irzOS
Интерфейс командной строки

Содержание

1. Доступ в интерфейс командной строки (CLI) 5
2. Навигация и управление 5
3. event 8
4. firewall 8
4.1. connections 8
4.2. defaults 9
4.3. filter 10
4.4. mangle 11
4.5. nat 13
4.6. raw 14
4.7. zone 16
5. ip 17
5.1. arp 17
5.2. interface 17
5.3. nhrp 18
5.4. route 19
5.4.1. list 19
5.4.2. rule 20
5.4.3. table 21
6. mobile 21
6.1. apn 21
6.2. modem 22
6.3. sms 23
7. network 24
7.1. bridge 24
7.2. device 26
7.3. ethernet 26
7.4. fdb 27
7.5. qos 27
7.5.1. filter 27
7.5.2. queue 28
8. peripheral 30
8.1. gnss to ip 30
8.2. gpio 30
8.3. poe 31
8.4. protect 32
8.5. serial port 32
9. radius 35
9.1. attribute 35
9.2. client 35

9.3. server 36
9.4. user 37
10. routing **37**
10.1. bfd 37
10.1.1. interface 38
10.1.2. settings 38
10.2. bgp 39
10.3. common 41
10.4. filter 41
10.5. ospf 42
10.5.1. area 42
10.5.2. instance 43
10.5.3. interface 44
10.6. status 45
11. service **46**
11.1. client 46
11.2. dhcp 47
11.2.1. lease 47
11.2.2. server 48
11.3. dns 49
11.4. iperf 50
11.5. l2tp server 50
11.6. link client 51
11.7. ntp 52
11.8. openvpn server 53
11.9. pinger 55
11.10. pptp server 56
11.11. snmp 57
11.12. udp broadcast relay 58
11.13. vrrp 59
11.14. zabbix 59
12. storage **61**
12.1. certificate 61
12.2. file 63
13. system **64**
13.1. access 64
13.1.1. radius 64
13.1.2. ssh 64
13.1.3. web 65
13.2. block dev 66
13.3. config 67
13.4. logging 67

13.5. management 68
13.6. package 69
14. tools **69**
15. tunnel **70**
15.1. eoip 71
15.2. gre 72
15.3. ipsec 73
15.3.1. association 73
15.3.2. connection 74
15.3.3. profile 75
15.3.4. proposal 76
15.3.5. status 76
15.4. l2tp 77
15.5. l2tp v3 78
15.6. openvpn 80
15.7. pptp 81
15.8. wireguard 82
15.8.1. interface 82
15.8.2. peer 83
16. wireless **84**
16.1. adapter 84
16.2. filter 85
16.3. network 85

1. Доступ в интерфейс командной строки (CLI)

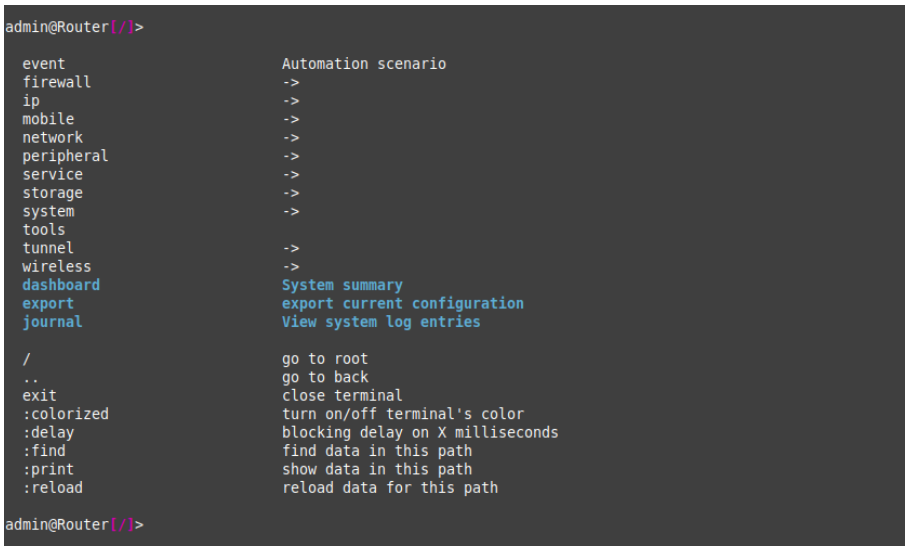
Доступ к интерфейсу командной строки (CLI) осуществляется по протоколу SSH. После успешной аутентификации пользователь получает доступ в CLI с правами, соответствующими учетной записи.

Процесс доступа:

1. Установить SSH-соединения с IP-адресом роутера (адрес роутера по умолчанию указан на наклейке на корпусе)
2. Пройти аутентификацию (указать пароль)
3. После этого устройство автоматически покажет интерфейс командной строки (cli)

```
user@desktop:~$ ssh admin@192.168.1.1
admin@192.168.1.1's password:
admin@Router[/]>
```

2. Навигация и управление



TAB - показать все разделы

? - показать все разделы с подсказками

.. - вернуться на один уровень выше

/ - вернуться в корневой раздел

dashboard - показать статусную информацию об устройстве

export - экспортировать текущую конфигурацию устройства. При вызове без аргументов в консоли будет показана текущая конфигурация полностью.

export ip - экспортировать конфигурацию раздела

export [TAB] **to-file=** экспортировать в файл

journal - системный лог. При вызове без аргументов в консоли будут показаны данные лога полностью.

journal [TAB] **filter=** показать строки, содержащие определенную информацию

journal [TAB] **last=** показать последние N строк

exit - закрыть терминал

colorized - включить/выключить цветовую схему

reload - обновить страницу

Зайти в конкретный раздел можно, перемещаясь последовательно по подразделам:

```
admin@iRZ-Router[/]>network
```

Ответ будет такой:

```
admin@iRZ-Router[/network]>
```

Также можно указать полный путь к разделу. Полный путь указывается последовательно, через пробел, без дополнительных символов, автодополнение по клавише TAB работает.

Например:

```
 network bridge
```

Ответ будет такой:

```
admin@iRZ-Router[/network bridge]>
```

Чтобы **просмотреть содержимое раздела**, нужно нажать **TAB** или **?**

```
admin@Router[/network bridge]>

  NAME       PORT   STP-VERSION
  bridge0    port1  none
             port2
             port3
             port4
             wifi1
  add
  apply
  clean
  export
  status
```

Добавить или удалить элементы

Чтобы добавить или удалить элементы из перечня нужно зайти в соответствующий раздел и написать имя добавляемого элемента (для удаления - со знаком минус)

Например:

Посмотреть список портов на bridge0

```
admin@iRZ-Router[/network bridge bridge0]>port
```

Ответ будет таким:

```
port1,port2,port3,port4
```

Добавить port 1 в список портов на bridge0:

```
admin@iRZ-Router[/network bridge bridge0]>port port1
```

Удалить port 1 из списка портов на bridge0:

```
admin@iRZ-Router[/network bridge bridge0]>port -port1
```

3. event

В разделе настраивается автоматическое выполнение команд роутера в ответ на определённые события или по расписанию. События могут быть связаны с изменением состояния сетевых интерфейсов, соединений и служб, получением SMS-сообщений или запуском по расписанию.

Для каждого события задаются источник и условия срабатывания. Если событие соответствует заданным условиям, роутер выполняет указанную CLI-команду. Это позволяет автоматизировать управление устройством и реагировать на изменения состояния сети без участия пользователя.

КОМАНДЫ

reorder	Изменить позицию объекта

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
description (*Description*)	Описание события
trigger (*Trigger*)	Подсистема-источник события (откуда пришло событие)
target (*Target*)	Объект-источник события **условия:** trigger = scheduler trigger = gpio trigger = gpi trigger = extra-gpi trigger = sms trigger = pinger trigger = defaultroute trigger = interface trigger = ipsec
value (*Value*)	Значение объекта для сравнения события **условия:** trigger = gpio trigger = gpi trigger = sms trigger = pinger trigger = defaultroute trigger = interface trigger = ipsec
action (*Action*)	CLI команда, выполняемая, если входящее событие соответствует конфигурации

4. firewall

Раздел предназначен для настройки межсетевого экрана (**Firewall**), обеспечивающего фильтрацию сетевого трафика и защиту от несанкционированного доступа. Конфигурация основана на **iptables** и позволяет управлять обработкой сетевых пакетов на различных этапах их прохождения через сетевой стек, а также настраивать правила фильтрации для отдельных зон межсетевого экрана.

4.1. connections

Раздел предназначен для мониторинга активных сетевых соединений, отслеживаемых механизмом Connection Tracker (conntrack). Этот механизм сохраняет информацию о состоянии соединений, позволяя межсетевому экрану применять правила фильтрации с учётом их состояния.

В разделе отображаются IP-адреса источника и назначения, используемый протокол, состояние TCP-соединения, время до удаления записи, а также счётчики переданных пакетов и байтов. Эти данные позволяют отслеживать сетевую активность и выявлять проблемы при передаче трафика.

Дополнительно предусмотрена возможность очистки таблицы отслеживания соединений (conntrack).

КОМАНДЫ

flush	Очистить таблицу conntrack

СВОЙСТВА

source	Адрес источника
destination	Адрес назначения
protocol (*Protocol*)	Протокол, инкапсулированный в IP
timeout (*Timeout*)	Интервал, через который сетевое соединение будет удалёно
tcp-state (*TCP State*)	Текущее состояние TCP соединения
mark (*Packet mark*)	Метка пакета
pkts (*Orig/Repl Packets*)	Количество пакетов переданных через соединение (исходящих/входящих)
bytes (*Orig/Repl Bytes*)	Количество байт переданных через соединение (исходящих/входящих)

4.2. defaults

Раздел предназначен для настройки политик межсетевого экрана по умолчанию. Эти политики определяют действие с сетевыми пакетами, для которых не сработало ни одно из правил соответствующей цепочки. Политика по умолчанию применяется после обработки всех правил цепочки, если ни одно из них не определило окончательное действие.

Настройки распространяются на три основные цепочки:

- **INPUT** — управляет входящим трафиком, предназначенным самому роутеру, например подключениями по HTTPS и SSH, ICMP-пакетами и VPN-соединениями.
- **OUTPUT** — управляет трафиком, исходящим от самого роутера, например DNS-запросами, запросами NTP-клиента и трафиком служб мониторинга.
- **FORWARD** — управляет транзитным трафиком, проходящим через роутер между сетевыми интерфейсами или зонами, например из LAN в WAN.

Дополнительно раздел позволяет включать отбрасывание некорректных пакетов, защиту от SYN Flood, механизмы отслеживания соединений и ускорения обработки трафика. Также доступны настройки TCP, включая SYN Cookies, ECN и Window Scaling, и выбор протоколов, для которых используются NAT Helper.

СВОЙСТВА

input (*Input*) **значения:** accept, drop	Политика по умолчанию для входящего трафика
output (*Output*) **значения:** accept, drop	Политика по умолчанию для исходящего трафика

forward (*Forward*) **значения:** accept, drop	Политика по умолчанию для пересылаемого (проходящего) трафика
drop-invalid (*Drop Invalid*) **значения:** true, false	Откидывать неидентифицированные пакеты
syn-flood (*SYN Flood*) **значения:** true, false	Зашита от SYN Flood атак
syn-flood-rate (*SYN Rate*)	Допустимый порог количества TCP SYN пакетов в секунду **условия:** syn-flood = true
syn-flood-burst (*SYN Burst*)	Допустимый мгновенный всплеск количества TCP SYN пакетов **условия:** syn-flood = true
tcp-syncookies (*SYN Cookies*) **значения:** true, false	Использовать TCP SYN cookies для противодействия TCP SYN flood
tcp-ecn (*TCP ECN*) **значения:** true, false	Использовать ECN (явное уведомление о перегруженности)
tcp-window-scaling (*TCP Window Scaling*) **значения:** true, false	Масштабирование TCP окна
use-conntrack (*Connection tracker*) **значения:** true, false	Механизм отслеживания соединений (conntrack)
flow-offloading (*Use FLOWOFFLOAD*) **значения:** true, false	Механизм разгрузки потока (Flow offloading)
nat-helper (*Nat helper*) **значения:** ftp, pptp, sip, snmp, tftp, rtsp, ras, q931	Технология NAT helper для выбранных протоколов

4.3. filter

Раздел предназначен для настройки правил фильтрации сетевого трафика. Эти правила позволяют управлять входящим, исходящим и транзитным трафиком, обеспечивая защиту сети от несанкционированного доступа.

Для каждого правила задаются условия фильтрации, включая зоны или интерфейсы источника и назначения, IP-адреса, протоколы и порты, а также действие: **ACCEPT** (принять), **DROP** (отбросить) или **REJECT** (отклонить). Правила обрабатываются последовательно. При совпадении пакета с условиями правила выполняется указанное действие, после чего дальнейшая обработка пакета в этой цепочке прекращается.

Если пакет не соответствует ни одному из правил, к нему применяется политика межсетевого экрана по умолчанию, настроенная в разделе */firewall defaults*. Такой подход позволяет создавать исключения из общих политик фильтрации для определённых служб и сетевых соединений.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить правило файрвола

chain (*Chain*) **значения:** input, forward, output	Цепочка правил таблицы
src (*source*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output
src-addr (*Source address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst (*destination*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = input
dst-addr (*destination address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol (*Protocol*) **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type (*ICMP Type*) **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark (*Firewall mark*) **пример:** 16, !453	Сравнение по метке пакета
action (*Action*) **значения:** accept, reject, drop	Действие над трафиком, попавшим под правило
policy (*IPSec Policy*) **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra (*Extra params*) **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы (поддержка синтаксиса iptables)

4.4. mangle

Раздел предназначен для настройки правил Mangle, позволяющих изменять отдельные атрибуты IP-пакетов. Основная функция Mangle заключается в классификации и маркировке пакетов. Метки не разрешают и не блокируют трафик напрямую, а используются другими подсистемами роутера для обработки трафика.

Правила Mangle применяются для реализации расширенных сетевых функций, таких как:

- **Маршрутизация на основе политик (PBR):** направление маркированного трафика через определённые WAN-интерфейсы или VPN-туннели с использованием соответствующих правил маршрутизации.

- **Качество обслуживания (QoS):** приоритизация трафика и управление пропускной способностью на основе меток пакетов.

Кроме того, правила Mangle позволяют изменять отдельные поля IP-заголовков, например DSCP для классификации трафика и TTL (Time-to-Live), а также настраивать максимальный размер TCP-сегмента (MSS).

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить правило файрвола
chain (*Chain*) **значения:** prerouting, input, forward, output, postrouting	Цепочка правил таблицы
src (*source*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output chain = postrouting
src-addr (*source address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst (*destination*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = input chain = prerouting
dst-addr (*destination address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol (*Protocol*) **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type (*ICMP Type*) **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark (*Firewall mark*) **пример:** 16, !453	Сравнение по метке пакета
action (*Action*) **значения:** accept, dscp, mark, tcpmss, ttl	Действие над трафиком, попавшим под правило **условия:** chain = input

set-mark (*Set mark*) **минимум:** 0, **максимум:** 4294967295	Метка, которую следует установить для пакета **условия:** action = mark
set-dscp (*DSCP Class*) **значения:** cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, be, af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, ef	Указать DiffServ класс в поле DSCP для приоретизации трафика **условия:** action = dscp
set-mss (*MSS value*) **значения:** clamp-mss-to-pmtu	Установить значение MSS в пакете TCP SYN **условия:** action = tcpmss
set-ttl (*Set TTL*) **пример:** 1, 255, +1, -1	Изменить значение TTL в пакете **условия:** action = ttl
policy (*IPSec Policy*) **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra (*Extra params*) **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.5. nat

Раздел предназначен для настройки правил трансляции сетевых адресов (Network Address Translation, NAT). Эти правила позволяют изменять IP-адреса и порты источника или назначения в пакетах, проходящих через роутер. NAT широко используется для организации обмена трафиком между частными и публичными сетями, а также для перенаправления подключений.

Доступны следующие действия:

- **ACCEPT:** Исключает соответствующий правилу трафик из трансляции в текущей цепочке NAT. Например, используется для создания исключений для трафика, направленного через определённый VPN-туннель или в другую частную сеть.
- **DNAT:** Изменяет IP-адрес или порт назначения пакета. Обычно используется для перенаправления входящих подключений на устройства во внутренней сети.
- **Redirect:** Перенаправляет трафик на сам роутер, при необходимости изменяя порт назначения.
- **SNAT:** Заменяет IP-адрес источника на заданный статический IP-адрес. Обычно используется, если WAN-интерфейс роутера имеет постоянный публичный IP-адрес.
- **Masquerade:** Динамически заменяет IP-адрес источника на текущий IP-адрес выходного интерфейса. Обычно используется для подключений с динамическим IP-адресом, например через сотовую сеть (LTE) или DHCP.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить правило файрвола

chain (*Chain*) **значения:** prerouting, postrouting, output	Цепочка правил таблицы
src (*source*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output chain = postrouting
src-addr (*source address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst (*destination*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = prerouting
dst-addr (*destination address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol (*Protocol*) **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола
icmp-type (*ICMP Type*) **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
mark (*Firewall mark*) **пример:** 16, !453	Сравнение по метке пакета
action (*Action*)	Действие над трафиком, попавшим под правило **условия:** chain = output chain = prerouting chain = postrouting
nat-addr (*NAT address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	Преобразовать адрес попавшего под правила пакета **условия:** chain = output && action = dnat chain = prerouting && action = dnat chain = postrouting && action = snat
redirect-port (*Redirect Port*) **пример:** 80, !80	Транслировать попавшие под правило пакеты на указаный порт **условия:** chain = output && action = redirect chain = prerouting && action = redirect
policy (*IPSec Policy*) **значения:** dir, pol, strict, reqid, spi, proto, mode, tunnel-src, tunnel-dst	Сопоставление для IPSec трафика
extra (*Extra params*) **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.6. raw

Раздел предназначен для настройки правил таблицы Raw, которая обрабатывает пакеты до передачи в систему отслеживания соединений (conntrack).

Основное назначение таблицы Raw — управление обработкой трафика до отслеживания соединений. Для пакетов, соответствующих условиям правила, доступны следующие действия:

- **ACCEPT:** Завершает обработку пакета в текущей цепочке Raw, позволяя продолжить его обработку другими механизмами сетевого стека.
- **DROP:** Отбрасывает пакет, блокируя его дальнейшую обработку.
- **NOTRACK:** Исключает пакет из механизма отслеживания соединений (conntrack).

Использование **NOTRACK** позволяет снизить нагрузку на процессор и память при обработке больших объёмов трафика, не требующего отслеживания соединений. Также этот механизм может применяться, если отслеживание соединений вызывает проблемы при обработке определённых протоколов.



Пакеты, к которым применено действие **NOTRACK**, не отслеживаются механизмом conntrack. Для такого трафика недоступна фильтрация по состояниям соединений, например *RELATED* и *ESTABLISHED*, а также стандартные механизмы NAT. Используйте эту функцию с учётом возможных последствий для безопасности сети.

КОМАНДЫ

reset-counters	Сброс счётчиков
reorder	Изменить позицию объекта

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить правило файрвола
chain (*Chain*) **значения:** output, prerouting	Цепочка правил таблицы
src (*source*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Источник трафика (интерфейс или зона) **условия:** chain = output
src-addr (*source address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес источника трафика
dst (*destination*) **значения:** /network device, /network ethernet, /wireless network, /ip interface, /mobile modem, /tunnel, /tunnel atunnel, /defaults server, /firewall zone	Назначение трафика (интерфейс или зона) **условия:** chain = prerouting
dst-addr (*destination address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1:80, :80, :80,443,5000-5010	IP адрес получателя трафика
protocol (*Protocol*) **значения:** dccp, ddp, egp, eigrp, encap, esp, etherip, ggp, gre, hmp, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, isis, iso-tp4, l2tp, ospf, pim, pup, rdp, rspf, rsvp, sctp, skip, st, tcp, udp, vmtp, vrrp, xns-idp, xtp, all	Сопоставление по имени протокола

icmp-type (*ICMP Type*) **значения:** address-mask-reply, host-redirect, pong, time-exceeded, address-mask-request, host-unknown, port-unreachable, timestamp-reply, any, host-unreachable, precedence-cutoff, timestamp-request, communication-prohibited, ip-header-bad, protocol-unreachable, TOS-host-redirect, destination-unreachable, network-prohibited, redirect, TOS-host-unreachable, echo-reply, network-redirect, required-option-missing, TOS-network-redirect, echo-request, network-unknown, router-advertisement, TOS-network-unreachable, fragmentation-needed, network-unreachable, router-solicitation, ttl-exceeded, host-precedence-violation, parameter-problem, source-quench, ttl-zero-during-reassembly, host-prohibited, ping, source-route-failed, ttl-zero-during-transit	Сопоставление по типу ICMP пакета **условия:** protocol = icmp
action (*Action*) **значения:** accept, drop, notrack	Действие над трафиком, попавшим под правило
extra (*Extra params*) **пример:** -m mac --mac-source FE:FF:FF:FF:FF:FF	Специальные аргументы

4.7. zone

Раздел предназначен для создания и настройки зон межсетевого экрана. Зоны используются для группировки источников и назначений сетевого трафика и позволяют упростить настройку правил фильтрации. Способ определения принадлежности трафика к зоне зависит от её типа:

- **Зона на основе интерфейсов:** Объединяет один или несколько сетевых интерфейсов (например, *eth0*, *br-lan*, *tun0*). Трафик, поступающий или исходящий через выбранные интерфейсы, относится к данной зоне. Такой подход используется для разделения физических и логических сегментов сети.
- **Зона на основе адресов:** Определяется списком IP-адресов или подсетей в формате CIDR. Трафик относится к данной зоне, если IP-адрес источника или назначения соответствует одной из записей списка, независимо от используемого сетевого интерфейса. Список адресов можно задать вручную или загрузить из файла. Это позволяет настраивать правила фильтрации без привязки к топологии сети.

Созданные зоны можно использовать в качестве источника и назначения трафика при настройке правил межсетевого экрана.

КОМАНДЫ

find	НЕТ ОПИСАНИЯ element - НЕТ ОПИСАНИЯ (обязательно)

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить зону файрвола
type (*Type*) **значения:** interface, address	Тип набора
entry (*Entry*)	Участники набора **условия:** type = interface type = address
include (*Include*) **значения:** /storage file	Выбрать файлы со списком участников набора **условия:** type = address

5. ip

Раздел предназначен для настройки параметров **сетевого уровня (Layer 3)**. Здесь доступны инструменты для управления сетевыми интерфейсами, разрешения адресов и настройки маршрутизации.

