

# РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

# Настройка туннелей на роутерах iRZ







# Содержание

1. Введение	4
1.1. Описание документа	4
1.2. Предупреждение	4
2. Примеры конфигураций OpenVPN	5
2.1. OpenVPN Layer 2: dev TAP	5
2.1.1. Пример настройки тоннеля без аутентификации (Authentication method: None)	5
2.1.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: St	າared 。
	0
2.1.3. Пример настроики тоннеля с аутентификацией по протоколу TLS, когда роутер высту	naer
	9
2.1.4. Пример настроики тоннеля с аутентификацией по протоколу TLS, когда роутер высту	naei
в роли клиента OpenVPN	11
2.2. OpenVPN Layer 3: dev TUN	12
2.2.1. Пример настройки тоннеля без аутентификации (Authentication method: None)	12
2.2.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: Sh	nared
Secret)	14
2.2.3. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер высту	лает
в роли сервера OpenVPN	16
2.2.4. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер высту	лает
в роли клиента OpenVPN	17
2.3. Инструкция по настройке тоннеля GRE (на примере роутеров iRZ R4)	19
2.3.1. Настройка GRE-тоннеля уровня L2 (на примере двух роутеров RU41)	19
2.3.2. Настройка GRE-тоннеля уровня L3 (на примере двух роутеров RU41)	22
2.4. Создание IPsec-тоннеля (на роутерах серии R4, R1)	25
3. Термины и сокращения	29
4. Контакты и поддержка	33





#### Рисунки

Рис. 2.1. Схема сети	5
Рис. 2.2. Настройка OpenVPN (без аутентификации), базовая ТАР (L2)	6
Рис. 2.3. Hacтройкa OpenVPN (без аутентификации), Bridge with Interface = None	7
Рис. 2.4. Настройка OpenVPN (с аутентификацией по ключу)	8
Рис. 2.5. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер	10
Рис. 2.6. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент	11
Рис. 2.7. Схема сети	12
Рис. 2.8. Настройка OpenVPN (без аутентификации), базовая TUN (L3)	13
Рис. 2.9. Настройка OpenVPN (с аутентификацией по ключу)	15
Рис. 2.10. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер	17
Рис. 2.11. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент	18
Рис. 2.12. Схема сети	19
Рис. 2.13. Настройка локальной сети	19
Рис. 2.14. Настройка WAN	20
Рис. 2.15. Настройка GRE-тоннеля	21
Рис. 2.16. Схема сети	22
Рис. 2.17. Настройка локальной сети	22
Рис. 2.18. Настройка WAN	23
Рис. 2.19. Настройка GRE-туннеля	24
Рис. 2.20. Настройка IPsec-тоннеля	25
Рис. 2.21. Параметры туннеля	27
Рис. 2.22. Параметр Authentication Method	28

### Таблицы

Таблица 2.1. Настройки OpenVPN Tunnel → TAP (L2), основные настройки	6
Таблица 2.2. Настройки OpenVPN Tunnel $\rightarrow$ TAP (L2), Bridge with Interface = None	7
Таблица 2.3. Ключи и сертификаты для аутентификации по протоколу TLS	9
Таблица 2.4. Настройки OpenVPN Tunnel → TUN (L3), основные настройки	13
Таблица 2.5. Настройки OpenVPN Tunnel → TUN (L3), Bridge with Interface = None	14
Таблица 2.6. Ключи и сертификаты для аутентификации по протоколу TLS	16





# 1. Введение

### 1.1. Описание документа

Данный документ содержит примеры корректной конфигурации сетевой службы OpenVPN, GRE, IPsec в решениях, построенных на базе роутеров iRZ. Для получения информации о работе самих устройств смотрите соответствующее руководство пользователя. Для получения информации о вебинтерфейсе роутеров смотрите документ «Руководство пользователя. Средства управления и мониторинга на роутерах iRZ».

Версия документа		Дата публикации	
1.0 (17.07.2017)		Основной документ	
Подготовлено:	Колмак О., Головин В.Н.	Проверено:	Колмак О.

## 1.2. Предупреждение

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

Внимание! 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. Примеры конфигураций OpenVPN

## 2.1. OpenVPN Layer 2: dev TAP

OpenVPN тоннель бывает двух типов: Ethernet Bridging и Routing. В данном разделе рассматривается тоннель OpenVPN типа Ethernet Bridging.

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

Всего четыре варианта настройки тоннеля, 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 тоннель 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.

