

# Настройка гостевого Wi-Fi на роутерах Mikrotik для одиночного роутера

 [interface31.ru/tech\\_it/2022/01/nastroyka-gostevogo-wi-fi-na-routerah-mikrotik.html](https://interface31.ru/tech_it/2022/01/nastroyka-gostevogo-wi-fi-na-routerah-mikrotik.html)

## Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настройка гостевого Wi-Fi на роутерах Mikrotik для одиночного роутера

Wi-Fi сегодня для многих стал практически синонимом слова "интернет", беспроводной доступ воспринимается как нечто само собой разумеющееся, а его отсутствие вызывает недоумение и удивление. Мы привыкли к тому, что Wi-Fi есть на работе, в гостях, в публичных местах и т.д. и т.п. Но то, что хорошо обычному пользователю доставляет массу забот системному администратору - неконтролируемые пользовательские устройства в периметре локальной сети. Выход здесь один - создание гостевой Wi-Fi сети и изоляция ее от сети предприятия.



### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.

В данной статье мы рассмотрим самый простой вариант - организацию гостевой Wi-Fi сети для одиночного роутера. Это может быть полезно для небольших предприятий и домашних сетей. Предприятиям полезно вынести в гостевую сеть как посетителей, так и личные устройства сотрудников. В домашних сетях тоже не следует раздавать доступ направо и налево всем друзьям и знакомым, ведь все что они хотят - это выйти в интернет, гостевая сеть прекрасный вариант сделать это не создавая угроз безопасности.

Далее подразумевается, что у вас уже есть настроенный роутер Mikrotik с основной Wi-Fi сетью, если это не так, то воспользуйтесь нашей статьей: [Базовая настройка роутера MikroTik](#).

### Настройка виртуального беспроводного интерфейса

Самым первым шагом создадим новый профиль безопасности, так как делать открытую гостевую сеть - это очень плохая идея, а для организаций еще и нарушение закона, требующего обязательную идентификацию пользователей. Для этого откроем **Wireless - Security Profiles** и добавим новый профиль. Настройки просты: **Mode - dynamic keys**, **Authentication Types - WPA PSK2, WPA2 Pre-Shared Key** - пароль доступа к сети, от 8 символов, **Name** - произвольное имя профиля, в нашем случае **guest**.

Команда для терминала, в качестве пароля мы задали 987654321:

```
/interface wireless security-profiles
add authentication-types=wpa2-psk eap-methods="" mode=dynamic-keys name=guest
supplicant-identity="" wpa2-pre-shared-key=987654321
```

Теперь перейдем в **Wireless - WiFi Interfaces** и добавим новый виртуальный интерфейс, нажав на кнопку с плюсом и выбрав в выпадающем меню **Virtual**.

Name	Actual MTU	Tx	Rx	Tx P
Wireless (Atheros AR9...	1500	424 bps	0 bps	

В открывшемся окне указываем режим работы интерфейса **Mode - ap bridge**, выбираем основной физический радиointерфейс **Master Interface - wlan1**, указываем желаемый **SSID** и выбираем созданный нами ранее для гостевой сети профиль безопасности в **Security Profiles**. Также снимаем флаг **Default Forward** что исключит общение гостевых устройств между собой. Остальные параметры оставляем по умолчанию.

The screenshot shows the 'New Interface' dialog box with the 'Wireless' tab selected. The configuration is as follows:

- Mode: ap bridge
- Secondary Channel: (empty)
- SSID: GUEST
- Master Interface: wlan1
- Security Profile: guest
- Interworking Profile: disabled
- WPS Mode: disabled
- VLAN Mode: no tag
- VLAN ID: 1
- Default AP Tx Rate: (empty) bps
- Default Client Tx Rate: (empty) bps
- Default Authenticate: ☒
- Default Forward: ☐
- Hide SSID: ☐

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Advanced Mode, Torch.

Bottom status bar: enabled, running, slave.

