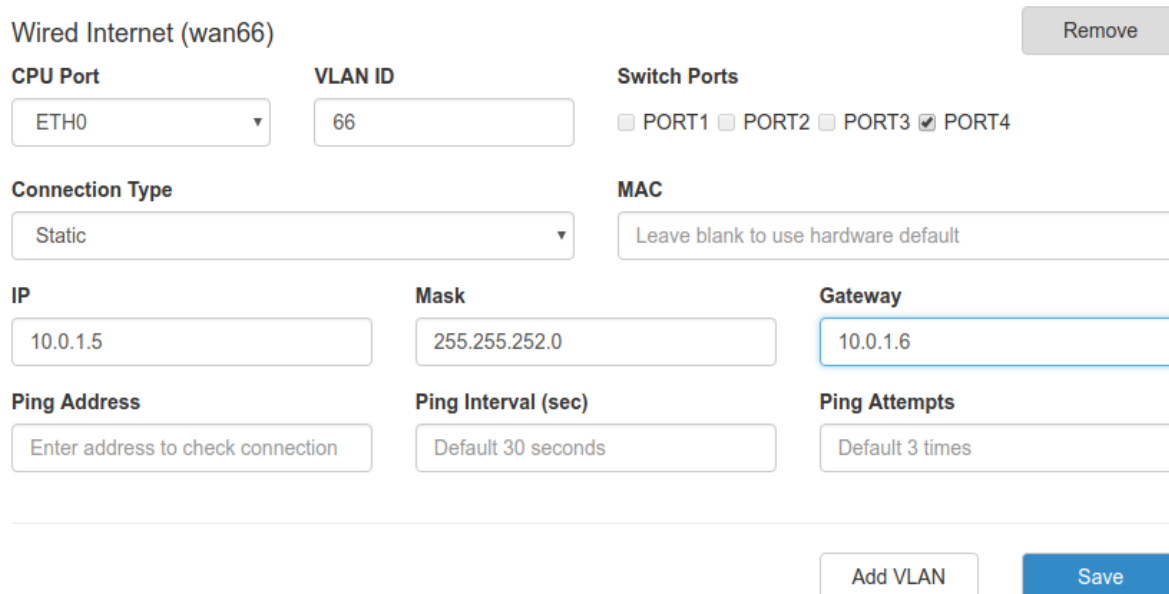


Рис. 11. Примеры конфигураций GRE. Настройка WAN

Далее необходимо настроить GRE-туннель (см. рисунок ниже):

6. Зайдите в раздел **VPN/Tunnels** → **GRE Tunnels**;
7. Добавьте новый туннель, нажав на кнопку **Add Tunnel**;
8. Введите имя туннеля (на выбор пользователя) в поле **Name**;
9. Выберите интерфейс, через который будет работать туннель в поле **Local Address**;
10. Укажите IP-адрес порта удаленного устройства, с которым будет построен туннель, в поле **Remote Address**;
11. Выберите на каком уровне будет работать туннель в поле **Network Type** (в данном примере рассматривается L3);
12. Укажите IP-адрес интерфейса в поле **Tunnel IP**; а также его маску в поле **Tunnel Mask** при необходимости, если не указывать — маска будет назначена автоматически и будет равна /32.
13. Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле **Firewall Zone** (правила можно настроить вручную в разделе **Services** → **Firewall**);
14. Укажите в поле **Keepalive Delay** временной интервал в секундах, по истечении которого идет проверка соединения со встречной стороной;
15. Укажите в поле **Keepalive Retries** количество неудачных попыток, после которых туннель GRE отключится. При получении первого ответа от встречной стороны соединение восстанавливается;
16. При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.

## Create new GRE

### Name

### Local Address

### Remote Address

### Network Type

### Tunnel IP

### Tunnel Mask

### GRE key

### Firewall Zone

### Keepalive Delay

### Keepalive Retries

Don't Fragment packets

Рис. 12. Примеры конфигураций GRE. Настройка GRE-туннеля

## 6. IPsec туннели

### 6.1. Настройка IPsec туннеля

Для создания IPsec-туннеля на роутере должна быть настроена локальная сеть и порты WAN.