В примерах настройки используется следующая схема сети:





### 2.1.1. Пример настройки тоннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-тоннеля с TAP (Layer 2) без аутентификации между сетевыми устройствами, 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. В поле Authentication Method выберите значение None;
- **5.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

RU41u				Wireless s for M2M w 2016-11-24 08:49:21	olu /orl
Status	Network	Serv	vices	Tools	
al Network	Enable OpenVPN Tuppel				
ed Internet	Device		Transport protocol		
bile Internet	TAP (L2)	¥	UDP	•	
eless Network	Remote		Port		
S servers	192.168.246.100		9995		
utes	Authentication method		Bridge with interface		
TP Client	None	•	lan	•	
	Ping interval		Ping timeout		
	60		120		
enVPN Tunnel	LZO Compression				
ec tunnels	Always	¥			
tch	Additional config				

Рис. 2.2. Настройка OpenVPN (без аутентификации), базовая TAP (L2)

### Таблица 2.1. Настройки OpenVPN Tunnel → TAP (L2), основные настройки

Поле	Описание
Device	Выбор виртуального интерфейса (в данном примере – <b>ТАР (L2)</b> )
Transport Protocol	Выбор транспортного протокола:
	UDP;
	TCP Server;
	TCP Client.
Remote	IP-адрес удаленного сетевого устройства (указывается если <b>Transport Protocol</b> = UDP или TCP Client)
Port	Номер порта, через который будет работать тоннель
Authentification Method	Метод авторизации (в данном примере – <b>None</b> )
Bridge with Interface	Создание моста с локальными интерфейсами роутера (дополнительные настройки см. в таблице 2.2)
Advanced Settings (нажи	ите на строчку Show advanced settings, чтобы открыть доступ к настройкам):
Ping Interval	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы тоннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-тоннель, если ответ от удаленного устройства не будет получен
LZO Compression	Включение или отключение сжатия данных, проходящих через тоннель

Если создать мост с LAN-портами (**Bridge with Interface = LAN**), тогда эти порты будут использоваться как интерфейсы для тоннеля.





Если не создавать мост (Bridge with Interface = None), тогда в настройках необходимо будет

дополнительно указать вручную адреса подсети, маску и шлюз по умолчанию, как показано на Рис. 2.3.

Status	Network	Servi	ices	Tools	
Local Natwork					
	Enable OpenVPN Tunnel				
Wired Internet	Device		Transport protocol		
Mobile Internet	TAP (L2)	¥	UDP v		
Wireless Network	Remote		Port		
DNS servers	192.168.246.100		9995		
Routes	Authentication method		Bridge with interfac	e	
	None	•	none	•	
PPTP Client	Local VPN endpoint IP address		VPN subnet mask		
GRE Tunnels	10.10.10.2		255.255.255.0		
OpenVPN Tunnel	Remote Subnet	Remote Subnet Mas	;k	Remote Gateway	
IPSec tunnels	192.168.10.0	255.255.255.0		10.10.10.1	
Switch	Ping interval		Ping timeout		
	60		120		
	LZO Compression				
	Always	•			
	Additional config				
				li li	
				Save	

Рис. 2.3. Настройка OpenVPN (без аутентификации), Bridge with Interface = None

Поле	Описание
Local VPN Endpoint IP Address	IP-адрес тоннеля на данном устройстве
VPN Subnet Mask	Маска IP-адреса тоннеля на данном устройстве
Remote Subnet	IP-адрес удаленной сети (на другом конце тоннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце тоннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце тоннеля)

Таблица 2.2. Настройки OpenVPN Tunnel → TAP	(L2), Bridge with Interface = None
---	------------------------------------

Поле Additional Config позволяет указывать конфигурационные параметры, которые роутер будет передавать, подключающемуся к нему сетевому устройству. 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





# 2.1.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-тоннеля с TAP (Layer 2) с аутентификацией по общему ключу между сетевыми устройствами, в веб-интерфейсе роутера:

- **1.** Зайдите в раздел Network  $\rightarrow$  OpenVPN Tunnel;
- 2. Поставьте галочку напротив пункта Enable OpenVPN tunnel;
- 3. Выберите в поле Device значение TAP (L2);
- 4. В поле Authentication Method выберите значение Shared Secret;
- 5. Добавьте заранее сгенерированный ключ в поле Shared Secret (см. описание далее);
- **6.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рис. 2.4).

	Enable OpenVPN Tunnel		
Wired Internet	Device	Transport protocol	
Mobile Internet	TAP (L2)	TCP Server	•
Wireless Network	Remote	Port	
DNS servers		9995	
Routes	Authentication method	Bridge with interface	
PPTP Client	Shared secret	• lan	•
	Shared Secret		
GRE Tunnels	BEGIN OpenVPN Static key V1		
OpenVPN Tunnel	03ffb4496658b9ed4628feee9a48b01f		
IPSec tunnels	c625234208dc195d5c33e275d1bef2a6		
Cwitch	c478549231a3320db44c1165520fa437		
Switch	3b48a71f73e8b03e05293de3158ce43f		
	69e8d5b6bc3211ac14269ebd0b089df8 fd16222a5bcd47df22256b89d5cd47b4		
	81ec2928b1068429dbe7c26c19e466bc		
	548b4ad42a3a96cd524f921032f50db2		
	9591223f6f09ba6fda1e5a4bec201b0a		
	57bce5603f31c66ddd8267525ccec321		
	7360bff0fc5714a15d7b0960bc0bd959		
	12e65592c16661ae580a9c73fc594731		
	672b4fb53f7aa89468a9d84b909ae526		
	e03cde09t44d45572a000c4674ce4687		
	END OpenVPN Static key V1		1,
	Ping interval	Ping timeout	
	60	120	
	LZO Compression		
	Always	<b>T</b>	
	Additional config		

Рис. 2.4. Настройка OpenVPN (с аутентификацией по ключу)





# 2.1.3. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN

Для настройки OpenVPN-тоннеля с TAP (Layer 2) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-сервера, 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. В поле Authentication Method выберите значение TLS Server;
- 5. Добавьте необходимые сертификаты и ключи в поля: CA Certificate, DH Parameter, Local Certificate, Local Private Key (см. далее описание);
- **6.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key**. Ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы тоннеля понадобятся файлы, указанные в таблице 2.3.