5.1. arp

Раздел предназначен для просмотра и управления ARP-таблицей роутера. Протокол разрешения адресов (Address Resolution Protocol, ARP) используется для определения MAC-адресов устройств по их IPv4-адресам в пределах локальной сети.

В разделе отображаются соответствия IP- и MAC-адресов, сетевые интерфейсы, состояние, тип и возраст ARP-записей.

Помимо просмотра динамически полученных записей, можно создавать статические ARP-записи, закрепляющие определённые MAC-адреса за IP-адресами на выбранных интерфейсах. Это позволяет управлять адресными соответствиями без использования динамического разрешения ARP. Также предусмотрена возможность очистки ARP-кэша.

КОМАНДЫ

flush	Очистить таблицу ARP записей

СВОЙСТВА

ip-address (*Ip address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	IP адрес
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
interface (*Interface*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel **пример:** bridge0	Интерфейс

5.2. interface

Раздел предназначен для настройки и управления логическими интерфейсами сетевого уровня (L3). Каждый интерфейс связывает IP-адрес и соответствующие сетевые параметры с базовым сетевым устройством, обеспечивая работу маршрутизации, межсетевого экрана и сетевых служб.

При настройке интерфейса можно управлять его административным состоянием и метрикой маршрута. Дополнительные параметры зависят от выбранного типа подключения:

- **Static:** Ручное назначение IP-адресов с указанием префикса подсети и шлюза по умолчанию.
- **DHCP Client:** Автоматическое получение IP-адреса от DHCP-сервера с возможностью настройки идентификаторов клиента и использования DNS-серверов, полученных от сервера.
- **PPPoE:** Установка соединения по протоколу Point-to-Point Protocol over Ethernet с настройкой учётных данных для аутентификации, параметров PPP и использования DNS-серверов, полученных от удалённой стороны.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
metric (*Metric*) **минимум:** 0, **максимум:** 8388608	Значение метрики маршрута
ip-address (*IP Address*)	IP адрес интерфейса **условия:** type = static
defaultroute (*Default Route*) **значения:** true, false	Добавить маршрут по умолчанию через этот интерфейс **условия:** type != static
gateway (*Gateway*) **пример:** 192.168.1.1	Адрес шлюза для маршрута по-умолчанию **условия:** type = static
peer-dns (*Peer DNS*) **значения:** true, false	Использовать полученные DNS серверы для разрешения имён **условия:** type = pppoe type = dhcp
pppoe-username (*Username*)	Имя пользователя для PPPoE аутентификации **условия:** type = pppoe
pppoe-password (*Password*)	Пароль для PPPoE аутентификации **условия:** type = pppoe
pppoe-ac (*Access Concentrator*)	Имя PPPoE Access Concentrator для подключения **условия:** type = pppoe
pppoe-service (*PPPoE service*)	Клиентская служба PPPoE, поддерживаемся AC **условия:** type = pppoe
pppoe-option (*PPPoE Options*) **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, padi-attempts, padi-timeout, mru, mtu	Дополнительные опции протокола PPP **условия:** type = pppoe
debug (*Debug*) **значения:** true, false	Режим подробного логгирования **условия:** type = pppoe
hostname (*Hostname*)	Переопределить hostname клиента в DHCP запросе **условия:** type = dhcp
dhcp-clientid (*Client ID*)	Уникальный Client ID (DHCP option 61) **условия:** type = dhcp
dhcp-vendorid (*Vendor ID*)	Уникальный Vendor ID (DHCP option 60) **условия:** type = dhcp

5.3. nhrp

В данном разделе выполняется настройка протокола **NHRP (Next Hop Resolution Protocol)**, который управляет работой многоточечных туннелей **GRE (mGRE)**. Основная задача протокола — сопоставлять логические IP-адреса туннелей с NBMA-адресами узлов сети. Это позволяет

устройствам автоматически обнаруживать друг друга и строить масштабируемые VPN-сети с минимальной ручной настройкой соединений между узлами.

Настройки раздела позволяют задавать статические соответствия адресов и управлять передачей группового (мультикаст) трафика внутри туннеля. Также поддерживается базовая аутентификация по общему секрету и предусмотрены режимы совместимости с сетевым оборудованием сторонних производителей.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
map (*Map*)	Запись сопоставляющая NHRP адрес узла с его NBMA адресом
multicast (*Multicast*) **значения:** nhs, dynamic	Направлять мультикаст трафик только хабам или всем узлам NHRP сети
holding-time (*Holding Time*)	Время (сек), в течение которого удаляется истёкшая запись сопоставления NHRP
flag (*Option flags*) **значения:** registration, cisco, no-unique, non-caching, shortcut, redirect, debug	Опции NHRP интерфейса
secret (*Auth secret*) **мин. длина:** 1, **макс. длина:** 8	Аутентификация по секрету, добавляется в каждый исходящий NHRP пакет

5.4. route

Данный раздел предназначен для управления **таблицей маршрутизации** и логикой пересылки пакетов. Здесь настраиваются статические маршруты, правила маршрутизации на основе политик (Policy-Based Routing) и стратегии использования нескольких таблиц для обеспечения эффективного распределения трафика.

5.4.1. list

Раздел предназначен для просмотра и управления статическими маршрутами роутера. Здесь можно создавать новые маршруты, изменять существующие и удалять их.

Статические маршруты задаются вручную и определяют порядок обработки трафика, направленного к указанным сетям или узлам. Для каждого маршрута можно настроить адрес назначения, шлюз, выходной интерфейс, метрику, тип маршрута и таблицу маршрутизации.

В отличие от маршрутов, полученных по протоколам динамической маршрутизации, и маршрутов непосредственно подключённых сетей, статические маршруты задаются вручную.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
dst-addr (*Target*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес сети или хост к которому нужно указать маршрут
gateway (*Gateway*) **пример:** 192.168.1.1	Шлюз для доступа к сети или адресу назначения **условия:** type = unicast

metric (*Metric*) **минимум:** 0, **максимум:** 8388608	Метрика маршрута, определяющая его предпочтительность
table (*Table*) **значения:** /ip route table, main	Таблица маршрутизации, для которой предназначен маршрут
src-addr (*Source Address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес для отправки трафика при использовании этого маршрута
type (*Type*) **значения:** unicast, unreachable, prohibit, blackhole	Тип маршрута
interface (*Source interface*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel **пример:** bridge0	Интерфейс для отправки трафика при использовании этого маршрута **условия:** type = unicast

5.4.2. rule

Раздел предназначен для настройки правил маршрутизации на основе политик (Policy-Based Routing, PBR). Эти правила позволяют управлять выбором маршрутов в зависимости от характеристик сетевого трафика.

В отличие от стандартной маршрутизации, при которой выбор маршрута обычно определяется адресом назначения, PBR позволяет учитывать дополнительные параметры пакета, включая IP-адрес источника, входящий интерфейс и метку. Если пакет соответствует условиям правила, маршрутизатор выполняет заданное действие: поиск маршрута в указанной таблице маршрутизации либо другое действие, предусмотренное настройками правила.

PBR используется для управления трафиком в сетях с несколькими WAN-подключениями, направления трафика определённых VLAN через VPN-туннели и разделения маршрутизации гостевой и корпоративной сетей. Правила обрабатываются в порядке приоритета: правила с меньшим значением приоритета проверяются первыми.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
interface (*Incoming Interface*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, any **пример:** bridge0	Сопоставление по интерфейсу источника пакета
src-addr (*Source Address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Сопоставление по адресу источника пакета
dst-addr (*Destination Address*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Сопоставление по адресу назначения пакета
mark (*Mark*) **минимум:** 0, **максимум:** 4294967295	Сопоставление по conntrack метке пакета
table (*Table*) **значения:** /ip route table	Таблица с маршрутами для сопоставленного пакета
action (*Rule Action*) **значения:** prohibit, unreachable, blackhole, throw	Тип предпринимаемого действия при совпадении правила

priority (*Priority*) **минимум:** 1, **максимум:** 9999999	Приоритет правила в порядке сопоставления

5.4.3. table

Раздел предназначен для создания и управления пользовательскими таблицами маршрутизации. Такие таблицы используются в сложных сценариях маршрутизации, в частности при настройке маршрутизации на основе политик (Policy-Based Routing, PBR), которая позволяет выбирать маршруты в зависимости от характеристик сетевого трафика.

Помимо системных таблиц маршрутизации, таких как *main* и *local*, можно создавать дополнительные именованные таблицы. При создании таблицы указывается её имя, а уникальный числовой идентификатор назначается автоматически. Каждая таблица содержит собственный набор маршрутов, что позволяет использовать разные маршруты для различных типов трафика.

Статические маршруты добавляются в таблицы в разделе */ip route list*. Правила, определяющие, для какого трафика следует выполнять поиск маршрута в той или иной таблице, настраиваются в разделе */ip route rule*.

СВОЙСТВА

number (*Number*) **минимум:** 16384, **максимум:** 99999	Уникальный номер таблицы маршрутизации

6. mobile

Раздел предназначен для настройки подключения к сотовой сети. Здесь доступны инструменты для управления параметрами мобильной связи, сотовыми модемами и SMS-сообщениями.

6.1. apn



Раздел предназначен для работы с SIM-картами виртуальных операторов (MVNO).

Виртуальные операторы могут использовать инфраструктуру нескольких базовых операторов связи. Для подключения к определённой сети может потребоваться отдельная комбинация имени точки доступа (APN) и кода сети оператора (MCC/MNC).

В разделе можно создавать профили подключения с заданными параметрами APN, MCC/MNC, аутентификации, технологии передачи данных и роуминга. Также предусмотрена возможность привязки профиля к определённому слоту SIM-карты.

Для большинства крупных операторов сотовой связи ручная настройка APN обычно не требуется, поскольку необходимые параметры определяются автоматически.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
mccmnc (*MCC/MNC code*) **пример:** 46000	PLMN код оператора (MCC and MNC)

apn (*APN/VPDN*) **пример:** bridge0, vpn-client1, user_1@example.com	APN или имя VPDN
username (*Username*) **макс. длина:** 39 **пример:** bridge0, vpn-client1, user_1@example.com	Имя пользователя для аутентификации
password (*Password*)	Пароль пользователя для аутентификации
auth (*Authentication*) **значения:** any, pap, chap	Протокол аутентификации
mode (*Mode*) **значения:** auto, /defaults modem_modes	Технология передачи данных
roaming (*Roaming*) **значения:** allowed, discard, only	Политика работы в роуминг сетях
slot (*SIM slot*) **значения:** any, /mobile slot	Применить профиль к слоту SIM карты
pincode (*Pincode*)	PIN-код SIM карты **условия:** slot != any

6.2. modem

Раздел предназначен для настройки и управления сотовым модемом роутера и его подключением к интернету. Здесь доступны параметры подключения, маршрутизации, управления SIM-картами и выбора частотных диапазонов.

В разделе можно настроить следующие параметры:

- **Маршрутизация:** Параметр *Metric* задаёт метрику интерфейса модема, а *Default Route* позволяет настроить использование сотового подключения в качестве маршрута по умолчанию.
- **Управление SIM-картами:** Можно выбрать используемые слоты SIM-карт. Для моделей с поддержкой переключения между SIM-картами также доступны выбор основной SIM-карты (*Primary SIM*) и настройка времени возврата к ней с резервной (*Primary Timeout*).
- **Подключение к сети:** Параметр *Connect Timeout* задаёт максимальное время попытки подключения через текущую SIM-карту.
- **Выбор частотных диапазонов:** Параметр *Specific Bands* позволяет выбрать предпочтительные частотные диапазоны для работы модема.

Дополнительно доступны настройки получения DNS-серверов (*Peer DNS*), размера MTU и отладки (*Debug*), а также возможность перезагрузки модема со сбросом питания.

Доступность отдельных функций зависит от модели роутера и установленного модема.

КОМАНДЫ

reset	Перезапуск модема со сбросом питания

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Не выполнять подключение через модем

modem-sim-slot (*SIM slots*) **значения:** $_available-sim-slots	Слоты SIM карт, с которыми модем может работать
modem-primary-sim (*Primary SIM*) **значения:** $modem-sim-slot	Слот основной SIM карты, на которой будет стремиться работать модем
modem-primary-sim-timeout (*Primary Timeout*)	Таймер (сек) спустя который модем переключится на основную SIM карту с резервной
modem-connect-timeout (*Connect Timeout*) **минимум:** 300	Таймер (сек) в течении которого пытаться установить соединение через текущую SIM карту
modem-band (*Specific bands*) **значения:** $_available-bands	Частоты, на которых будеть пытаться работать модем, если выбрано
protocol (*Protocol*) **значения:** auto, ppp	Протокол дозвона модема
metric (*Metric*) **минимум:** 101, **максимум:** 900	Метрика интерфейса модема
defaultroute (*Default route*) **значения:** true, false	Добавить маршрут по умолчанию через этот интерфейс
peerdns (*Peer DNS*) **значения:** true, false	Использовать полученные DNS серверы для разрешения имён
mtu (*MTU*) **минимум:** 400, **максимум:** 1500	MTU интерфейса
debug (*Debug*) **значения:** true, false	включить отладочные сообщения. требует перезагрузки модема

6.3. sms

Раздел предназначен для отправки и получения SMS-сообщений через сотовый модуль роутера.

Чтение SMS

В разделе отображается список последних полученных SMS-сообщений. Список работает как циклический журнал и хранит до 10 последних сообщений. Если журнал заполнен, при поступлении нового SMS самое старое сообщение автоматически удаляется.

Для каждого сообщения указываются отправитель, текст, время отправки и время получения устройством. Также предусмотрена возможность удаления отдельных сообщений и очистки списка.

Отправка SMS

В разделе можно создавать и отправлять SMS-сообщения на телефонные номера в международном формате. При наличии нескольких модемов можно выбрать модем, через который будет отправлено сообщение.

Для успешной отправки необходимо выполнение следующих условий:

- На установленной SIM-карте должна быть подключена услуга SMS, а баланс счёта должен быть достаточным для отправки сообщения.
- Роутер должен быть зарегистрирован в сети оператора сотовой связи и находиться в зоне её покрытия.

КОМАНДЫ

send-sms	Отправить SMS на произвольный номер phone-number - Номер телефона (обязательно) message - Текст SMS сообщения (обязательно) modem - Отправить SMS сообщение с определённого модема

СВОЙСТВА

from (*sender*)	Имя или номер отправителя SMS
text (*message*)	Текст SMS сообщения
sent (*timestamp*)	Время отправки сообщения SMS центром
received	Время получения SMS сообщения на устройство

7. network

Раздел предназначен для управления физической и логической сетевой инфраструктурой роутера. Здесь доступны инструменты для настройки сетевых подключений, коммутации на канальном уровне (Layer 2) и обмена данными между устройствами внутренней сети.

7.1. bridge

Раздел предназначен для создания и управления программными сетевыми мостами канального уровня (Layer 2). Сетевой мост функционирует как виртуальный коммутатор, объединяя несколько физических или логических сетевых интерфейсов (например, Ethernet-порты и VLAN-подинтерфейсы) в единый широковещательный домен.

Помимо объединения интерфейсов, раздел предоставляет следующие возможности:

- **Spanning Tree Protocol (STP):** Настройка протоколов STP/RSTP для предотвращения образования петель в сетях с резервными соединениями. Доступны параметры приоритета моста, таймеров протокола и защиты портов BPDU Guard.
- **IGMP Snooping:** Оптимизация передачи мультикаст-трафика за счёт отслеживания IGMP-сообщений и передачи группового трафика только через порты, на которых находятся участники соответствующих мультикаст-групп. Дополнительно можно настроить параметры обработки IGMP-запросов.
- **Настройка производительности:** Управление длиной очереди передачи (TX Queue) для настройки обработки пакетов сетевым мостом.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
tx-queue-len (*TX Queue*)	Максимальное количество пакетов в очереди интерфейса
port (*Port*) **значения:** /network device, /network ethernet, /wireless network, /tunnel	Участники сетевого моста

vlan-default-pvid (*Vlan Default Pvid*) **минимум:** 1, **максимум:** 4095	Port Vlan ID, который будет присвоен не тэгированным пакетам переданным в этот порт **условия:** vlan-filtering = true
igmp-snooping (*IGMP snooping*) **значения:** true, false	Отправлять мультикаст трафик только получателям, подключившимся к мультикаст группе
igmp-mc-querier (*IGMP Querier*) **значения:** true, false	Предотвращение дублирования мультикаст трафика от нескольких маршрутизаторов **условия:** igmp-snooping = true
igmp-query-interval (*IGMP Query*)	Интервал (сек) между отправкой Querry сообщений **условия:** igmp-snooping = true
igmp-query-resp-interval (*IGMP Response*)	Время ожидания ответа от хоста на Querry сообщения **условия:** igmp-snooping = true
igmp-hash-max (*IGMP Hash*)	Размер hash таблицы IGMP записей **условия:** igmp-snooping = true
igmp-robustness (*IGMP Robustness*)	Количество Querry без ответа, после отправки которых удалится IGMP запись **условия:** igmp-snooping = true
stp-version (*STP Version*) **значения:** none, rstp, stp	Выбор спецификации STP протокола
stp-bpdu-guard (*STP BPDU Guard*) **значения:** $port	Выключить порт при получении BPDU **условия:** stp-version != none
stp-treeprio (*STP Treeprio*) **минимум:** 1, **максимум:** 15	Приоритет узла внутри дерева **условия:** stp-version != none
stp-maxage (*STP Maxage*) **минимум:** 6, **максимум:** 40	Считать что связь с Root Bridge потеряна, если от него не получено BPDU за этот интервал **условия:** stp-version != none
stp-fdelay (*STP Forward*) **минимум:** 6, **максимум:** 40	Время ожидания перехода порта из одного состояния в другое **условия:** stp-version != none
stp-maxhops (*STP Hops*) **минимум:** 6, **максимум:** 40	Максимальное число прыжков до любого коммутатора **условия:** stp-version != none
stp-hello (*STP Hello*) **минимум:** 1, **максимум:** 10	Интервал отправки BPDU сообщений корневым коммутатором **условия:** stp-version != none
stp-ageing (*STP Ageing*) **минимум:** 10, **максимум:** 1000000	Время нахождения MAC-адреса в FDB от получения последнего пакета с этого адреса **условия:** stp-version != none
stp-txholdcount (*STP TX Hold Count*) **минимум:** 1, **максимум:** 10	Максимальное число отправляемых BPDU в секунду **условия:** stp-version != none

7.2. device

Раздел предназначен для создания и управления логическими сетевыми устройствами канального уровня (Layer 2). Такие устройства создаются на основе существующих сетевых интерфейсов и используются для организации сетевой инфраструктуры, например для разделения трафика с помощью VLAN.

При создании устройства выбирается его тип и настраиваются соответствующие параметры. В зависимости от типа могут быть доступны настройки базового сетевого устройства, идентификатора VLAN, MTU и длины очереди передачи.

Созданные устройства можно добавлять в сетевые мосты в разделе */network bridge* для коммутации на канальном уровне или использовать в разделе */ip interface* для настройки IP-интерфейсов сетевого уровня (Layer 3).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
type (*Type*) **значения:** vlan	Тип устройства
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес устройства **условия:** type != vlan
mtu (*MTU*) **минимум:** 70, **максимум:** 65535	MTU интерфейса
tx-queue-len (*TX Queue*)	Максимальное количество пакетов в очереди интерфейса
device (*Host device*) **значения:** /network ethernet, /tunnel	Создать новое устройство поверх другого устройства
vid (*VLAN ID*) **минимум:** 6, **максимум:** 4094	Идентификатор VLAN, которым тегируются кадры

7.3. ethernet

Раздел предназначен для настройки параметров физических Ethernet-портов роутера на физическом (Layer 1) и канальном (Layer 2) уровнях. Эти настройки определяют работу портов и используются при их дальнейшем включении в сетевые мосты или настройке IP-интерфейсов.

В разделе можно настроить параметры портов для обеспечения совместимости с подключёнными устройствами и оптимизации работы сети. Основные настройки включают выбор **скорости соединения и дуплексного режима**, в том числе для устранения проблем с автосогласованием, изменение **MTU** в соответствии с требованиями сети, а также включение **неизбирательного режима (Promiscuous Mode)** для приёма кадров независимо от их адреса назначения. Этот режим может использоваться при анализе и диагностике сетевого трафика.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес порта

mtu (*MTU*) **минимум:** 70, **максимум:** 1500	MTU (байт) ethernet порта
promisc (*Promiscuous Mode*) **значения:** true, false	Порт будет принимать все пакеты, независимо от того, кому они адресованы
speed (*Speed*) **значения:** /defaults ether_port_speed	Скорость ethernet порта
duplex (*Duplex*) **значения:** half, full	Могут ли данные передаваться одновременно в обе стороны **условия:** speed = auto

7.4. fdb

Раздел предназначен для просмотра таблицы MAC-адресов сетевого моста (Forwarding Database, FDB). Таблица содержит MAC-адреса устройств и порты моста, через которые они доступны.

Мост автоматически изучает MAC-адреса устройств по входящим кадрам и добавляет их в таблицу. На основе этих данных он определяет, через какой порт передавать трафик, что позволяет избежать лишней рассылки кадров.

В разделе отображаются MAC-адреса, связанные с ними интерфейсы, возраст и тип записей. Эта информация помогает проверять сетевые подключения и выявлять проблемы на канальном уровне (Layer 2). Раздел доступен только для чтения.

СВОЙСТВА

mac (*MAC*)	MAC адрес сетевого устройства
device (*Device*)	L2 интерфейс, ассоциированный с этим MAC адресом
age (*Age*)	Как давно была добавлена запись в FDB таблицу
type (*Type*)	Является ли сетевое устройство внешним или самим интерфейсом

7.5. qos

Данный раздел предназначен для настройки политик **Quality of Service (QoS)**, которые позволяют приоритизировать определенные типы сетевого трафика для обеспечения стабильной работы критически важных приложений. Конфигурация обеспечивает точный контроль над распределением полосы пропускания и управление скоростью передачи трафика.

7.5.1. filter

Раздел предназначен для настройки правил классификации сетевого трафика для дальнейшей обработки системой Quality of Service (QoS). Классификация определяет, какой трафик будет обрабатываться с заданным приоритетом.

Система обрабатывает классификаторы в порядке их приоритета: классификаторы с меньшим значением приоритета проверяются первыми. Каждый классификатор проверяет пакеты на соответствие заданным условиям, таким как метка conntrack, IP-адреса источника и назначения, порты, протокол или другие параметры IP-пакета. Для расширенной классификации можно использовать фильтр *U32*.

При совпадении пакета с условиями классификатора трафик направляется в заданный класс обслуживания или полосу приоритетной очереди для дальнейшей обработки планировщиком. Это

позволяет разделять трафик по типам (например, VoIP, потоковое видео и массовые загрузки данных) и применять к ним разные уровни обслуживания.