Добавить новый IPsec-туннель можно, нажав на кнопку **Add Tunnel**.

Разрешить или запретить работу уже настроенного туннеля можно, поставив галочку в поле **Enable**.

Изменить параметры или удалить туннель можно с помощью кнопок **Edit** и **Remove**.

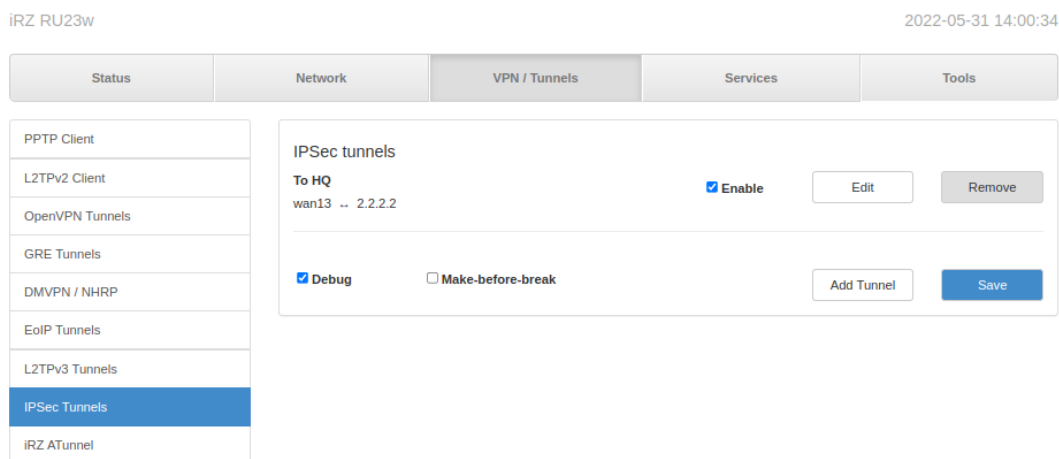


Рис. 13. Вкладка IPsec/Tunnels. Раздел IPsec tunnels

Чекбокс **Debug** увеличивает количество отладочной информации в логе.

Чекбокс **Make-before-break** включает соответствующий метод повторной аутентификации. В этом случае сначала создаются дубликаты SA (Security Associations), перекрывающиеся с существующими, а только затем удаляются старые. Это позволяет избежать разрывов соединения.



Для того чтобы метод **Make-before-break** работал, нужно чтобы оба одноранговых узла могли обрабатывать перекрывающиеся SA.