Поле	Файл	Описание	
CA Certificate	ca.crt	Сертификат удостоверяющего центра	
DH Parameter	dh1024.pem	Файл Диффи-Хелмана для защиты передаваемых данных от расшифровки	
Local Certificate	server.crt	Сертификат сервера OpenVPN	
Local Private Key	server.key	Приватный ключ сервера OpenVPN, секретный	

Таблица 2.3. Ключи и сертификаты для аутентификации по протоколу TLS

Из полученных файлов необходимо будет скопировать зашифрованные данные, которые начинаются строкой "BEGIN CERTIFICATE", а заканчиваются "END CERTIFICATE", и вставить текст в соответствующие поля согласно таблице 2.3. Пример настройки показан на рис. 2.5.



			tor inizini v
ocal Network	Enable OpenVPN Tunnel		
Vired Internet	Device	Transport protocol	
Iobile Internet	TAP (L2)	TCP Client	T
eless Network	Remote	Port	
servers		9995	
	Authentication method	Bridge with interface	
	TLS Server	▼ lan22	v
ent.	Ca Certificate		
ls	BEGIN CERTIFICATE		*
nnel	MIID1DCCA22gAwiBAgiJAJZzMYh	171sJMA0GCSgGSlb3DQEBBQUAMIGjMQswCQYD	-
			1
	DH Parameter		*
	BEGIN DH PARAMETERS MIGHAoGBANyKsLW7LmwW85jQr	C8BEZdos8twYzGKgNc4Yu9wSncxBXCgm80CknN5	
	O7fg8lrSyCEaRu1Zi/oJONTnEHOP	JaBeGPuUpdFOxGOYoLe31JYT+uGL8hueGKl8	•
	Local Certificate		
	BEGIN CERTIFICATE		*
	MIIENDCCA52gAwiBAgiBATANBgk		-
	CZAJBGINVBAGTAINQMROWEWYDY	QOHEWX10FBI0GVyczJ1CIIICXEDAOB <u>0</u> NVBA01B1RI	11
	Local private key		
	BEGIN PRIVATE KEY		*
	MIICEAIBADANBgkghkiG9w0BAQE 6XrRc8Xes+gKUyTsTLtjGGkRkIRVI	FAASCAmiwggJeAgEAAoGBALg/LnKXPSAdZc5C ?eChcS9kDH/R7MuGO7Ktl3NIrt5uHi/je51t	-
	Diss interval	Disc time at	1
		Ping timeout	
	60	120	
	LZO Compression		
	Adaptive	Ŧ	

Рис. 2.5. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

При выборе протокола передачи данных в поле **Transport Protocol** следует учитывать, что по протоколу UDP тоннель будет работать быстрее всего, так как при использовании протокола TCP Server роутер будет ожидать установления соединения от удаленного устройства. При выборе TCP Client (необходимо будет указать в поле **Remote** – адрес устройства) – роутер будет сам инициировать соединение с удалённым устройством.





# 2.1.4. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN

Для настройки OpenVPN-тоннеля с TAP (Layer 2) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-клиента, 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. В поле Authentication Method выберите значение TLS Client;
- 5. Добавьте необходимые сертификаты и ключи в поля: CA Certificate, Local Certificate, Local Private Key (см. далее описание);
- **6.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.1.2, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**, **Local Certificate**, **Local Private Key**. Ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы тоннеля понадобятся файлы, указанные в таблице 2.3, кроме файла Диффи-Хелмана. Пример настройки показан на рис. 2.6.

	Enable OpenVPN Tunnel	
ired Internet	Device	Transport protocol
obile Internet	TAP (L2)	TCP Client
ireless Network	Remote	Port
NS servers		9995
outes	Authentication method	Bridge with interface
	TLS Client	▼ lan22
I P Client	Ca Certificate	
E Tunnels	BEGIN CERTIFICATE	
enVPN Tunnel	MIID1DCCAz2gAwlBAgIJAJZzMYhh VOOGEwJSVTELMAkGA1UECBMC	71sJMA0GCSqGSIb3DQEBBQUAMIGjMQswCQYD U1AxFTATBqNVBAcTDFN0UGV0ZXJzYnVyZzEQMA4G
Sec tunnels		
tch		
Non	MIENDCCA52gAwlBAglBATANBgkg	hkiG9w0BAQQFADCBozELMAkGA1UEBhMCUlUx
	CzAJBgNVBAgTAINQMRUwEwYDV	2QHEwxTdFBldGVyc2J1cmcxEDAOBgNVBAoTB1Rl
	Local private key	
	BEGIN PRIVATE KEY	
	6XrRc8Xes+qKUyTsTLtjGGkRkIRVP	AASCAIIIWggbeageAAogBacg/LiikXPSAuzcsc eChcS9kDH/R7MuGO7Ktl3NIn5uHi/je51t
	Ping interval	Ping timeout
	60	120
	LZO Compression	
	Adaptive	×
	Adaptive Additional config	Ŧ

Рис. 2.6. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент





### 2.2. OpenVPN Layer 3: dev TUN

OpenVPN тоннель бывает двух типов: Ethernet Bridging и Routing. В данном разделе рассматривается тоннель OpenVPN типа Routing.