В терминале настроек побольше, вам также потребуется указать **MAC-адрес**, который следует взять у физического беспроводного интерфейса.

```
/interface wireless
add default-forwarding=no disabled=no keepalive-frames=disabled mac-
address=AA:BB:CC:DD:EE:FF \
master-interface=wlan1 multicast-buffering=disabled name=wlan2 security-
profile=guest ssid=GUEST \
wds-cost-range=0 wds-default-cost=0 wps-mode=disabled
```

Если у вас двухдиапазонная точка доступа и вы желаете создать в каждом из них гостевые сети, то создайте еще один виртуальный беспроводной интерфейс и укажите в качестве **Master Interface** второй беспроводной адаптер. Рабочую частоту, ширину канала, мощность и прочие настройки виртуальный адаптер наследует от физического интерфейса. Т.е. гостевая сеть будет работать на том же канале и с такими же параметрами, как и основная.

После чего перейдем в **Bridge** и создадим новый сетевой мост, в параметре **ARP** укажем **reply-only**, что заставит роутер отвечать на канальном уровне только известным устройствам, что значительно ограничит самодеятельность в гостевой сети, так гости смогут работать только с настройками, полученными от роутера, самостоятельно настроить сетевые параметры не получится.

The screenshot shows a 'New Interface' dialog box with the following fields and values:

- Name: bridge2
- Type: Bridge
- MTU: (empty)
- Actual MTU: (empty)
- L2 MTU: (empty)
- MAC Address: (empty)
- ARP: reply-only
- ARP Timeout: (empty)
- Admin. MAC Address: (empty)
- Ageing Time: 00:05:00
- IGMP Snooping: ☐
- DHCP Snooping: ☐
- Fast Forward: ☒

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Torch.

Status bar at the bottom: enabled, running, slave.

В командной строке это же действие:

```
/interface bridge
add arp=reply-only name=bridge2
```

Затем добавим в этот мост созданные нами виртуальные беспроводные интерфейсы, с помощью графического интерфейса в разделе **Bridge - Ports** или в консоли:

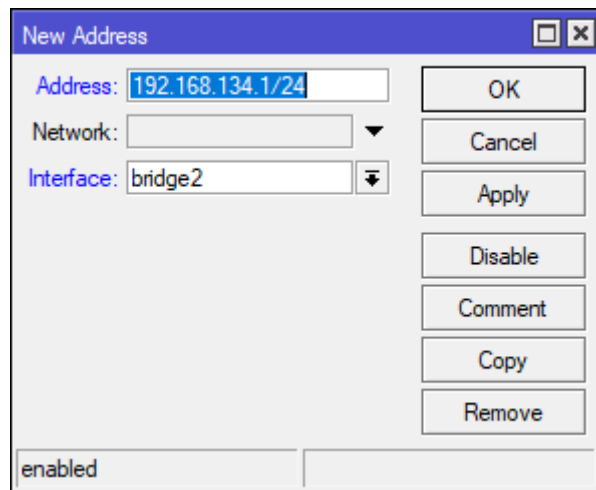
```
/interface bridge port
add bridge=bridge2 interface=wlan2
```

После чего назначим ему IP-адрес, для гостевой сети следует выбрать отдельный диапазон адресов, не пересекающийся с вашими сетями, в нашем примере это будет 192.168.134.0/24, адресом роутера в этом случае будет 192.168.134.1. Откроем **IP - Addresses** и добавим новый адрес, его следует указать в формате **192.168.134.1/24** (что соответствует маске 255.255.255.0), в поле **Interface** выберите интерфейс созданного на предыдущем шаге сетевого моста, у нас это **bridge2**.