СВОЙСТВА

interface (*Interface*) **значения:** /ip interface, /mobile modem	Имя интерфейса, к которому применяется очередь
prio (*Prio*)	Приоритет классификатора, фильтр с меньшим приоритетом проверяется раньше
handle (*Handle*) **минимум:** 0, **максимум:** 4294967295	Сопоставление по conntrack метке пакета
queue (*Queue*) **значения:** /network qos queue	Направить классифицированный трафик в этот класс
band (*Band*) **значения:** 1, 2, 3	Направлять классифицированный трафик в эту полосу очереди типа prio
u32-ip-filter (*U32 IP filter*) **значения:** dst, dport, src, sport, protocol, dscp, icmp_code, icmp_type	Классификация IP пакета по совпадению битовых значений
u32 (*U32*) **пример:** 0x00/0xff, 0x00/0xff at 0	Классификация IP пакета по 32-битному значению и маске с произвольным смещением

7.5.2. queue

Раздел предназначен для создания и управления очередями, которые обрабатывают сетевой трафик в соответствии с правилами классификации QoS. Здесь выбираются алгоритмы распределения полосы пропускания, приоритизации трафика и управления перегрузками сети.

Доступны следующие типы очередей:

- **Fair (Справедливая):** Бесклассовая дисциплина, обеспечивающая справедливое распределение полосы пропускания между потоками данных. Помогает уменьшить задержки при высокой нагрузке на сеть.
- **FIFO (First-In, First-Out):** Простая бесклассовая очередь, в которой пакеты обрабатываются в порядке поступления, без приоритизации.
- **HTB (Hierarchical Token Bucket):** Классовая дисциплина, позволяющая создавать иерархию классов трафика, задавать гарантированную и максимальную полосу пропускания и использовать свободную полосу других классов.
- **PRIO (Priority):** Классовая дисциплина, распределяющая трафик по полосам приоритета. Пакеты из более приоритетных полос обрабатываются первыми. Дисциплина не ограничивает скорость передачи трафика.
- **RED (Random Early Detection):** Бесклассовая дисциплина для предотвращения перегрузок. Позволяет отбрасывать или маркировать пакеты до полного заполнения очереди, чтобы снизить нагрузку на сеть.

Типы **Fair**, **FIFO** и **PRIO**, как правило, не требуют сложной настройки.



Настройка RED требует понимания принципов работы алгоритма и влияния его параметров на производительность сети. Рекомендуется использовать консервативные значения и проверять изменения перед применением в рабочей сети.

СВОЙСТВА

band (*Band*) **значения:** 1, 2, 3	Прикрепить очередь к указанной полосе очереди типа prio **условия:** queue = htb && type = class root = true
htb-rate (*HTB rate*) **пример:** 4096, 512k, 10m	Максимальная гарантированная полоса пропускания для этого класса и всех потомков **условия:** queue = htb
htb-ceil (*HTB ceil*) **пример:** 4096, 512k, 10m	Полоса пропускания доступная с учётом заимствования **условия:** queue = htb
htb-burst (*HTB burst*) **пример:** 4096, 512k, 10m	Количество байт отправленных на htb-ceil скорости, до переключения на следующий класс **условия:** queue = htb
htb-prio (*HTB prio*) **значения:** 1, 2, 3, 4, 5, 6, 7, 8	Приоритет класса, класс с меньшим приоритетом проверяется раньше **условия:** queue = htb && type = class
htb-default (*HTB default*) **значения:** /network qos queue	Отправлять весь неклассифицированный трафик в этот класс **условия:** queue = htb && type = qdisc
htb-r2q (*HTB r2q*) **минимум:** 1	Частота вычисления DRR квантов для HTB планировщика **условия:** queue = htb && type = qdisc
htb-quantum (*HTB quantum*) **минимум:** 1	Сколько байт может передать поток внутри класса **условия:** queue = htb
red-min (*RED min*) **минимум:** 1	Средний размер очереди (байт), при котором становится возможной маркировка пакетов **условия:** queue = red
red-max (*RED max*) **минимум:** 1	Средний размер очереди (байт), при котором вероятность маркирования достигает максимума **условия:** queue = red
red-probability (*RED probability*) **пример:** 0, 0.01, 1	Максимальная вероятность маркировки **условия:** queue = red
red-limit (*RED limit*) **минимум:** 1	Фактический предел очереди (байт). Последующие пакеты будут отброшены **условия:** queue = red
red-burst (*RED burst*) **минимум:** 1	Интервал (байт) между подгонкой среднего размера очереди к реальному **условия:** queue = red
red-avpkt (*RED avpkt*) **минимум:** 1	Размер пакета (байт), используемый для расчёта среднего размера очереди **условия:** queue = red
red-bandwidth (*RED bandwidth*) **минимум:** 1 **пример:** 4096, 512k, 10m	Скорость интерфейса, используется для расчётов, не ограничивает трафик **условия:** queue = red

red-ecn (*RED ECN*) **значения:** true, false	Explicit Congestion Notification, уведомляет удалённые хосты о превышении полосы пропускания **условия:** queue = red
red-harddrop (*RED harddrop*) **значения:** true, false	Принудительно отбрасывасывать пакеты если средний размер очереди превысит значение red-max **условия:** queue = red
red-adaptive (*RED adaptive*) **значения:** true, false	Динамически изменять red-probability что бы соответствовать усреднённому размеру очереди **условия:** queue = red

8. peripheral

Данный раздел предназначен для управления аппаратными периферийными устройствами роутера и внешними интерфейсами подключения. Здесь представлены инструменты для работы с портами ввода-вывода, управления питанием и настройки портов последовательной связи для подключаемого оборудования.

8.1. gnss to ip

Раздел предназначен для настройки передачи данных **GNSS/GPS** по IP-сети. Роутер может передавать навигационные координаты в формате **NMEA** на внешний сервер для интеграции с системами мониторинга или управления автопарком.

Настройки позволяют выбрать протокол передачи, задать интервал отправки данных и отфильтровать определённые типы сообщений **NMEA**. Также можно настроить задержку переподключения и ожидание подтверждения от сервера.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
ip-address (*Server*) **пример:** example.com:80, 192.168.1.1:80	Адрес сервера
protocol (*Protocol*) **значения:** udp, tcp	протокол передачи
interval (*Interval*) **значения:** 1, 5, 10, 20, 40, 60, 300, 600	интервал отправки
identifier (*Identifier*)	строка начальной идентификации
reconnect (*Reconnect*) **минимум:** 1, **максимум:** 60	задержка переподключения
need-ack (*Need ack*) **значения:** true, false	ожидать подтверждения от сервера
filter (*Filter*) **значения:** RMC, GGA, GSA, GSV, GLL, VTG	фильтр для данных NMEA

8.2. gpio

Раздел предназначен для настройки входов и выходов общего назначения (GPIO) роутера. GPIO позволяют взаимодействовать с внешними устройствами и электрическими цепями: отслеживать изменение состояния входов и управлять подключёнными компонентами через выходы.

Наличие GPIO, их количество и электрические характеристики зависят от модели роутера. Подробная информация приведена в руководстве пользователя и на сайте производителя.



• Подавать напряжение на вход GPIO можно только после полного включения роутера.
• Напряжение на входе GPIO не должно превышать напряжение питания роутера.
• Несоблюдение этих требований приведёт к необратимому повреждению роутера и аннулированию гарантии производителя.



Если к GPIO не подключён резистор 10 кОм, напряжение на входе GPIO должно совпадать с напряжением питания роутера. При наличии резистора 10 кОм допускается разница между напряжением питания роутера и напряжением на входе GPIO.

СВОЙСТВА

direction (*Direction*) **значения:** in, out	Направление работы порта **условия:** .type = gpi .type = gpo
value (*Value*) **значения:** high, low	Логический уровень напряжения на порту **условия:** direction = in
trigger (*Trigger*) **значения:** none, rising, falling, both	Генерировать событие по спаду, по фронту **условия:** direction = in
debounce (*Debounce*)	Интервал отскока (мсек), нейтрализация дребезга **условия:** direction = in

8.3. poe

Данный раздел предоставляет средства управления и мониторинга для функционала Power over Ethernet (PoE), **доступного только на определенных моделях роутеров, оснащенных соответствующим аппаратным обеспечением**, например на роутерах серии R10.

Роутер оснащен системой «Защитник PoE», которая не только подает питание на подключенные устройства, но и активно отслеживает каждый порт на предмет электрических неисправностей (таких как короткое замыкание или перегрузка по току), а также пытается автоматически восстановить его работу.

Состояние портов и работа

Вы можете отслеживать состояние каждого PoE-порта в реальном времени:

- **Disabled:** Порт административно выключен, питание не подается.
- **Enabled:** Порт активен и успешно подает питание на подключенное устройство.
- **Error:** Обнаружена неисправность, и система автоматически прекратила подачу питания на порт в целях безопасности.

Обработка ошибок и самовосстановление

Когда срабатывает механизм защиты, «Защитник PoE» запускает последовательность автоматического восстановления:

1. Первая попытка восстановления выполняется через **2 секунды** после обнаружения неисправности.

2. Если первая попытка неудачна, вторая попытка выполняется через **5 секунд**.

Если обе попытки неудачны, порт остается в состоянии *Error* для предотвращения повреждения роутера или подключенного устройства и требует ручного вмешательства.

Ручное вмешательство

Для управления портом в состоянии «Error» или для его настройки:

- **Чтобы проверить ошибку:** Выберите конкретный порт, и просмотрите описание последней зафиксированной ошибки и время ее возникновения.
- **Чтобы вручную подать питание:** После устранения физической проблемы с помощью **Apply** повторно перезапустите порт.
- **Чтобы включить/отключить порт:** Выберите нужный порт и измените состояние флажка **Disabled**.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Не включать PoE на порту при загрузке системы

8.4. protect

Данный раздел предназначен для управления сервисом **protectd**, который обеспечивает активную электрическую защиту для портов ввода-вывода общего назначения (GPIO).

Сервис отслеживает GPIO на предмет неисправностей, таких как короткое замыкание или перегрузка по току. При обнаружении сбоя **Protectd** автоматически отключает соответствующий порт, чтобы предотвратить повреждение внутренних цепей роутера. Порт будет оставаться в отключенном состоянии (состоянии ошибки) до тех пор, пока проблема не будет устранена и сервис не будет перезапущен вручную с этой страницы.

Действие перезапуска следует выполнять только после того, как внешняя физическая неисправность (например, короткое замыкание в подключенной проводке) была устранена.

КОМАНДЫ

restart	Перезапуск защиты GPIO

8.5. serial port

Раздел предназначен для настройки физических портов RS232 и RS485 роутера, позволяя использовать его в качестве многофункционального шлюза Serial-to-IP. Эта функция позволяет инкапсулировать данные последовательного порта в IP-пакеты и передавать их по сети, обеспечивая удалённый доступ и интеграцию оборудования с последовательными интерфейсами в современные IP-системы.

Ключевым параметром конфигурации является **Режим работы (Mode)**, который определяет, как роутер обрабатывает данные последовательного порта:

- **Server Mode:** Роутер ожидает входящие TCP-соединения на указанном порту. Удалённый клиент подключается к роутеру для получения доступа к подключённому последовательному устройству.

- **Client Mode:** Роутер инициирует TCP-соединение с удалённым сервером и пересылает ему данные, полученные с локального последовательного порта.
- **Modbus TCP Mode:** Роутер работает как шлюз Modbus, преобразуя запросы Modbus TCP из сети в запросы Modbus RTU для подключённого ведомого устройства (slave).
- **NTRIP Client Mode:** Специализированный режим для подключения к NTRIP Caster, получения корректирующих данных GNSS и их передачи на подключённое последовательное устройство (например, высокоточный GNSS-приёмник). Режим доступен при установленном компоненте NTRIP Client.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
mode (*Mode*) **значения:** client, server, modbustcp	Режим работы последовательного порта **условия:** /defaults/ntripclient_installed = true
host (*Host*)	Адрес удалённого хоста **условия:** mode = client
ntrip-mode (*NTRIP mode*) **значения:** auto, ntrip1, http, rtsp, udp	Транспорт для обмена данными **условия:** mode = ntripclient && ntripclient_installed = true
local-baudrate (*Baudrate*) **значения:** 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	Скорость передачи через последовательный порт
local-parity (*Parity*) **значения:** none, odd, even	Контрольный бит чётности
local-stop-bits (*Stop bits*) **значения:** 1, 2	Число стоп-бит в посылке
local-data-bits (*Data bits*) **значения:** 8, 7	Число бит данных в посылке **условия:** mode = client mode = server mode = ntripclient
local-flowcontrol (*Flowcontrol*) **значения:** none, soft, hard	Управление потоком
remote-proto (*Remote Protocol*) **значения:** raw, rfc2217	Протокол последовательно порта удалённой стороны **условия:** mode = client mode = server
remote-baudrate (*Remote baudrate*) **значения:** 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200	Скорость передачи через последовательный порт **условия:** remote-proto = rfc2217 && mode = client
remote-parity (*Remote parity*) **значения:** none, odd, even	Контрольный бит чётности **условия:** remote-proto = rfc2217 && mode = client
remote-stop-bits (*Remote stop bits*) **значения:** 1, 2	Число стоп-бит в посылке **условия:** remote-proto = rfc2217 && mode = client
remote-data-bits (*Remote data bits*) **значения:** 8, 7	Число бит данных в посылке **условия:** remote-proto = rfc2217 && mode = client

remote-flowcontrol (*Remote flowcontrol*) **значения:** none, soft, hard	Управление потоком **условия:** remote-proto = rfc2217 && mode = client
remote-acknowledgement (*Remote acknowledgement*) **значения:** true, false	Требовать от удалённой стороны подтверждения настроек **условия:** remote-proto = rfc2217 && mode = client
remote-acknowledgement-timeout (*Acknowledgement timeout*)	Таймаут подтверждения настроек удалённой стороной **условия:** remote-proto = rfc2217 && mode = client
banner (*Banner*)	Баннер отправляемый при соединении **условия:** remote-proto = raw && mode = client remote-proto = raw && mode = server
local-accumulation-interval (*Accumulation interval*) **минимум:** 1	Период (мсек) между чтением данных из последовательного порта в буфер для последующей отправки буфера целиком **условия:** mode != modbustcp
local-accumulation-attempts (*Accumulation attempts*)	Сколько раз читать данные из последовательного порта для накопления буфера **условия:** mode != modbustcp
reconnect-delay (*Reconnect delay*) **минимум:** 1	Задержка (сек) после разрыва до повторного подключения
peer-timeout (*Peer timeout*) **минимум:** 0	Разорвать соединение если удалённая сторона бездействует дольше указанного времени (сек)
bind (*Bind*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel **пример:** bridge0	Выбор интерфейса или адреса для ожидания подключения **условия:** mode = modbustcp mode = server
port (*Port*) **пример:** 80, !80	Порт для ожидания подключения **условия:** mode = modbustcp mode = server
ntrip-mountpoint (*Ntrip mountpoint*)	Mountpoint или другой критерий согласования набора данных **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-user (*NTRIP User*)	Имя пользователя для аутентификации и/или согласования набора данных **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-password (*NTRIP password*)	Пароль пользователя **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-nmea (*NTRIP NMEA*)	Строка NMEA данных для отправки на сервер **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-bitrate (*NTRIP Bitrate*) **значения:** true, false	Исходящий bitrate **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-initudp (*NTRIP Initudp*) **значения:** true, false	Отправка предварительного UDP пакета для обработки файрволом **условия:** mode = ntripclient && ntripclient_installed = true

ntrip-udpport (*UDP Port*) **пример:** 80, !80	Выбрать локальный UDP порт **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-proxyhost (*NTRIP proxy host*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес прокси сервера **условия:** mode = ntripclient && ntripclient_installed = true
ntrip-protocol (*NTRIP protocol*) **значения:** none, rts_cts, xon_xoff	Протокол контроля потока для последовательного порта **условия:** mode = ntripclient && ntripclient_installed = true
failopen-timeout (*Failopen timeout*)	Задержка до коммуникации с последовательным портом после ошибки
debug (*Debug*) **значения:** true, false	Режим подробного логгирования

9. radius

Раздел предназначен для настройки протокола **RADIUS (Remote Authentication Dial-In User Service)**, обеспечивающего централизованную поддержку функций **AAA** (аутентификация, авторизация и учет). Данный функционал позволяет устройству управлять доступом к сети, разграничивать права пользователей и фиксировать статистику сессий в рамках сетевой инфраструктуры.

9.1. attribute

Подраздел предназначен для настройки пользовательских **атрибутов RADIUS**, включаемых в ответные пакеты сервера. Эти атрибуты используются для передачи параметров авторизации от RADIUS-сервера клиентскому устройству.

В разделе можно настроить два атрибута: *Management-Privilege-Level* для определения уровня административных привилегий пользователя и *Denied-Schemas* для ограничения доступа к определённым схемам конфигурации системы. Для каждого атрибута задаётся соответствующее значение.

СВОЙСТВА

attribute (*Attribute*) **значения:** Management-Privilege-Level, Denied-Schemas	Имя RADIUS атрибута
value (*Value*)	Значение атрибута

9.2. client

Подраздел предназначен для настройки **серверов сетевого доступа (NAS)**, которым разрешено взаимодействовать с роутером, работающим в режиме RADIUS-сервера. В качестве NAS могут выступать внешние сетевые устройства, например другие роутеры или точки доступа, которые идентифицируются по IP-адресам. Для каждого устройства задаётся общий секретный ключ, используемый для аутентификации RADIUS-клиента.

Дополнительно можно включить обязательную проверку наличия атрибута *Message-Authenticator* в запросах RADIUS для обеспечения целостности сообщений при обмене данными аутентификации.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
ip-address (*IP Address*) **пример:** 192.168.1.1	IP адрес NAS клиента
secret (*Shared Secret*) **мин. длина:** 8	Общий секретный ключ для RADIUS
require-ma (*Require MA*) **значения:** true, false	Требовать наличия атрибута Message-Authenticator

9.3. server

Подраздел предназначен для настройки глобальных параметров работы роутера в режиме **RADIUS-сервера**. Здесь определяются параметры приёма и обработки входящих запросов аутентификации и учёта сеансов от сетевых устройств.

В разделе можно настроить порты для запросов аутентификации и учёта сеансов, а также включить защищённую передачу данных по протоколу **TLS**. При использовании TLS необходимо настроить сертификат сервера и файл центра сертификации (CA). Дополнительно можно указать порт TLS-соединений и минимальную поддерживаемую версию протокола.

Также можно включить подробное логирование событий аутентификации (*Debug Logging*) для выявления и устранения ошибок.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
auth-port (*Authentication Port*) **минимум:** 1024, **максимум:** 65535	Порт для аутентификации (RADIUS Auth)
acct-port (*Accounting Port*) **минимум:** 1024, **максимум:** 65535	Порт для аккаунтинга (RADIUS Acct)
tls (*TLS*) **значения:** true, false	Разрешить TLS транспорт для подключений
tls-port (*TLS Port*) **минимум:** 1024, **максимум:** 65535	Порт для TLS подключений **условия:** tls = true
ca (*TLS CA File*) **значения:** /storage certificate	Сертификат удостоверяющего цетра (CA) **условия:** tls = true
cert (*TLS Certificate*) **значения:** /storage certificate	Сертификат для аутентификации и шифрования **условия:** tls = true
tls-min-version (*TLS Minimum Version*) **значения:** 1.0, 1.1, 1.2, 1.3	Минимальная версия TLS **условия:** tls = true
debug (*Debug Logging*) **значения:** true, false	Включить логирование всех событий аутентификации

9.4. user

Подраздел предназначен для управления локальной базой пользователей встроенного **RADIUS-сервера**. Здесь можно создавать и настраивать учётные записи пользователей, задавать данные для аутентификации и параметры доступа.

Поддерживаются способы аутентификации **PAP** и **EAP**. Для EAP доступны типы PEAP, TTLS и TLS, которые обычно используются в сетях **WPA-Enterprise** и **802.1X**. Для каждого пользователя можно назначить ранее настроенные атрибуты ответа RADIUS, определяющие права доступа и параметры сеанса после успешной аутентификации.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
auth-type (*Authentication Type*) **значения:** pap, eap	Протокол аутентификации пользователя
eap-type (*EAP Type*) **значения:** peap, ttls, tls	Тип EAP аутентификации (WPA-Enterprise / 802.1x) **условия:** auth-type = eap
password (*Password*)	Пароль пользователя RADIUS **условия:** auth-type = eap && eap-type = tls
eap-method (*EAP Method*) **значения:** mschap-v2, pap, any	Метод аутентификации внутри EAP-туннеля **условия:** auth-type = eap && eap-type = peap auth-type = eap && eap-type = ttls
reply-attr (*Reply Attribute*) **значения:** /radius attribute	Определяют права и параметры сессии пользователя после аутентификации

10. routing

Данный раздел предназначен для настройки протоколов динамической маршрутизации и механизмов оптимизации путей передачи трафика. Здесь сосредоточены инструменты для конфигурации обмена информацией о доступности сетей между соседями и поддержания актуальных маршрутов в сложных сетевых инфраструктурах.

10.1. bfd

В данном разделе настраиваются глобальные параметры протокола **BFD** для всего роутера. Поскольку за обслуживание всех сессий мониторинга в системе отвечает единый фоновый процесс, конфигурация представляет собой один общий набор настроек, а не список отдельных записей.

Параметры раздела позволяют указывать IP-адреса соседей для контроля связности и активировать ранее настроенные BFD-интерфейсы. Одной из ключевых функций является поддержка сессий **multihop**, которые позволяют отслеживать доступность узлов, не имеющих прямого физического соединения с роутером и находящихся на расстоянии нескольких сетевых переходов. При включении режима multihop становятся доступны специфические настройки временных интервалов и порогов обнаружения сбоев, адаптированные для работы через несколько сегментов сети.

10.1.1. interface

В данном разделе настраиваются индивидуальные параметры протокола **Bidirectional Forwarding Detection (BFD)** для отдельных сетевых интерфейсов. BFD предназначен для быстрого обнаружения нарушений связности между соседними маршрутизаторами. Использование BFD позволяет протоколам динамической маршрутизации быстрее обнаруживать сбои соединения и переключать маршруты, не дожидаясь срабатывания стандартных таймеров.

Параметры раздела позволяют задавать интервалы отправки и приёма управляющих пакетов BFD, а также множитель обнаружения, определяющий время, по истечении которого сессия считается недоступной при отсутствии пакетов от соседнего устройства. Дополнительно можно включить пассивный режим, при котором роутер ожидает получения пакета BFD от соседнего устройства для установления сессии.