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

Всего четыре варианта настройки тоннеля, 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 тоннель 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.

В примерах настройки используется следующая схема сети:



Рис. 2.7. Схема сети

#### 2.2.1. Пример настройки тоннеля без аутентификации (Authentication method: None)

Для настройки OpenVPN-тоннеля с TUN (Layer 3) без аутентификации между сетевыми устройствами, 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. В поле Authentication Method выберите значение None;
- **5.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).



Status	Network	Services	Tools
.ocal Network	Enable OpenVPN Tunnel		
Wired Internet	Device	Transport protocol	
Mobile Internet	TUN (L3)	TCP Server	
Wireless Network	Remote	Port	
DNS servers		9995	
Routes	Authentication method	Bridge with interface	
PPTP Client	None	• none	
· · · · ·	Local VPN endpoint IP address	Remote VPN endpoint I	P address
GRE Tunnels	10.10.10.1	10.10.10.2	
OpenVPN Tunnel	Remote Subnet	Remote Subnet Mask	
IPSec tunnels	192.168.40.0	255.255.255.0	
Switch	Ping interval	Ping timeout	
	60	120	
	LZO Compression		
	Always	Ŧ	
	Additional config		

#### Рис. 2.8. Настройка OpenVPN (без аутентификации), базовая TUN (L3)

#### Таблица 2.4. Настройки OpenVPN Tunnel → TUN (L3), основные настройки

Поле	Описание
Device	Выбор виртуального интерфейса (в данном примере – <b>TUN (L3)</b> )
Transport Protocol	Выбор транспортного протокола:
	UDP;
	TCP Server;
	TCP Client.
Remote	IP-адрес удаленного сетевого устройства (указывается если <b>Transport Protocol</b> = UDP или TCP Client)
Port	Номер порта, через который будет работать тоннель
Authentification Method	Метод авторизации (в данном примере – <b>None</b> )
Bridge with Interface	Создание моста с локальными интерфейсами роутера (в данном примере неактивно)
Advanced Settings (нажм	иите на строчку Show advanced settings, чтобы открыть доступ к настройкам):
Ping Interval	Время в секундах, через которое будут отсылаться ICMP-пакеты для проверки доступности удаленного сетевого устройства (и соответственно работы тоннеля)
Ping Timeout	Время ожидания в секундах, через которое устройство попытается заново создать OpenVPN-тоннель, если ответ от удаленного устройства не будет получен
LZO Compression	Включение или отключение сжатия данных, проходящих через тоннель

Поле Bridge with Interface не активно в данной конфигурации, из-за специфики работы OpenVPN с маршрутизацией.





Поле	Описание
Local VPN Endpoint IP Address	IP-адрес тоннеля на данном устройстве*
Remote VPN Endpoint IP Address	Удаленный IP-адрес тоннеля (устройство на другом конце тоннеля)*
Remote Subnet	IP-адрес удаленной сети (на другом конце тоннеля), который необходим для создания маршрута в таблице маршрутизации
Remote Subnet Mask	Маска удаленной сети (на другом конце тоннеля)
Remote Gateway	Шлюз удаленной сети (на другом конце тоннеля)

Таблица 2.5. Настройки OpenVPN Tunnel → TUN (L3), Bridge with Interface = None

\* Так как тоннель OpenVPN с маршрутизацией является тоннелем по типу point-to-point, поэтому адреса в этих полях должны указываться с учётом маски сети /32 (255.255.255.255) и не должны совпадать с адресами локальных сетей на концах тоннеля.

Поле Additional Config позволяет указывать конфигурационные параметры, которые роутер будет передавать, подключающемуся к нему сетевому устройству. 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

# 2.2.2. Пример настройки тоннеля с аутентификацией по ключу (Authentication method: Shared Secret)

Для настройки OpenVPN-тоннеля с TUN (Layer 3) с аутентификацией по общему ключу между сетевыми устройствами, 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. В поле Authentication Method выберите значение Shared Secret;
- 5. Добавьте заранее сгенерированный ключ в поле Shared Secret (см. описание далее);
- 6. А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).

При выборе данного метода аутентификации, большинство настроек в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поле **Shared Secret**, в котором указывается общий ключ. Сам ключ необходимо заранее сгенерировать и распространить на устройствах участниках (см. рис. 2.4).



