

Настраиваем RoMON для удаленного управления роутерами Mikrotik

 interface31.ru/tech_it/2022/02/nastraivaem-romon-dlya-udalennogo-upravleniya-routerami-mikrotik.html

Записки IT специалиста

Технический блог специалистов ООО "Интерфейс"

- [Главная](#)
- Настраиваем RoMON для удаленного управления роутерами Mikrotik

Оборудование Mikrotik предоставляет администраторам богатые возможности по управлению и администрированию, включая инструменты удаленного доступа. Вы можете без проблем настраивать роутер, находящийся за многие километры от вашего рабочего места и никого этим сегодня не удивить. Тем не менее бывают задачи, когда нужно получить управление оборудованием, к которому не имеется прямого доступа, в этом случае нам на помощь придет специальная технология от Mikrotik - RoMON.



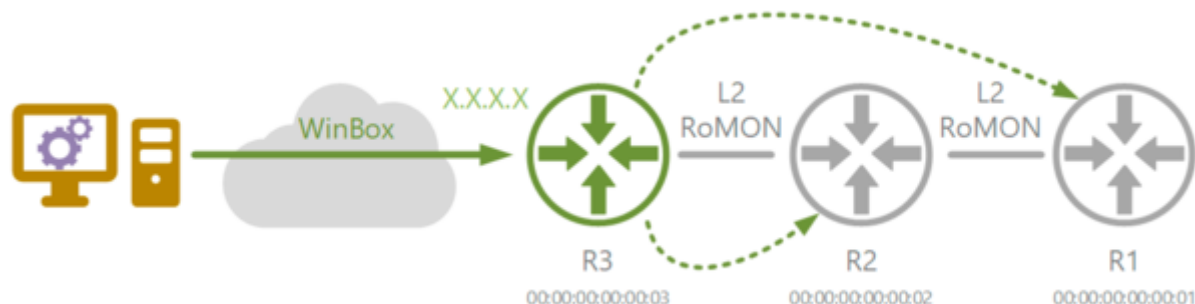
Онлайн-курс по MikroTik

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.

Что такое RoMON?

RoMON (Router Management Overlay Network) - специальная технология компании Mikrotik предназначенная для обнаружения одноранговых устройств с Router OS и построения сети управления между ними. Для этого используется давно известная всем администраторам Mikrotik возможность подключения к устройству по MAC-адресу. RoMON позволяет обнаруживать устройства в общем широковещательном сегменте L2 и устанавливать связи между ними, при этом работа не ограничена только одним широковещательным сегментом, мы можем соединять роутеры как гирлянды и управлять ими с любого доступного нам устройства.

Рассмотрим следующую схему:



У нас имеется условная цепочка из роутеров **R1 - R2 - R3**, при этом возможность каким-либо образом подключиться извне мы имеем только к последнему. Задача - настроить удаленный доступ к управлению всеми устройствами. Мы специально не стали обозначать каких-либо сетей или адресов роутеров, потому что это не имеет никакого значения, единственное условие - любые два роутера должны видеть друг друга по L2 и иметь возможность соединиться через MAC-Telnet. При этом роутер R3 может ничего не знать о существовании R1, но для построения RoMON сети вполне достаточно, что он имеет соединение с роутером R2, который в свою очередь соединяется с R1.

Таким образом можно строить достаточно длинные цепочки между роутерами не снижая уровень безопасности и не создавая подключений извне туда, где это будет нежелательно, да и защитить одно устройство, с которого будет осуществляться доступ к остальному сетевому оборудованию проще, чем поддерживать безопасность множества узлов.

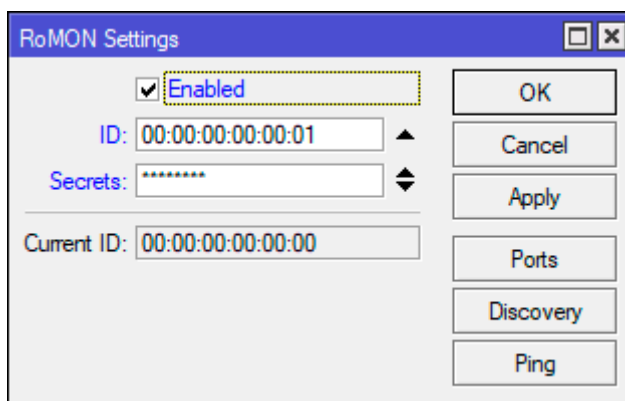
Настройка RoMON

Настройка RoMON проста, для этого откроем Winbox на целевом роутере и перейдем в **Tools - RoMON**, в открывшемся окне установите флаг **Enabled** и укажите в поле **Secrets** секретную фразу для взаимной аутентификации роутеров. Внутри RoMON сети устройства определяются при помощи идентификаторов, в качестве которых используется один из MAC-адресов устройства, это может быть неудобно, поэтому можно задать собственные идентификаторы, для этого откорректируйте поле **ID**.

