Безопасный режим в Mikrotik или как всегда оставаться на связи

Записки IT специалиста

Технический блог специалистов ООО"Интерфейс"

- Главная
- Безопасный режим в Mikrotik или как всегда оставаться на связи

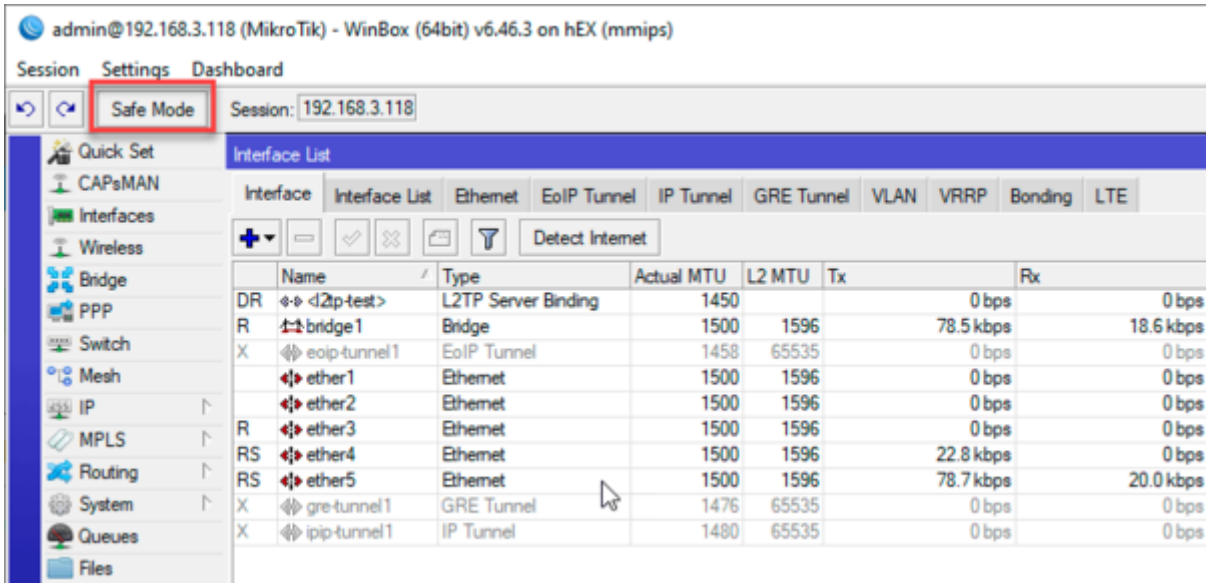
Старая сисадминская примета гласит: "удаленная настройка брандмауэра - к выезду на объект" и в большинстве случаев это действительно так. С другой стороны реалии современной жизни подразумевают преимущественно удаленную работу. Как быть? С одной стороны тратить время на дорогу в десятки или сотни километров ради пяти минут на месте, с другой - ехать, возможно, все равно придется, только уже экстренно. Но есть и третий вариант: спокойно работать удаленно, используя возможности безопасного режима RouterOS, о чем мы и расскажем в этой статье.

Потерять связь с удаленным роутером можно по множеству причин. Все мы люди и всем нам свойственно ошибаться. Это могут быть как ошибки в сетевой конфигурации, так и просто ошибочные действия, чаще всего непреднамеренные, например, один мой коллега случайно отключил внешний интерфейс на роутере случайно нажав на кнопку с крестиком. Поэтому, насколько бы вы не были уверенны в правильности своих действий, даже если вы уже много раз так делали, никогда нельзя сбрасывать со счетов возможность возникновения нештатных ситуаций.