## Edit tunnel: To HQ (ipsec1)

### Description

To HQ

### Source Address

wan13

### Remote Address

2.2.2.2

### Local Identifier

left

### Remote Identifier

right

### Key Exchange Mode

ikev2

### DPD Delay (sec)

5

### Local Subnets

+ Subnet Address

### Remote Subnets

+ Subnet Address

### Local Source Address Type

Config

### Remote Source Address Type

None

### Local Source IP

10.44.25.1

### Phase #1

#### Lifetime

28800

#### IKE Encryption

aes256

#### IKE Hash

sha256

#### DH Group

14

### Phase #2

#### Lifetime

3600

#### ESP Encryption

aes256

#### ESP Hash

sha1

#### PFS Group

<none>

### Authentication Method

psk

### Pre-Shared Key

.....|

Close

Apply changes

Рис. 14. Примеры конфигураций IPsec. Настройка IPsec-туннеля

Таблица 3. Параметры туннеля

Поля	Описание
Description	Описание туннеля (на выбор пользователя)
Source Address	Физический интерфейс, через который будет работать туннель <b>Default</b> – через интерфейс, являющийся на данный момент активным WAN-портом, другие варианты - <b>SIM1, SIM2, WAN</b>
Remote Address	IP-адрес порта удаленного хоста, с которым строится туннель. Можно указать несколько адресов через ПРОБЕЛ. IPSec выполняет попытки подключения к хостам в порядке перечисления. Таймаут подключения 60 сек. Если в течение этого времени подключение не произошло, происходит переключение на следующий адрес и так по кругу.
Local Identifier	Локальный идентификатор (наименование, указывается пользователем)
Remote Identifier	Идентификатор удаленной стороны (наименование, указывается пользователем)
Key Exchange Mode	Версии протокола обмена ключей при установлении туннеля - <b>IKEv1</b> или <b>IKEv2</b>
Exchange Mode	<b>Только</b> при условии <b>Key Exchange Mode</b> версии <b>IKEv1</b> . Режим установления соединения между участниками туннеля ( <b>Main</b> – основной, <b>Aggressive</b> – более быстрый, но без обеспечения защиты подлинности на данном этапе).
Dead Peer Detect	Интервал в секундах, через который будет определяться доступность узла на противоположном конце туннеля ( <b>0</b> – отключение данной функции)
Local Subnets	Список адресов сетей с локальной стороны, между которыми устанавливается туннель (записываются в формате CIDR)
Remote Subnets	Список адресов сетей с удаленной стороны, между которыми устанавливается туннель (записываются в формате CIDR)
Local Source Address Type	Тип получения виртуального IP адреса для локальной стороны ( <b>None</b> - не настраивается, <b>Config</b> - автоматически, <b>Manual</b> - вручную)
Remote Source Address Type	Тип получения виртуального IP адреса для удаленной стороны ( <b>None</b> - не настраивается, <b>Config</b> - автоматически, <b>Manual</b> - вручную)
Local Source IP	Виртуальный IP адрес локальной стороны, используемый туннелем
Remote Source IP	Виртуальный IP адрес удаленной стороны, используемый туннелем
Authentication Method	<b>psk</b> – по общему ключу, <b>pubkey</b> – по сертификату и ключу RSA



На оборудовании iRZ в целях безопасности для входящих подключений запрещено использование функции IPsec с параметрами: KeyExchangeMode = ikev1, Aggressive mode=yes, Authentication Method = PSK.

Таблица 4. Параметры Phase #1

Поля	Описание
Lifetime	Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение минимум в два раза больше, чем у фазы 2 (например, 24 часа или 86400 секунд).
IKE Encryption	Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES.
IKE Hash	Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-512, SHA-384, MD5.
DN Group	Выбор криптографического алгоритма, который позволяет двум точкам обмениваться ключами через незащищенный канал. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ.

Таблица 5. Параметры Phase #2

Поля	Описание
Lifetime	Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение меньше, чем у фазы 1 (например, 1 час или 3600 секунд).
ESP Encryption	Выбор алгоритма шифрования: AES 128, AES 192, AES 256, 3DES.
ESP Hash	Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-384, SHA-512, MD5.
PFS Group	Выбор криптографического алгоритма, который удостоверяет, что ключи, используемые в фазе 2 не получены от фазы 1. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ.

**Authentication Method**

pubkey

**CA Certificate**

Upload CA PEM certificate

**Local Certificate**

Upload PEM certificate

**Key**

Upload PEM key

Close Apply changes

Рис. 15. Способ аутентификации pubkey



После удаления туннеля загруженные сертификаты удаляются автоматически при нажатии кнопки Save.



## 6.2. Статус IPsec туннеля

На вкладке **Status** представлена информация о состоянии туннелей, настроенных на роутере.

IPsec tunnel — информация о работе IPsec туннеля

### IPsec IKEv1 tunnel (HQ)

Status	Waiting for traffic between SA	Established	
Source	sim1	Remote	3.3.3.3
SA (Local - Remote)	dynamic - 2.2.2.2/32	Status	Waiting for traffic between SA
SA (Local - Remote)	dynamic - 4.4.4.4/32	Status	Waiting for traffic between SA
Phase1	aes256 / sha256 / DH:14	Phase2	aes256 / sha1 / PFS:15

### IPsec IKEv2 tunnel (Center)

Status	Waiting for traffic between SA	Established	
Source	default route	Remote	3.3.3.4
Local SA	default route	Remote SA	5.5.5.5/24 6.6.6.6/24
Phase1	aes256 / sha256 / DH:14	Phase2	aes256 / sha1 / PFS:NONE

Рис. 16. Пример информации в разделе IPsec tunnel

Таблица 6. Поля в разделе Status для IPsec туннеля

Поле	Описание
Status	Текущий статус туннеля
Source	Локальный интерфейс, через который будет работать туннель ( <b>Default route</b> – через интерфейс, являющийся на данный момент активным WAN-портом)
Remote	Доменное имя или IP-адрес порта удаленного устройства, с которым будет построен туннель
SA (Local - Remote)	Security Associations, политики безопасности
Phase 1, 2	Параметры аутентификации и шифрования для Фазы 1 и Фазы 2

Поле **Status** описывает текущее состояние туннеля. Возможные значения поля описаны в таблице ниже.