Или выполните в терминале:

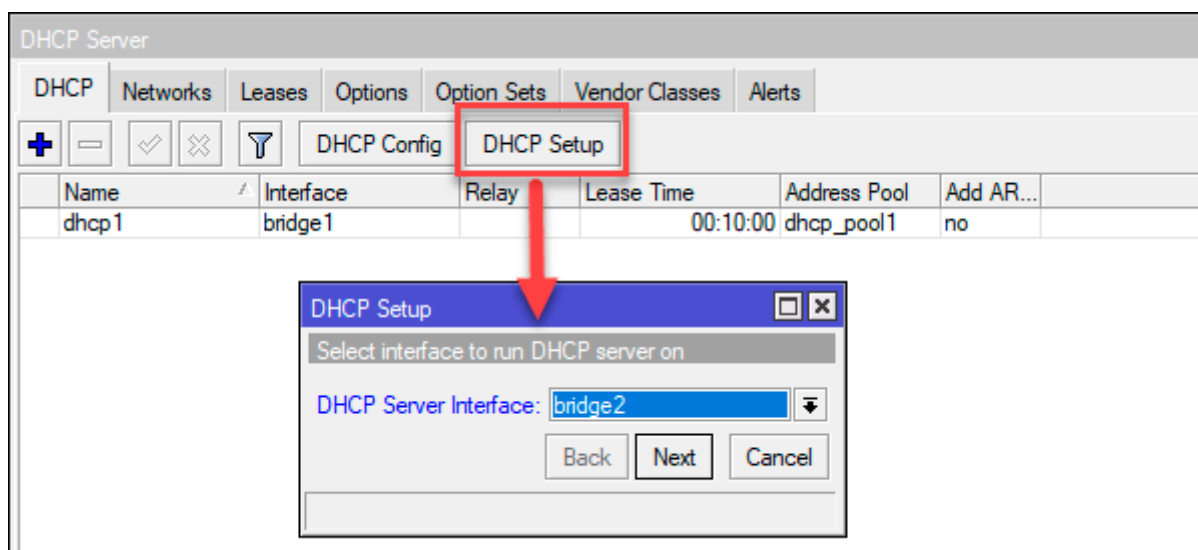
```
/ip address
add address=192.168.134.1/24
interface=bridge2 network=192.168.134.0
```

Если вам нужно несколько гостевых сетей с разным уровнем доступа, то создайте нужное количество виртуальных сетевых интерфейсов и мостов (по одному для каждой сети), а также присвойте каждой сети свой диапазон адресов.



## Настройка базовых сетевых служб: DHCP, DNS, NAT

Для настройки DHCP-сервера воспользуемся мастером, для этого перейдем в **IP - DHCP Server - DHCP** и нажмем кнопку **DHCP Setup**, в открывшемся мастере выберем интерфейс - **bridge2** и последовательно ответим на ряд вопросов, задав сеть, пул адресов, адрес шлюза и т.д.



А вот при указании DNS-сервера следует подумать, мы можем указать адрес роутера и использовать уже имеющуюся на нем службу, но в ряде случаев это может быть нежелательно, например, у вас имеются записи для внутренних служб, и вы не хотите их утечки во внешнюю сеть. Либо вам нужно дополнительно фильтровать содержимое, отдаваемое гостевым пользователям. В этом случае в качестве DNS-сервера можно указать адрес любого публичного сервиса, который подходит под ваши требования.

С другой стороны собственный DNS сервер позволяет самостоятельно блокировать некоторые ресурсы, более подробно вы можете прочитать об этом [здесь](#).

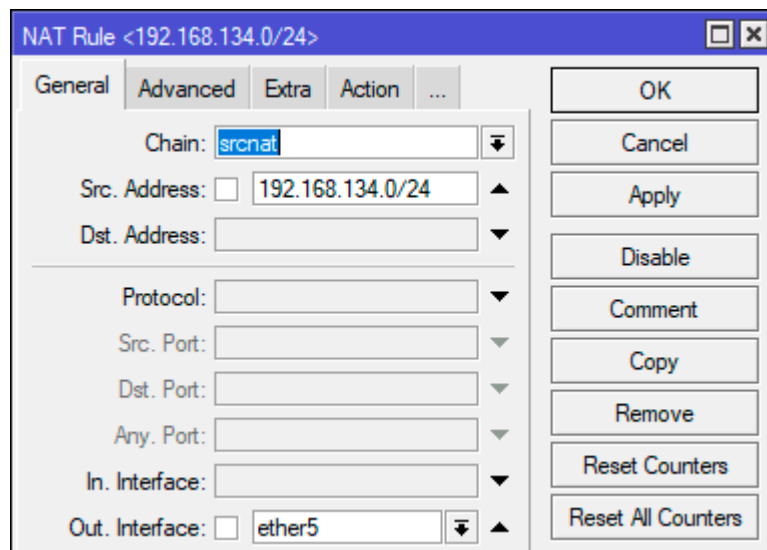
После завершения работы мастера откройте созданную запись в **IP - DHCP Server - DHCP** и установите флаг **Add ARP For Leases**, теперь сервер будет динамически добавлять MAC-адреса клиентов, получивших аренду в ARP-таблицу, чтобы они