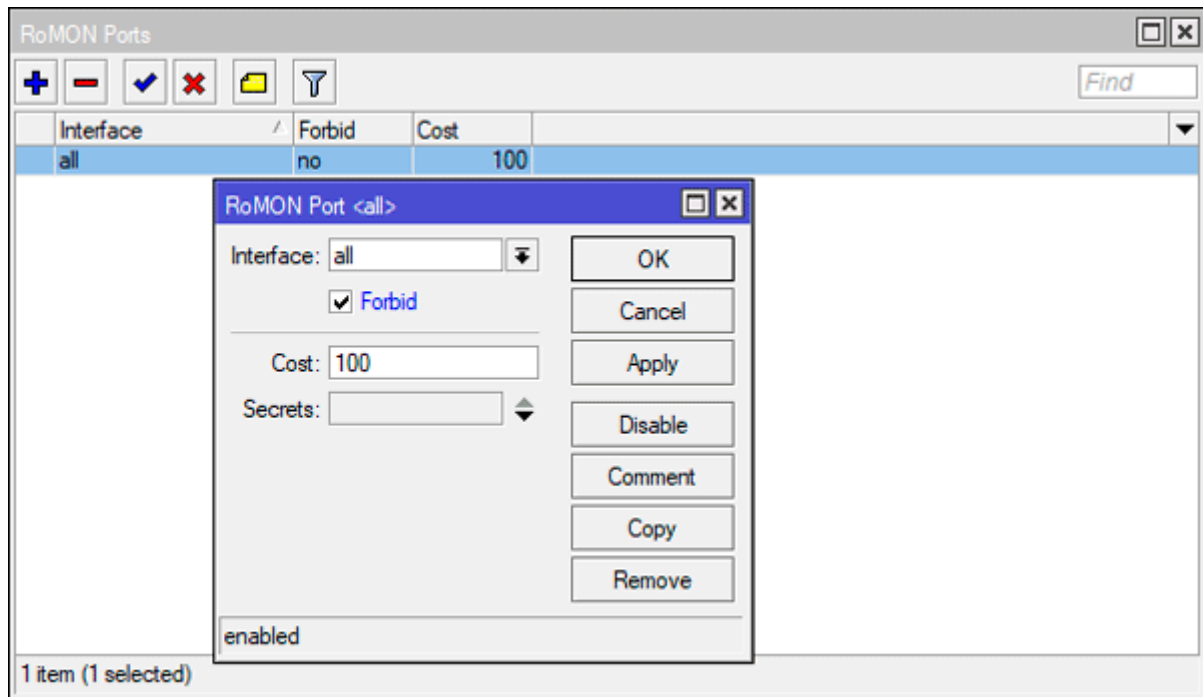
Те же действия в терминале:

```
/tool romon
set enabled=yes id=00:00:00:00:00:01
secrets=MySecret
```

На этом настройку можно бы было и закончить, но в этом случае RoMON будет работать на всех интерфейсах, что нежелательно по соображениям безопасности. Поэтому выполним ряд дополнительных настроек. В



предыдущем окне нажмем кнопку Ports и прежде всего запретим подключаться с любого интерфейса. Откроем единственную имеющуюся запись с указанием в поле **Interface - all** и установим для нее флаг **Forbid**.

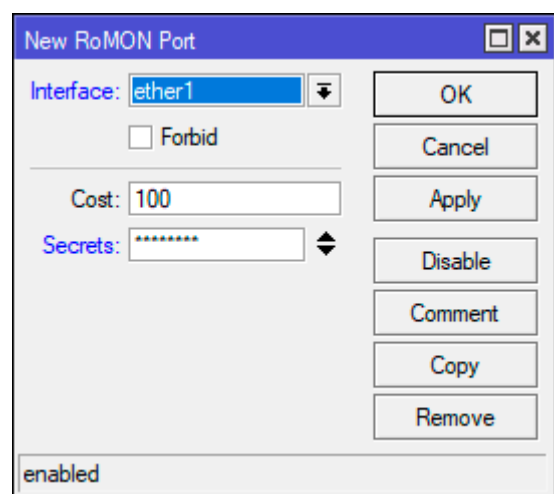


Теперь настроим отдельные правила для портов, как правило нет никаких проблем определить какой именно порт роутера смотрит в сторону другого устройства, в нашем случае это будут порты ether1 и ether5, при этом будем считать, что ether1 находится по схеме слева от роутера, а ether5 - справа. Т.е. для R1 задействован только ether1, для R3 - ether5, а для R2 - оба указанных порта.