Таблица 7. Возможные значения поля Status

<b>Поле</b>	<b>Описание</b>
Network not available	Адрес источника с локальной стороны (Source Address) не доступен
Waiting for traffic between SA	Ожидание трафика между локальной (Local subnets / Source Address) и удалённой стороной (Remote Subnets / Remote Address) чтобы инициировать обмен ключами и согласование политик
Phase 1 established	Обмен ключами прошёл успешно, Phase 1 построена, Phase 2 не построена. Трафик не идёт
Installed	Туннель построен, трафик шифруется
Down	Роутер ожидает подключения клиентов (Remote Address указан как 0.0.0.0)

## 7. DMVPN / NHRP туннели (только для роутеров серии R4, R2, R50)

**Dynamic Multipoint VPN (DMVPN)** — виртуальная частная сеть с возможностью динамического создания туннелей между узлами. Роутеры iRZ для данного туннеля могут выступать только в роли Spoke- маршрутизатора.

Для создания данного туннеля необходимо в разделе **VPN/Tunnels** → **DMVPN/NHRP** нажать кнопку **Add Tunnel** и на открывшейся странице настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

**Edit tunnel: mgre1**

<b>Description</b>	<b>Local NBMA Address</b>	<b>Remote NBMA Address</b>
<input type="text"/>	<input type="text" value="&lt;default&gt;"/>	<input type="text" value="IP or domain name"/>
<b>Local Tunnel Address</b>	<b>HUB Tunnel Address</b>	<b>Tunnel Netmask</b>
<input type="text" value="IP address"/>	<input type="text" value="IP address"/>	<input type="text" value="ex. 255.255.255.0"/>
<b>GRE key</b>	<b>Holding Time (sec.)</b>	<b>Firewall Zone</b>
<input type="text" value="Leave blank if not used"/>	<input type="text" value="default 7200 sec."/>	<input type="text" value="&lt;none&gt;"/>

**No Caching**       **Allow Shortcuts**

**HUB is Cisco**

**Use IPSec Protection**

Рис. 17. Страница настроек DMVPN/NHRP

Таблица 8. Настройки DMVPN/NHRP

Поля	Описание
Description	Описание или название туннеля.
Local NBMA Address	Локальный адрес сети - NBMA(Non Broadcast Multiple Access), необходимо выбрать один из интерфейсов роутера; значение <default> означает использование интерфейса с маршрутом по умолчанию.
Remote NBMA Address	Удаленный адрес NBMA — указывается только IP адрес.
Local Tunnel Address	Туннельный IP адрес данного роутера.
HUB Tunnel Address	Туннельный IP адрес HUBа к которому происходит подключение.
Tunnel Netmask	Маска сети туннеля.
GRE key	Идентификационный ключ GRE туннеля в случае если данный функционал используется в конфигурации.
Holding Time (sec.)	Время (в секундах) в течение которого информация о соседнем NBMA хосте считается действительной.
Firewall Zone	Зона, в которой будет находиться туннель и соответственно политики фаервола, которые будут применяться к данному туннелю.
No Caching	Отключает кэширование информации о пирах из пересылаемых пакетов ответа на разрешение NHRP. Это можно использовать для уменьшения потребления памяти в больших подсетях NBMA.
Allow Shortcuts	Разрешает помещение в таблицу маршрутизации только тех префиксов, которые реально используются в данный момент времени.
HUB is Cisco	Данная настройка позволяет ввести ключ аутентификации в случае если хабом является оборудование компании Cisco.

HUB is Cisco

Cisco Authentication

No Unique

Allow Redirects

No Unique	Флаг неуникальности ip-адреса туннеля в базе nhpr на hub-маршрутизаторе
Allow Redirects	Разрешает направлять трафик напрямую между spoke маршрутизаторами в обход хаба
Use IPSec Protection	Открывает дополнительное поле с возможностью настроить шифрование туннеля с помощью IPSec

В случае использования шифрования туннеля с помощью технологии IPSec необходимо настроить соответствующие параметры туннеля. Подробная информация о каждом параметре приведена в разделе [IPsec туннели](#).