могли работать в гостевой сети. По окончании аренды такая запись будет удалена и даже если клиент перенастроил свое устройство на статический адрес через некоторое время он потеряет доступ к сети. В связи с этим обратите внимание на параметр **Lease Time**, который задает время аренды адреса, по умолчанию это 10 минут, вполне разумный интервал, но вы можете как увеличить его (если это сеть для личных устройств сотрудников) или уменьшить, чтобы ускорить освобождение адресов.

Чтобы настроить DHCP-сервер в терминале выполните:

```
/ip pool
add name=dhcp_pool2 ranges=192.168.134.100-192.168.134.199
/ip dhcp-server network
add address=192.168.134.0/24 dns-server=192.168.134.1 gateway=192.168.134.1
/ip dhcp-server
add add-arp=yes address-pool=dhcp_pool2 disabled=no interface=bridge2 name=dhcp2
```

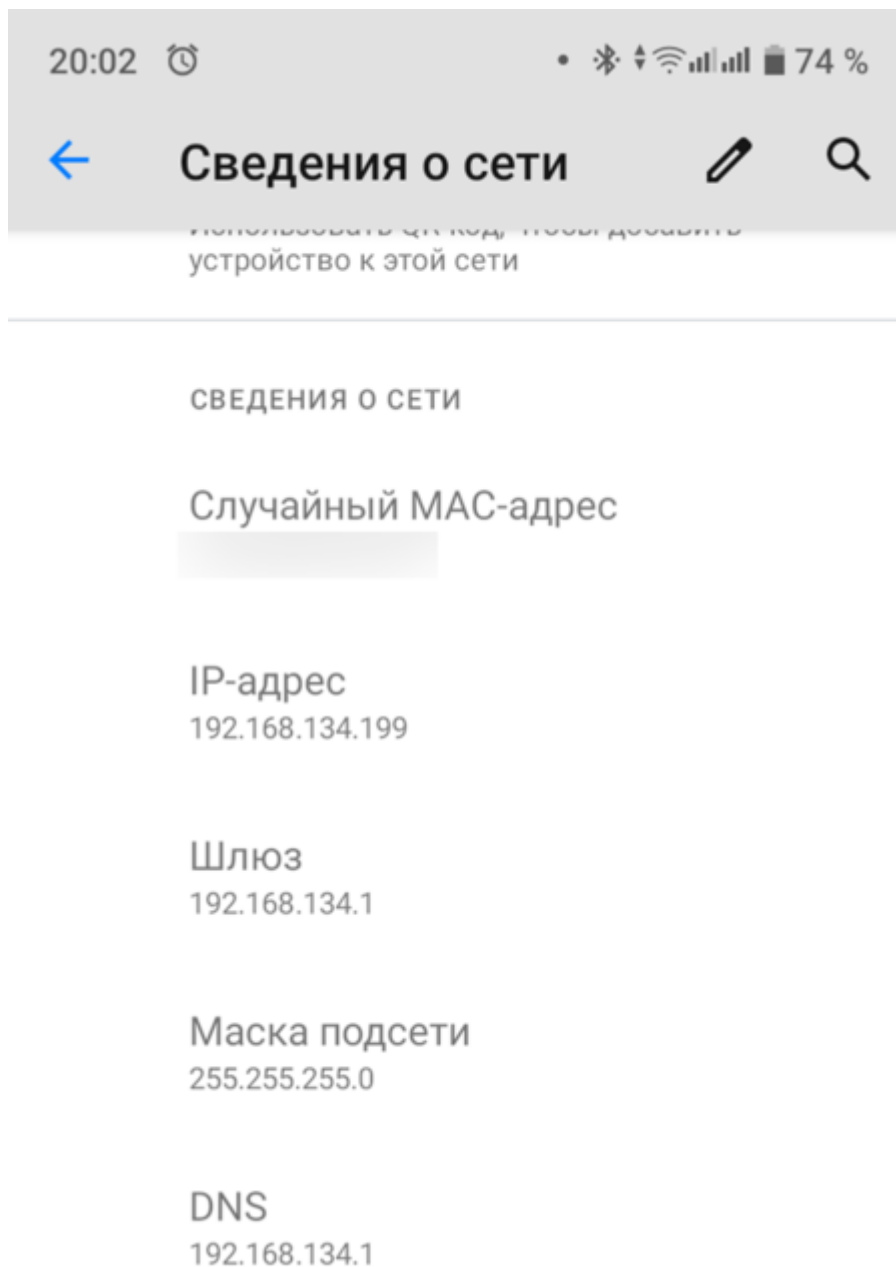
Для того, чтобы клиенты гостевой сети могли выходить в интернет, следует настроить NAT, перейдем в **IP - Firewall - NAT** и создадим новое правило: **Chain - srcnat, Src. Address - 192.168.134.0/24** - диапазон гостевой сети, **Out. Interface** - внешний интерфейс, через который осуществляется выход в интернет, в нашем случае **ether5**. На закладке **Action** ставим действие **masquerade**.