				for M2M
осаі метмогк	Enable OpenVPN Tunnel			
Vired Internet	Device		Transport protocol	
Iobile Internet	TUN (L3)	v	TCP Server	
Vireless Network	Remote		Port	
DNS servers			9995	
loutes	Authentication method		Bridge with interface	
	Shared secret	v	lan	
	Local VPN endpoint IP address		Remote VPN endpoint IP address	
GRE Tunnels	10.10.10.1		10.10.10.2	
penVPN Tunnel	Shared Secret			
	c6e5b3d0944ee931060/158b405b0bed c478549231a3320db44c1165520fa437 3b48a71/73e8b03e05293de3158ce43f 69e8d5b6bc3211ac14269ebd0b089df8 fd16232e5bed47df23355b88d5ed47b4 81ec2928b1068429dbe7c26c19e466bc 548b4ad42a3a96cd524f921032f50db2 9591223f6109ba6fda1e5a4bec201b0a 57bce5603f31c66ddd8267525cce4321 7360bff0tc5714a15d7b0960bc0bd959 12e65592c16661ae580a9c73fc594731 672b4fbs3f7aa89468a9d84b909ae526 e03cde09f44d45572a000c4674ce4687 END <u>OpenVPN</u> Static key <u>V1</u>			
	Remote Subnet		Remote Subnet Mask	
	192.168.40.0		255.255.255.0	
	Ping interval		Ping timeout	
	60		120	
	LZO Compression			

Рис. 2.9. Настройка OpenVPN (с аутентификацией по ключу)

-





# 2.2.3. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли сервера OpenVPN

Для настройки OpenVPN-тоннеля с TUN (Layer 3) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-сервера, 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. В поле Authentication Method выберите значение TLS Server;
- 5. Добавьте необходимые сертификаты и ключи в поля: CA Certificate, DH Parameter, Local Certificate, Local Private Key (см. далее описание);
- **6.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.4 и 2.5).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**, **DH Parameter**, **Local Certificate**, **Local Private Key**. Необходимые ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы тоннеля понадобятся файлы, указанные в таблице 2.6.

Поле	Файл	Описание			
CA Certificate	ca.crt	Сертификат удостоверяющего центра			
DH Parameter	dh1024.pem	Файл Диффи-Хелмана для защиты передаваемых данных от расшифровки			
Local Certificate	server.crt	Сертификат сервера OpenVPN			
Local Private Key	server.key	Приватный ключ сервера OpenVPN, секретный			

Таблица 2.6. Ключи и сертификаты для аутентификации по протоколу TLS

Из полученных файлов необходимо будет скопировать зашифрованные данные, которые начинаются строкой "BEGIN CERTIFICATE", а заканчиваются "END CERTIFICATE", и вставить текст в соответствующие поля согласно таблице 2.6. Пример настройки показан на рис. 2.10.



			fi	or M2N	
лк	Enable OpenVPN Tunnel				
iet	Device		Transport protocol		
net	TUN (L3)	Ŧ	TCP Server	•	
work	Remote		Port		
			9995		
	Authentication method		Bridge with interface		
	TLS Server	•	lan	v	
	Local VPN endpoint IP address		Remote VPN endpoint IP address		
	10.10.10.1		10.10.10.2		
nnel	Ca Certificate				
6	BEGIN CERTIFICATE			*	
	MIID1DCCA22qAwIBAqIJAJZzMYhh71sJMA0G VQQGEwJSVTELMAkGA1UECBMCU1AxFTAT	CSqGSIb3DQE BgNVBAcTDFN	BBQUAMIGIMQswCQYD I0UGV0ZXJzYnVyZzEQMA4G	•	
	DH Parameter				
	BEGIN DH PARAMETERS MIGHAoGBANyKsLW7LmwW85jOrC8BEZdost Q7fq8IrSyCEaRu1Zi/oJONTnEHOPJaBeGPuU	ItwYzGKqNc4Yu pdFOxGOYoLe3	9wSncxBXCgm80CknN5 1.1YT+uGL8hueGKl8	•	
	Local Certificate				
	BEGIN CERTIFICATE MIIENDCCA52gAwIBAgIBATANBgkghkiG9w0B CzAJBgNVBAgTAINOMRUWEWYDVQQHEwxT	AQQFADCBozE dFBldGVyc2J1c	ELMAKGA1UEBhMCUIUx mcxEDAOBgNVBAoTB1RI	•	
	Local private key				
	BEGIN PRIVATE KEY MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmi 6XrRc8Xes+qKUyTsTLtjGGkRkIRVPeChcS9kD	wggJeAgEAAoG H/R7MuGO7Ktl	SBALg7LnKXPSAdZc5C SNIn5uHi/je51t	•	
	Remote Subnet		Remote Subnet Mask		
	192.168.40.0		255.255.255.0		
	Ping interval		Ping timeout		
	60		120		
	LZO Compression				
	Always	•			

Рис. 2.10. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – сервер

# 2.2.4. Пример настройки тоннеля с аутентификацией по протоколу TLS, когда роутер выступает в роли клиента OpenVPN

Для настройки OpenVPN-тоннеля с TUN (Layer 3) с аутентификацией по протоколу TLS между сетевыми устройствами, при этом роутер выступает в роли OpenVPN-клиента, 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. В поле Authentication Method выберите значение TLS Client;
- 5. Добавьте необходимые сертификаты и ключи в поля: CA Certificate, Local Certificate, Local Private Key (см. далее описание);
- **6.** А также настройте остальные параметры на странице в зависимости от требуемой конфигурации (см. таблицы 2.1 и 2.2).