Таблица 9. Настройка шифрования туннеля с помощью IPSec

Поля	Описание
Local Identifier	Локальный идентификатор.
Remote Identifier	Идентификатор удаленной стороны.
Key Exchange Mode	Предназначено для переключения между первой и второй версиями обмена ключей.
Authentication Method	Способ аутентификации узлов туннеля: psk – по общему ключу, rsasig – по сертификату и ключу RSA (то же что и pubkey).
DPD Delay (sec.)	Интервал отправки DPD и keepalive пакетов.
DPD Timeout (sec.)*	Интервал по которому рвётся соединение.
Aggressive Mode*	Включение/отключение более активного [быстрого] режима (без обеспечения защиты подлинности).



Редактирование DPD Timeout и Aggressive Mode возможно только в режиме IKEv1 для Key Exchange Mode.

## 8. EoIP туннели

Ethernet over IP (EoIP) — тип туннеля, разработанный компанией MikroTik, представляет собой Ethernet туннель точка-точка поверх IP подключения. Данный туннель создает мост между двумя роутерами как будто эти роутеры подключены друг к другу напрямую через физические ethernet порты. Такой туннель можно создавать поверх любого другого туннеля или подключения, умеющего транспортировать протокол IP. Пример настроек туннеля приведен на рисунке ниже.

### Create new EoIP

The screenshot shows the 'Create new EoIP' configuration window. It contains the following fields and options:

- Name:** A text input field with the placeholder 'Name'.
- Local Address:** A dropdown menu currently showing 'loopback'.
- Remote Address:** A dropdown menu currently showing 'Only remote IP'.
- Add to Bridge or Create New:** A dropdown menu currently showing '<new network>'. Below this field, there are two checkboxes: 'Add to existing network' (unchecked) and 'Create new network' (checked).
- Tunnel IP:** A text input field with the placeholder 'Local IP address for tunnel'.
- Tunnel Mask:** A text input field with the placeholder 'Netmask'.
- Tunnel ID:** An empty text input field.
- Firewall Zone:** A dropdown menu currently showing '<none>'.

At the bottom right of the form, there are two buttons: 'Close' and 'Apply Changes'.

Рис. 18. Настройка EoIP-туннеля

Для создания туннеля необходимо проделать следующие шаги:

1. Зайдите в раздел **VPN / Tunnels** → **EoIP Tunnels** и создайте новый туннель кнопкой **Add Tunnel**.
2. В открывшихся настройках туннеля укажите имя туннеля в поле **Name**, если требуется.
3. В поле **Local Address** укажите интерфейс через который будет работать туннель.
4. В поле **Remote Address** необходимо указать адрес удаленной точки туннеля.
5. В поле **Add to Bridge or Create New** необходимо выбрать локальную сеть с которой будет создан мост или же задать отдельный адрес туннельного интерфейса.
6. В случае если в предыдущем пункте выбран вариант задания отдельного адреса для интерфейса туннеля необходимо в полях **Tunnel IP** и **Tunnel Mask** указать IP адрес и маску сети для интерфейса туннеля.

7. Поле **Tunnel ID** предназначено для задания идентификационного номера туннеля, в случае если создается несколько туннелей с терминованием на одной удаленной точке, для того чтобы текущий роутер и удаленный могли различать пакеты разных туннелей.
8. Поле **Firewall Zone** предназначено для ассоциации туннеля с одной из зон фаервола.

## 9. L2TPv3 туннели

L2TPv3 (англ. Layer 2 Tunneling Protocol — протокол туннелирования второго уровня версия 3) — в компьютерных сетях туннельный протокол, использующийся для поддержки виртуальных частных сетей.

Для настройки туннеля необходимо зайти в раздел VPN/Tunnels → L2TPv3 и добавить новый туннель по кнопке Add Tunnel.

В открывшемся окне настроек (см. рисунок ниже) заполнить поля согласно таблице приведенной далее.