Для добавления правила нажмем плюс и в открывшемся окне укажем желаемый **порт** и **секрет** для него. Обращаем ваше внимание, что RoMON использует вначале секрет, указанный для порта, а в его отсутствии глобальный секрет, который мы указали при включении RoMON.

Также отметим еще один доступный параметр - **Cost** - это "стоимость" подключения, может оказаться полезен, если к одному роутеру могут вести несколько цепочек и вы хотите явно отдать приоритет одной из них. Чем меньше суммарная стоимость маршрута - тем выше его приоритет.

Теперь вариант команд для терминала, здесь мы приведем пример для роутера R2 и настроим сразу два интерфейса:



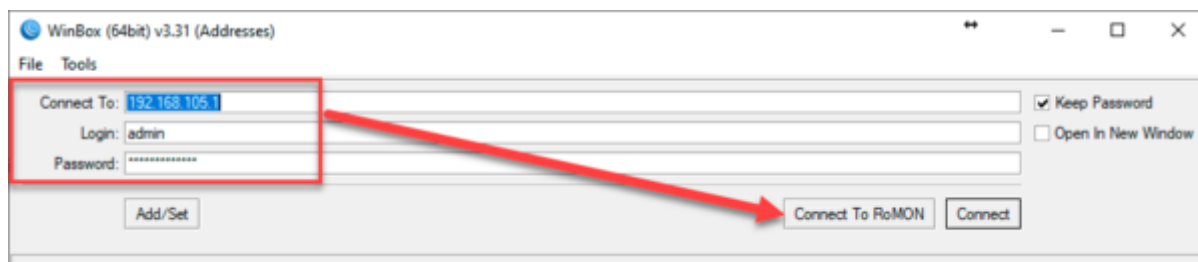
```
/tool romon port
set [ find default=yes ] forbid=yes
add disabled=no interface=ether1 secrets=MySecret
add disabled=no interface=ether5 secrets=MySecret
```

Аналогичные настройки следует выполнить на каждом роутере входящем в цепочку. Никаких особых сложностей они не представляют.

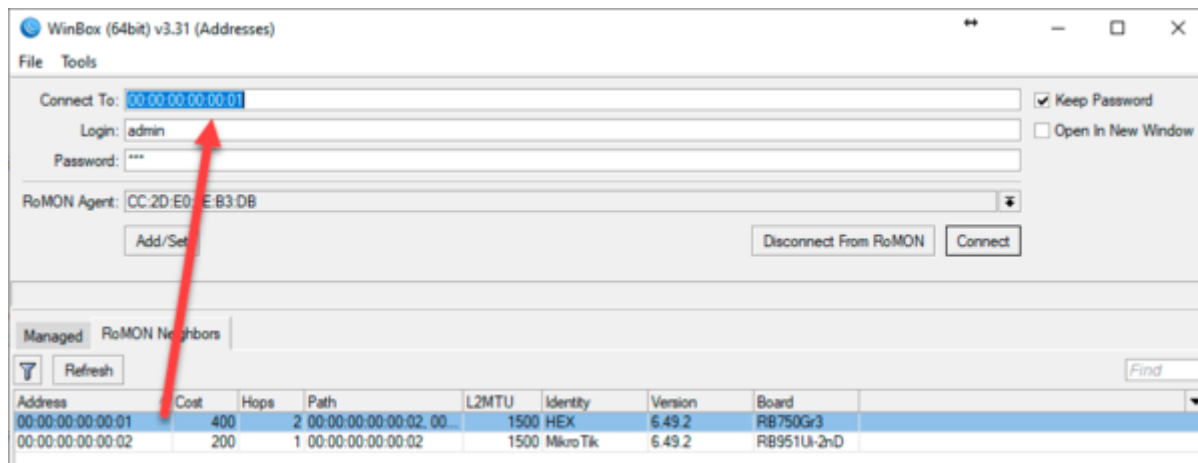
Некоторые важные уточнения: RoMON **не использует шифрование**, защита передаваемых данных полностью лежит на прикладном приложении, вы можете использовать Winbox или SSH. Секрет используется только для взаимной аутентификации роутеров и должен быть одинаков у всех устройств входящих в сеть управления. Мы рекомендуем задавать как локальный секрет для порта, так и глобальный, что повысит уровень безопасности даже при неверных настройках RoMON (открыт доступ со всех портов).