При выборе данного метода аутентификации, все настройки в окне интерфейса такие же, как в разделе 2.2.1, к ним прибавляется лишь поля для указания сертификатов и ключей: **CA Certificate**,





Local Certificate, Local Private Key. Ключи и сертификаты необходимо получить либо от сертификационного центра, либо создать свой собственный сертификационный центр и создать на его основе требуемые ключи и сертификаты. Для работы тоннеля понадобятся файлы, указанные в таблице 2.6, кроме файла Диффи-Хелмана. Пример настройки показан на рис. 2.11.

prk	
Enable OpenVPN Tunnel	
Device	Transport protocol
TUN (L3)	TCP Server
etwork Remote	Port
s	9995
Authentication method	Bridge with interface
TLS Client	▼ lan
Local VPN endpoint IP address	Remote VPN endpoint IP address
10.10.10.1	10.10.10.2
Tunnel Ca Certificate	
elsBEGIN CERTIFICATE	
MIID1DCCAz2gAwiBAgIJAJZzMYhh71 VQQGEwJSVTELMAKGA1UECBMCU1	<u>sJMA0GCSqGSlb3DQEBBQUAMIGjMQswCQYD</u> 1AxFTATBgNVBAcTDEN0UGV0ZXJzYnVyZzEQMA4G
MILENDCCASZQAWIBAQIBATANBQKabi CZAJBQNVBAQTAINQMRUWEWYDVQC	xiG9w0BAQQFADCBozELMAkGA1UEBhMCUlUx 2HEwxTdFBldGVyc2J1cmcxEDAOBgNVBAoTB1R!
MIICeAIBADANBgkghkiG9w0BAQEFA	ASCAmlwggJeAgEAAoGBALg7LnKXPSAdZc5C
6XrRc8Xes+gKUyTsTLtjGGkRkIRVPeC	ChcS9kDH/R7MuGO7Ktl3NIrt5uHi/je51t
Remote Subnet	Remote Subnet Mask
192.168.40.0	255.255.255.0
Ping interval	Ping timeout
60	120
LZO Compression	
LZO Compression Always	Ŧ

Рис. 2.11. Настройка OpenVPN (с аутентификацией по протоколу TLS), роутер – клиент





## 2.3. Инструкция по настройке тоннеля GRE (на примере роутеров iRZ R4)

### 2.3.1. Настройка GRE-тоннеля уровня L2 (на примере двух роутеров RU41)

В примерах настройки используется следующая схема сети:



Рис. 2.12. Схема сети

Для настройки GRE-тоннеля уровня L2, в веб-интерфейсе роутера (см. рис. 2.13):

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

Status	Network	Services	Tools
Local Network	Local Network (lan)		Remove
Wired Internet		Switch Ports	
Mobile Internet	ETH0 1	🖉 LAN1 🖉 LAN2 🖉 LAN3 🖉 LAN4	WAN
Wireless Network		Mask	
DNS servers	10.0.3.1	255.255.255.0	
Routes			
PPTP Client			
GRE Tunnels			Add VLAN Save
OpenVPN Tunnel			







Далее необходимо настроить WAN-порт роутера (см. рис. 2.14):

- 4. Зайдите в раздел Network → Wired Internet;
- **5.** Укажите тип подключения в поле **Connection Type** (**Static** статический адрес, **DHCP** адрес получаемый по DHCP);

Status	Network	Network		vices	Tools	
Local Network	Wired Internet (wan)					Remove
Wired Internet	CPU port	VLAN I	þ	Switch Ports		
Mobile Internet	ETH1 •	2		LAN1 LAN2	LAN3 LAN4	🖉 WAN
Wireless Network	Connection type			MAC		
DNS servers	Static		Ŧ	f0:81:af:00:0f:56		
Routes	IP		Mask		Gateway	
PPTP Client	10.0.1.5		255.255.255.0		10.0.1.6	
	Ping address		Ping interval (sec	)	Ping attempts	
GRE Tunnels	Enter address to check con	nection	Default 30 saecor	nds	Default 3 times	
OpenVPN Tunnel						
IPSec tunnels					Add VLAN	Save

Рис. 2.14. Настройка WAN





Далее необходимо настроить GRE-тоннель (см. рис. 2.15):

- 6. Зайдите в раздел Network → GRE Tunnels;
- 7. Добавьте новый тоннель, нажав на кнопку Add Tunnel;
- 8. Введите имя тоннеля (на выбор пользователя) в поле Name;
- **9.** Выберите локальный интерфейс, через который будет работать тоннель в поле Local Address (поскольку в данном примере показана настройка через WAN-порт, то соответственно **WAN**);
- **10.** Укажите IP-адрес порта удаленного устройства, с которым будет построен тоннель, в поле **Remote Address**;
- **11.** Выберите на каком уровне будет работать тоннель в поле **Network Type** (в данном примере рассматривается **L2**);
- 12. Выберите в каком интерфейсе будет работать GRE-тоннель, выбрав значение в поле Interface (если Interface = LAN или WAN, то дополнительных настроек не требуется, если Interface = <Custom Network> [пользовательская сеть], то необходимо будет указать IP-адрес пользовательского интерфейса в поле Tunnel IP и маску сети в поле Tunnel Mask);
- Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле Firewall Zone (правила можно настроить вручную в разделе Services → Firewall);
- **14.** При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.

