BGP MikroTik (Border Gateway Protocol)

07 июля 2026 года

BGP (Border Gateway Protocol) — это протокол динамической маршрутизации, который используют, чтобы обмениваться маршрутами между разными автономными системами (AS). Проще говоря, это "язык", на котором крупные сети (например, провайдеры) договариваются, как доставить трафик друг к другу. В масштабах интернета BGP — основной протокол, который держит всё вместе.

В MikroTik BGP нужен не для обычной домашней сети, а когда есть несколько каналов в интернет, пиринг с провайдерами, анонс своих подсетей или получение списков маршрутов (например, для фильтрации).

Ключевые понятия:
AS (Autonomous System) — независимая сеть под единым управлением (например, ваш провайдер или ваша компания). У каждой AS есть номер (ASN): публичный (глобальный) или приватный (только внутри).
eBGP — BGP между разными AS (ваш роутер ↔ провайдер).
iBGP — BGP внутри одной AS (между вашими роутерами, если у вас большая сеть).
Router ID — уникальный идентификатор роутера в BGP. Обычно берут стабильный IP (лучше с loopback-интерфейса).
Peer (сосед) — второй роутер, с которым вы устанавливаете BGP-сессию.
Анонс (advertise) — вы сообщаете соседу: "У меня есть такие подсети, вези туда трафик".
Приём маршрутов — сосед говорит вам: "Вот куда можно добраться через меня".
BGP работает поверх TCP 179. Если фаервол блокирует этот порт — сессия не поднимется.

Когда реально используют BGP на MikroTik
- Multi-homing (два и более провайдера): чтобы автоматически переключаться между каналами и балансировать нагрузку.
- Анонс своих публичных подсетей в интернет (если у вас есть свой блок IP и ASN).
- Получение префикс-листов от сервисов фильтрации (например, списки "заблокированных" подсетей), чтобы заворачивать трафик в туннель или блокировать.
- Сложные схемы маршрутизации в больших сетях (филиалы, датацентры).

Для типичного "дома/малый офис" с одним провайдером BGP не нужен: хватит статических маршрутов или DHCP от провайдера.

Как настроить BGP на MikroTik (простой пример для eBGP с провайдером)
Допустим:
Ваш ASN: 65001
ASN провайдера: 3356
IP вашего интерфейса к провайдеру: 192.0.2.10/30
IP провайдера: 192.0.2.9
Подсеть, которую вы анонсируете: 203.0.113.0/24

RouterOS v7 (актуальная)
```
# 1. Создаём шаблон BGP с вашим ASN и Router ID
/routing bgp template add name=MyBGP as=65001 router-id=192.0.2.10 routing-table=main
# 2. Добавляем соседа (peer)
/routing bgp connection add name=ProviderPeer template=MyBGP remote.address=192.0.2.9 remote.as=3356
hold-time=180
# 3. Анонсируем свою подсеть
/routing bgp network add network=203.0.113.0/24 template=MyBGP
```

RouterOS v6 (старый синтаксис)
```
/routing bgp instance add name=MyBGP as=65001 router-id=192.0.2.10
/routing bgp peer add name=ProviderPeer instance=MyBGP remote-address=192.0.2.9 remote-as=3356
/routing bgp network add network=203.0.113.0/24 instance=MyBGP
```

Что обязательно проверить после настройки
Статус сессии:
```
v7: /routing/bgp/session print
v6: /routing bgp peer print
```

Ищите флаг E (Established). Если нет — смотрите логи и фаервол.
Маршрутизация: /ip route print — должны появиться маршруты от провайдера и ваш анонс должен быть виден у него (это видно только на стороне провайдера).
Фаервол: разрешите TCP 179 между адресами BGP-пиров.
Фильтры: без фильтров можно случайно «слить» все свои маршруты в интернет или принять лишнее. На практике всегда

используют prefix-list и route-maps.

Важные нюансы и безопасность
- Никогда не анонсируйте чужие подсети. Это "BGP hijacking" и может вызвать серьёзные проблемы.
- Ставьте max-prefix (ограничение на число маршрутов от пира), чтобы при сбое у провайдера не завалить роутер миллионами маршрутов.
- Используйте MD5-аутентификацию, если провайдер требует (параметр password в настройках пира).
- Планируйте Router ID: он должен быть стабильным, иначе сессия будет "мигать".

BGP может пригодиться, если:
- хотите автоматически переключать трафик между основным Ethernet и резервным LTE, используя несколько провайдеров и выбирая лучшие маршруты;
- планируете получать префикс-листы и заворачивать трафик в OpenVPN/туннель по BGP-маршрутам (есть готовые сервисы, которые отдают такие списки по BGP);
- строите отказоустойчивую сеть с несколькими аплинками и хотите управлять выбором маршрута не вручную, а через политики BGP.

Частые ошибки и как их быстро найти
- "TCP connection established" в логах — это только начало: TCP поднялся, но BGP ещё не договорился (OPEN/KEEPALIVE). Смотрите именно BGP-сессии, а не просто TCP.
- Неправильный ASN или IP пира — сессия не перейдёт в Established.
- Фаервол блокирует TCP 179 — часто забывают открыть именно этот порт.
- Разные Router ID или шаблоны (в v7) — сессия не поднимается.