Create new L2TP

---

<b>Name</b>	
<input type="text" value="Name"/>	
<b>Local Address</b>	<b>Remote Address</b>
<input type="text" value="loopback"/>	<input type="text" value="Only remote IP"/>
<b>Add to Bridge or Create New</b>	<b>Firewall Zone</b>
<input type="text" value="&lt;new network&gt;"/>	<input type="text" value="&lt;none&gt;"/>
<b>Tunnel IP</b>	<b>Tunnel Mask</b>
<input type="text" value="Local IP address for tunnel"/>	<input type="text" value="Netmask"/>
<b>Tunnel ID</b>	<b>Remote Tunnel ID</b>
<input type="text" value="0"/>	<input type="text"/>
<b>Session ID</b>	<b>Remote Session ID</b>
<input type="text" value="0"/>	<input type="text"/>
<b>Encapsulation</b>	<b>L2 Specific Header Type</b>
<input type="text" value="ip"/>	<input type="text" value="none"/>

---

Рис. 19. Настройка L2TPv3-туннеля



Таблица 10. Настройки L2TP3

Поля	Описание
Name	Название туннеля.
Local Address	Локальный интерфейс на роутере через который будет устанавливаться соединение.
Remote Address	IP-адрес удаленной сети, участвующей в туннеле.
Add to Bridge or Create New	Установление моста с каким-то из локальных интерфейсов (lan) роутера или создание отдельного интерфейса со своей подсетью - <new network>.
Tunnel IP	IP адрес туннельного интерфейса.
Tunnel Mask	Маска сети туннельного интерфейса.
Tunnel ID	ID — идентификатор туннеля на данном устройстве.
Session ID	ID — идентификатор сессии на данном устройстве.
Firewall Zone	Включение туннельного интерфейса в одну из зон фаервола.
Remote Tunnel ID	ID — идентификатор удаленного конца туннеля.
Remote Session ID	ID — идентификатор сессии на удаленном конце туннеля.
Encapsulation	Выбор способа идентификации сессии туннеля, для синхронизации настройки с двух сторон туннеля.
L2 Specific Header Type	Указывает специальное поле подуровня L2TPv3 Layer 2 для использования в заголовках пакетов данных в соответствии с RFC3931

## 10. Термины и сокращения

**GSM** – стандарт сотовой связи («СПС-900» в РФ);

**GPRS** – стандарт передачи данных в сетях операторов сотовой связи «поколения 2.5G» основанный на пакетной коммутации (до 56 Кбит/с);

**EDGE** – преемник стандарта GPRS, представитель «поколения 2.75G», основанный на пакетной коммутации (до 180 Кбит/с);

**HSPA (HSDPA, HSUPA)** – технология беспроводной широкополосной радиосвязи, использующая пакетную передачу данных и являющаяся надстройкой к мобильным сетям WCDMA/UMTS, представитель «поколения 3G» (HSUPA - до 3,75 Мбит/с, HSDPA - до 7,2 Мбит/с);

**WCDMA** – стандарт беспроводной сотовой связи;

**3G** - общее описание набора стандартов, описывающих работу в широкополосных мобильных сетях UMTS и GSM: GPRS, EDGE, HSPA;

**IP-сеть** – компьютерная сеть, основанная на протоколе IPv4 (Internet Protocol) - межсетевой протокол 4 версии. IP-сеть позволяет объединить для взаимодействия и передачи данных различные виды устройств (роутеры, компьютеры, сервера, а так же различное узкоспециализированное оборудование);

**IP-адрес** – адрес узла (компьютера, роутера, сервера) в IP-сети;

**Внешний IP-адрес** – IP-адрес в сети Интернет, предоставленный провайдером услуг связи в пользование клиенту на своём/его оборудовании для обеспечения прямой связи с оборудованием клиента через сеть Интернет;

**Фиксированный внешний IP-адрес** – внешний IP-адрес, который не может измениться ни при каких условиях (смена типа оборудования клиента и др.) или событиях (переподключение к сети провайдера и др.); единственной возможностью сменить фиксированный IP-адрес является обращение к провайдеру;