Z RU41w	Edit tunnel: tunnel01 (gre1t	un)			2016	5-10-04 12:3
Status	Name				Тоо	ls
	tunnel01					
Local Network	Local address				Edit	Remove
Vired Internet	wan			•		
Aobile Internet	Remote address					
Vireless Network	10.0.1.6				d Tunnel	Save
NS servers	Network type					
coutes	L2 layer			Ŧ		
PTP Client	Interface					
RE Tunnels	<custom network=""></custom>			v		
penVPN Tunnel	Tunnel IP		Tunnel mask			
'Sec tunnels	172.0.1.6		255.255.255.0			
	Firewall zone					
	<none></none>			Ŧ		
	✓ Don't Fragment					
			Close	Save changes		
			0.036	Save changes		

Рис. 2.15. Настройка GRE-тоннеля





## 2.3.2. Настройка GRE-тоннеля уровня L3 (на примере двух роутеров RU41)

В примерах настройки используется следующая схема сети:



Рис. 2.16. Схема сети

Для настройки GRE-тоннеля уровня L3, в веб-интерфейсе роутера (см. рис. 2.17):

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

Status	Network	Services	Tools
Local Network	Local Network (lan)		Remove
Wired Internet	CPU port VI AN ID	Switch Ports	
Mobile Internet	ETHO VLAND	🖉 LAN1 🖉 LAN2 🖉 LAN3 🖉 LAN4	WAN
Wireless Network	IP	Mask	
DNS servers	10.0.3.1	255.255.255.0	
Routes			
PPTP Client			
GRE Tunnels			Add VLAN Save







Далее необходимо настроить WAN-порт роутера (см. рис. 2.18):

- 4. Зайдите в раздел Network → Wired Internet;
- **5.** Укажите тип подключения в поле **Connection Type** (**Static** статический адрес, **DHCP** адрес получаемый по DHCP);

Status	Network		Services		Tools	
Local Network	Wired Internet (wan)					Remove
Wired Internet	CPU port	VLAN ID	)	Switch Ports		
Mobile Internet	ETH1 •	2		LAN1 LAN2	LAN3 LAN4	🖉 WAN
Wireless Network	Connection type			МАС		
DNS servers	Static			f0:81:af:00:0f:56		
Routes	IP		Mask		Gateway	
PPTP Client	10.0.1.5		255.255.255.0		10.0.1.6	
	Ping address		Ping interval (sec)		Ping attempts	
GRE Tunnels	Enter address to check connection		Default 30 saeconds		Default 3 times	
OpenVPN Tunnel						
IPSec tunnels					Add VLAN	Save

Рис. 2.18. Настройка WAN





Далее необходимо настроить GRE-тоннель (см. рис. 2.15):

- 6. Зайдите в раздел Network → GRE Tunnels;
- 7. Добавьте новый тоннель, нажав на кнопку Add Tunnel;
- 8. Введите имя тоннеля (на выбор пользователя) в поле Name;
- **9.** Выберите локальный интерфейс, через который будет работать тоннель в поле Local Address (поскольку в данном примере показана настройка через WAN-порт, то соответственно **WAN**);
- **10.** Укажите IP-адрес порта удаленного устройства, с которым будет построен тоннель, в поле **Remote Address**;
- **11.** Выберите на каком уровне будет работать тоннель в поле **Network Type** (в данном примере рассматривается **L3**);
- 12. Укажите IP-адрес интерфейса в поле Tunnel IP;
- 13. Выберите правило работы межсетевого экрана (firewall), если необходимо, выбрав значение в поле Firewall Zone (правила можно настроить вручную в разделе Services → Firewall);
- **14.** При необходимости, поставьте устройству запрет на фрагментацию (разделение) пакета на маршруте следования, поставив галочку напротив пункта **Don't fragment**.

Name		
gre1		
Local address		
wan		٣
Remote address		
10.0.1.6		
Network type		
L3 layer		٣
Tunnel IP		
172.0.1.6		
Firewall zone		
<none></none>		٣
✓ Don't Fragment		

Рис. 2.19. Настройка GRE-туннеля





### 2.4. Создание IPsec-тоннеля (на роутерах серии R4, R1)

Для создания IPsec-тоннеля на роутере должна быть настроена локальная сеть и порты WAN, затем в веб-интерфейсе роутера (см. рис. 2.20):

**1.** Зайдите в раздел Network  $\rightarrow$  IPsec Tunnels;

В данном разделе в полях **Port** и **NAT-T Port** уже занесены значения, чаще всего используемые при создании тоннелей по стандартам IPsec. Поле **Port** указывает на порт, через который будут работать тоннели, если настраиваемый роутер имеет внешний «белый» IP-адрес. А поле **NAT-T Port** указывает тоннелю через какой порт будет осуществляться связь в случае, если роутер находится в зоне NAT.