СВОЙСТВА

min-rx-interval (*Min Rx Interval*) **минимум:** 1, **максимум:** 4294967	Минимальный интервал приёма (мс), анонсируемый соседу — ограничивает частоту, с которой сосед генерирует управляющие BFD-пакеты
min-tx-interval (*Min Tx Interval*) **минимум:** 1, **максимум:** 4294967	Желаемый интервал отправки (мс) управляющих BFD-пакетов (совместно с Min Rx Interval, анонсируемым соседом)
multiplier (*Multiplier*) **минимум:** 1, **максимум:** 255	Количество пропущенных пакетов (с интервалом min-rx/tx-interval), после которого сессия считается недоступной
passive (*Passive*) **значения:** true, false	Не отправлять BFD-пакеты, пока роутер не получит BFD-пакет от другой стороны

10.1.2. settings

В данном разделе настраиваются глобальные параметры протокола **BFD**. Поскольку в системе все BFD-сессии обслуживаются единым фоновым процессом, параметры конфигурации являются общими для всего роутера.

Настройки позволяют указывать IP-адреса соседей для контроля связности, выбирать активные интерфейсы, а также управлять сессиями **multihop** для взаимодействия с узлами, находящимися за пределами локальной подсети. Для multihop-сессий предусмотрены специфические настройки таймеров и множителей обнаружения сбоев.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
neighbor (*Neighbor*)	IP-адрес соседа
interface (*Interface*) **значения:** /routing bfd interface	Интерфейсы, используемые этим протоколом
multihop (*Multihop*) **значения:** true, false	Включить multihop-соседей (сессии с адресами, не находящимися на directly connected линке)

multihop-neighbor (*Multihop neighbor*)	Multihop-соседи: удалённый адрес и локальный адрес отправителя через двоеточие **условия:** multihop = true
multihop-min-rx-interval (*Multihop Min Rx Interval*) **минимум:** 1, **максимум:** 4294967	Минимальный интервал приёма (мс) для multihop-сессий **условия:** multihop = true
multihop-min-tx-interval (*Multihop Min Tx Interval*) **минимум:** 1, **максимум:** 4294967	Желаемый интервал отправки (мс) для multihop-сессий **условия:** multihop = true
multihop-multiplier (*Multihop multiplier*) **минимум:** 1, **максимум:** 255	Множитель для multihop-сессий **условия:** multihop = true
multihop-passive (*Multihop passive*) **значения:** true, false	Не отправлять BFD-пакеты для multihop-сессий, пока не получен пакет от другой стороны **условия:** multihop = true

10.2. bgp

Данный раздел предназначен для настройки протокола **BGP (Border Gateway Protocol)** — основного протокола динамической маршрутизации, используемого для обмена данными между различными сетями (автономными системами) или внутри крупных сетевых инфраструктур. BGP позволяет роутеру автоматически определять оптимальные пути к удаленным сетям и анонсировать собственные доступные маршруты соседним устройствам.

Процесс настройки включает установку сессий с «соседями» (пирами) путем указания их IP-адресов и номеров автономных систем (AS). Система поддерживает как прямые соединения, так и режим **multihop** для случаев, когда соседний узел находится за пределами локальной подсети. Для обеспечения стабильности и безопасности предусмотрены настройки таймеров сессии, парольная защита, а также интеграция с протоколом **BFD** для мгновенного обнаружения разрывов связи.

Раздел также предоставляет доступ к продвинутым функциям, таким как работа в режиме **Route Reflector** для масштабирования внутренних сетей и управление распределением маршрутов с помощью гибких фильтров импорта и экспорта. Фильтры могут настраиваться непосредственно в интерфейсе или загружаться из внешних файлов конфигурации для реализации сложных политик маршрутизации.

КОМАНДЫ

route-stats	Статистика изменений маршрутов в виде таблицы

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
router-id (*Router ID*) **пример:** 192.168.1.1	Router ID, переопределяющий глобальную настройку
local-as (*Local AS*) **минимум:** 1, **максимум:** 4294967295	Идентификатор автономной системы
local-addr (*Local address*) **пример:** 192.168.1.1, 192.168.1.1:51820	Локальный IP-адрес. Порт по умолчанию — 179

neighbor-as (*Neighbor AS*) **минимум:** 1, **максимум:** 4294967295	Идентификатор автономной системы
neighbor-addr (*Neighbor address*) **пример:** 192.168.1.1, 192.168.1.1:51820	Сосед, с которым будет установлена эта сессия. Порт по умолчанию — 179
multihop (*Multihop*) **значения:** true, false	Использовать, если указанный IP-адрес соседа не входит ни в одну из локальных подсетей
ttl (*Ttl*) **минимум:** 1, **максимум:** 255	Количество хопов **условия:** multihop = true
hold-time (*Hold Time*)	Время в секундах ожидания Keepalive-сообщения от другой стороны, после которого соединение считается устаревшим. Ноль означает, что keepalive не используются
keepalive-time (*Keepalive Time*) **минимум:** 1, **максимум:** 65535	Интервал в секундах между отправкой двух последовательных Keepalive-сообщений. По умолчанию = hold-time/3
password (*Password*) **макс. длина:** 80	Ключ аутентификации, встраиваемый в конфигурацию BIRD как строковый литерал в кавычках
bfd (*Use BFD*) **значения:** true, false	Использовать протокол BFD как вспомогательный механизм быстрого обнаружения потери соседа
next-hop-self (*Next Hop Self*) **значения:** true, false	Заставить этот роутер анонсировать себя как next hop для маршрутов, отправляемых этому соседу
reflection (*Reflection*) **значения:** true, false	Работать как route reflector и считать соседа route-reflection клиентом
cluster-id (*Cluster ID*) **пример:** 3232235777, 192.168.1.1	Опция для предотвращения петель route reflection. По умолчанию совпадает с router id **условия:** reflection = true
extra (*Extra Options*) **значения:** default-bgp_med, default-bgp_local_pref, med-metric, allow-bgp_med, allow-bgp_local_pref	НЕТ ОПИСАНИЯ
use-filter-file (*Use filter file*) **значения:** true, false	Использовать конфигурацию фильтра из файла вместо параметров
export-filter-file (*Export Filter File*) **значения:** /storage file	Файл конфигурации фильтра в синтаксисе BIRD **условия:** use-filter-file = true
import-filter-file (*Import Filter File*) **значения:** /storage file	Файл конфигурации фильтра в синтаксисе BIRD **условия:** use-filter-file = true
default-export (*Default export*) **значения:** accept, reject	Фильтр экспорта по умолчанию **условия:** use-filter-file = ""
default-import (*Default import*) **значения:** accept, reject	Фильтр импорта по умолчанию **условия:** use-filter-file = ""
export-filter (*Export filter*) **значения:** /routing filter	Фильтр экспорта **условия:** use-filter-file = ""

import-filter (*Import filter*) **значения:** /routing filter	Фильтр импорта **условия:** use-filter-file = ""

10.3. common

В данном разделе настраиваются глобальные параметры демона маршрутизации BIRD. Эти настройки применяются ко всей подсистеме маршрутизации, а не к отдельным протоколам.

Параметры раздела позволяют включать и отключать конфигурацию, задавать *Router ID* для идентификации роутера в протоколах маршрутизации и определять периодичность сканирования списка сетевых интерфейсов. Также можно указать интерфейсы, исключаемые при анонсировании маршрутной информации.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
router-id (*Router ID*) **пример:** 3232235777, 192.168.1.1	4-байтовое целое число (0-4294967295), которое должно быть уникальным в пределах AS (число или адрес IPv4)
scan-time (*Routes scan time*) **минимум:** 0, **максимум:** 4294967295	Интервал в секундах между сканированиями списка сетевых интерфейсов. 0 — сканировать только при старте, без периодического опроса
exclude (*Routing Excludes*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel	Исключить интерфейсы из анонсирования

10.4. filter

Данный раздел предоставляет инструменты для управления распределением маршрутов с помощью **фильтров маршрутизации**. Фильтры позволяют детально контролировать, какая маршрутная информация будет приниматься от соседних устройств или передаваться им. Применение этих правил помогает оптимизировать маршрутизацию, снизить риск появления маршрутных петель и ограничить распространение нежелательных маршрутов в сети.

Настройка включает определение условий для проверки маршрутов, таких как сетевые префиксы, их допустимая длина и источник происхождения маршрута (например, **Static**, **OSPF** или **BGP**). Для каждого правила назначается действие: разрешить (*accept*) или отклонить (*reject*) соответствующие маршруты. Кроме того, для сетей **OSPF** фильтры позволяют корректировать метрики маршрутов, тем самым влияя на процесс выбора оптимального пути в среде динамической маршрутизации.

СВОЙСТВА

action (*Rule action*) **значения:** accept, reject	Действие правила
match (*Rule match*) **значения:** true, false	Совпадение с префиксом (true) или несовпадение (false)
prefix (*Rule prefix*) **пример:** 192.168.1.0/24	Префикс сети

source (*Route source*) **значения:** any, static, connected, ospf, bgp	Источник маршрута
min-length (*Minimum prefix length*) **минимум:** 0, **максимум:** 32	Минимальная длина префикса маршрута
max-length (*Maximum prefix length*) **минимум:** 0, **максимум:** 32	Максимальная длина префикса маршрута
ospf-metric-1 (*OSPF Metric type 1*) **минимум:** 0, **максимум:** 16777214	Задание метрики OSPF типа 1 для маршрутов, прошедших правило. Только для OSPF
ospf-metric-2 (*OSPF Metric type 2*) **минимум:** 1, **максимум:** 16777214	Задание метрики OSPF типа 2 для маршрутов, прошедших правило. Только для OSPF

10.5. ospf

В данном разделе выполняется настройка протокола **OSPF (Open Shortest Path First)** — протокола динамической маршрутизации, предназначенного для эффективного распределения трафика в крупных внутренних сетях. Использование протокола обеспечивает автоматический расчёт маршрутов и быструю сходимость при изменении топологии сети.

10.5.1. area

Раздел предназначен для настройки областей OSPF. Протокол OSPF использует разделение на области для создания иерархической структуры сети, что упрощает управление маршрутизацией и повышает масштабируемость в крупных сетях.

При создании области ей присваивается имя и идентификатор (*OSPF Area ID*), а также выбирается экземпляр OSPF (*Instance*), к которому она будет относиться. Использование нескольких экземпляров OSPF позволяет создавать на одном устройстве независимые домены маршрутизации, например для сегментации сети.

После определения области ей назначаются сетевые интерфейсы в разделе *OSPF / Interface* для включения маршрутизации в ее пределах.

КОМАНДЫ

ranges	Состояние IP-диапазонов area, включая внешние для NSSA, в виде таблицы

СВОЙСТВА

id (*OSPF Area ID*) **пример:** 3232235777, 192.168.1.1	Идентификатор OSPF area
type (*Type*) **значения:** standard, nssa, stub	Тип area
summary (*Summary*) **значения:** true, false	Пропускать в area сводные маршруты (Type-3 Summary LSA) из других area; без этого — только маршрут по умолчанию (totally stubby) **условия:** type = nssa type = stub
default-nssa (*Default nssa*) **значения:** true, false	Анонсировать в NSSA маршрут по умолчанию (Type-7 default) **условия:** type = nssa && summary = true

default-cost (*Default cost*) **минимум:** 1, **максимум:** 16777214	Стоимость маршрута по умолчанию, передаваемого в сеть **условия:** type = nssa type = stub
default-cost2 (*Default cost (type 2)*) **минимум:** 1, **максимум:** 16777214	Стоимость маршрута по умолчанию для NSSA как внешняя метрика Type-2: не складывается с внутренней стоимостью пути. Если задано, перекрывает default-cost **условия:** type = nssa && summary = true && default-nssa = true
interface (*Interface*) **значения:** /routing ospf interface	Интерфейс area
network (*Network*)	Определение IP-диапазонов area
stubnet (*Stubnet*)	Сети, не являющиеся транзитными между OSPF-роутерами
external (*External*)	Определение внешних IP-диапазонов для NSSA area **условия:** type = nssa

10.5.2. instance

Раздел предназначен для настройки и управления отдельными экземплярами OSPF. Каждый экземпляр представляет собой независимый процесс маршрутизации OSPF, что позволяет запускать на одном роутере несколько экземпляров протокола.

Экземпляр OSPF объединяет настройки маршрутизации, политики фильтрации и связанные с ним области OSPF. Основные возможности раздела:

- Назначение *Router ID* для экземпляра OSPF с возможностью переопределения глобального значения.
- Настройка фильтров импорта и экспорта для управления обменом маршрутами между OSPF и таблицей маршрутизации.
- Установка действий по умолчанию для маршрутов, не соответствующих правилам фильтрации: принять (*accept*) или отклонить (*reject*).
- Использование файлов конфигурации BIRD вместо настройки фильтров через параметры интерфейса.
- Привязка областей OSPF к соответствующему экземпляру.

Дополнительно раздел позволяет просматривать информацию о соседних маршрутизаторах и статистику изменений маршрутов для каждого экземпляра OSPF.

КОМАНДЫ

route-stats	Статистика изменений маршрутов в виде таблицы
neighbors	Соседи этого экземпляра OSPF в виде таблицы

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
router-id (*Router ID*) **пример:** 192.168.1.1	Router ID, переопределяющий глобальную настройку

use-filter-file (*Use filter file*) **значения:** true, false	Использовать конфигурацию фильтра из файла вместо параметров
export-filter-file (*Export Filter File*) **значения:** /storage file	Файл конфигурации фильтра в синтаксисе BIRD **условия:** use-filter-file = true
import-filter-file (*Import Filter File*) **значения:** /storage file	Файл конфигурации фильтра в синтаксисе BIRD **условия:** use-filter-file = true
default-export (*Default export*) **значения:** accept, reject	Действие экспорта по умолчанию **условия:** use-filter-file = ""
default-import (*Default import*) **значения:** accept, reject	Действие импорта по умолчанию **условия:** use-filter-file = ""
export-filter (*Export filter*) **значения:** /routing filter	Фильтр экспорта **условия:** use-filter-file = ""
import-filter (*Import filter*) **значения:** /routing filter	Фильтр импорта **условия:** use-filter-file = ""
area (*Area*) **значения:** /routing ospf area	Area, входящие в этот экземпляр OSPF

10.5.3. interface

В данном разделе сетевые интерфейсы назначаются настроенным областям OSPF, что позволяет активировать протокол на соответствующих сегментах сети. Это обеспечивает установление соседства между маршрутизаторами и обмен маршрутной информацией через указанные интерфейсы.

Параметры раздела позволяют управлять работой OSPF на отдельных интерфейсах: настраивать таймеры *Hello* и *Dead*, задавать *Priority* для участия в выборах DR/BDR и определять *Cost* интерфейса, влияющую на выбор маршрутов алгоритмом SPF. Дополнительно можно включить аутентификацию OSPF для защиты обмена маршрутной информацией.

В *Пассивном режиме* сеть продолжает анонсироваться через OSPF, но интерфейс не отправляет пакеты протокола и не устанавливает соседство с другими маршрутизаторами. Этот режим обычно используется для анонсирования локальных сетей, в которых отсутствуют другие маршрутизаторы OSPF.

КОМАНДЫ

neighbors	Соседи OSPF на этом интерфейсе в виде таблицы

СВОЙСТВА

cost (*Interface cost*) **минимум:** 1, **максимум:** 65535	Метрика (стоимость) интерфейса
hello (*Hello interval*) **минимум:** 1, **максимум:** 65535	Интервал отправки Hello (сек)
wait (*Wait interval*) **минимум:** 2, **максимум:** 4294967295	Интервал ожидания (сек), по умолчанию = 4×hello

dead (*Dead interval*) **минимум:** 2, **максимум:** 4294967295	Интервал недоступности соседа (сек), по умолчанию = 5×hello
bfd (*Use BFD*) **значения:** true, false	Использовать протокол BFD как вспомогательный механизм быстрого обнаружения потери соседа
priority (*Interface priority*) **минимум:** 0, **максимум:** 255	Приоритет интерфейса (0 — интерфейс никогда не станет DR/BDR)
authentication (*Authentication type*) **значения:** none, cryptographic, simple	Тип аутентификации
password (*Password*) **макс. длина:** 8	Ключ аутентификации, встраиваемый в конфигурацию BIRD как строковый литерал в кавычках **условия:** authentication = none authentication = cryptographic
type (*Network type*) **значения:** broadcast, auto, nonbroadcast, pointopoint, pointomultipoint	Тип сети
neighbor (*Neighbor*)	Сосед, которому отправляются Hello-сообщения в сетях NBMA или PtMP **условия:** type = nonbroadcast type = pointomultipoint
strict (*Strict NBMA*) **значения:** true, false	Принимать Hello только от адресов из списка «neighbor»; без этого принимаются Hello от любого адреса в этом сегменте **условия:** type = nonbroadcast type = pointomultipoint
stub (*Passive mode*) **значения:** true, false	Пассивный режим
retransmit (*Retransmit interval*) **минимум:** 2, **максимум:** 4294967295	Интервал повторной отправки (сек)
transmit-delay (*Transmit delay*) **минимум:** 1, **максимум:** 65535	Задержка перед отправкой (сек)

10.6. status

Раздел предназначен для просмотра таблицы маршрутизации BIRD. Здесь отображаются маршруты, полученные из различных источников, включая протоколы динамической маршрутизации **OSPF** и **BGP**. Эта информация позволяет отслеживать выбор маршрутов и выявлять проблемы сетевой связности.

Для каждого маршрута отображаются сеть назначения, тип маршрута, экземпляр протокола, источник маршрута и его приоритет. Отдельный признак *Best path* указывает, выбран ли маршрут как лучший для пересылки трафика. Дополнительно могут отображаться шлюз следующего перехода, выходной интерфейс и специфические атрибуты протоколов, такие как метрики OSPF и путь автономных систем (AS Path) в BGP.

СВОЙСТВА

network (*Network*)	Сеть назначения
route-type (*Route type*)	Тип маршрута
protocol (*Protocol instance*)	Экземпляр протокола, от которого получен маршрут
selected (*Best path*) **значения:** true, false	Выбран лучшим (используется для пересылки трафика)

preference (*Preference*)	Внутренний приоритет BIRD для этого пути
since (*Since*)	Время появления маршрута
gateway (*Gateway*)	Шлюз следующего перехода **условия:** gateway != ""
interface (*Interface*)	Исходящий интерфейс **условия:** interface != ""
proto-type (*Source type*)	Источник маршрута на уровне протокола (например, для OSPF отличает внутренние маршруты — OSPF/OSPF-IA — от внешних, редистрибутированных — OSPF-E1/OSPF-E2)
origin (*BGP origin*)	Атрибут BGP origin **условия:** origin != ""
as-path (*BGP AS-path*)	Атрибут BGP AS-path **условия:** as-path != ""
next-hop (*BGP next-hop*)	Атрибут BGP next-hop **условия:** next-hop != ""
local-pref (*BGP local preference*)	Атрибут BGP local preference **условия:** local-pref != ""
med (*BGP MED*)	Атрибут BGP MED **условия:** med != ""
tag (*OSPF route tag*)	Тег маршрута OSPF (например, используется для защиты от петель при редистрибуции) **условия:** tag != ""
ospf-metric1 (*OSPF Metric 1*)	Внутренняя метрика OSPF (Type 1) **условия:** ospf-metric1 != ""
ospf-metric2 (*OSPF Metric 2*)	Внешняя метрика OSPF (Type 2, для редистрибутированных маршрутов) **условия:** ospf-metric2 != ""
router-id (*OSPF router-id*)	Router-id источника маршрута (ASBR/ABR) **условия:** router-id != ""
attributes (*Other attributes*)	Прочие атрибуты маршрута **условия:** attributes != ""

11. service

Данный раздел предназначен для управления ключевыми системными службами и вспомогательными приложениями, расширяющими функциональность роутера. Эти сервисы обеспечивают выполнение сетевых задач, мониторинг, безопасность и административные функции, необходимые для эксплуатации устройства в специализированных сетевых средах.

11.1. client

Раздел предназначен для создания и управления профилями пользователей различных VPN и туннельных сервисов, работающих на роутере, например L2TP, OpenVPN и PPTP.

Вместо настройки пользователей отдельно для каждого сервиса можно создать единый профиль и назначить ему один или несколько доступных сервисов. Это упрощает управление пользователями и обеспечивает единообразие настроек аутентификации.

Каждый профиль содержит имя пользователя и пароль для аутентификации. Также можно назначить клиенту определённый IP-адрес туннеля (**Tunnel IP**) и настроить маршруты (**Route**) к сетям, расположенным за удалённой стороной. Эти маршруты добавляются в локальную таблицу маршрутизации роутера для обеспечения связи с удалёнными сетями.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Не использовать профиль пользователя
service (*Service*) **значения:** /defaults services	Сервисы, которыми пользователь может пользоваться
password (*Password*)	Пароль пользователя
tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	IP адрес назначаемый для туннельного интерфейса удалённой стороны
route (*Route*)	Адреса за удалённой стороной для добавления локального маршрута

11.2. dhcp

Данный раздел предназначен для настройки службы **DHCP (Dynamic Host Configuration Protocol)**, которая автоматизирует назначение сетевых параметров подключенным устройствам. Роутер выполняет роль централизованного узла для распределения IP-адресов, что значительно упрощает администрирование сети, исключая необходимость ручной настройки каждого сетевого узла.

11.2.1. lease

Подраздел предназначен для просмотра IP-адресов, выданных DHCP-сервером роутера, и управления записями аренды (DHCP leases).

В таблице отображаются сведения об арендах, включая MAC-адрес клиента, назначенный IP-адрес и время истечения срока аренды.

Основная функция подраздела — управление арендами DHCP, в частности создание **статических аренд** (резервирований адресов). Статическая аренда закрепляет определённый IP-адрес за устройством по его MAC-адресу. Это удобно для серверов, принтеров и других устройств, которым требуется постоянный IP-адрес.

Для создания резервирования можно выбрать существующую динамическую аренду и воспользоваться функцией **Make static** либо вручную добавить статическую запись, указав IP-адрес и MAC-адрес устройства. Также можно включить создание DNS-записи и указать полное доменное имя (FQDN) для разрешения имени хоста.

КОМАНДЫ

make-static	Сделать динамическую запись lease постоянной

СВОЙСТВА

interface (*Interface*) **значения:** /service dhcp server, auto	Интерфейс, на котором может быть выдана статическая запись lease
ip (*Host IP*) **пример:** 192.168.1.1	IP адрес хоста
mac (*Host MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес хоста
dns (*DNS entry*) **значения:** true, false	Добавить DNS запись для разрешения IP адреса
fqdn (*FQDN*) **пример:** localhost, example.com, sample.example.com	Указать имя хоста для разрешения IP адреса

11.2.2. server

Подраздел предназначен для настройки и управления DHCP-сервисами на сетевых интерфейсах роутера. Здесь можно настроить порядок выдачи IP-адресов клиентам в определённом сегменте сети.