**Динамический IP-адрес** – IP-адрес, который может меняться при каждом новом подключении к сети;

**Динамический внешний IP-адрес** – внешний IP-адрес в сети Интернет, изменяющийся, как правило, в одном из следующих случаев:

- при каждом новом подключении к Интернет;
- по истечении срока аренды клиентского локального IP-адреса;
- через заданный промежуток времени;
- в соответствии с другой политикой клиентской адресации провайдера;

**Локальный IP-адрес:**

- IP-адрес, назначенный локальному интерфейсу роутера, как правило локальный IP-адрес должен находиться в адресном пространстве обслуживаемой роутером сети;

- IP-адрес, присвоенный оборудованием Интернет-провайдера клиентскому устройству в момент подключения к Интернет; данный IP-адрес не может быть использован для получения доступа к клиентскому устройству из вне (через сеть Интернет), он позволяет только пользоваться доступом в Интернет;

**Серый/частный/приватный IP-адрес** – см. определение для термина "**локальный IP-адрес**";

**Узел сети** – объект сети (компьютерной/сотовой), способный получать от других узлов сети и передавать этим узлам служебную и пользовательскую информацию;

**Клиент/клиентский узел/удаленный узел/удалённое устройство** – устройство, территориально удалённое от места, либо объекта/узла, обсуждаемого в конкретно взятом контексте;

**Сетевой экран (firewall)** – программный аппаратный комплекс, призванный выполнять задачи защиты обслуживаемой роутером сети, её узлов, а так же самого роутера от: нежелательного трафика, несанкционированного доступа, нарушения их работы, а так же обеспечения целостности и конфиденциальности передаваемой информации на основе predetermined администратором сети правил и политик обработки трафика в обоих направлениях;

**(Удалённая) командная строка, (удалённая) консоль роутера** – совокупность программных средств (серверная и клиентская программы Telnet/SSH), позволяющая осуществлять управление роутером посредством консольных команд при отсутствии физического доступа к устройству;

**Служебный трафик** – трафик, содержащий в себе служебную информацию, предназначенную для контроля работы сети, поддержания целостности передаваемых пользовательских данных и взаимодействия сетевых служб двух и более узлов между собой;

**Пользовательские данные (в сети)** – информация, создаваемая или используемая оборудованием в сети пользователя, для передачи, обработки и хранения которой было разработано техническое решение;

**Нежелательный трафик** – трафик, не несущий полезной нагрузки, который тем не менее генерируется одним или несколькими узлами сети, тем самым создавая паразитную нагрузку на сеть;

**Сетевая служба** – служба, обеспечивающая решения вопросов обработки, хранения и/или передачи информации в компьютерной сети;

**Сервер** – этот термин может быть использован в качестве обозначения для:

- серверной части программного пакета используемого в вычислительном комплексе;
- роли компонента, либо объекта в структурно-функциональной схеме технического решения, развёртываемого с использованием роутера;
- компьютера, предоставляющего те или иные сервисы (сетевые службы, службы обработки и хранения данных и прочие);

**Провайдер** – организация, предоставляющая доступ в сеть Интернет;

**Оператор сотовой связи** – организация, оказывающая услуги передачи голоса и данных, доступа в Интернет и обслуживания виртуальных частных выделенных сетей (VPN) в рамках емкости своей сотовой сети;

**Относительный URL-путь** – часть строки web-адреса в адресной строке браузера, находящаяся после доменного имени или IP-адреса удалённого узла, и начинающаяся с символа косой черты

(символ «/»), пример:

Исходный web-адрес: <http://192.168.1.1/index.php>

Относительный путь: /index.php

**"Crossover"-патчкорд** – сетевой кабель, проводники которого обжаты таким образом, что его можно использовать для прямого подключения роутера к компьютеру без необходимости использования коммутационного оборудования;

**Учётная запись, аккаунт** – другое название "личного кабинета" пользователя Интернет-сайта, позволяющего вносить и редактировать его личные данные, настройки;

**USB-накопитель** – запоминающее устройство, подключаемое к роутеру через USB-интерфейс, и используемое для сохранения/считывания служебной информации роутера; может быть использовано для резервирования настроек роутера, их восстановления, а так же для автоматической конфигурации службы OpenVPN (не сервера OpenVPN).