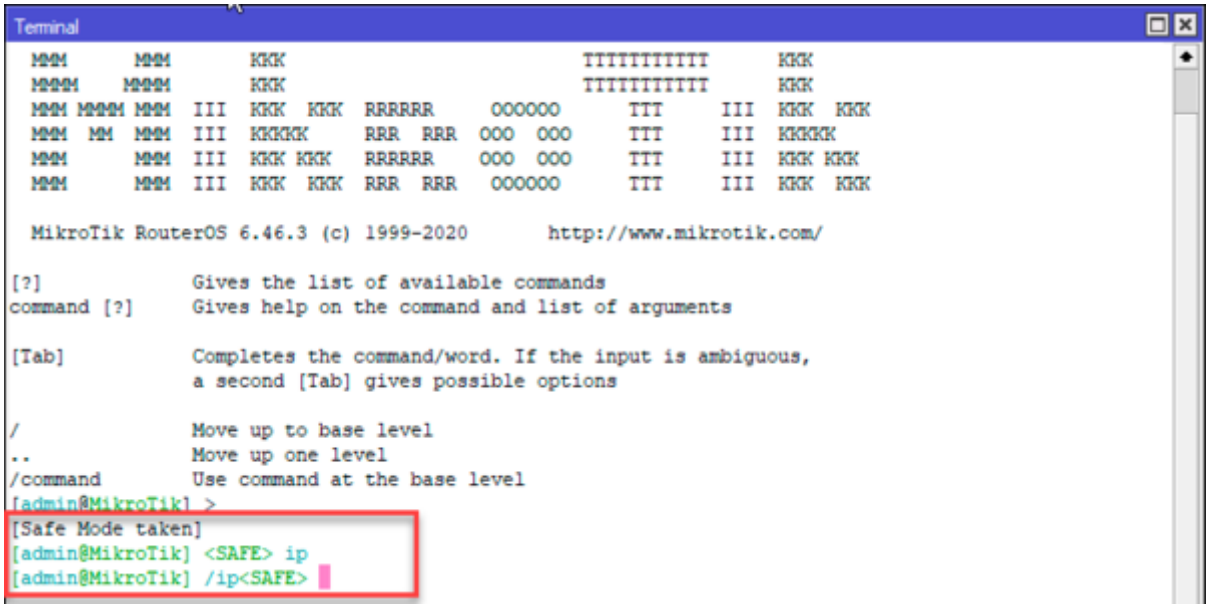
Хорошо если роутер находится в относительной доступности или на той стороне есть кто-то, кто может исправить вашу ошибку хотя бы в телефонном режиме, в противном случае придется готовится к незапланированному выезду и, как оно обычно происходит, не в самое удобное время. При этом далеко не все администраторы знают, что RouterOS предоставляет достаточно эффективный инструмент для исключения подобных ситуаций и называется он - **Safe Mode** или безопасный режим.

Его смысл заключается в том, что внесенные изменения не сразу записываются в память устройства, а только после **явного подтверждения** администратором, которым является ручной выход из безопасного режима. В случае потери связи с устройством через некоторое время будет выполнен откат настроек. Это время определяется тайм-аутом TCP и не превышает 9 минут.

Чтобы включить безопасный режим следует нажать кнопку **Safe Mode** в Winbox:



или использовать сочетание клавиш **Ctrl+x** в терминале, после чего в приглашении командной строки появится **<SAFE>**:



Теперь можно выполнять потенциально опасные действия не опасаясь потерять связь с устройством. Если после выполнения очередной операции связь с устройством все-таки прервалась, то у вас будет некоторое время, чтобы выпить кофе и подумать над тем, что именно вы сделали не так. Хотя, скорее всего, кофе выпить вы не успеете.

Также к отмене всех сделанных изменений приведет закрытие окна Winbox или терминала с включенным безопасным режимом. Этим можно воспользоваться, если вы просто хотите быстро откатить все внесенные изменения.

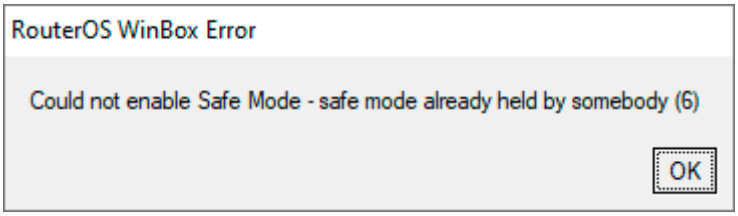
Чтобы выйти из безопасного режима с сохранением внесенных изменений следует явно отжать кнопку **Safe Mode** в Winbox или еще раз выполнить сочетание клавиш **Ctrl+x** в терминале, также изменения сохраняются при выходе из терминала командой:

```
/quit
```

Работа в безопасном режиме имеет свои особенности, которые нужно обязательно учитывать. Количество хранимых шагов ограничено, согласно документации, роутер может сохранять в памяти не более 100 действий, если вы превысите это количество, то сеанс автоматически выйдет из безопасного режима и изменения не смогут быть отменены. Поэтому рекомендуется вносить изменения небольшими порциями, каждый раз выходя из безопасного режима и входя в него повторно. В терминале для этого можно использовать двойное нажатие **Ctrl+x**.