Основным параметром является **Mode** (режим работы), который определяет, будет ли роутер работать как DHCP-сервер или DHCP-ретранслятор.

Режим сервера (Server Mode)

В режиме **Server** роутер самостоятельно выдаёт IP-адреса клиентам в выбранной сети. Можно настроить пул IP-адресов (*IP pool*), время аренды (*Leasetime*) и сетевые параметры, передаваемые клиентам, включая шлюз по умолчанию (*Router*) и DNS-серверы (*DNS server*). Для дополнительных требований сети также предусмотрена настройка *DHCP Options*.

Режим ретранслятора (Relay Mode)

В режиме **Relay** роутер не выдаёт IP-адреса самостоятельно, а принимает DHCP-запросы на выбранном интерфейсе и пересылает их на удалённый DHCP-сервер. Это позволяет централизованно управлять выдачей IP-адресов. В данном режиме можно указать адрес удалённого сервера (*Server*) и настроить обработку DHCP-опции 82 при ретрансляции запросов.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
mode (*Mode*) **значения:** server, relay	Режим обработки DHCP запросов
server (*Server*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес DHCP сервера для переадресации запросов **условия:** mode = relay
relay-mode (*Relay Mode*) **значения:** append, replace, forward, discard	Действие над DHCP пакетом содержащим опцию 82 **условия:** mode = relay && suboption = true mode = relay && suboption = ""
remote-id (*Remote ID*)	Option 82 Remote ID **условия:** mode = relay

hops (*Maximum hops*) **максимум:** 255	Максимальное количество прыжков (hop) прежде чем DHCP пакет будет отброшен **условия:** mode = relay
suboption (*Enable RFC 3527*) **значения:** true, false	Send link selection suboption for directly connected clients **условия:** mode = relay
debug (*Debug*) **значения:** true, false	Режим подробного логгирования **условия:** mode = relay
pool (*IP pool*)	Пул IP адресов для выдачи клиентам **условия:** mode = server
router **пример:** 192.168.1.1	IP адрес шлюза (Опция 3) **условия:** mode = server
dns-server (*DNS server*)	IP адрес DNS сервера (Опция 6) **условия:** mode = server
ntp-server (*NTP server*)	IP адрес NTP сервера (Опция 42) **условия:** mode = server
leasetime (*Leasetime*) **значения:** 30m, 1h, 4h, 12h, 24h, 7d	Время аренды IP адреса **условия:** mode = server
flags (*Flags*) **значения:** authoritative, no-override, sequential-ip, rapid-commit	Параметр DHCP сервера **условия:** mode = server
option (*DHCP Options*) **значения:** tftp-server, bootfile-name, classless-static-route	Дополнительные DHCP опции **условия:** mode = server

11.3. dns

Раздел предназначен для настройки встроенной службы DNS (Domain Name System) роутера, которая выполняет пересылку и кэширование DNS-запросов в локальной сети. Роутер принимает запросы от устройств, пересылает их вышестоящим DNS-серверам и сохраняет ответы в кэше для ускорения последующих обращений.

В разделе доступны следующие возможности:

- **Пересылка DNS-запросов:** Можно указать вышестоящие *DNS-серверы* для обработки обычных запросов. Функция **DNS Forwarding** также позволяет настроить условную пересылку запросов для определённых доменов (например, корпоративного домена) на другие DNS-серверы.
- **Разрешение локальных имён:** Функция *Static-Host* позволяет создавать локальные DNS-записи типа A, сопоставляя имена устройств с их IP-адресами (например, *nas.lan* с *192.168.1.10*).
- **Защита от DNS rebinding:** Функция защищает локальную сеть от атак DNS rebinding, блокируя ответы вышестоящих DNS-серверов, содержащие частные IP-адреса (RFC 1918). Можно настроить исключения для определённых доменов, а также разрешить ответы с адресами localhost, в том числе используемые DNS-блоклистами.

- **Привязка к интерфейсам:** Можно указать локальные *интерфейсы*, на которых DNS-сервер будет принимать запросы от клиентов.

СВОЙСТВА

dns-address (*DNS Server*)	Адрес DNS сервера для пересылки запросов
dns-forwarding (*DNS Forwarding*)	Доменная зона и её DNS сервер для разрешения IP адресов
interface (*Interface*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel	Интерфейс для обслуживания DNS запросов
static-host (*Static host*)	Статическая A-запись DNS
rebind-protection (*Rebind Protection*) **значения:** true, false	Защита от атаки DNS rebind (отбрасывание ответов с адресом из RFC1918)
rebind-localhost (*Rebind localhost*) **значения:** true, false	Разрешить ответы с адресом из диапазона 127.0.0.0/8 (DNS based blacklist) **условия:** rebind-protection = true
rebind-domain (*Rebind domain*)	Разрешить ответы с адресом из RFC1918 для доменного имени **условия:** rebind-protection = true

11.4. iperf

В данном разделе предоставляется доступ к утилите **iPerf** — инструменту для проведения нагрузочного тестирования и измерения производительности сети. С помощью iPerf можно проверить реальную пропускную способность и производительность сетевого соединения между двумя точками, генерируя управляемый поток трафика.

Сервис может работать в двух режимах:

- **Режим клиента (Client):** Роутер генерирует трафик и отправляет его на удаленный iPerf-сервер. Пользователь может настроить длительность теста, количество параллельных потоков данных, а также запустить тест в обратном режиме (когда роутер принимает данные, а не отправляет их).
- **Режим сервера (Server):** Роутер ожидает входящий трафик от удаленного iPerf-клиента на заданном порту, выступая в роли принимающей стороны для измерения пропускной способности.

КОМАНДЫ

client	Запустить клиентское приложение host - Адрес хоста (обязательно) time - Время (сек) работы stream - Число параллельно работающих процессов reverse - Запустить в обратном режиме (сервер отправляет, клиент принимает пакеты)
server	Запустить серверное приложение port - Порт приложения

11.5. l2tp server

Раздел предназначен для настройки встроенного L2TPv2-сервера роутера, который позволяет удалённым пользователям устанавливать L2TP-туннели для доступа к локальной сети. Основные

настройки включают IP-адрес сервера внутри туннеля (**IP Address**) и пул IP-адресов (**IP Pool**), из которого назначаются адреса подключающимся клиентам.

Основным параметром является метод шифрования (**Encryption**), который определяет способ защиты туннеля. Доступны следующие варианты:

- **IPsec (рекомендуется):** Использование L2TP поверх IPsec (**l2tp/ipsec**) обеспечивает шифрование передаваемых данных. Этот вариант доступен при установленном компоненте IPsec. При его выборе роутер автоматически создаёт необходимое IPsec-соединение и правила межсетевого экрана.



При использовании шифрования IPsec необходимо настроить предварительно согласованный ключ (PSK) для аутентификации туннеля. Без настройки параметров аутентификации IPsec туннель не сможет полноценно работать.

- **MPPE (Microsoft Point-to-Point Encryption):** Встроенный метод шифрования, использующий аутентификацию MS-CHAPv2. Подходит для клиентов, не поддерживающих IPsec.
- **None (без шифрования):** L2TP-туннель без шифрования. Использование этого варианта в публичных сетях настоятельно не рекомендуется.

Аутентификация пользователей выполняется централизованно. L2TP-сервер проверяет учётные данные клиентов по профилям пользователей, настроенным в разделе */service client*.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
ip-addr (*IP address*) **пример:** 192.168.1.1	IP адрес туннельного интерфейса
ip-pool (*IP pool*)	Диапазон IP адресов, назначаемых клиентам
auth (*Authentication*) **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption (*Encryption*) **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option (*Options*) **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug (*Debug*) **значения:** true, false	Режим подробного логгирования

11.6. link client

Раздел предназначен для настройки клиента, который подключает роутер к **Линк** — централизованной платформе для удалённого управления устройствами. Устанавливая защищённое постоянное соединение с сервером управления, клиент обеспечивает возможность удалённого мониторинга, управления конфигурацией и диагностики устройства через единую панель.

В разделе указывается адрес сервера (*Server*), к которому подключается роутер. Периодические сообщения *Keepalive* используются для информирования сервера о доступности устройства, а параметр *Force update* определяет интервал отправки полного отчёта о состоянии роутера.

Для защиты передаваемых данных используется указанный ключ шифрования (*Encryption Key*).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
server (*Server*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес управляющего Link сервера
update-interval (*Force update*)	Интервал (сек) между отправкой полного отчета на сервер удалённого управления
keep-alive-interval (*Keepalive*)	Интервал (сек) отправки keepalive сообщения информирующий о доступности устройства
key (*Encryption Key*)	Ключ для шифрования данных

11.7. ntp

Раздел предназначен для настройки службы протокола сетевого времени (Network Time Protocol, NTP), которая обеспечивает синхронизацию системного времени роутера. Точное время необходимо для корректного ведения журналов, аутентификации с использованием сертификатов и работы многих сетевых протоколов.

Роутер может выполнять две роли NTP:

- **NTP-клиент (синхронизация времени):** Роутер синхронизирует системное время с внешними NTP-серверами, указанными в списке *Pool*. Он периодически опрашивает эти серверы для поддержания точного времени.
- **NTP-сервер (источник времени для локальной сети):** При включении параметра *Server* роутер работает как NTP-сервер для локальной сети. Клиентские устройства могут использовать IP-адрес роутера в качестве источника времени. Это позволяет синхронизировать время устройств локальной сети и сократить NTP-трафик к внешним серверам.

В зависимости от модели роутера и его аппаратных возможностей также может быть доступна синхронизация времени по GPS или через сотовую сеть.

Мониторинг состояния синхронизации

Функция **Info** предоставляет подробную информацию о состоянии синхронизации NTP-клиента.

КОМАНДЫ

info	Информация о состоянии NTP клиента
get-modem-time	Показать время, которое модем получает от сотовой сети

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
pool (*Pool*)	Пул серверов для синхронизации

server (*Server*) **значения:** true, false	Разрешить обрабатывать NTP запросы клиентов
sync-with-gps (*Synchronize with GPS*) **значения:** true, false	Разрешить синхронизацию времени с GPS
sync-with-modem (*Synchronize with modem*) **значения:** true, false	Разрешить синхронизацию времени с сотовой сетью

11.8. openvpn server

Данный раздел позволяет настроить роутер в качестве надежного и гибко настраиваемого сервера OpenVPN.

Инфраструктура открытых ключей (PKI) и ключи

Безопасная работа основана на наборе сертификатов и ключей:

- **CA Certificate:** Файл *Ca* является корнем доверия для вашего VPN. Все клиентские и серверные сертификаты должны быть подписаны этим Центром Сертификации.
- **Сертификат сервера:** *Cert* — это публичный сертификат сервера, который он предъявляет клиентам для подтверждения своей подлинности.
- **Ключ TLS-аутентификации:** Ключ *Tls-Auth* обеспечивает дополнительный уровень HMAC-аутентификации для канала управления, повышая устойчивость сервера к DoS-атакам и сканированию портов. Вы можете создать новый ключ с помощью функции **Generate TA Key**. Этот ключ сохраняется в разделе *Storage* / *File* и должен быть передан всем клиентам.

Аутентификация пользователей

OpenVPN поддерживает два основных метода аутентификации клиентов:

1. **Аутентификация только по сертификату:** Доступ предоставляется исключительно на основании валидного клиентского сертификата, подписанного CA сервера. Имя пользователя и пароль не требуются.
2. **Аутентификация по сертификату и имени пользователя/паролю:** Обеспечивает двухфакторную аутентификацию. Доступ предоставляется, только если **одновременно** предъявлен валидный клиентский сертификат и введены верные имя пользователя и пароль. Логика проверки следующая:
    - Если имя пользователя не существует на роутере, доступ **запрещен**.
    - Если имя пользователя существует, но пароль не совпадает, доступ **запрещен**.
    - Если имя пользователя и пароль верны, доступ **разрешен**.

Для включения аутентификации по имени пользователя и паролю, нужно создать соответствующий профиль для этого пользователя в разделе *Service* / *Clients*, обязательно указав для него пароль.

КОМАНДЫ

generate-ta-key	Сгенерировать файл случайного ключа, используемый как TA Key или Static Key filename - Имя конфигурации (обязательно)

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
dev-type (*Dev type*) **значения:** tun, tap	Тип виртуального интерфейса
protocol (*Protocol*) **значения:** tcp, udp	Транспортный протокол туннеля
port (*Port*) **пример:** 80, !80	Порт для входящих подключений
tunnel-ip (*Tunnel IP*) **пример:** 10.10.10.1/24	Адрес туннельного интерфейса
pool (*Pool*) **пример:** 10.10.10.10-10.10.10.20	Пул IP адресов для выдачи клиентам
cipher (*Cipher*) **значения:** AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-192-GCM, AES-256-CBC, AES-256-GCM	Алгоритм шифрования туннеля
auth (*Auth*) **значения:** MD5, SHA1, SHA256, SHA384, SHA512	HMAC алгоритм для аутентификации
tls-mode (*TLS Mode*) **значения:** none, tls-auth, tls-crypt	Дополнительные опции при установлении TLS сессии
ta-key (*TA Key*) **значения:** /storage file	Ключ дополнительной HMAC аутентификации **условия:** tls-mode != none && tls-mode != ""
ca (*Ca*) **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA)
cert (*Cert*) **значения:** /storage certificate	Локальный сертификат (включая приватный ключ)
keepalive (*Keepalive*) **пример:** 10 60	Настроить ping клиентского соединения и перезапуск в случае недоступности
push (*Push to client*) **значения:** route-metric, route-delay, redirect-gateway, ip-win32, dhcp-option, inactive, ping, ping-exit, ping-restart, setenv, auth-token, persist-key, persist-tun, topology, echo, comp-lzo, socket-flags, sndbuf, rcvbuf	Отправить выбранные параметры в клиентскую конфигурацию
push-route (*Push route*)	Отправить маршруты в клиентскую конфигурацию
flag (*Flag*) **значения:** allow-recursive-routing, auth-nocache, client-to-client, comp-noadapt, disable, duplicate-cn, fast-io, float, mtu-test, multihome, ncp-disable, nobind, opt-verify, passtos, persist-key, persist-local-ip, persist-remote-ip, persist-tun, ping-timer-rem, pull, push-peer-info, push-reset, remote-random, route-nopull, single-session, suppress-timestamps, tcp-nodelay, tls-client, tls-exit, tls-server, username-as-common-name	Дополнительные опции туннеля

extra (*Extra parameters*) **значения:** auth-retry, bcast-buffers, comp-lzo, compress, connect-freq, connect-retry, connect-retry-max, connect-timeout, ecdh-curve, explicit-exit-notify, fragment, hand-window, hash-size, ifconfig-pool-netmask, ifconfig-push-local, ifconfig-push-netmask, inactive, key-direction, keysize, link-mtu, max-clients, mssfix, mtu-disc, ping, ping-exit, ping-restart, prng, pull-filter-accept, pull-filter-ignore, pull-filter-reject, rcvbuf, reneg-bytes, reneg-pkts, reneg-sec, replay-persist, replay-window, resolv-retry, shaper, sndbuf, tcp-queue-limit, tls-timeout, tls-version-min, tran-window, tun-mtu, tun-mtu-extra, txqueuelen, verb, verify-client-cert, verify-x509-name, x509-username-field	Дополнительные параметры туннеля

11.9. pinger

Раздел Pinger настраивает автоматическую службу, выполняющую две основные задачи: общий мониторинг соединений и динамическое управление отказоустойчивостью WAN-каналов.

В качестве инструмента мониторинга он может быть настроен на периодическую проверку доступности любого целевого хоста с помощью различных типов проверок (ICMP, TCP и т.д.). Это позволяет отслеживать состояние любого важного канала или сервиса.

Однако его основное автоматическое действие — это управление приоритетом маршрутизации для обеспечения отказоустойчивости.

Когда Pinger обнаруживает ухудшение качества такого маршрута — на основе заданных пользователем порогов — он увеличивает метрику маршрута, **снижая** его приоритет.

Автоматическое изменение метрики применяется **специально и исключительно к тем интерфейсам, которые настроены как «Маршрут по умолчанию»**.

Это действие понижает приоритет проблемного канала, в результате чего система маршрутизации автоматически отдает предпочтение альтернативному маршруту по умолчанию с лучшей (более низкой) метрикой.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
type (*Type*) **значения:** icmp, arping, http, tcp	Метод проверки доступности сетевого узла
host (*Host*)	Список адресов для проверки доступности сетевого узла **условия:** type = tcp
interval (*Interval*) **минимум:** 10	Интервал между проверками
retries (*Retries*) **минимум:** 1	Порог неудачных проверок до перезапуска интерфейса
count (*Request count*) **минимум:** 1	Число пакетов для проверки в рамках одной попытки **условия:** type = arping type = http type = icmp
size (*Packet size*) **минимум:** 1, **максимум:** 65535	Размер пакета **условия:** type != http
rtt-threshold (*RTT Threshold*)	Порог round-trip времени, превышение которого считается неудачей

loss-threshold (*Loss Threshold*)	Порог потерянных пакетов, превышение которого считается неудачей **условия:** type = icmp type = arping type = http

11.10. pptp server

Раздел предназначен для настройки встроенного PPTP-сервера (Point-to-Point Tunneling Protocol) роутера, который позволяет удалённым пользователям устанавливать VPN-туннели для доступа к локальной сети.

Основные настройки включают IP-адрес сервера внутри туннеля (*IP Address*) и пул IP-адресов (*IP Pool*), из которого назначаются адреса подключающимся клиентам.

Основным параметром является метод шифрования (**Encryption**), который определяет способ защиты туннеля. Доступны следующие варианты:

- **IPsec (рекомендуется для безопасности):** Трафик PPTP передаётся через зашифрованный IPsec-туннель. Этот вариант доступен при установленном компоненте IPsec. При его включении роутер автоматически создаёт необходимую конфигурацию:
- IPsec-соединение (*pptp_server_connection*) и ассоциацию (*pptp_server_association*).
- Соответствующее правило межсетевого экрана (*pptp_server_autogenerated*).

При использовании шифрования IPsec необходимо настроить предварительно согласованный ключ (PSK) для аутентификации туннеля. Без настройки параметров аутентификации IPsec туннель не сможет корректно работать.

- **MPPE (Microsoft Point-to-Point Encryption):** Встроенный метод шифрования, использующий аутентификацию MS-CHAPv2.
- **None (без шифрования):** Незашифрованный PPTP-туннель. Использование этого варианта в публичных сетях **настоятельно не рекомендуется**, поскольку он не обеспечивает конфиденциальность данных.

Аутентификация пользователей выполняется централизованно по профилям, настроенным в разделе */service client*.

При указании диапазонов адресов в полях *IP Address* и *IP Pool* необходимо учитывать их преобразование в специальный формат. Например:

• 1.1.1.2-1.1.1.10 → 1.1.1.2-10

• 1.1.2.10-1.1.5.10 → 1.1.2-5.10 (т.е. от 1.1.2.10 до 1.1.5.10)

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
ip-addr (*IP address*)	IP адрес туннельного интерфейса
ip-pool (*IP pool*)	Диапазон IP адресов, назначаемых клиентам
auth (*Authentication*) **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe

encryption (*Encryption*) **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option (*Options*) **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug (*Debug*) **значения:** true, false	Режим подробного логгирования

11.11. snmp

Раздел предназначен для настройки встроенного SNMP-агента (Simple Network Management Protocol), который позволяет централизованной системе управления сетью (NMS) отслеживать состояние роутера. Протокол SNMP предоставляет стандартизированный доступ к различным рабочим данным устройства, таким как загрузка ЦП, использование памяти, статистика интерфейсов и уровень сигнала сотовой связи.

Роутер поддерживает две основные версии протокола, каждая из которых обеспечивает различный уровень безопасности.

SNMPv2c

Это более простая и широко используемая версия, в которой для контроля доступа применяется строка сообщества (*Community*). Эта строка выполняет роль общего пароля между роутером и системой управления сетью.



Строка Community передаётся по сети в открытом виде. Поэтому SNMPv2c следует использовать только в доверенных, защищённых сетях.

SNMPv3

Эта версия предоставляет современную модель безопасности на основе пользователей (User-based Security Model, USM), поддерживающую аутентификацию пользователей и шифрование данных. Уровень безопасности гибко настраивается.

Разрешение на запись

Параметр *Writable*, доступный для обеих версий, позволяет системе управления сетью не только считывать данные (GET-запросы), но и изменять состояние роутера (SET-запросы), например управлять состоянием GPIO. Включать этот параметр следует с особой осторожностью и только при необходимости.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
version (*Protocol version*) **значения:** v2c, v3	Версия протокола
port (*Service port*) **пример:** 80, !80	Порт для обслуживания входящих запросов

community (*Community*) **пример:** bridge0, vpn-client1, user_1@example.com	Community, критерий для аутентификации входящих запросов
sys-name (*Name*) **пример:** bridge0, vpn, client_1	Имя устройства для идентификации в системе мониторинга
sys-contact (*Contact*)	Контактные данные устройства для идентификации в системе мониторинга
sys-location (*Location*)	Локация устройства для идентификации в системе мониторинга
sys-description (*Description*)	Описание устройства для идентификации в системе мониторинга
username (*Username*)	Имя пользователя **условия:** version = v3
auth-passphrase (*Auth passphrase*) **мин. длина:** 8	Парольная фраза (SHA) для аутентификации **условия:** version = v3
priv-passphrase (*Priv passphrase*) **мин. длина:** 8	Парольная фраза (SHA) для шифрования трафика **условия:** version = v3
security-level (*Security level*) **значения:** noauth, auth, priv	Уровень защиты данных при опросе **условия:** version = v3
writable (*Writable*) **значения:** true, false	Разрешить вносить изменения и управлять роутером

11.12. udp broadcast relay

Данный раздел предназначен для настройки службы **UDP Broadcast Relay**, которая обеспечивает ретрансляцию широковещательных UDP-пакетов между различными сетевыми интерфейсами. Этот функционал необходим для протоколов, работающих на основе широковещательных запросов (например, для обнаружения сервисов или поиска устройств), которые по своей природе не выходят за пределы одной подсети.