**Сертификат** – электронный или печатный документ, выпущенный удостоверяющим центром, для подтверждения принадлежности владельцу открытого ключа или каких-либо атрибутов;

**Корневой сертификат** – сертификат выданный и подписанный одним и тем же центром сертификации;

**Ключ сервера** – блок криптографической информации, позволяющий серверу OpenVPN подтвердить свою подлинность в момент попытки получения доступа клиентом к сети, обслуживаемой данным сервером;

**Ключ клиента/пользователя** – блок криптографической информации, позволяющий пользователю, либо клиентскому узлу идентифицировать себя в системе, к которой он осуществляет попытку доступа;

**Топология сети** – термин, позволяющий описать конфигурацию сети на разных уровнях взаимодействия информационных систем. Как правило, топология сети формируется администратором/архитектором сети исходя из поставленных задач, решаемых техническим решением, основная идея которого реализуется данной сетью;

**Сетевой интерфейс** – данный термин имеет несколько определений:

- Аппаратная часть роутера, позволяющая осуществлять на низких уровнях взаимодействия связь с удалёнными узлами, а так же обмениваться с ними информацией;
- Программный виртуальный объект ОС, позволяющий определить правила и порядок следования и обмена информацией между узлами компьютерной сети;

**OpenVPN** – открытый бесплатный программный продукт, позволяющий создать защищённую виртуальную среду передачи данных внутри IP-сети. Поскольку OpenVPN представляет из себя многофункциональный программный пакет, в различном контексте термин «OpenVPN» может иметь различные значения, самые распространённые из которых: «сервер доступа к сети OpenVPN», «клиент, позволяющий подключиться к OpenVPN-сети», «сеть, либо сектор/уровень/слой сети, подразумевающий использование ПО OpenVPN»;

**OpenVPN-сеть** – IP-сеть, построенная на базе сети, созданной ПО OpenVPN;

**(Виртуальное) адресное пространство OpenVPN-сети** – адресное пространство IP-сети OpenVPN, призванное добавить сегмент в совокупность всех сетей на пути следования пользовательских данных, то есть обеспечить чёткую декомпозицию маршрута, тем самым упрощая проектирование и обслуживание всего вычислительного комплекса, построенного на базе ПО OpenVPN в целом;

**OpenVPN-клиент** – см. клиентский узел;

**Туннель** – виртуальная сущность/технология/объект, позволяющая логически выделить конкретно взятый поток данных между двумя узлами, заключая его в отдельное от общего адресное пространство; Авторизация – процедура предоставления надлежащих прав субъекту (пользователю/участнику/клиенту/клиентскому узлу) системы после получения от него запроса на доступ к системе и прохождения проверки его подлинности (аутентификации);

**Аутентификация** – процедура проверки подлинности субъекта (пользователя/участника/клиента/ клиентского узла) системы путём сравнения предоставленных им на момент подключения реквизитов с реквизитами, соотнесёнными с указанным именем пользователя/логином в базе данных.

## 11. Контакты

Новые версии прошивок, документации и сопутствующего программного обеспечения можно получить, обратившись по следующим контактам:

### Санкт-Петербург

сайт компании в Интернете	<a href="http://www.radiofid.ru">www.radiofid.ru</a>
тел. в Санкт-Петербурге	+7 (812) 318 18 19
e-mail	<a href="mailto:support@radiofid.ru">support@radiofid.ru</a>
Telegram	@irzhelpbot

Наши специалисты всегда готовы ответить на все Ваши вопросы, помочь в установке, настройке и устранении проблемных ситуаций при эксплуатации оборудования.

В случае возникновения проблемной ситуации, при обращении в техническую поддержку, следует указывать версию программного обеспечения, используемого в роутере. Так же рекомендуется к письму прикрепить журналы запуска проблемных сервисов, снимки экранов настроек и любую другую полезную информацию. Чем больше информации будет предоставлено сотруднику технической поддержки, тем быстрее он сможет разобраться в сложившейся ситуации.



Перед обращением в техническую поддержку настоятельно рекомендуется обновить программное обеспечение роутера до актуальной версии.



Нарушение условий эксплуатации (ненадлежащее использование роутера) лишает владельца устройства права на гарантийное обслуживание.