Или в терминале:

```
/ip firewall nat  
add action=masquerade chain=srcnat out-interface=ether5 src-  
address=192.168.134.0/24
```

Теперь самое время сделать небольшую паузу и попробовать подключиться к нашей гостевой Wi-Fi сети, убедитесь, что устройство получает адрес и у него есть доступ в интернет.

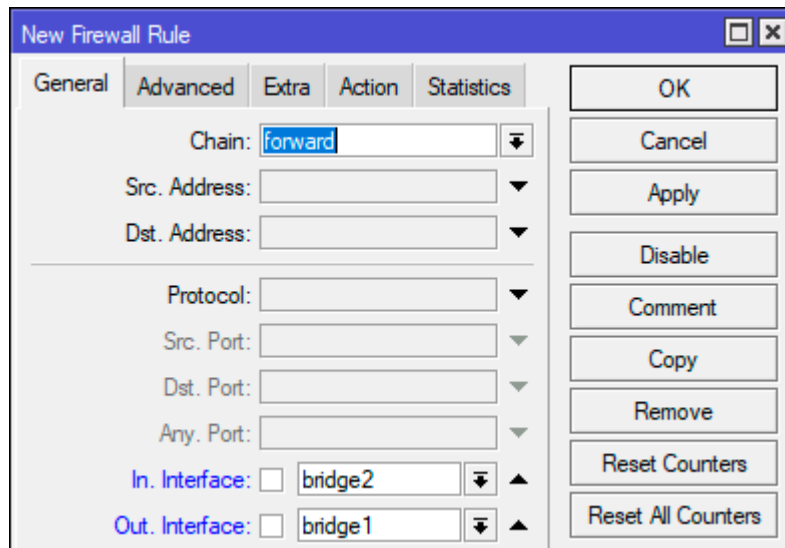


Если вы нигде не ошиблись - все должно работать.

## Изолируем гостевую сеть при помощи брандмауэра

Гостевая Wi-Fi сеть работает - и это хорошо, теперь самое время принять кое-какие меры безопасности. Прежде всего изолируем ее от основной сети. Открываем IP - Firewall - Filtres и создаем следующее правило: **Chain - Forward, In. Interface - bridge2, Out. Interface - bridge1**, на закладке **Action** ставим действие **drop**, тем самым полностью запретив транзитный трафик из гостевой сети в основную (**bridge1**).