При совместной работе нескольких администраторов может возникнуть ситуация, когда одна из сессий уже находится в безопасном режиме, попытка включить безопасный режим еще в одной сессии через Winbox не увенчается успехом:

Если же выполнить аналогичную попытку в терминале, то получим совершенно иной результат:

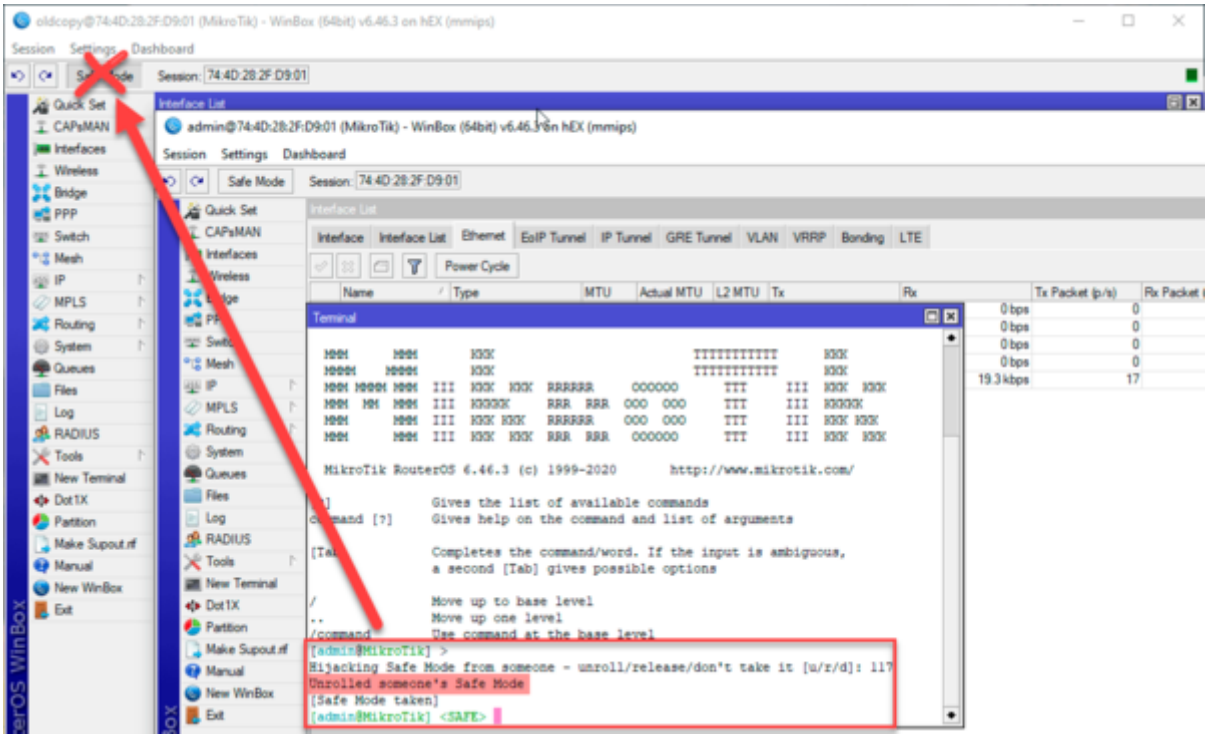


Здесь нам доступны следующие действия:

- **u - unroll** - откатить изменения и перевести текущий сеанс в безопасный режим

- **r - release** - принять изменения и перевести текущий сеанс в безопасный режим
- **d - don't take** - оставить без изменений

О результатах первых двух действий другой администратор получит уведомление, но только в том случае, если безопасный режим использовался в терминале. Если же один из администраторов включил безопасный режим через Winbox, а второй забрал его через терминал, то никаких уведомлений первый администратор **не получит** и визуально кнопка Safe Mode **будет оставаться нажатой**. Это может привести к опасным ситуациям, когда первый администратор будет считать, что безопасный режим у него включен, но на самом деле все изменения будут применяться непосредственно на устройстве.



Поэтому мы категорически не рекомендуем перехватывать безопасный режим при многопользовательской работе без непосредственного согласования с коллегами, потому как это может создать неоднозначную ситуацию, чреватую серьезными проблемами.

Чтобы обезопасить себя от перехвата безопасного режима следует перед внесением очередных изменений выключить безопасный режим и снова включить. Если вы работаете через Winbox, то столкнетесь с описанной выше ошибкой, а в терминале получите запрос на захват режима. При возникновении подобной ситуации мы рекомендуем сразу связаться с коллегами и согласовать последующие действия.

Еще одной особенностью безопасного режима является его реакция на выключение питания устройства или его аварийную перезагрузку, в этом случае все изменения внесенные в безопасном режиме **будут применены**. Поэтому если ваше

оборудование находится в местах, где возможны перебои с энергоснабжением, то рекомендуем обязательно позаботиться о бесперебойном питании.

Обрыва интернет-соединения указанная особенность не касается, такая ситуация будет обработана как обрыв связи с последующим откатом изменений. Аналогичная реакция будет и на аварийное завершение работы клиентского устройства, где был запущен Winbox или терминал.

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.