2. Добавьте новый IPsec-тоннель, нажав на кнопку Add Tunnel;

iRZ RU41u			2017-01-27 06:02:55	
Status	Network	Services	Tools	
Local Network	IPSec tunnels			
Wired Internet	Port 500	NAT-T Port		
Mobile Internet	Suu 4000			
Poutes				
DNS servers	test ++ 192.168.246.100		Edit Remove	
PPTP Client				
OpenVPN tunnel			Add Tunnel Save	
GRE tunnels				
IPSec tunnels				
Switch				

#### Рис. 2.20. Настройка IPsec-тоннеля





Далее необходимо настроить параметры тоннеля (см. рис. 2.21):

- 3. Введите имя тоннеля (на выбор пользователя) в поле Name;
- Выберите физический порт, через который будет работать тоннель, выбрав значение в поле Source Address (Default – через порт, являющийся на данный момент активным WAN-портом, или через другие интерфейсы: SIM1, SIM2, WAN);
- **5.** Укажите IP-адрес порта удаленного устройства, с которым будет построен тоннель, в поле **Remote Address**;
- 6. Укажите интервал в секундах, через который будет определяться доступность узла на противоположном конце тоннеля, указав значение в поле **Dead Peer Detect** (0 отключение данной функции);
- Выберите режим установления соединения между участниками тоннеля, выбрав значение в поле Exchange Mode (Main – основной, Aggressive – более активный [быстрый], но без обеспечения защиты подлинности);
- 8. Настройте параметры SA Info, для работы IPsec SA:

SAInfo			
Local Address	IP-адрес локальной сети, участвующей в тоннеле		
Local Netmask	Сетевая маска локальной сети, участвующей в тоннеле		
Remote Address	IP-адрес удаленной сети, участвующей в тоннеле		
Remote Netmask	Сетевая маска удаленной сети, участвующей в тоннеле		

9. Настройте фазу 1 и фазу 2, заполнив соответствующие поля в блоках Phase #1 и Phase #2:

Phase #1 (фаза 1)	
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)
Encryption Algorithm	Выбор алгоритма шифрования: AES, AES 128, AES 192, AES 256, DES, 3DES.
Hash Algorithm	Выбор алгоритма для проверки целостности данных: SHA-1, SHA-256, SHA-384, MD5.
DH Group	Выбор криптографического алгоритма, который позволяет двум точкам обмениваться ключами через незащищенный канал. Числа – обозначают сложность ключа, чем выше, тем надежнее ключ.
Phase #2 (фаза 2)	
Lifetime	Время жизни ключа в секундах, создаваемого на этапе фазы. Рекомендуется устанавливать значение меньше, чем у фазы 1 (например, 1 час или 3600 секунд)
Encryption Algorithm	Выбор алгоритма шифрования: AES, AES 128, AES 192, AES 256, DES, 3DES.
Authentication Algorithm	Выбор алгоритма для проверки целостности данных: НМАС SHA-1, НМАС SHA- 256, НМАС SHA-384, НМАС 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.





Edit tunnel: tes	t					
Name						
test						
Source address Remote addr		ress	ess Dead peer detect (seconds			
wan	•	192.168.24	6.100	30		
Exchange mode						
main						•
Sainfo						
+ Local Ad	dress	Local Netmask		Remote A	ddress	Remote Netmask
- 192.168	8.1.1	255.255.255.0	)	192.168	.114.1	255.255.255.0
Phase #1 Lifetime			Phase #2 Lifetime			
3600				3600		
Encryption algor	rithm		Encryption algorithm			
aes v			aes v			
Hash algorithm			Authentication algorithm			
sha1 •			hmac_sh	a1	v	
DH group			PFS group			
none •			none		•	
Authentication method						
pre_shared_key						•
Pre-Shared Key						
Password						
Local Indentifier Type Local Indentifier						
<none> v</none>						
Remote Indentifier Type Remote Indentifier						
<none></none>	<none> •</none>					
					Clos	Save changes

Рис. 2.21. Параметры туннеля





**10.** Выберите способ аутентификации узлов тоннеля, выбрав значение в поле Authentication **Method** (pre-shared key – по общему ключу, rsasig – по сертификату и ключу RSA);

Authentication method				
rsasig			•	
Certificate				
Upload	PEM certificate			
Кеу				
Upload	PEM key			

Рис. 2.22. Параметр Authentication Method

Сертификат и ключ необходимо получить от сертификационного центра (СА) и распространить среди участников тоннеля.

#### 11. Выберите признаки идентификации ключей:

Local Identifier Type	Тип локального идентификатора
Remote Identifier Type	Тип удаленного идентификатора
Local Identifier	Значение локального идентификатора
Remote Identifier	Значение удаленного идентификатора

Значения идентификаторов могут быть в виде:

None – без идентификатора;

IP Address – IP-адрес;

FQDN – FQDN-адрес (полный доменный адрес, например, irz.net);

User FQDN – пользовательский FQDN-адрес (например, sales@irz.net);

**ASN1DN** – известное имя в формате описания ASN.1 (ASN.1 Distinguished Name).





## 3. Термины и сокращения

#### Сетевые технологии

**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;

**ІР-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 2 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 предопределённых 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 iRZ;
- 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).

#### **Технология 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»;

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

(Виртуальное) адресное пространство ОрепVPN-сети – адресное пространство IP-сети ОрепVPN, 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, позволющая 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.





# 4. Контакты и поддержка

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

Санкт-Петербург		
сайт компании в Интернете:	www.radiofid.ru	
тел. в Санкт-Петербурге:	+7 (812) 318 18 19	
e-mail:	support@radiofid.ru	

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. Также 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.

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

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