Использование RoMON

Согласно условиям задачи мы имеем возможность подключения через Winbox к роутеру R3. Теперь, после того как настроили RoMON мы можем подключиться к сети управления нажав на кнопку **Connect To RoMON** и указав при этом параметры доступа к нужному роутеру.



После чего ниже появится полный список роутеров в сети управления и мы можем получить доступ к любому из них используя идентификатор, для доступа к роутерам следует использовать учетные данные существующих пользователей, секрет RoMON используется исключительно для взаимной аутентификации устройств и указывать его нигде не надо.



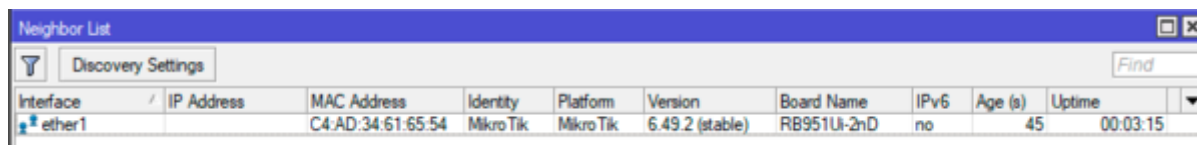
При этом вы всегда можете видеть текущую стоимость подключения, количество устройств в цепочке и их идентификаторы, а также краткие сведения об устройствах, включающие модель и версию RouterOS.

Подключение к роутеру по MAC Telnet

Данная тема не относится напрямую к RoMON, но очень близко связана с ней. В процессе работы у вас может появиться удаленное новое устройство, которое либо нужно настроить для работы в удаленной сети, либо вообще после настройки передать далее. И хорошо если у вас есть возможность подключиться к одному из узлов удаленной сети, запустить там Winbox и выполнить необходимые настройки. А если нет?

Второй вариант - это настройка RoMON, как мы видели, для этого нужно получить доступ к каждому устройству, что тоже не всегда возможно. Что делать? Выезжать на точку? Не спешите, в большинстве случаев все можно сделать удаленно.

По умолчанию обнаружение и подключение через MAC Telnet доступны на всех портах, кроме "внешнего", таким в SOHO-устройствах обычно является ether1, поэтому достаточно подключить новое устройство в сеть любым портом, кроме первого. Затем переходим на контролируемое устройство, имеющее доступ в тот же широковещательный сегмент что и новый роутер и открываем **IP - Neighbor** где мы можем увидеть всех соседей в одноранговой сети. Все что нам понадобится отсюда - это MAC-адрес нужного устройства.



Interface	IP Address	MAC Address	Identity	Platform	Version	Board Name	IPv6	Age (s)	Uptime
ether1	192.168.1.1	C4:AD:34:61:65:54	MikroTik	MikroTik	6.49.2 (stable)	RB951Ui-2nD	no	45	00:03:15

После чего открываем терминал и выполняем команду:

```
/tool mac-telnet host=01:12:34:56:78:90
```

Где 01:12:34:56:78:90 - MAC-адрес требуемого устройства. Теперь мы можем полноценно работать с данным роутером в терминале, даже можем выполнить полный сброс, доступ через MAC Telnet будет активирован по умолчанию:

```
/system reset-configuration no-defaults=yes skip-backup=yes
```

После чего достаточно активировать RoMON и получить полный доступ к устройству.