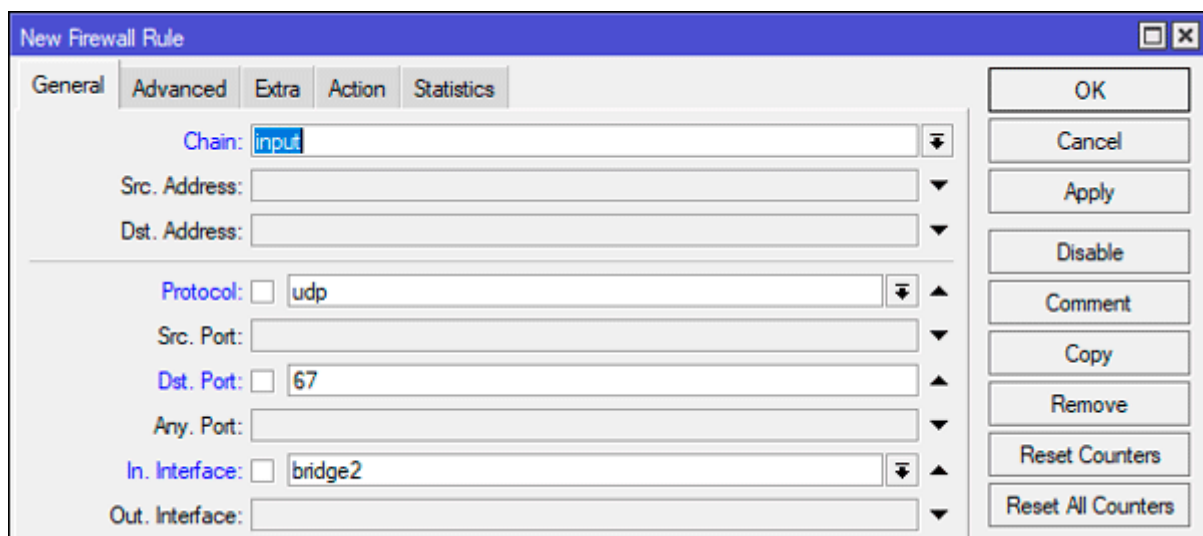




В терминале:

```
/ip firewall filter
add action=drop chain=forward in-interface=bridge2 out-interface=bridge1
```

Теперь изолируем от гостевой сети сам роутер, все что нужно от него клиентам - это получение IP-адреса по DHCP и доступ к DNS-серверу устройства, ничего больше видеть они не должны. Ок, разрешаем доступ к DHCP-серверу, создаем еще одно правило: **Chain - input, Protocol - udp, Dst. port - 67, In. Interface - bridge2**, так как действие по умолчанию **accept** - просто сохраняем правило.



Если вы предоставляете гостям собственный DNS, то добавьте еще одно такое-же правило, но измените номер порта на **53 UDP**, на котором работает служба имен, если же раздаете адреса внешних DNS-серверов, то открывать доступ к созданному не нужно. Затем создадим запрещающее правило, оно очень простое: **Chain - input, In. Interface - bridge2**, на закладке **Action** ставим действие **drop**. Теперь все остальные запросы к роутеру будут отклоняться.

Этот же набор правил в терминале:

```
/ip firewall filter
add action=accept chain=input dst-port=67 in-interface=bridge2 protocol=udp
add action=accept chain=input dst-port=53 in-interface=bridge2 protocol=udp
add action=drop chain=input in-interface=bridge2
```

Это минимальный набор правил для типовой конфигурации, в случае наличия дополнительных сетей и интерфейсов вам может потребоваться создать дополнительные правила с учетом особенностей вашей конфигурации. Общие принципы должны быть понятны из этого раздела: блокируем транзитный трафик из гостевой сети к остальным сетям и изолируем сам роутер.