Настройка позволяет объединять в группы сетевые интерфейсы, между которыми должен передаваться широковещательный трафик. Для предотвращения циклических передач и возникновения петель каждому экземпляру ретранслятора назначается уникальный идентификатор, обеспечивающий корректную обработку трафика в выбранном сегменте.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
interface (*Interface*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel	Интерфейсы участвующие в ретрансляции широковещательных пакетов
id (*ID*) **минимум:** 0, **максимум:** 99	ID экземпляра для предотвращения петель ретрансляции
debug (*Debug*) **значения:** true, false	Включение и отключение режима увеличеснного логирования

11.13. vrrp

Раздел предназначен для настройки протокола VRRP (Virtual Router Redundancy Protocol), который обеспечивает высокую доступность шлюза по умолчанию, позволяя нескольким роутерам использовать общий виртуальный IP-адрес.

В irzOS VRRP настраивается на выбранном сетевом интерфейсе. Параметр *Virtual IP* определяет адрес, который устройства локальной сети используют в качестве шлюза по умолчанию, а *Virtual ID* задаёт идентификатор группы виртуального маршрутизатора. Роутеры, входящие в одну группу, работают как единый виртуальный маршрутизатор.

В группе один роутер выполняет роль **Master (основной)** и обрабатывает трафик, а остальные работают как **Backup (резервные)**. Параметр *Priority* определяет приоритет выбора основного роутера: чем выше значение, тем выше приоритет. При отказе основного роутера его роль автоматически принимает доступный резервный роутер с наивысшим приоритетом.

Параметр *Preemption* позволяет роутеру с более высоким приоритетом перехватывать роль Master при возвращении в сеть. Дополнительные настройки позволяют назначить виртуальный MAC-адрес, задать интервал отправки объявлений VRRP и настроить аутентификацию сообщений протокола.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
virtual-ip (*Virtual IP*)	Виртуальный IP адрес выступающий шлюзом по умолчанию для сети
virtual-mac (*Virtual MAC*) **значения:** true, false	Назначить виртуальный MAC адрес интерфейсу
preemption-mode (*Preemption*) **значения:** true, false	Разрешить перехват роли master если приоритет маршрутизатора выше
virtual-id (*Virtual ID*) **минимум:** 1, **максимум:** 255	Идентификатор виртуального маршрутизатора
priority (*Priority*) **минимум:** 1, **максимум:** 255	Приоритет VRRP маршрутизатора
delay (*Delay*) **минимум:** 1, **максимум:** 3600	Интервал (сек) между отправкой VRRP-advertise сообщений
auth (*Authentication type*) **значения:** none, pw, ah	Тип аутентификации для протокола
key (*Key*) **мин. длина:** 1, **макс. длина:** 8	Парольная фраза для аутентификации пакетов VRRP **условия:** auth = ah auth = pw

11.14. zabbix

Данный раздел предназначен для настройки встроенного Zabbix-агента, который позволяет осуществлять мониторинг состояния и производительности роутера с помощью Zabbix-сервера. Агент может работать в двух режимах, которые могут использоваться одновременно.

Режимы работы

- **Пассивные проверки:** В этом режиме Zabbix-сервер сам подключается к агенту на роутере для запроса данных. Необходимо указать IP-адрес *Сервера*, с которого разрешены входящие соединения. Этот режим требует, чтобы порт агента (по умолчанию 10050) был доступен для Zabbix-сервера.
- **Активные проверки:** В этом режиме агент сам инициирует соединение с Zabbix-сервером для отправки данных. Этот режим часто предпочтительнее для устройств, находящихся за межсетевым экраном или NAT. Необходимо указать адрес *Server Active*, чтобы агент знал, куда отправлять данные.

Настройка безопасности (TLS)

Вы можете защитить обмен данными между агентом и сервером с помощью шифрования TLS. Способ защиты соединения настраивается независимо для пассивных (*TLSAccept*) и активных (*TLSConnect*) режимов:

- **psk:** Шифрование с использованием общего ключа (Pre-Shared Key) и идентификатора.
- **cert:** Шифрование с использованием SSL-сертификатов для аутентификации.
- **unencrypted:** Обмен данными происходит в открытом виде (не рекомендуется для публичных сетей).

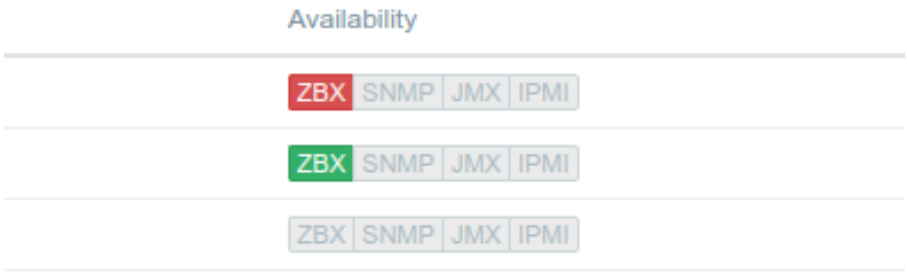
Настройка Zabbix-сервера

Для упрощения интеграции вы можете скачать готовый шаблон для Zabbix-сервера из Базы знаний.

Предоставляемый шаблон предназначен **только для настройки активных проверок** (Zabbix agent active).

Для работы в пассивном режиме необходимо настроить все элементы данных и триггеры на Zabbix-сервере вручную.

Индикатор доступности агента на сервере (значок ZBX в столбце «Доступность») отображает состояние **пассивных проверок**:



- **Горит зеленым:** Пассивные проверки проходят успешно.
- **Горит красным:** Есть проблема с пассивными проверками (например, таймаут, сетевая недоступность).
- **Не подсвечен (серый):** Для узла сети не настроены пассивные проверки (например, если используется шаблон только с активными проверками).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
hostname (*Hostname*)	Уникальное имя устройства для идентификации на сервере
port (*Port*) **минимум:** 1024, **максимум:** 32767	Порт для приёма пассивных проверок с сервера
server (*Server*)	Адрес сервера, с которого принимаются входящие подключения
server-active (*Server active*)	Адрес сервера для отправки результатов активных проверок
buffer-send (*Buffer Send*) **минимум:** 1, **максимум:** 3600	Время (сек), через которое пытаться отправить данные на сервер **условия:** server-active != ""
buffer-size (*Buffer Size*) **минимум:** 2, **максимум:** 65535	Размер буфера (байт), используемого для накопления данных перед отправкой на сервер **условия:** server-active != ""
tls-accept (*TLSAccept*) **значения:** unencrypted, psk, cert	Тип шифрования для приема входящих подключений
tls-connect (*TLSConnect*) **значения:** unencrypted, psk, cert	Тип шифрования для исходящих соединений
ca (*CA certificate*) **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA) **условия:** tls-connect = cert tls-accept = cert
cert (*Certificate*) **значения:** /storage certificate	Сертификат для аутентификации и шифрования **условия:** tls-connect = cert tls-accept = cert
psk (*Pre-shared Key*) **мин. длина:** 32, **макс. длина:** 128 **пример:** 001d6bbe06dc9ad18824a4a78b699805, e560cb0d918d26d31b4f642181f5f570ad89a390931102e5391d08327b1a484e9	Pre-shared Key для шифрования подключений **условия:** tls-connect = psk tls-accept = psk
identity (*PSK identity*)	PSK identity string **условия:** tls-connect = psk tls-accept = psk

12. storage

Данный раздел предназначен для управления локальным хранилищем данных, сертификатами и системными файлами. Здесь обеспечивается централизованный доступ к загруженным файлам конфигурации, скриптам и криптографическим ресурсам, необходимым для обеспечения безопасности системы и удаленного управления устройствами.

12.1. certificate

Данный раздел предназначен для управления сертификатами TLS и закрытыми ключами. Они необходимы для обеспечения безопасности сервисов, работающих на роутере, таких как веб-интерфейс (HTTPS), OpenVPN, IPsec и других.

Создание и получение сертификатов

Вы можете получить сертификаты для роутера несколькими способами:

- **CSR create (запрос на подпись сертификата):** Стандартный способ получения сертификата от доверенного публичного удостоверяющего центра (CA). Вы создаёте CSR, отправляете его в CA и получаете подписанный сертификат, который затем можно импортировать.
- **Cert Create:** Позволяет создавать сертификаты X.509. Можно создать **самоподписанный сертификат** для внутренних сетей, тестирования или случаев, когда не требуется сертификат, которому доверяют публичные удостоверяющие центры. Также можно подписать новый сертификат с помощью существующего сертификата CA.
- **CSR sign:** Позволяет подписать CSR другого устройства (например, другого роутера или клиента) с помощью сертификата CA, хранящегося на роутере.
- **Cert Import:** Позволяет импортировать существующие сертификаты и закрытые ключи, созданные вне роутера.

Управление и использование сертификатов

После добавления сертификата в хранилище им можно управлять:

- **Cert Export:** Позволяет создавать резервные копии сертификатов и ключей или передавать сертификаты клиентам. Экспорт поддерживается в форматах PKCS#12 и PEM. В зависимости от выбранных параметров экспортируемый файл может включать сертификат, его закрытый ключ и дополнительные сертификаты. Формат PKCS#12 поддерживает защиту паролем.

КОМАНДЫ

cert-create	Создать сертификат name - Имя нового файла (обязательно) ca - Сертификат удостоверяющего цетра (CA) authority - Сертификат может быть использован для подписания pkey-size - Размер приватного ключа cn - Имя субъекта (обязательно) alt-name - Альтернативное имя субъекта org - Имя организации субъекта unit - Юнит организации субъекта state - Область субъекта country - Страна субъекта location - Местоположение субъекта days - Срок действия сертификата
csr-create	Создать CSR файл name - Имя нового файла CSR (обязательно) pkey-size - Размер публичного ключа passphrase - Парольная фраза для файла сертификата cn - Имя субъекта (обязательно) alt-name - Альтернативное имя субъекта org - Имя организации субъекта unit - Юнит организации субъекта state - Область субъекта country - Страна субъекта location - Местоположение субъекта
csr-sign	Подписать CSR name - CSR файл для подписания (обязательно) ca - Сертификат удостоверяющего цетра (CA) (обязательно) alt-name - Альтернативное имя субъекта days - Срок действия подписанного сертификата passphrase - Парольная фраза для файла сертификата
cert-export	Экспорт сертификата в формате PKCS12 или PEM name - Файл сертификата для экспорта (обязательно) include-pkey - Вложить приватный ключ в экспортируемый файл passphrase - Парольная фраза для файла сертификата additional-cert - Добавить дополнительный сертификат в связку pem - Экспортировать сертификат в формате PEM вместо PKCS#12
cert-import	Импорт сертификата name - Файл сертификата для импорта (обязательно) passphrase - Парольная фраза для файла сертификата

rename	Изменить имя файла сертификата new-name - Имя нового файла (обязательно)
reissue	Перевыпустить сертификат с новыми назначениями ключа key-usage - Определить назначение сертификата (обязательно) eku - Расширенное использование ключа (Extended Key Usage)

СВОЙСТВА

issuer (*Issuer*)	Наименование центра сертификации, выдавшего сертификат
subject (*Subject*)	Наименование субъекта
authority (*CA flag*) **значения:** true, false	Сертификат может быть использован для подписания
alt-name (*Alt name*)	Альтернативное Наименование субъекта **условия:** alt-name != ""
not-before (*Not before*)	Дата, до которой сертификат не действителен
not-after (*Not after*)	Дата, после которой сертификат не действителен
fingerprint (*Fingerprint*)	Хэш сертификата
key-usage (*Key Usage*) **значения:** digital-signature, key-encipherment, key-agreement, key-cert-sign, crl-sign, encipher-only, decipher-only, data-encipherment, non-repudiation	Определить назначение сертификата
eku (*Extended Key Usage*) **значения:** server-auth, client-auth, ocsp-signing, time-stamping	Расширенное использование ключа (Extended Key Usage)

12.2. file

Данный раздел представляет собой интерфейс для управления файлами, хранящимися на роутере. Он служит основным инструментом для загрузки, скачивания и организации файлов, необходимых для различных системных операций, таких как резервные копии конфигурации, образы прошивок или пользовательские скрипты.

Файловый менеджер различает два основных места хранения:

- **Временное хранилище:** Файлы находятся в энергозависимой памяти (ОЗУ) и будут удалены при перезагрузке системы. Обычно используется как промежуточная область для файлов перед их установкой или импортом определённым сервисом.
- **Постоянное хранилище:** Файлы записываются в энергонезависимую флеш-память роутера и сохраняются после перезагрузки.

С помощью этого интерфейса можно загружать файлы во временное хранилище, скачивать существующие файлы, импортировать их из временного хранилища в постоянное или удалять.

КОМАНДЫ

upload	Загрузить файл
download	Загрузить файл с устройства
import	Импорт файла на устройство

СВОЙСТВА

file-type (*File type*)	Тип файла

file-size (*File size*)	Размер файла
last-change (*Last change*)	Время последнего изменения файла
last-access (*Last access*)	Время последнего открытия файла

13. system

Данный раздел предназначен для базового обслуживания, администрирования и настройки параметров системы. Здесь собраны инструменты управления доступом, устройствами памяти, системными журналами и программным обеспечением.

13.1. access

Данный подраздел предназначен для настройки механизмов аутентификации и авторизации при управлении роутером. Здесь осуществляется централизованный контроль доступа пользователей к устройству, включая поддержку как локальных, так и сетевых протоколов безопасности.

13.1.1. radius

В данном разделе выполняется настройка централизованной аутентификации и авторизации пользователей по протоколу **Remote Authentication Dial-In User Service (RADIUS)**.

При использовании данной схемы роутер выступает в роли **сервера сетевого доступа (Network Access Server, NAS)**. При попытке входа в систему устройство передает учетные данные пользователя на выделенный RADIUS-сервер для проверки подлинности. Для взаимодействия требуется уникальный идентификатор роутера и корректный секретный ключ для авторизации на стороне сервера.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Отключить Radius аутентификацию
server (*Server*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Сервер аутентификации
nas-id (*NAS Id*) **макс. длина:** 32 **пример:** bridge0, vpn-client1, user_1@example.com	Уникальный идентификатор NAS
secret (*Secret*)	Пароль для аутентификации NAS на RADIUS сервере

13.1.2. ssh

Данный раздел предназначен для настройки встроенного SSH-сервера роутера, который предоставляет безопасный, зашифрованный доступ к командной строке для расширенного администрирования, настройки и диагностики.

Помимо включения или отключения службы и изменения прослушиваемого порта, в разделе можно настроить криптографические алгоритмы, используемыми SSH-сервером. Это позволяет администраторам усилить профиль безопасности устройства, отключая более слабые алгоритмы и обеспечивая соответствие определенным корпоративным или нормативным политикам безопасности.

Можно настроить следующие криптографические компоненты:

- **Cipher:** Определяет алгоритмы симметричного шифрования для обеспечения конфиденциальности данных.
- **Host Key Algorithms:** Определяет алгоритмы открытого ключа, которые сервер может использовать для подтверждения своей подлинности.
- **KEX Algorithms:** Управляет методами, используемыми для безопасной генерации и обмена сеансовыми ключами.
- **MAC Algorithms:** Указывает алгоритмы хеширования, используемые для обеспечения целостности и подлинности сообщений.



Изменение этих криптографических настроек предназначено для опытных пользователей. Некорректная конфигурация может привести к невозможности подключиться к роутеру по SSH. Изменяйте эти параметры только в том случае, если это требуется для соответствия определенной политике безопасности.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
port (*Port*) **пример:** 22, 51820	Порт SSH подключения
cipher (*Cipher*) **значения:** chacha20-poly1305@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com	Выбор определённого алгоритма шифрования
host-key-alg (*Host Key Algorithms*) **значения:** rsa-sha2-512, rsa-sha2-256, ssh-rsa, ssh-ed25519	Выбор определённого алгоритма аутентификации
kex-alg (*KEX Algorithms*) **значения:** curve25519-sha256, curve25519-sha256@libssh.org, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, diffie-hellman-group-exchange-sha256, diffie-hellman-group16-sha512, diffie-hellman-group18-sha512, diffie-hellman-group14-sha256	Выбор определённого алгоритма обмена ключами
mac-alg (*MAC Algorithms*) **значения:** umac-64-etm@openssh.com, umac-128-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha1-etm@openssh.com, umac-64@openssh.com, umac-128@openssh.com, hmac-sha2-256, hmac-sha2-512, hmac-sha1	Выбор определённого алгоритма проверки целостности

13.1.3. web

Данный раздел предназначен для настройки доступа к веб-интерфейсу управления роутером. Он позволяет управлять протоколами (HTTP/HTTPS) и портами, используемыми для административного доступа.

Основной настройкой является включение безопасного доступа по **HTTPS** с помощью функции *Use HTTPS*. Это шифрует все взаимодействие между вашим браузером и роутером, защищая ваши учетные данные и данные конфигурации от перехвата. Хотя доступ по стандартному **HTTP** возможен, он не является зашифрованным и должен использоваться только в полностью доверенных сетях.

Для включения HTTPS необходимо выбрать *Файл сертификата* (публичный сертификат сервера) и *Файл ключа* (соответствующий ему закрытый ключ) из хранилища сертификатов. Использование собственного, доверенного сертификата устраняет предупреждения безопасности в браузере и обеспечивает защищенный административный сеанс.

Для дополнительного усиления безопасности вы можете:

- Изменить прослушиваемый *Порт* со значения по умолчанию на нестандартный.
- Указать минимальную версию протокола TLS (*TLS Minimum*), чтобы обеспечить использование современных, безопасных криптографических стандартов.

СВОЙСТВА

use-http (*Use HTTP*) **значения:** true, false	Разрешить доступ по HTTP
http-port (*HTTP Port*) **пример:** 80, !80	Порт для обработки входящих HTTP запросов **условия:** use-http = true
use-https (*Use HTTPS*) **значения:** true, false	Разрешить доступ по HTTPS
https-port (*HTTPS Port*) **пример:** 80, !80	Порт для обработки входящих HTTPS запросов **условия:** use-https = true
cert (*Certificate*) **значения:** /storage certificate	Сертификат для аутентификации и шифрования **условия:** use-https = true
tls (*Min TLS-version*) **значения:** 1.1, 1.2, 1.3	Минимальная разрешенная версия TLS **условия:** use-https = true
redirect-to-https (*Redirect to HTTPS*) **значения:** true, false	Перенаправлять входящие HTTP запросы на HTTPS порт **условия:** use-https = true && use-http = true

13.2. block dev

Данный раздел предоставляет возможность управления доступными блочными устройствами хранения и служит интерфейсом настройки **файловой системы overlay**.

С помощью функции *Overlay_dev* можно выбрать какой носитель использовать основным. Это позволяет эффективно расширить память роутера для установки дополнительных программных пакетов и хранения крупных файлов конфигурации.



Внимательно ознакомьтесь со следующими пунктами перед началом работы:

• **Форматирование и потеря данных:** При выборе внешнего накопителя для использования в качестве основного он **будет отформатирован**, что приведет к потере всей имеющейся на нем информации.

• **Потеря пакетов при возврате:** При переключении с внешнего носителя обратно на внутреннюю память все пакеты, установленные на внешний накопитель, будут утеряны.

• **Перезагрузка при извлечении:** Физическое извлечение внешнего накопителя, когда он используется в качестве основного, приведет к немедленной перезагрузке устройства.

Для SD-карт поддерживаются следующие файловые системы: FAT32, EXT2, EXT3, EXT4, F2FS, JFFS2 и NTFS.

Файловые системы exFAT и BFS не поддерживаются. Перед использованием SD-карты в роутере рекомендуется убедиться, что она отформатирована в одну из поддерживаемых файловых систем.



Для работы будет использоваться **только первый раздел** выбранного накопителя. Объем этого раздела должен быть достаточным для предполагаемого использования (например, для установки пакетов или хранения данных).

КОМАНДЫ

overlay_dev	Выбрать устройство для монтирования как overlay device - Имя устройства (обязательно)

13.3. config

Этот раздел предоставляет инструменты для управления конфигурацией роутера. Система использует двухэтапную модель конфигурации: изменения сначала вносятся во временную, «кандидатскую» конфигурацию и должны быть явно зафиксированы (*commit*), прежде чем они станут частью постоянной, «текущей» (running) конфигурации.

Конфигурационный файл содержит в себе основной набор параметров для работы роутера. В частности элементами конфигурации роутера могут быть: пароли, ключи, хэши и сертификаты для работы различных служб.



Импорт конфигурации от несовместимой версии прошивки или другой модели устройства может привести к нестабильной работе или сделать устройство недоступным после фиксации изменений.

КОМАНДЫ

revert	Откатить все изменения
commit	Сохранить текущую запущенную конфигурацию
export	Экспорт текущей запущенной конфигурации include-files - Включить импортированные в /storage/file файлы в экспортируемую конфигурацию
import	Импорт файла конфигурации file - Файл конфигурации для импорта (обязательно)
default	Вернуть настройки по умолчанию reset-storage - Очистить все разделы /storage file - Файл для импорта после сброса настроек

13.4. logging

Данный раздел настраивает работу службы системного журнала, которая регистрирует все значимые операционные события: от входа пользователей и изменения настроек до ошибок и системных предупреждений. Эта страница позволяет вам управлять местом назначения и способом хранения этих важных сообщений.

Ведение журнала может осуществляться в двух основных направлениях:

- **На удаленный Syslog-сервер:** Эта функция позволяет в реальном времени отправлять сообщения журнала на удаленный сервер. Вы можете указать адрес сервера и транспортный протокол (например, UDP или TCP). Опция *Prefix* позволяет легко идентифицировать сообщения от данного устройства на центральном сервере.
- **В локальный файл:** В качестве альтернативы вы можете включить опцию *Log to file*, чтобы хранить журналы локально на роутере. Это полезно для диагностики и устранения неисправностей на самом устройстве, особенно когда удаленный сервер недоступен.



Размер файла журнала, отображаемый в разделе */storage/file*, может иметь нулевое значение, даже если ведение журнала в файл активно. Это связано с тем, что значение не обновляется в реальном времени. Для принудительного обновления и отображения актуального размера необходимо нажать непосредственно на **file** в пути к разделу.

СВОЙСТВА

remote-host (*Remote*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Удалённая сторона для приёма лога
remote-proto (*Transport*) **значения:** tcp, udp	Транспортный протокол для отправки лога
remote-prefix (*Prefix*)	Префикс для записей, отправляемых на удалённый сервер
file-log (*Log to file*) **значения:** true, false	Записывать лог в файл
file-name (*File*)	Имя файла для записи лога **условия:** file-log = true
file-size (*File size*) **минимум:** 1, **максимум:** 8192	Не превышать указанный размер (Кбайт) файла **условия:** file-log = true

13.5. management

Этот раздел является основным местом для настройки базовых системных параметров и выполнения важных операций по обслуживанию.

Он позволяет определить идентификационные параметры роутера (такие как имя хоста и часовой пояс) и выполнять общесистемные команды. Отсюда можно перезагрузить устройство, обновить прошивку, выполнить сброс к заводским настройкам или сгенерировать диагностический отчет для устранения неисправностей.