Смена секрета RoMON

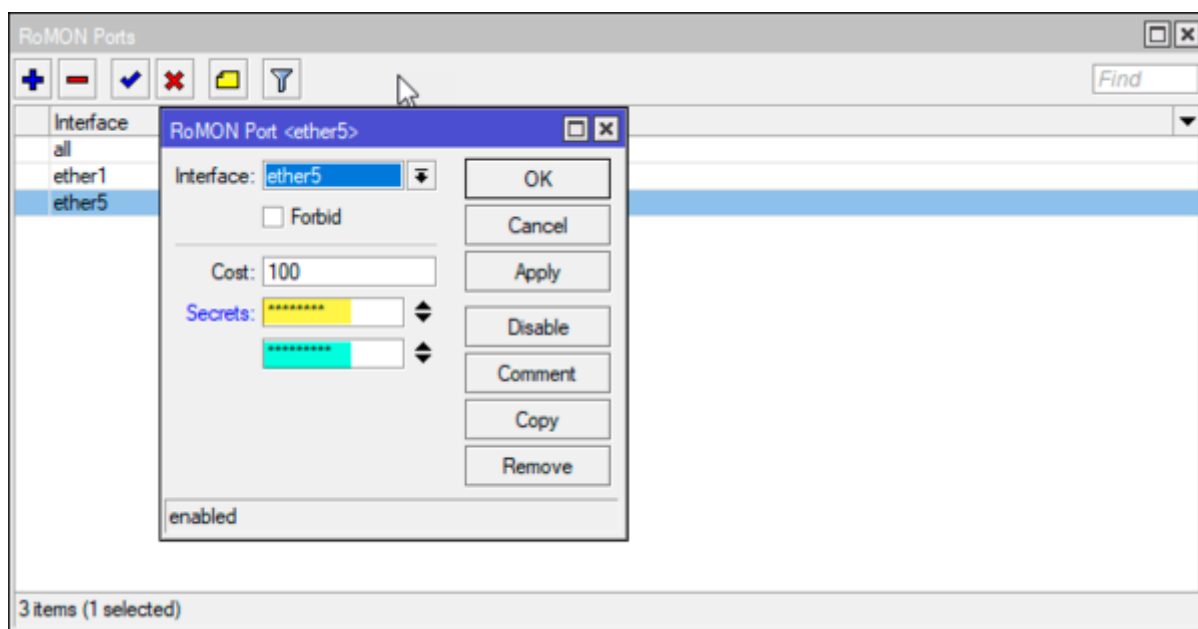
В процессе эксплуатации сети RoMON может возникнуть потребность изменить секрет, либо установить его, если вы ранее не использовали аутентификацию, очень важно сделать это так, чтобы не потерять в процессе смены секрета доступ к

управляемым устройствам. К счастью, сделать это несложно, нужно лишь строго соблюдать необходимую последовательность действий.

Напомним, что RoMON не использует шифрование, а секретная фраза используется для вычисления хеш-функции при помощи которой производится аутентификация сообщений, таким образом, все узлы, которые владеют секретом могут убедиться, что пакет пришел от доверенного узла и примут его.

RoMON позволяет указать несколько секретов, как глобальных, так и для порта. При этом сам узел будет использовать первый в списке секрет, но сможет принимать пакеты с хешами сформированными при помощи любых других секретов, перечисленных в списке. Эту возможность мы и будем использовать.

Откроем список секретов и добавим в него новый секрет, при этом **первым** в списке располагаем **старый секрет** (выделен желтым), а ниже новый секрет (выделено зеленым).



В терминале это будет выглядеть так, для глобального секрета:

```
/tool romon  
set enabled=yes id=00:00:00:00:00:02 secrets=old_secret,new_secret
```

Для порта:

```
/tool romon port  
add disabled=no interface=ether5 secrets=old_secret,new_secret
```

Данный шаг следует выполнить на всех управляемых устройствах. После чего каждое из них будет продолжать использовать старый секрет, но сможет принимать пакеты с хешем сформированным при помощи нового секрета.

Выполнив указанное действие переходим к следующему: для каждого из устройств в списке паролей ставим **первым новый секрет**, а **вторым старый**. Также повторяем это действие на всех управляемых устройствах. Теперь роутеры для связи друг с другом будут использовать новые секреты, но смогут принимать пакеты со старым хешем.

После того, как на всех роутерах первым в списке установлен новый секрет, и вы убедились в наличии связи с каждым из них - можно перейти к заключительному этапу - **удалить из списков старый секрет**.

На первый взгляд процедура может показаться немного сложной и избыточной, но именно такой порядок действий гарантирует что вы не потеряете связь ни с одним устройством в процессе изменения секретов на них. Также учтите, что пустой секрет тоже является секретом и, если вы до этого не использовали аутентификацию в качестве старого секрета следует оставлять пустое поле, а в терминале использовать пустое значение, состоящее из двух, идущих подряд, кавычек.

```
secrets="",new_secret
```

Как видим, RouterOS предоставляет администратору достаточно широкий круг простых и удобных инструментов управления и RoMON - один из них. Он не претендует на универсальность и его нельзя однозначно рекомендовать к употреблению везде где-только можно, но в ряде сценариев он может оказаться незаменимым, обеспечивая привычный уровень удобства администрирования даже при отсутствии прямого доступа к устройству.

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.