## Ограничение скорости в гостевой сети

Гостей может быть много, а исходящий канал не резиновый, тем более что современные мобильные устройства позволяют просматривать видео в высоких разрешениях, что может привести к повышенной нагрузке на сеть. Поэтому мы поступим просто - ограничим скорость гостевой сети, никаких сложных настроек производить не будем, просто сделаем одно ограничение на всех, как оно будет делиться между клиентами нас особо не волнует.

Для ограничения трафика используются очереди - **Queues**, обратите внимание, что для работы очередей должен быть отключен Fasttrack. Перейдем в **Queues - Simple Queues** и создадим простую очередь. В поле **Target** укажем интерфейс гостевой сети - **bridge2**, **Dst** - интерфейс выхода в интернет, в нашем случае **ether5**. В **Max Limit** укажем ограничения для входящего и исходящего трафика, мы поставили по 10 Мбит/с.

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: bridge2

Dst.: ether5

Target Upload Target Download

Max Limit: 10M 10M bits/s

Burst

Burst Limit: unlimited unlimited bits/s

Burst Threshold: unlimited unlimited bits/s

Burst Time: 0 0 s

Time

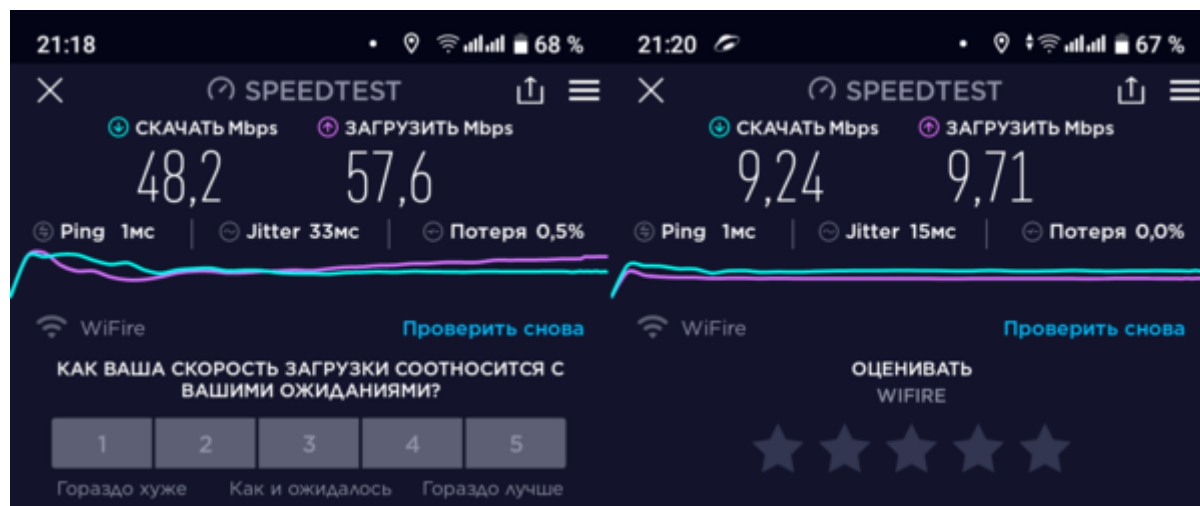
enabled

OK Cancel Apply Disable Comment Copy Remove Reset Counters Reset All Counters Torch

В терминале:

```
/queue simple
add dst=ether5 max-limit=10M/10M name=queue1 target=bridge2
```

Теперь еще раз подключимся и проверим работу ограничений, несложно убедиться, что все работает так, как задумывалось:



Как видим, настроить гостевую Wi-Fi сеть на оборудовании Mikrotik совсем несложно, а широкие возможности RouterOS позволяют существенно повысить уровень ее безопасности, максимально ограничив гостям сетевые возможности.

### Онлайн-курс по MikroTik

Научиться настраивать MikroTik с нуля или систематизировать уже имеющиеся знания можно на [углубленном курсе по администрированию MikroTik](#). Автор курса, сертифицированный тренер MikroTik Дмитрий Скоромнов, лично проверяет лабораторные работы и контролирует прогресс каждого своего студента. В три раза больше информации, чем в вендорской программе MTCNA, более 20 часов практики и доступ навсегда.