КОМАНДЫ

change	Изменить локальное время и дату на устройстве isotime - Изменить локальное время на устройстве isodate - Изменить локальную дату устройстве
report	Получить отчёт об ошибках устройства
reboot	Перезагрузить устройство
upgrade	Обновить встроенное ПО file - Файл во временной памяти (обязательно) reset-config - Вернуть настройки по умолчанию reset-storage - Очистить все разделы /storage

СВОЙСТВА

hostname (*Hostname*) **пример:** localhost, example.com, sample.example.com	Hostname устройства
timezone (*Time zone*) **значения:** UTC-12, UTC-11, UTC-10, UTC-9, UTC-8, UTC-7, UTC-6, UTC-5, UTC-4, UTC-3, UTC-2, UTC-1, UTC, UTC+1, UTC+2, UTC+3, UTC+4, UTC+5, UTC+6, UTC+7, UTC+8, UTC+9, UTC+10, UTC+11, UTC+12, UTC+13, UTC+14	Часовой пояс устройства

13.6. package

Данный раздел предоставляет интерфейс для управления программными пакетами, установленными на роутер. Он позволяет расширять функциональность устройства путем установки новых приложений или библиотек.

На странице отображается список всех установленных пакетов, а также информация о них, такая как *версия*, *зависимости*, *размер* и краткое *описание*.

Управление пакетами

- **Установка пакета:** *Install* позволяет выбрать файл пакета (например, в формате *.ipk*), который был предварительно загружен во временное хранилище роутера.
- **Удаление пакета:** *Clean* используется для удаления (деинсталляции) выбранного пакета из системы.

КОМАНДЫ

install	Установить пакет file - Файл во временной памяти (обязательно)

СВОЙСТВА

version (*Version*)	Версия установленного пакета
depends (*Depends*)	Зависимости пакета
size (*Size*)	Количество место занимаемого установленными файлами
description (*Description*)	Описание пакета, предоставленное разработчиком

14. tools

Данный раздел предоставляет набор утилит для диагностики сети и устранения неполадок, которые запускаются по требованию. В отличие от разделов конфигурации, эти инструменты выполняют разовые операции для анализа и устранения проблем в реальном времени.

Доступные утилиты позволяют выполнять различные диагностические задачи, такие как проверка доступности сети на разных уровнях, анализ сетевого трафика, установление клиентских соединений с удалёнными узлами, просмотр системных журналов и загрузка файлов из удалённых ресурсов на роутер.

Некоторые утилиты доступны только через интерфейс командной строки (CLI).

КОМАНДЫ

download	Загрузить файл на устройство url - Адрес ресурса (обязательно) to-file - Сохранить файл с этим именем username - Имя пользователя для аутентификации password - Пароль для аутентификации save - Сохранить файл в хранилище
ping	Ping удалённого узла host - Адрес хоста (обязательно) interface - Интерфейс count - Число отправляемых пакетов size - Размер пакета
sniffer	Сетевой анализатор пакетов interface - Интерфейс для захвата пакетов (обязательно) proto - Фильтр по протоколу src-addr - Фильтр по IP адресу источника пакета dst-addr - Фильтр по IP адресу назначения пакета src-port - Фильтр по порту источника пакета dst-port - Фильтр по порту назначения пакета src-mac - Фильтр по MAC адресу источника пакета dst-mac - Фильтр по MAC адресу назначения пакета append - Логический оператор связывания для фильтров count - Число отправляемых пакетов file - Сохранить дамп пакетов в файл
arping	ARP Ping удалённого узла host - Адрес хоста (обязательно) interface - Интерфейс (обязательно) count - Число отправляемых пакетов
traceroute	traceroute к удалённому узлу host - Адрес хоста (обязательно) max_hops - Предельное количество прыжков до узла protocol - Использовать ICMP Echo пакеты вместо UDP датаграм port - Порт приложения
resolve	Выполнить DNS запрос для удаленного хоста host - Адрес хоста (обязательно) dns-server - IP адрес
blink	Мигаем индикатором питания duration - Время (сек) мигания светодиода
telnet	Telnet подключение к удалённому узлу host - Адрес хоста (обязательно) interface - Интерфейс port - Порт приложения
journal	Открыть системный журнал filter - Регулярное выражение для фильтрации вывода last - Показать последние N-строк
dashboard	Сводная информация о системе
ssh	SSH подключение к удалённому узлу host - Адрес хоста (обязательно) username - Имя пользователя (обязательно) port - Порт приложения

15. tunnel

Раздел предназначен для настройки всех необходимых типов туннелей.

В информационном блоке для настроенных туннелей **EoIP**, **GRE**, **L2TP-v2**, **L2TP-v3**, **NHRP**, **PPTP**, **VXLAN**, отображается его текущее состояние в строке status. Это значение является краткой сводкой состояния объекта, которое также может отображаться в виде двухбуквенного кода в колонке STATE (Состояние объекта) в таблице туннелей.

Возможные значения представлены в таблице ниже.

Статус объекта/STATE	Статус туннеля/state	Значение
S	down	Соединение было установлено, но затем разорвано.
S	pending	Туннель находится в процессе установки соединения.
S	no carrier	Отсутствует соединение с удаленной стороной туннеля.
RS	running	Туннель успешно установлен и работает в штатном режиме.
XS	disabled	Туннель был отключен вручную.
ES	error	При работе туннеля возникла ошибка конфигурации или функционирования.

15.1. eoip

Данный раздел предназначен для настройки туннелей Ethernet over IP (EoIP), позволяющих расширять сети второго уровня между удалёнными точками через IP-сеть.

Туннель EoIP инкапсулирует полные Ethernet-кадры в пакеты GRE (Generic Routing Encapsulation), создавая виртуальное Ethernet-соединение «точка-точка» между двумя роутерами. При добавлении туннельного интерфейса в мост на каждом роутере два отдельных сегмента LAN могут быть объединены в единый широковещательный домен, работая так, как если бы они были соединены физическим Ethernet-кабелем.

Настройка включает указание удалённого узла (*Remote IP*) в виде IP-адреса или FQDN и идентификатора туннеля (*Tunnel ID*), который должен совпадать на обоих концах соединения. Также можно выбрать локальный адрес или исходящий интерфейс с помощью параметра *Local IP* и настроить дополнительные параметры, такие как MTU и TTL.

Протокол EoIP, изначально разработанный компанией MikroTik, самостоятельно не шифрует передаваемый трафик. Если установлен компонент IPsec, параметр *Encryption* позволяет включить защиту IPsec с использованием предварительно согласованного ключа (PSK). EoIP также может работать поверх существующего VPN-туннеля на базе IP, например OpenVPN, при наличии сетевой связности между конечными точками туннеля.

При использовании IPsec для защиты EoIP-туннеля по умолчанию применяется протокол обмена ключами IKEv1 для обеспечения совместимости с типовыми настройками EoIP/IPsec на оборудовании MikroTik.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса

tunnel-id (*Tunnel ID*) **минимум:** 1, **максимум:** 65535	ID туннеля
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
mtu (*MTU*) **минимум:** 70, **максимум:** 65535	MTU интерфейса
ttl (*TTL*) **минимум:** 1, **максимум:** 255	TTL интерфейса
dscp (*DSCP*)	DSCP метка, присваемая GRE трафику
encryption (*Encryption*) **значения:** none	Метод защиты туннеля
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec

15.2. gre

Данный раздел предназначен для настройки туннелей GRE (Generic Routing Encapsulation) — универсального протокола для инкапсуляции различных протоколов сетевого уровня в IP-туннели типа «точка-точка».

Основное преимущество GRE заключается в возможности передавать трафик, который не может напрямую маршрутизироваться через стандартную IP-сеть, например трафик не-IP-протоколов или многоадресной рассылки (multicast). GRE также часто используется для создания оверлейных сетей, например для передачи IPv6-трафика через сеть, работающую только на IPv4 (и наоборот).

Раздел позволяет настроить адреса конечных точек туннеля (*Local IP* и *Remote IP*), IP-адрес туннельного интерфейса (*Tunnel IP*) и необязательный параметр *Key*, который используется для идентификации конкретного туннеля при наличии нескольких GRE-соединений с одним удалённым узлом.

Дополнительные настройки включают MTU, TTL, DSCP и флаг DF для управления обработкой пакетов. Встроенный механизм Keepalive, настраиваемый с помощью параметров *Keepalive Delay* и *Keepalive Retries*, отслеживает доступность удалённого узла и переводит туннель в состояние DOWN при достижении заданного количества неудачных проверок.

Сам по себе GRE не обеспечивает шифрование. Если установлен компонент IPsec, параметр *Encryption* позволяет включить защиту IPsec с использованием предварительно согласованного ключа (PSK).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)

tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
key (*Key*) **минимум:** 0, **максимум:** 4294967295	GRE key туннеля
encryption (*Encryption*) **значения:** none	Метод защиты туннеля
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
mtu (*MTU*) **минимум:** 70, **максимум:** 65535	MTU туннельного интерфейса
ttl (*TTL*) **минимум:** 1, **максимум:** 255	TTL туннельного интерфейса
dscp (*DSCP*)	DSCP метка, присваемая GRE трафику
do-not-frag (*DF Flag*) **значения:** true, false	Установить флаг запрета фрагментации пакета
keepalive-delay (*Keepalive Delay*) **минимум:** 0, **максимум:** 4294967	Интервал отправки keepalive пакета в отсутствии трафика в туннеле
keepalive-retries (*Keepalive Retries*) **минимум:** 0, **максимум:** 4294967295	Число попыток до перехода в состояние DOWN **условия:** keepalive-delay != "" && keepalive-delay != 0

15.3. ipsec

Данный подраздел предназначен для настройки протоколов **IPsec (Internet Protocol Security)**, обеспечивающих аутентификацию и шифрование данных между сетевыми узлами. IPsec гарантирует конфиденциальность, целостность и проверку источника трафика при передаче через небезопасные IP-сети.

15.3.1. association

Данный раздел предназначен для настройки основных политик безопасности IPsec. Эти политики связаны с ассоциациями безопасности (SA), которые в терминологии IKEv2 называются Child SA. Они определяют, какой сетевой трафик соответствует политике, как он обрабатывается и между какими узлами.

Основная функция раздела — настройка локальных и удалённых селекторов трафика (*Local TS* и *Remote TS*). Селекторы определяют трафик, на который распространяется действие политики IPsec. Указывая IP-адреса или подсети, протоколы и порты, можно создавать правила, соответствующие требованиям безопасности сети.

Каждая политика связана с определённым *Connection*, который задаёт параметры соединения между узлами, и может использовать *Proposal*, определяющий алгоритмы шифрования и контроля целостности ESP для второй фазы согласования защищённого соединения. Такой подход обеспечивает модульность и масштабируемость конфигурации.



Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, позволяя добавлять или изменять политики без разрыва существующих активных ассоциаций безопасности. Для принудительного завершения конкретной SA перейдите в раздел */tunnel ipsec status*.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
connection (*Connection*)	IKE соединение для согласования SA
proposal (*Proposal*) **значения:** /tunnel ipsec proposal	Алгоритм шифрования и аутентификации ESP
auto (*Startup action*) **значения:** route, start	Действие после применения конфигурации SA
type (*SA type*) **значения:** tunnel, transport, passthrough, drop	Согласование режима работы SA
leftsubnet (*Local TS*)	Источники трафика для согласования с локальной стороны
rightsubnet (*Remote TS*)	Источники трафика для согласования с удалённой стороны

15.3.2. connection

Данный раздел предназначен для настройки соединений IKE (Internet Key Exchange). Соединение IKE определяет идентификаторы и параметры безопасности взаимодействующих узлов и устанавливает защищённый канал управления (IKE SA). Этот канал используется для согласования ассоциаций безопасности IPsec, защищающих передачу данных. В терминологии IKEv2 такие ассоциации называются Child SA.

Основные настройки включают:

- Определение узлов соединения путём указания локального адреса или исходящего интерфейса (*Local IP*) и адреса удалённого шлюза (*Remote IP*).
- Выбор версии IKE (*IKEv1* или *IKEv2*), используемой для согласования параметров соединения.
- Указание идентификаторов узлов (*Local ID* и *Remote ID*) и выбор метода аутентификации (*Auth method*). Поддерживаются аутентификация по предварительно согласованному ключу (PSK) и аутентификация по открытому ключу (на основе сертификатов).
- Выбор *IKE Profile*, определяющего алгоритмы шифрования и контроля целостности, используемые для защиты канала управления IKE.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, позволяя добавлять или изменять конфигурации соединений без разрыва существующих активных ассоциаций безопасности. Для принудительного завершения конкретной SA перейдите в раздел */tunnel ipsec status*.

СВОЙСТВА

left (*Local IP*) **значения:** /ip interface, /mobile modem, auto	Локальный адрес туннеля или интерфейс
right (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
keyexchange (*IKE version*) **значения:** ikev2, ikev1	Версия протокола IKE для безопасного согласования SA
profile (*IKE Profile*) **значения:** /tunnel ipsec profile	IKE/ISAKMP профиль шифрования и аутентификации SA

leftid (*Local ID*)	Локальный IKE идентификатор для аутентификации **условия:** auth = pubkey
rightid (*Remote ID*)	IKE идентификатор для аутентификации удалённой стороны
auth (*Auth method*) **значения:** psk, pubkey	Метод аутентификации между сторонами
psk (*Pre-shared key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** auth = psk
cert (*Certificate*) **значения:** /storage certificate	Сертификат (включая закрытый ключ) **условия:** auth = pubkey
leftsourceip (*Virtual IP*) **пример:** 192.168.1.1, %config	Virtual IP для использования в качестве источника трафика
rightsourceip (*Remote Virtual IP*) **пример:** 192.168.1.1/24, 192.168.1.1-192.168.1.100, %config	Выделить виртуальный адрес для удалённой стороны

15.3.3. profile

Данный раздел предназначен для создания повторно используемых **IKE-профилей**. Каждый профиль представляет собой именованный набор криптографических алгоритмов и параметров, определяющих процесс установления ассоциации безопасности IKE (IKE SA), которая в терминологии IKEv1 также называется SA первой фазы.

Использование профилей позволяет стандартизировать и упростить настройку IPsec. Вместо повторного указания одинаковых наборов алгоритмов для каждого соединения можно создать профиль и использовать его в нескольких IKE-соединениях.

Профиль определяет основные параметры безопасности для согласования IKE, включая:

- Допустимые алгоритмы *Encryption*, *Hash* и *Pseudo-random Function*.
- Группу Диффи — Хеллмана (*DH Group*), используемую для безопасного обмена ключами.
- Параметр *IKE Lifetime*, определяющий интервал обновления ключей IKE SA.
- Параметры Dead Peer Detection (*DPD*), определяющие, как роутер отслеживает доступность удалённого IKE-пира и какое действие (*DPD Action*) выполняет, если пир перестаёт отвечать. Для IKEv1 параметр *DPD Timeout* задаёт время ожидания ответа, по истечении которого соединение разрывается.

Функция *Apply* в этом разделе выполняет «мягкую» перезагрузку, позволяя добавлять или изменять профили без разрыва существующих активных ассоциаций безопасности. Для принудительного завершения конкретной SA перейдите в раздел */tunnel ipsec status*.

СВОЙСТВА

encryption (*Encryption*) **значения:** aes128, aes192, aes256, 3des	Алгоритм шифрования для безопасной передачи данных
hash (*Hash*) **значения:** sha1, sha256, sha384, sha512, md5	Хэш-функция проверки подлинности

prf (*Pseudo-random Function*) **значения:** sha1, sha256, sha384, sha512, md5	Псевдослучайная хэш-функция для получения материала ключа
dh (*DH Group*) **значения:** modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192	Протокол Diffie-Hellman для обмена ключами
ikelifetime (*IKE Lifetime*)	Интервал времени до пересогласования IKE/ISAKMP SA
dpddelay (*DPD Delay*)	Интервал отправки DPD пакета (если нет иного трафика)
dpdtimeout (*DPD Timeout*)	Таймаут без ответа на DPD пакет, через который прервать IKEv1 соединение
dpdaction (*DPD Action*) **значения:** hold, restart, clear, none	Действие, выполняемое при разрыве соединения по таймауту

15.3.4. proposal

Данный раздел предназначен для создания повторно используемых **профилей IPsec (Proposals)**. Каждый профиль представляет собой именованный набор алгоритмов и параметров безопасности, определяющих способ защиты трафика средствами IPsec (Фаза 2 в IKEv1 или дочерние SA в IKEv2).

Аналогично профилям IKE, профили IPsec обеспечивают модульный подход к управлению политиками безопасности. При создании профиля задаются алгоритмы *Encryption* и *Auth*, используемые протоколом ESP (Encapsulating Security Payload) для обеспечения конфиденциальности и целостности данных.

Основные параметры профиля включают:

- Криптографические алгоритмы защиты данных (*Encryption*, *Auth*).
- Параметр *PFS Group*, определяющий группу Диффи — Хеллмана, используемую для обеспечения совершенной прямой секретности (Perfect Forward Secrecy, PFS). PFS также можно отключить.
- Параметр *Lifetime*, задающий время жизни ассоциации безопасности IPsec в секундах.

Созданные профили можно использовать в разделе */tunnel ipsec association* для применения единых настроек защиты данных к нескольким туннелям.

СВОЙСТВА

encryption (*Encryption*) **значения:** aes128, aes192, aes256, 3des	Алгоритм шифрования для безопасной передачи данных
auth (*Auth*) **значения:** sha1, sha256, sha384, sha512, md5	HMAC алгоритм для аутентификации
pfs (*PFS Group*) **значения:** modp768, modp1024, modp1536, modp2048, modp3072, modp4096, modp6144, modp8192, none	Алгоритм PFS, гарантирует что DH ключи не будут использованы повторно
lifetime (*Lifetime*)	Интервал времени (сек) до пересогласования

15.3.5. status

Данный раздел отображает текущее рабочее состояние IPsec-соединений и связанных с ними ассоциаций безопасности (SA). Он предназначен для проверки установленных туннелей и

диагностики проблем с сетевым подключением.

Страница отображает результаты применения настроек, заданных в разделах */tunnel ipsec connection* и */tunnel ipsec association*. Здесь можно проверить идентификаторы локальной и удалённой сторон (*Local ID* и *Remote ID*), а также согласованные селекторы трафика (*Local TS* и *Remote TS*), чтобы убедиться, что туннель установлен между нужными узлами и используется для предполагаемого трафика.

Параметр *SA state* отображает текущее состояние ассоциации безопасности, например *Waiting for traffic* или *Phase 1 established*, что помогает выявлять ошибки конфигурации и проблемы с сетью. Таблица также содержит информацию о времени работы SA (*SA uptime*), согласованных алгоритмах шифрования и контроля целостности, а также счётчики принятого и переданного трафика (*Rx/Tx counter*).

В разделе также можно принудительно завершить выбранную SA и изменить уровень детализации журналирования IPsec для диагностики неполадок.

КОМАНДЫ

debug	Изменить уровень детализации логгирования level - Уровень детализации логирования (обязательно)

СВОЙСТВА

association (*Association*)	IPSec SA **условия:** association != ""
uniqueid (*SA unique ID*)	Уникальный идентификатор SA
status (*SA state*)	Статус SA
local (*Local address*)	Адрес с которого строится туннель
local-id (*Local ID*)	Локальной IKE идентификатор
remote (*Remote address*)	Адрес на который строится туннель
remote-id (*Remote ID*)	IKE идентификатор удалённой стороны
uptime (*SA uptime*)	Время с момента установки SA
encryption (*Encryption algorithm*)	Согласованый алгоритм шифрования
integrity (*Integrity algorithm*)	Согласованый алгоритм проверки целостности
prf (*Pseudo-Random Function*)	Согласованый PRF алгоритм
dh (*Diffie Hellman Group*)	Согласованая группа DH
local-ts (*Local TS*)	Источник трафика с локальной стороны
remote-ts (*Remote TS*)	Источник трафика с удалённой стороны
expires (*rekey/reauth countdown*)	Время до истечения SA (rekeying/reauthentication)
reqid (*Reqid*)	Уникальный номер SA
rx-tx (*Rx/Tx counter*)	Счётчик полученного / отправленного трафика

15.4. l2tp

Данный раздел предназначен для настройки роутера в качестве клиента L2TPv2, позволяющего устанавливать туннель с удалённым L2TP-сервером. L2TPv2 обеспечивает передачу сессий Point-to-Point Protocol (PPP) через IP-сети и обычно используется для подключения к корпоративным сетям или сервисам удалённого доступа.

Основная настройка включает указание IP-адреса или FQDN удалённого сервера (*Remote IP*), а также имени пользователя (*Username*) и пароля (*Password*) для аутентификации. Дополнительно можно указать локальный адрес или интерфейс (*Local IP*) и выбрать тип аутентификации (*Authentication type*) в соответствии с требованиями сервера.

Сам по себе L2TPv2 не обеспечивает шифрование. Для защиты передаваемых данных можно включить шифрование (*Encryption*) с использованием MPPE или IPsec, если соответствующий компонент установлен. При использовании MPPE поддерживается только аутентификация MSCHAPv2. Для аутентификации туннеля с использованием IPsec применяется предварительно согласованный ключ (PSK).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN или IP адрес)
username (*Username*)	Имя пользователя
password (*Password*)	Пароль пользователя
auth (*Authentication*) **значения:** any, chap, mschap, mschap-v2, pap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption (*Encryption*) **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option (*Options*) **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug (*Debug*) **значения:** true, false	Режим подробного логгирования

15.5. l2tp v3

Данный раздел предназначен для настройки туннелей L2TPv3 (Layer 2 Tunneling Protocol version 3) — стандартизированного IETF протокола для создания соединений второго уровня типа «точка-точка» поверх IP-сетей.

В отличие от L2TPv2, протокол L2TPv3 работает независимо от PPP и обеспечивает более универсальный механизм передачи трафика второго уровня. Его основная функция заключается в инкапсуляции и передаче полных Ethernet-кадров с помощью виртуального соединения типа «псевдопровод» (pseudowire), которое может объединять два удалённых сетевых сегмента.

Для настройки необходимо определить конечные точки туннеля (*Local IP* и *Remote IP*), а также указать локальные и удалённые идентификаторы туннеля и сессии (*Tunnel ID*, *Peer Tunnel ID*,

Session ID и *Peer Session ID*). Значения идентификаторов должны быть согласованы между обеими сторонами соединения.

Дополнительные настройки включают MTU туннеля и режим инкапсуляции (*Encapsulation*), позволяющий передавать трафик L2TPv3 непосредственно поверх IP или с использованием UDP.

L2TPv3 не обеспечивает встроенного шифрования. Если компонент IPsec установлен, можно включить защиту туннеля с помощью IPsec через параметр *Encryption*, используя предварительно согласованный ключ (PSK).

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0, 192.168.1.1	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
encryption (*Encryption*) **значения:** none	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
macaddr (*MAC*) **пример:** FE:FF:FF:FF:FF:FF	MAC адрес
mtu (*MTU*) **минимум:** 70, **максимум:** 65535	MTU интерфейса
l2spec-type (*L2 Spec*) **значения:** default, none	Тип заголовка (header) для второго уровня
tunnel-id (*Tunnel ID*) **минимум:** 1, **максимум:** 4294967295	ID туннеля
peer-tunnel-id (*Peer Tunnel ID*) **минимум:** 1, **максимум:** 4294967295	ID туннеля удалённой стороны
session-id (*Session ID*) **минимум:** 1, **максимум:** 4294967295	ID сессии туннеля
peer-session-id (*Peer Session ID*) **минимум:** 1, **максимум:** 4294967295	ID сессии удалённой стороны
encap (*Encapsulation*) **значения:** ip, udp	Тип инкапсуляции протокола
udp-dport (*Peer UDP Port*) **минимум:** 1024 **пример:** 80, !80	UDP порт удалённой стороны в случае UDP энкапсуляции **условия:** encap = udp
udp-sport (*UDP Port*) **минимум:** 1024 **пример:** 80, !80	UDP порт для UDP энкапсуляции **условия:** encap = udp

15.6. openvpn

Данный раздел предназначен для настройки клиента OpenVPN — VPN-решения с открытым исходным кодом, используемого для создания защищённых соединений между удалёнными сетями и организации удалённого доступа.

OpenVPN поддерживает интерфейсы *TUN* для маршрутизируемых соединений третьего уровня и *TAP* для Ethernet-туннелей второго уровня. Передача данных может осуществляться по протоколам *UDP* или *TCP* в зависимости от требований сети.

Настройка включает указание адреса удалённого сервера, транспортного протокола и параметров безопасности. OpenVPN поддерживает аутентификацию с использованием TLS и сертификатов, а также конфигурации со статическим ключом. Дополнительные параметры позволяют настроить алгоритмы шифрования и аутентификации, учётные данные пользователя и защиту TLS-соединения с помощью *tls-auth* или *tls-crypt*.

КОМАНДЫ

generate-ta-key	Сгенерировать файл случайного ключа, используемый как TA Key или Static Key filename - Имя конфигурации (обязательно)

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*)	Адрес удалённого хоста (FQDN ил IP адрес)
tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
dev-type (*Device Type*) **значения:** tun, tap	Тип виртуального интерфейса
protocol (*Protocol*) **значения:** tcp, udp	Транспортный протокол туннеля
encryption (*Encryption*) **значения:** none, tls, static-key	Метод шифрования туннеля
static-key (*Static key*) **значения:** /storage file	PSK файл для шифрования статическим ключем **условия:** encryption = static-key
cipher (*Cipher*) **значения:** AES-128-CBC, AES-128-GCM, AES-192-CBC, AES-192-GCM, AES-256-CBC, AES-256-GCM	Алгоритм шифрования туннеля **условия:** encryption = tls encryption = static-key
auth (*Auth*) **значения:** MD5, SHA1, SHA256, SHA384, SHA512, none	HMAC алгоритм для аутентификации **условия:** encryption = tls encryption = static-key
tls-mode (*TLS Mode*) **значения:** none, tls-auth, tls-crypt	Дополнительные опции при установлении TLS сессии **условия:** encryption = tls

ta-key (*TA Key*) **значения:** /storage file	Ключ дополнительной HMAC аутентификации **условия:** tls-mode != none && tls-mode != ""
ca (*Ca*) **значения:** /storage certificate	Публичный ключ удостоверяющего цетра (CA) **условия:** encryption = tls
cert (*Cert*) **значения:** /storage certificate	Локальный сертификат (включая приватный ключ) **условия:** encryption = tls
username (*Username*)	Имя пользователя для аутентификации **условия:** encryption = tls
password (*Password*)	Пароль пользователя для аутентификации **условия:** encryption = tls
flag (*Flag*) **значения:** allow-recursive-routing, auth-nocache, auth-user-pass-optional, client-to-client, comp-noadapt, fast-io, float, mtu-test, multihome, ncp-disable, nobind, opt-verify, passtos, persist-key, persist-local-ip, persist-remote-ip, persist-tun, ping-timer-rem, pull, push-peer-info, push-reset, remote-random, route-nopull, single-session, suppress-timestamps, tcp-nodelay, tls-client, tls-exit, tls-server, username-as-common-name	Дополнительные опции туннеля
extra (*Extra parameters*) **значения:** auth-retry, bcast-buffers, comp-lzo, compress, connect-freq, connect-retry, connect-retry-max, connect-timeout, ecdh-curve, explicit-exit-notify, fragment, hand-window, hash-size, ifconfig_local, ifconfig_remote, ifconfig_netmask, ifconfig-push-local, ifconfig-push-netmask, inactive, key-direction, keysize, link-mtu, lport, max-clients, mssfix, mtu-disc, ping, ping-exit, ping-restart, prng, pull-filter-accept, pull-filter-ignore, pull-filter-reject, rcvbuf, remote-cert-tls, reneg-bytes, reneg-pkts, reneg-sec, replay-persist, replay-window, resolv-retry, shaper, sndbuf, topology, tcp-queue-limit, tls-timeout, tls-version-min, tran-window, tun-mtu, tun-mtu-extra, txqueuelen, verb, verify-client-cert, verify-x509-name, x509-username-field	Дополнительные параметры туннеля

15.7. pptp

Данный раздел предназначен для настройки роутера в качестве клиента PPTP (Point-to-Point Tunneling Protocol), позволяющего устанавливать VPN-туннель с удалённым PPTP-сервером, как правило, для доступа к частным сетям.

PPTP — устаревший VPN-протокол, отличающийся относительно простой настройкой. Основные параметры включают IP-адрес или FQDN удалённого сервера (*Remote IP*), учётные данные для аутентификации (*Username* и *Password*) и тип аутентификации (*Authentication type*). Также можно указать локальный адрес или интерфейс (*Local IP*).

Параметр *Encryption* поддерживает шифрование MPPE, для которого требуется аутентификация MSCHAPv2. Если компонент IPsec установлен, также можно включить защиту с помощью IPsec, используя предварительно согласованный ключ (PSK).

PPTP является устаревшим протоколом с известными уязвимостями безопасности. Его использование настоятельно не рекомендуется в случаях, когда важна защита данных. Для безопасного удалённого доступа рекомендуется использовать современные VPN-протоколы, такие как IPsec или OpenVPN.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
local-ip (*Local IP*) **значения:** /ip interface, /mobile modem, /tunnel wireguard interface, /tunnel atunnel, /defaults server, /tunnel, auto **пример:** bridge0	Локальный адрес туннеля или интерфейс
remote-ip (*Remote IP*) **пример:** localhost, sample.example.com, 8.8.8.8	Адрес удалённого хоста (FQDN ил IP адрес)
username (*Username*)	Имя пользователя
password (*Password*)	Пароль пользователя
auth (*Authentication*) **значения:** any, chap, mschap, mschap-v2, pap, eap	Выбор протокола для аутентификации **условия:** encryption = mppe
encryption (*Encryption*) **значения:** none, mppe	Метод защиты туннеля **условия:** /defaults/ipsec_installed = true
psk (*Pre-Shared Key*) **мин. длина:** 8	Общий PSK ключ для аутентификации и обмена ключами **условия:** encryption = ipsec
ppp-option (*Options*) **значения:** lcp-echo-failure, lcp-echo-interval, lcp-max-configure, lcp-max-failure, lcp-max-terminate, lcp-restart, ipcp-accept-local, ipcp-accept-remote, ipcp-max-configure, ipcp-max-failure, ipcp-max-terminate, ipcp-restart, mru, mtu	Опции демона протокола Point-to-Point
debug (*Debug*) **значения:** true, false	Режим подробного логгирования

15.8. wireguard

В данном подразделе настраивается протокол **WireGuard**, который использует современные методы шифрования для создания защищенных туннелей между сетевыми устройствами.

15.8.1. interface

Данный раздел предназначен для настройки локального сетевого интерфейса WireGuard, который выступает одной из конечных точек защищённого VPN-туннеля. Для идентификации интерфейса используется пара криптографических ключей. Публичный ключ (*Public Key*) служит криптографическим идентификатором, по которому удалённые пиры распознают интерфейс, заменяя традиционные имена пользователей и сертификаты.

При создании нового интерфейса поля *Private Key* и *Public Key* заполняются автоматически, при этом публичный ключ вычисляется на основе приватного. Дополнительная настройка включает назначение IP-адреса туннельного интерфейса (*Tunnel IP*) в виртуальной VPN-сети и указание порта (*Port*) для приёма входящих подключений от пиров.



Одной настройки интерфейса недостаточно для установления рабочего туннеля. Необходимо также настроить удалённые пиры, которым разрешено подключаться к этому интерфейсу, в разделе */tunnel wireguard peer*.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
tunnel-ip (*Tunnel IP*) **пример:** 192.168.1.1, 192.168.1.0/24, 192.168.1.1/255.255.255.0	Адрес туннельного интерфейса
priv-key (*Private key*) **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Приватный ключ для аутентификации и шифрования трафика
pub-key (*Public key*) **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Публичный ключ для аутентификации и шифрования трафика
port (*Port*) **пример:** 22, 51820	Порт для входящих подключений
mtu (*MTU*) **минимум:** 70, **максимум:** 65535	MTU интерфейса
fw-mark (*Mark*)	Установить метку для пакетов, ассоциированных с этим интерфейсом

15.8.2. peer

Данный раздел предназначен для настройки удалённых пиров, которым разрешено взаимодействовать с локальным интерфейсом WireGuard. Каждый пир представляет собой удалённую конечную точку VPN-туннеля.

Настройка пира выполняет две основные функции: **аутентификацию** и **маршрутизацию**.

- **Аутентификация**: Каждый пир идентифицируется по публичному ключу (*Public key*). Успешно пройти аутентификацию может только пир, владеющий соответствующим закрытым ключом. Дополнительный предварительно согласованный ключ (*Pre-shared key*) обеспечивает ещё один уровень криптографической защиты.
- **Маршрутизация**: Параметр *Allowed IP* определяет IP-адреса и сети, связанные с пиром. Для исходящего трафика он определяет, какому пиру направлять пакеты с соответствующими адресами назначения. Для входящего трафика принимаются только расшифрованные пакеты, адреса источников которых соответствуют списку разрешённых адресов.

Параметр *Remote IP* задаёт адрес и порт удалённого пира. Дополнительно можно настроить интервал *Keepalive* для поддержания соединения через межсетевые экраны с отслеживанием состояний и устройства NAT.

КОМАНДЫ

generate-psk	Сгенерировать и добавить PSK ключ

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
interface (*Interface*) **значения:** /tunnel wireguard interface	Сетевой интерфейс Wireguard

remote-ip (*Remote IP*) **пример:** 192.168.1.1, 192.168.1.1:51820	Комбинация IP-адреса и порта (51820) удаленного однорангового узла
allowed-ip (*Allowed IP*)	Адрес, ассоциированный с этим Peer для обеспечения маршрутизации
pub-key (*Public key*) **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Публичный ключ для аутентификации и шифрования трафика
psk (*Pre-shared key*) **пример:** ABC123abc456ABC789abc123ABC456abc789Abc123A=	Дополнительный ключ для увеличения безопасности
keepalive (*Keepalive*) **минимум:** 0, **максимум:** 65535	Интервал (сек) отправки keepalive пакета

16. wireless

Данный раздел предназначен для централизованной настройки всех аспектов Wi-Fi функционала роутера. Конфигурация имеет многоуровневую структуру, что обеспечивает детальный контроль как над физическим радио-оборудованием, так и над логическими беспроводными сетями.

Процесс настройки обычно выполняется в следующем порядке:

1. **Adapter:** Настройка начинается на физическом уровне в разделе *Адаптер*, где определяются низкоуровневые параметры радио, такие как код страны, доступные каналы и мощность передачи.
2. **Network:** Поверх настроенного адаптера создается одна или несколько логических *Сетей*. Именно здесь определяется режим работы (Точка доступа, Клиент, Mesh), задается имя сети (SSID) и настраивается ее профиль безопасности (например, WPA3).
3. **Filter:** Для дополнительного уровня контроля доступа в разделе *MAC-фильтр* можно создать именованные списки MAC-адресов, которые затем применяются к конкретной сети.

Для устройств, оснащенных несколькими Wi-Fi модулями, каждый модуль настраивается через этот интерфейс независимо. Это позволяет реализовывать гибкие сценарии развертывания, например, одновременное создание точек доступа на 2.4 ГГц и 5 ГГц (опционально).

16.1. adapter

Данный раздел предназначен для низкоуровневой настройки физических Wi-Fi-адаптеров, установленных в роутере. Настройки здесь определяют базовые рабочие параметры самого оборудования, напрямую управляя его поведением в радиоэфире и обеспечивая соответствие нормативным требованиям.

Настройка на этом уровне включает в себя установку ограничений, специфичных для страны, выбор доступных каналов и определение мощности передачи. Это первоначальный этап настройки и необходимое условие для создания одной или нескольких виртуальных точек доступа, которые будут передавать идентификаторы SSID.

КОМАНДЫ

scan	Поиск WiFi сетей

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
country (*Country*) **значения:** AD, AE, AF, AI, AL, AM, AN, AR, AS, AT, AU, AW, AZ, BA, BB, BD, BE, BF, BG, BH, BL, BM, BN, BO, BR, BS, BT, BY, BZ, CA, CF, CH, CI, CL, CN, CO, CR, CU, CX, CY, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, ET, FI, FM, FR, GB, GD, GE, GF, GH, GL, GP, GR, GT, GU, GY, HK, HN, HR, HT, HU, ID, IE, IL, IN, IR, IS, IT, JM, JO, JP, KE, KH, KN, KP, KR, KW, KY, KZ, LB, LC, LI, LK, LS, LT, LU, LV, MA, MC, MD, ME, MF, MH, MK, MN, MO, MP, MQ, MR, MT, MU, MV, MW, MX, MY, NG, NI, NL, NO, NP, NZ, OM, PA, PE, PF, PG, PH, PK, PL, PM, PR, PT, PW, PY, QA, RE, RO, RS, RU, RW, SA, SE, SG, SI, SK, SN, SR, SV, SY, TC, TD, TG, TH, TN, TR, TT, TW, TZ, UA, UG, US, UY, UZ, VC, VE, VI, VN, VU, WF, WS, YE, YT, ZA, ZW, default	Выбор страны для применения регуляторных ограничений
channels (*Channels*) **значения:** $_channels	Список WiFi каналов для работы адаптера
txpower (*Transmit power*) **значения:** auto, $_txpowers	Мощность исходящего сигнала
htmode (*HT mode*) **значения:** none, $_htmodes	Режим повышенной производительности, определяющий ширину канала
frag-threshold (*Fragment threshold*) **минимум:** 256, **максимум:** 2346	Размер (байт) посылки, превышение которого ведёт к его фрагментации
rts-threshold (*RTS threshold*) **минимум:** 0, **максимум:** 2347	Размер (байт) посылки, после превышения которого включается механизм RTS/CTS
beacon (*Beacon*) **минимум:** 15, **максимум:** 65535	Интервал (мсек) отправки AP beacon

16.2. filter

Данный раздел предназначен для создания и управления списками контроля доступа (ACL) на основе MAC-адресов для беспроводных сетей. Эти списки обеспечивают дополнительный уровень контроля доступа, позволяя ограничивать подключения устройств по MAC-адресам.

Система поддерживает политики разрешения и запрета подключений по списку MAC-адресов. При применении фильтра к беспроводной сети выбранная политика определяет, будет ли устройствам из списка разрешён или запрещён доступ. MAC-фильтрацию также можно отключить.

В данном разделе создаются именованные списки фильтров и выполняется управление ими. Применение фильтра к конкретной беспроводной сети и выбор политики *MAC filter* осуществляются в разделе */wireless network*.

СВОЙСТВА

mac (*MAC address*)	MAC адрес WiFi устройства

16.3. network

Данный раздел предназначен для настройки логических беспроводных сетей, каждая из которых работает на основе физического *Adapter*. Каждая настроенная сеть представляет собой

отдельный беспроводной сервис, например точку доступа (AP), транслирующую SSID, клиентское подключение к вышестоящей Wi-Fi-сети или узел mesh-сети.

Режимы работы

Основным параметром является *Mode*, который определяет роль беспроводной сети:

- **Точка доступа (ap):** Наиболее распространённый режим. Роутер транслирует *SSID*, к которому могут подключаться клиентские устройства.
- **Клиент (sta):** Роутер подключается к существующей Wi-Fi-сети, обычно для использования её в качестве WAN-канала или объединения сетей через мост.
- **Узел mesh-сети (mesh):** Специализированный режим для построения распределённой самовосстанавливающейся mesh-сети с другими совместимыми устройствами. Доступность режима зависит от аппаратной платформы роутера.

Безопасность и контроль доступа

Помимо выбора режима работы, раздел позволяет настроить основные параметры безопасности и контроля доступа для каждой сети:

- **Аутентификация:** Настройка параметров безопасности путём выбора типа *Encryption* (например, WPA2/WPA3) и указания ключа сети (*Key*).
- **Контроль доступа:** В режиме *ap* параметр *MAC filter* позволяет разрешать или запрещать подключения на основе заранее созданного списка MAC-адресов, а также отключать MAC-фильтрацию. Список выбирается из созданных в разделе */wireless filter*. Доступность параметра зависит от выбранного типа шифрования.
- **Изоляция клиентов:** В режиме *ap* включение параметра *Isolate Clients* запрещает беспроводным устройствам, подключённым к одному SSID, напрямую обмениваться данными друг с другом.

СВОЙСТВА

disabled (*Disabled*) **значения:** true, false	Выключить конфигурацию
adapter (*Adapter*) **значения:** /wireless adapter	WiFi адаптер
mode (*Mode*) **значения:** ap, sta, mesh	Режим работы в беспроводной WiFi сети
encryption (*Encryption*) **значения:** none, psk-mixed+ccmp, psk2+ccmp, wpa-mixed+ccmp, wpa2+ccmp, sae	Тип шифрования данных в беспроводной WiFi сети **условия:** mode = mesh
ssid (*SSID*)	Имя беспроводной WiFi сети для её идентификации в эфире
key (*Key*) **мин. длина:** 8	Пароль аутентификации в беспроводной WiFi сети **условия:** encryption = psk-mixed+ccmp encryption = psk2+ccmp encryption = sae
wds (*WDS*) **значения:** true, false	Use 4-address mode to allow transparent ethernet bridging **условия:** mode != mesh

wmm (*WMM*) **значения:** true, false	WiFi Multimedia Mode включает механизм QoS для мультимедиа трафика
mesh-forward (*Mesh Forwarding*) **значения:** true, false	Пересылать пакеты не предназначенные для этой mesh станции **условия:** mode = mesh
mesh-ttl (*Mesh TTL*)	Количество прыжков, которые пакет может пройти внутри mesh сети **условия:** mode = mesh
mesh-rssi-threshold (*Mesh RSSI limit*) **минимум:** -100, **максимум:** 1	Требование минимального RSSI необходимого для поддержания связи внутри mesh сети **условия:** mode = mesh
hidden (*Hide SSID*) **значения:** true, false	Отключить вещание beacon **условия:** mode = ap
mtu (*MTU*) **минимум:** 256, **максимум:** 2304	MTU интерфейса
isolate (*Isolate Clients*) **значения:** true, false	Запретить клиентам коммуницировать друг с другом **условия:** mode = ap
mac-filter (*MAC filter*) **значения:** deny, allow, disable	Политика ACL для фильтрации беспроводных устройств **условия:** mode = ap && encryption != wpa-mixed+ccmp && encryption != wpa2+ccmp
mac-list (*Mac list*) **значения:** /wireless filter	ACL беспроводных устройств **условия:** mode = ap && mac-filter != disable && encryption != wpa-mixed+ccmp && encryption != wpa2+ccmp
auth-server (*Authentication server*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес сервера аутентификации **условия:** encryption = wpa-mixed+ccmp && mode != sta encryption = wpa2+ccmp && mode != sta
auth-secret (*Authentication secret*)	Общий ключ сервре аутентификации **условия:** encryption = wpa-mixed+ccmp && mode != sta encryption = wpa2+ccmp && mode != sta
acct-server (*Accounting server*) **пример:** 192.168.1.1, example.com, 192.168.1.1:80	Адрес сервера для аккаунтинга **условия:** encryption = wpa-mixed+ccmp && mode != sta encryption = wpa2+ccmp && mode != sta
acct-secret (*Accounting secret*)	Общий ключ аккаунтинг сервера **условия:** encryption = wpa-mixed+ccmp && mode != sta encryption = wpa2+ccmp && mode != sta
eap-method (*EAP method*) **значения:** peap, tls, ttls	EAP authentication method **условия:** mode = sta && encryption = wpa-mixed+ccmp mode = sta && encryption = wpa2+ccmp
eap-auth-method (*Authentication method*) **значения:** pap, mschap-v2	WPA/WPA2 enterprise authentication method **условия:** encryption = wpa-mixed+ccmp && mode = sta && eap-method = ttls encryption = wpa2+ccmp && mode = sta && eap-method = ttls encryption = wpa-mixed+ccmp && mode = sta && eap-method = peap encryption = wpa2+ccmp && mode = sta && eap-method = peap

eap-username (*Username*) **пример:** bridge0, vpn-client1, user_1@example.com	Логин пользователя для аутентификации WPA/WPA2 Enterprise **условия:** encryption = wpa-mixed+ccmp && mode = sta encryption = wpa2+ccmp && mode = sta
eap-password (*Password*)	Пароль пользователя для аутентификации WPA/WPA2 Enterprise **условия:** encryption = wpa-mixed+ccmp && mode = sta && eap-method = peap encryption = wpa2+ccmp && mode = sta && eap-method = peap encryption = wpa-mixed+ccmp && mode = sta && eap-method = ttls encryption = wpa2+ccmp && mode = sta && eap-method = ttls
ca (*CA certificate*) **значения:** /storage certificate	CA сертификат **условия:** encryption = wpa-mixed+ccmp && mode = sta encryption = wpa2+ccmp && mode = sta
cert (*Certificate*) **значения:** /storage certificate	Сертификат для аутентификации **условия:** encryption = wpa-mixed+ccmp && mode = sta encryption = wpa2+ccmp && mode = sta